UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS ECONÓMICAS

"EVALUACIÓN DE CONTROLES SEGÚN EL MODELO COBIT, PARA LA ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES"

TESIS

PRESENTADA A LA HONORABLE JUNTA DIRECTIVA DE LA FACULTAD DE CIENCIAS ECONÓMICAS

POR

LUIS GUILLERMO DIONICIO TEO

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

Guatemala, mayo de 2011

MIEMBROS DE LA JUNTA DIRECTIVA
FACULTAD DE CIENCIAS ECONÓMICAS

Decano	Lic. José Rolando Secaida Morales
Secretario	Lic. Carlos Roberto Cabrera Morales
Vocal 1º	Lic. Albaro Joel Girón Barahona
Vocal 2º	Lic. Mario Leonel Perdomo Salguero
Vocal 3º	Lic. Juan Antonio Gómez Monterroso
Vocal 4º	P.C. Edgar Arnoldo Quiché Chiyal
Vocal 5º	P.C. José Antonio Vielman

PROFESIONALES QUE REALIZARON LOS
EXÁMENES DE ÁREAS PRÁCTICAS BÁSICAS

Matemática-Estadística	Lic. Edgar Ranulfo Valdés Castañeda
Auditoría	Lic. Mario Danilo Espinoza Aquino
Contabilidad	Lic. Mario Leonel Perdomo Salguero

PROFESIONALES QUE REALIZARON
EXAMEN PRIVADO DE TESIS

Presidente	Lic. Salvador Giovanni Garrido Valdéz
Examinador	Lic. Jorge Luis Monzón Rodríguez
Examinador	Licda. Enma Yolanda Chacón Ordóñez

López Cordón & Asociados
CONTADORES PUBLICOS Y AUDITORES

Guatemala, 23 de febrero de 2011

Licenciado
José Rolando Secaida Morales
Decano
Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad.

Señor Decano:

Conforme a la designación que se sirvió hacerme, tengo el agrado de manifestarle que he asesorado el trabajo de tesis "EVALUACIÓN DE CONTROLES SEGÚN EL MODELO COBIT, PARA LA ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES", efectuado por el señor Luis Guillermo Dionicio Teo, previo a optar al Título de Contador Público y Auditor, en el grado académico de Licenciado.

Considero que el trabajo resalta adecuadamente la importancia del tema y puede considerarse como un valioso medio para la evaluación del control interno informático de acuerdo a estándares internacionales en las empresas dedicadas a la distribución de vehículos automotores.

Al considerar que el trabajo presentado por el señor Luis Guillermo Dionicio Teo cumple con los requisitos correspondientes, recomiendo su aprobación para discusión y defensa en Examen General Público.

Agradezco al señor Decano la oportunidad que me ha conferido y me suscribo como su atento servidor.

Lic. Oscar Noé López Cordón
Colegiado CPA-381
Asesor de Tesis

Oscar Noe Lopez Cordon
Contador Público y Auditor
CPA. 381

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE
CIENCIAS ECONOMICAS
Edificio "S-8"
Ciudad Universitaria, Zona 12
Guatemala, Centroamérica

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA, DIÉCISIETE DE MAYO DE DOS MIL ONCE.

Con base en el Punto CUARTO, inciso 4.1, subinciso 4.1.1 del Acta 12-2011 de la sesión celebrada por la Junta Directiva de la Facultad el 5 de mayo de 2011, se conoció el Acta AUDITORÍA 78-2011 de aprobación del Examen Privado de Tesis, de fecha 29 de marzo de 2011 y el trabajo de Tesis denominado: "EVALUACIÓN DE CONTROLES SEGÚN EL MODELO COBIT, PARA LA ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES", que para su graduación profesional presentó el estudiante **LUIS GUILLERMO DIONICIO TEO**, autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

FACULTAD DE CIENCIAS ECONOMICAS
EL SECRETARIO
Guatemala, C. A.

LIC. JOSE ROLANDO SECAIDA MORALES
DECANO

FACULTAD DE CIENCIAS ECONOMICAS
EL DECANO
GUATEMALA, C. A.

Smp.

Ingrid

DEDICATORIA

A DIOS: Por su infinita bondad. Porque me ha bendecido inmensamente permitiéndome llegar a cumplir mis metas.

A MI MADRE: Eddi Elizabeth Teo Mejía Vda. de Dionicio. Como agradecimiento por tantos sacrificios y esfuerzos. Con mucho amor.

A MI PADRE: Luis Medardo Dionicio Mendez (Q.E.P.D). Como tributo a su memoria.

A MI ESPOSA: Claudia Jeanneth Antillón. Por su gran amor, apoyo y comprensión en todo momento.

A MIS HIJOS: Luis Enrique, Claudia Daniela y Paula Valeria. Mi fuente de inspiración y fortaleza para seguir adelante.

A MIS HERMANOS: Carolina, Rolando y Jennifer. Con amor fraternal.

A MIS SOBRINOS: Edgar, Andrea, Gerardo, Andrés, Miguel, Luis Angel, Derick y Sofía. Con mucho cariño.

A MIS ABUELAS: Zoila Albertina Mejía (Q.E.P.D.) y Manuela de Jesús Méndez. Por todo su cariño y sabios consejos.

A MIS TÍOS, PRIMOS Y CUÑADOS: Con mucho aprecio.

A MIS SUEGROS: Mario Enrique Antillón y Clara Luz Flores de Antillón. Con especial aprecio.

A MI FAMILIA: Con sincero afecto.

A MIS AMIGOS: Por todo su apoyo incondicional.

A MI ASESOR: Lic. Óscar Noé López Cordón. Por su orientación profesional y amistad.

CONTENIDO

Página

CAPÍTULO II

EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES

INTRODUCCIÓN

Las empresas distribuidoras de vehículos automotores necesitan de la tecnología informática para procesar la gran cantidad de información que generan debido al tipo de productos y servicios que ofrecen, incluyendo vehículos, repuestos y accesorios originales, lubricantes y talleres de servicio que representan cientos de transacciones diarias entre movimientos de inventario, ordenes de servicio, compras, ventas y otros, donde el recurso tecnológico representa una gran ventaja, pero también un gran riesgo sino se cuenta con los controles necesarios que permitan la continuidad y calidad de la información generada por los sistemas informáticos al momento de aplicarle cambios o efectuar nuevas adquisiciones.

El Departamento de Informática desempeña una función crítica en este tipo de empresas, pues administra sus recursos informáticos, el procesamiento electrónico de sus datos, además de que brinda el soporte y mantenimiento de los elementos y servicios básicos para su información, para lo cual necesita contar con una estructura organizativa y procedimientos bien definidos que le permitan apoyar debidamente a la organización en el logro de sus objetivos.

Los Objetivos de Control de Información y Tecnología Relacionada (COBIT, por sus siglas en inglés) son un modelo de control de aceptación general a nivel internacional en materia de control informático y aseguramiento de información, porque permite evaluar la medida en que los controles informáticos alinean los recursos de tecnología informática con los objetivos generales del negocio, para garantizar razonablemente a usuarios internos y externos, el suministro oportuno y confiable de la información que necesitan para la toma de decisiones.

Es por ello que el presente trabajo de tesis denominado: EVALUACIÓN DE CONTROLES SEGÚN EL MODELO COBIT, PARA LA ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES" pretende aportar a los Contadores Públicos y Auditores que desarrollan su actividad como Auditores Internos en una empresa de este tipo, los lineamientos necesarios para desarrollar una auditoría de sistemas evaluando los controles aplicados por el departamento de informática en base al modelo de los Objetivos de Control de Información y Tecnología Relacionada (COBIT), con la finalidad de soportar su opinión en base a criterios internacionales de aceptación general que agreguen mayor valor a sus conclusiones y recomendaciones ante la administración de la empresa.

El trabajo está desarrollado en capítulos siguiendo una secuencia lógica que permita a los interesados adentrarse en el contenido del tema.

En el primer capítulo se describen las características de las empresas distribuidoras de vehículos automotores, su estructura organizacional, los productos y servicios que ofrecen y la regulación legal que rige su actuación.

El contenido del segundo capítulo se desarrolla en torno a la definición del departamento de informática, su importancia para este tipo de empresas, además de explicar de forma general la estructura organizacional y medidas de seguridad necesarias para el debido cumplimiento de sus funciones.

Mediante el tercer capítulo se analiza la definición e importancia de la auditoría interna en la evaluación de sistemas de información, la normativa que sirve de base para su actuación, incluyendo las normas de la Asociación de Auditoría y Control de Sistemas de Información (ISACA) que tiene a su cargo la emisión y mantenimiento del modelo COBIT. En este capítulo también se describen los lineamientos generales de las Guías de Auditoría COBIT y un breve resumen de la metodología necesaria para la aplicación de una auditoria de sistemas informáticos.

En el capítulo cuarto se definen los Objetivos de Control para Información y Tecnología Relacionada (COBIT), sus principales componentes y la forma en que los procesos de cada uno de sus dominios logran vincularse de acuerdo a la forma natural en que se desarrollan en un ambiente de tecnología informática. Además se describen las formas de medición que ofrece el modelo y la forma de aplicar una evaluación de procesos mediante el modelado de madurez del control informático que sirve de base para la ejecución del caso práctico.

El contenido del caso práctico del capítulo quinto, establece la forma de aplicar una evaluación de controles mediante el modelo de madurez de COBIT, que representa la herramienta base del trabajo de auditoría interna realizado en esta investigación y que al final permite confirmar la hipótesis planteada al inicio con respecto a los aspectos del modelo COBIT que deben evaluarse para brindar una seguridad razonable a la administración sobre la continuidad y calidad de los recursos informáticos durante la adquisición y mantenimiento de soluciones informáticas por parte del departamento de informática de una empresa distribuidora de vehículos automotores.

CAPÍTULO I

ASPECTOS GENERALES DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES

1.1 Definición

Las empresas dedicadas a la distribución de vehículos automotores son entes autónomos de control y decisión que enfocan sus recursos hacia el logro de beneficios económicos mediante la satisfacción de las necesidades de vehículos automotores en el libre mercado de la Ciudad de Guatemala.

"Vehículo automotor es aquel que tiene como función principal la carga y transporte de cosas y/o transporte de personas en forma permanente, que se mueve por sí mismo y está destinado a transitar por vía terrestre" (17:1)

1.2 Características

Entre las características principales de este tipo de empresas se encuentran las siguientes:

- Como unidad económica, su composición implica un conjunto de elementos (recursos tecnológicos, humanos y de capital), que van orientados hacia un fin común.
- De acuerdo a la magnitud de la empresa, así será el número de departamentos en que se dividirá su propia organización.
- Se encuentran reguladas por un marco legal, ya sean individuales o colectivas, conforme las especificaciones del Código de Comercio de Guatemala.
- Son susceptibles a contraer derechos y obligaciones por poseer personería jurídica propia.
- Deben cumplir con las estipulaciones Legales y Tributarias de acuerdo a la legislación vigente.
- Deben cumplir con requerimientos específicos derivados de la actividad de distribución de vehículos que realizan, como pagos anuales de membrecía y apoyo en eventos de la gremial de importadores y distribuidores de vehículos.

1.3 Naturaleza

Una empresa de este ramo comercial se crea para comprar e importar, vender y controlar. Cuando se inician las operaciones de una de estas empresas por lo regular tendrán la función de comprar los

productos al extranjero (importación), venderlos (mercadeo), respaldar sus ventas (repuestos y servicios) y analizar sus resultados financieros (finanzas y control).

1.4 Objetivos Generales

Los principales objetivos de una empresa distribuidora de vehículos automotores son:

- Cumplir con una función económica propiciando el intercambio monetario y la generación de riqueza.
- Cumplir una función social al generar fuentes de empleo y contribuir al mejoramiento de la calidad de vida de sus empleados.
- Busca la obtención de un beneficio económico mediante la satisfacción de alguna necesidad de orden general o social.
- Tiene como finalidad primordial la obtención del lucro, ofreciendo a sus clientes vehículos, repuestos, accesorios y servicios de la más alta calidad, buscando detectar y satisfacer sus expectativas y necesidades.

1.5 Formas de Organización

Pueden ser constituidas como sociedades o empresas individuales, de acuerdo a la normativa legal vigente en la República de Guatemala, para lo cual deberán cumplir con los requisitos de constitución, inscripción y obtención de personalidad jurídica que estipula el Código de Comercio Decreto No. 2-70.

1.6 Estructura Organizacional

La mayoría de las empresas distribuidoras de vehículos automotores presentan una estructura organizacional similar, conformada por los distintos departamentos necesarios para su correcto funcionamiento y control de sus actividades.

A continuación se detallan los principales departamentos que conforman este tipo de empresas:

- Consejo de Administración:
  Órgano en el que se delega la administración de una sociedad mercantil.

- Gerencia General:
  Ejerce la representación legal de la sociedad y tiene a su cargo la gestión de los negocios sociales.

- Auditoría Interna:
  Encargado de brindar a la administración la seguridad razonable del cumplimiento de sus objetivos mediante la constante evaluación del control interno, procesos y resultados financieros.

- Recursos Humanos:
  Responsable de la selección, contratación, formación, empleo y retención del recurso humano necesario para la empresa.

- Informática:
  Tiene a su cargo la administración de los recursos informáticos de la empresa.

- Contabilidad:
  Encargado de llevar a cabo los asuntos contables y financieros de la empresa.

- Jurídico:
  Responsable de brindar asesoramiento en materia legal.

- Importaciones:
  Realiza los trámites necesarios para la internación de los productos adquiridos en el extranjero y su correspondiente costeo hasta colocarlos en disponibilidad de ser vendidos en territorio nacional.

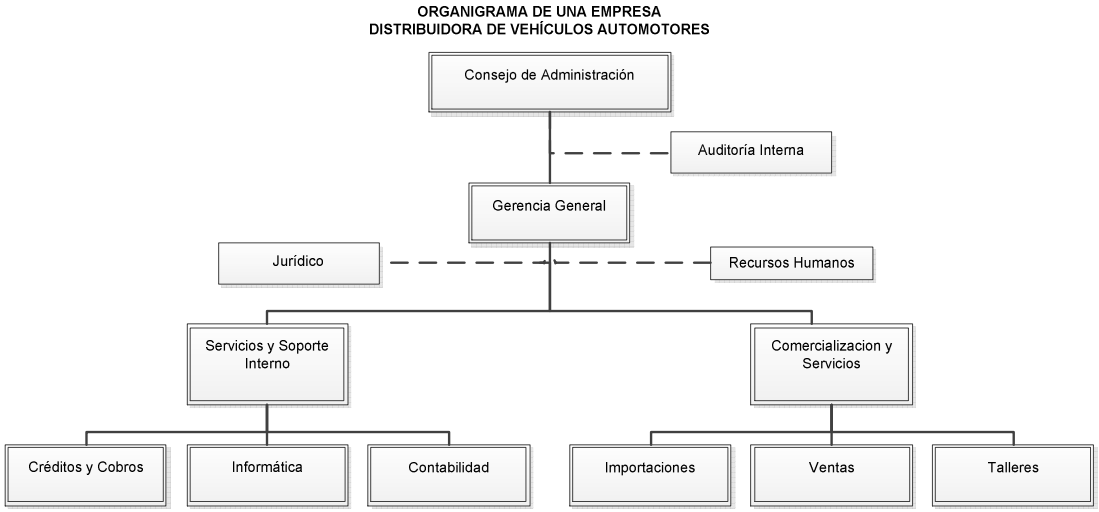
- Créditos y Cobros:
  Encargado de la evaluación y otorgamiento de créditos y la recuperación de los fondos derivados de los mismos.

- Ventas:
  Unidad encargada de persuadir a un mercado acerca de la existencia de los productos ofrecidos por la empresa.

- Compras:
  Encargado de realizar las adquisiciones que necesite la empresa, con la cantidad y calidad requerida y a un precio adecuado.

- Talleres de Servicio:
  Brindan el seguimiento y servicio adecuado a los vehículos vendidos por la empresa.

A continuación se presenta el organigrama de la estructura organizacional para este tipo de empresas:



Fuente: Organigrama de Empresa Modelo

1.7 Legislación Aplicable

Las principales leyes aplicables a este tipo de empresas, son:

1.7.1 Código de Comercio (Decreto No. 2-70)

Regula lo concerniente a la libre empresa, facilitando su organización y regulando sus operaciones, encuadrándolas dentro de las limitaciones justas y necesarias que permiten al Estado mantener la vigilancia sobre las mismas.

1.7.2 Código de Trabajo (Decreto No. 330 y sus reformas)

Regula los derechos y obligaciones de patronos y trabajadores, con ocasión del trabajo, y crea instituciones para resolver sus conflictos.

1.7.3 Código Tributario (Decreto No. 6-91 y sus reformas)

Rige las relaciones jurídicas que se originan de los tributos establecidos por el Estado, con excepción de las relaciones tributarias aduaneras y municipales, a las que aplicarán de forma supletoria.

1.7.4 Ley del Impuesto sobre la renta (Decreto No. 26-92 y sus reformas) y su reglamento (Acuerdo Gubernativo No. 596-97)

Establece un impuesto sobre la renta que obtenga toda persona individual o jurídica, nacional o extranjera, domiciliada o no en el país, así como cualquier ente, patrimonio o bien que especifique esta ley, que provenga de la inversión de capital, del trabajo o de la combinación de ambos.

1.7.5 Ley del Impuesto al valor agregado (Decreto No. 27-92 y sus reformas) y su reglamento (Acuerdo Gubernativo No. 424-2006)

Establece un impuesto al valor agregado sobre ciertos actos y contratos gravados por las normas de esta ley, generados por venta o permuta de bienes muebles o de derechos reales sobre ellos, la prestación de servicios en el territorio nacional, las importaciones, el arrendamiento de bienes muebles o inmuebles, la destrucción o pérdida o cualquier hecho que implique faltante de inventario, la venta o permuta de bienes inmuebles, entre otros.

1.7.6 Ley del Impuesto del timbre y papel sellado especial para protocolos (Decreto No. 37-92)

Establece un impuesto de timbres y papel sellado especial para protocolos, sobre los documentos que contienen actos y contratos establecidos en esta ley, entre los cuales se puede mencionar los contratos civiles y mercantiles, documentos otorgados en el extranjero, documentos públicos o privados cuya finalidad sea la comprobación del pago con bienes o dinero, ciertos comprobantes de pago emitidos por aseguradoras o afianzadoras, comprobantes de pago de premios de loterías, rifas y sorteos y otros.

1.7.7 Ley del Impuesto de Solidaridad (Decreto No. 73-2008)

Impuesto a cargo de las personas individuales o jurídicas, así como los fideicomisos, los contratos de participación, las sociedades irregulares, las sociedades de hecho, el encargo de confianza, las sucursales, agencias o establecimientos permanentes o temporales de personas extranjeras que operan en el país, las copropiedades, las comunidades de bienes, los patrimonios hereditarios indivisos y otras formas de organización empresarial, que dispongan de patrimonio propio, realicen actividades mercantiles o agropecuarias en el territorio nacional y que obtengan un margen bruto superior al cuatro por ciento (4%) de sus ingresos brutos y que no estén registrados bajo el régimen del impuesto sobre la renta del pago o retención del 5% sobre ingresos brutos.

Su base imponible la constituye la que sea mayor entre:

- la cuarta parte de sus activos netos; o
- la cuarta parte de sus ingresos brutos

Se debe utilizar la base de los ingresos brutos en el caso de los contribuyentes cuyo activo neto sea más de cuatro veces sus ingresos brutos.

La tasa impositiva se establece del 1% y debe liquidarse dentro del mes inmediato siguiente a la finalización de cada trimestre calendario.

1.7.8 Ley de Prevención del Lavado de Dinero y Otros Activos (Decreto No. 67-2001)

Tiene por objeto prevenir, controlar, vigilar y sancionar el lavado de dinero u otros activos provenientes de la comisión de cualquier delito, y establece las normas que para el efecto deberán observar las personas obligadas y las autoridades competentes incluidas en el artículo 18 de esta ley.

Dentro de su artículo 18, se mencionan a las personas individuales o jurídicas que entre otras actividades realicen compraventa de divisas, donde se pueden incluir a las empresas distribuidoras de vehículos automotores por razón de su giro habitual de negocios de importación.

Las personas obligadas deberán adoptar, desarrollar o ejecutar programas, normas, procedimientos y controles internos idóneos para evitar el uso indebido de sus productos y servicios en actividades de lavado de dinero u otros activos.

Además obliga a llevar un registro diario de las transacciones en efectivo, ocasionales o habituales, en moneda nacional o extranjera que superen el monto de diez mil dólares de los Estados Unidos de América o su equivalente en moneda nacional, las cuales se deberán reportar mensualmente dentro de los primeros cinco días hábiles del mes siguiente de efectuadas las transacciones, en los formularios que para el efecto proporcione la Intendencia de Verificación Especial (IVE). Además deberán comunicar a dicha intendencia las transacciones que se consideren sin fundamento económico legal evidente o que puedan considerarse sospechosas o inusuales.

1.7.9 Ley para prevenir y reprimir el financiamiento del terrorismo (Decreto No. 58-2005)

Esta ley fue declarada de interés público y tiene por objeto adoptar medidas para la prevención y represión del financiamiento del terrorismo, considerado delito de lesa humanidad y que va contra el derecho internacional.

Dentro del régimen de personas obligadas, considera las establecidas en la Ley contra el lavado de dinero y otros activos, pero crea también un régimen especial de personas que por la naturaleza de sus actividades, estarán obligadas a proporcionar a la Superintendencia de Bancos, a través de la Intendencia de Verificación Especial, las informaciones y reportes que esta les requiera para el cumplimiento de sus funciones. Asimismo, deberán permitir a la Superintendencia, el libre acceso a todas sus fuentes y sistemas de información para la verificación o ampliación de las informaciones proporcionadas por ellas mismas, o cuando sea necesarios para el análisis de casos relacionados con el financiamiento de terrorismo.

Dentro de las actividades aplicables en este régimen especial, se refiere a las personas individuales o jurídicas que realicen actividades de compra venta de vehículos automotores, por lo que estas empresas estarán obligadas a establecer controles específicos que le permitan informar a la Intendencia de Verificación Especial acerca de las transacciones diarias o sospechosas de acuerdo a los lineamientos que la presente ley y la ley contra el lavado de dinero u otros activos establecen.

1.7.10 Ley del Impuesto de Circulación de Vehículos Terrestres, Marítimos y Aéreos (Decreto No. 70-94)

Establece un impuesto anual sobre circulación de vehículos terrestres, marítimos y aéreos, que se desplacen en el territorio nacional, las aguas y espacio aéreo comprendido dentro de la soberanía del Estado de Guatemala.

Una de las disposiciones que se refiere directamente a las empresas distribuidoras de vehículos automotores se encuentra en el artículo 29, inciso d) que dice lo siguiente:

"Para los vehículos nuevos importados directamente de fábrica, por empresas distribuidoras cuyo objeto principal sea la venta al consumidor final, el pago por placas de distribuidor hará cualquier día del año, dependiendo de las necesidades de las empresas distribuidoras." (4:15)

1.7.11 Leyes aplicables a la importación

Las empresas distribuidoras de vehículos automotores, como empresas importadoras de vehículos nuevos, conocidas como agencias, deben registrarse ante la Superintendencia de Administración Tributaria como tales, registrando también las marcas de los vehículos a importar.

Como agencias registradas, los valores de las facturas de sus proveedores son aceptados en la aduana y forman, junto con el flete y seguro, la base para la determinación de los Derechos Arancelarios a la Importación (DAI), que en el caso de vehículos oscila entre 0 y 20% según el Sistema Arancelario Centroamericano (SAC).

"El Código Aduanero Uniforme Centroamericano –CAUCA- aprobado por Resolución 223-2008 (COMIECO-XLIX) del Consejo de Ministros de Integración Económica, en el Artículo 41, señala que el Arancel Centroamericano de Importación, que figura como Anexo A del Convenio sobre el Régimen Arancelario y Aduanero Centroamericano, es el instrumento que contiene al nomenclatura para la clasificación oficial de la mercancías que sean susceptibles de ser importadas al territorio de los Estados Centroamericanos, así como los derechos arancelarios a la importación y las normas que regulan la ejecución de sus disposiciones.

El Sistema Arancelario Centroamericano (SAC) constituye la clasificación oficial de las mercancías de importación y exportación a nivel centroamericano.

El Arancel Centroamericano de Importación está constituido por el Sistema Arancelario Centroamericano (S.A.C.) y los correspondientes Derechos Arancelarios a la Importación (D.A.I)." (17:1)

Los principales requisitos que debe cumplir una importación, son:

- Factura comercial.
- Lista de empaque con el detalle de motor, chasis y motor.

- Documento de embarque:
    - Bill of landing (transporte marítimo).
    - Guía aérea (transporte aéreo)
    - Carta de Porte (transporte terrestre)
- Copia del Certificado de Seguro.
- De no contar con lo anterior, se estipulan diferentes porcentajes de determinación de valor de seguro sobre el valor FOB (Free on board), así:
    - Vía marítima 1.65%
    - Vía aérea 2.2%
    - Vía Terrestre 1.675%
- Certificado sanitario, avalado por el Ministerio de Salud (Generalmente para productos alimenticios).
- Código del importador.
- Licencia de importador.

1.8 Productos y servicios

El principal producto que ofrecen estas empresas son los vehículos automotores como pickups, camiones, automóviles y motocicletas, que pueden ser de distintas marcas de prestigio mundial y son mayormente importados desde la casa fabricante, debido a que no se existe ninguna fábrica de este tipo en el territorio nacional.

Las empresas distribuidoras de vehículos automotores deben respaldar la inversión de sus clientes con una cadena de servicios y suministros que se resumen en los siguientes:

- Repuestos originales:
  Para cada modelo de vehículo que se vende en la empresa se deben identificar las piezas de mayor demanda y rotación mediante estimaciones del proveedor o criterio de los encargados de esa unidad.

- Servicios de taller:
  Se necesita contar con el respaldo de servicios especializados para las marcas distribuidas, con la finalidad de mantener la reputación de agencia ante los clientes, y cumplir con los requerimientos mínimos que pueda exigir la casa matriz de la marca.

CAPÍTULO II

EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES

2.1 Definición del departamento de informática

Es el departamento encargado de administrar los recursos informáticos de una empresa, el proceso electrónico de datos, así como el soporte y mantenimiento de los elementos o servicios básicos de información de la empresa, también denominados como infraestructura tecnológica.

"La organización de este departamento debe cubrir funciones relativas a seguridad, desarrollo y mantenimiento de aplicaciones, soporte técnico para administración de redes y sistemas, y operaciones."(3:134)

Para las empresas distribuidoras de vehículos automotores que procesan su información por medios computarizados, la importancia del departamento de informática radica en la dependencia de los procesos del negocio en la tecnología informática, donde el debido cumplimiento de las funciones de este departamento influye directamente en el logro de sus objetivos.

El departamento de informática está conformado básicamente por los siguientes cuatro elementos:

- El equipo físico o "hardware" utilizado para operar el sistema. Incluye unidades centrales de proceso o "CPU", servidores de datos y aplicaciones, infraestructura de telecomunicaciones, accesorios de interfaz con el usuario, como monitores, teclados, ratones, bocinas, audífonos, unidades de energía de respaldo o "ups", impresoras y otros.

- Los sistemas o "software" que incluyen el sistema principal y las aplicaciones específicas o paquetes computacionales, sistemas de comunicación y otros.

- Los datos, que constituyen la materia prima para generar la información. Aunque muchas veces estos dos términos se utilizan indistintamente, la diferencia entre dato e información es que los datos son señales individuales en bruto y sin ningún significado que son manipuladas por el computador (hardware y software) para producir la información deseada, y

- El recurso humano necesario para administrar y dar mantenimiento a los elementos anteriores.

2.2 Comité de Dirección

La alta gerencia debe designar un comité de planeación y dirección para la supervisión de la función de sistemas de información y sus actividades.

Este es un factor importante para asegurar que el departamento de informática concuerde con la misión y visión del negocio. Es deseable, pero no muy común que un miembro de la Junta Directiva que entienda los riesgos y temas de la tecnología informática dirija este comité. El comité debería incluir representantes de la alta dirección, de la gerencia usuaria, y del departamento de informática.

"Entre las funciones primarias que realiza este comité se encuentran:

- Revisar los planes de corto y largo plazo del departamento de informática.
- Revisar y aprobar las adquisiciones importantes de hardware y software, dentro de los límites aprobados por la junta directiva.
- Aprobar y monitorear los proyectos de alta relevancia y el estado de los planes y presupuestos de sistemas, establecer prioridades, aprobar normas y procedimientos, y monitorear el desempeño general de sistemas.
- Revisar y aprobar las estrategias para servicios externos (outsourcing) de ciertas actividades o todas las actividades de sistemas, y la globalización, o traslado al extranjero de las funciones de sistemas.
- Revisar los recursos y su asignación de acuerdo a términos de tiempo, personal y equipo.
- Decidir respecto a la centralización o descentralización de responsabilidades.
- Apoyar el desarrollo e implementación de un programa de administración de seguridad información en toda la organización.
- Reportar a la Junta Directiva sobre las actividades de sistemas."(3:105)

2.3 Personal que integra el departamento de informática

Para administrar el departamento de informática es necesario realizar una adecuada división del personal de la siguiente forma:

- Gerencia del departamento
- Mesa de ayuda a usuarios (help desk)
- Personal especializado encargado del análisis y programación del sistema.

- Personal para la administración del equipo (reparaciones, instalación de sistemas, administración de redes, etc.) y el soporte a la infraestructura tecnológica.

2.3.1 Gerencia del departamento

Cumple la función de enlace entre las necesidades informáticas de la empresa y los usuarios de los servicios computacionales, por lo tanto, la persona que funge como gerente de informática deberá tener sólidos conocimientos de sistemas, equipos informáticos y de la infraestructura necesaria para su funcionamiento. Generalmente se recomienda que el encargado posea el título de Ingeniero en Sistemas o Licenciado en Administración de Sistemas.

2.3.2 Mesa de ayuda a usuarios (support / help desk)

Es una unidad especializada que tiene a su cargo el apoyo a los usuarios finales de los sistemas de información. La atención que brinda puede ser derivada de consultas sobre la utilización de software o sobre problemas técnicos de los equipos. Las actividades de la mesa de ayuda se deben documentar, para contar con información estadística de los problemas de hardware y software encaminada a la mejora de los servicios.

"Algunas de las funciones de soporte de la mesa de ayuda a usuarios (help desk), son:

- Determinar el origen de los problemas de cómputo y emprender las acciones correctivas apropiadas.
- Iniciar los reportes de problemas que se requieran y asegurar que los problemas sean resueltos a su debido tiempo.
- Obtener conocimientos detallados del sistema operativo y del software de otros sistemas.
- Responder a las interrogantes relativas a sistemas específicos.
- Controlar la instalación de software del vendedor y del sistema para mejorar su eficiencia y personalizar el sistema sobre la base de los requisitos de la organización y a la configuración de las computadoras.
- Brindar soporte técnico al procesamiento computarizado de las telecomunicaciones.
- Mantener documentación del software del vendedor, incluyendo la emisión de nuevas versiones (releases) y resolución de problemas, así como documentación de los sistemas y utilerías desarrolladas localmente.
- Comunicarse con las operaciones de sistemas para señalar patrones anormales en llamadas o comportamiento de aplicaciones." (3:353)

2.3.3 Departamento de Análisis y Programación de Sistemas

El departamento de sistemas tiene a su cargo la administración del sistema principal, la implementación de mejoras, así como el desarrollo y administración de los proyectos informáticos.

El departamento de sistemas puede dividirse en:

- Sección de análisis de sistemas:
  Se encarga de evaluar la funcionalidad y mejora de los sistemas, así como recibir los proyectos informáticos, determinando los requerimientos de tiempo y recursos para su implementación.

- Sección de programación de sistemas:
  Tiene a su cargo realizar la programación del sistema, o los nuevos programas, considerando el análisis realizado por los analistas de sistemas.

- Sección de Aseguramiento de Calidad:
  Cumple la labor de revisión y garantía de calidad, así como la estandarización de la metodología del desarrollo de sistemas y atención a los usuarios durante la implementación.

2.3.4 Departamento de soporte a la Infraestructura Tecnológica

Es el encargado de administrar la información resultante del proceso electrónico de datos, las copias de respaldo o back-up del sistema, realizar mantenimiento preventivo y correctivo a los equipos, el manejo de telecomunicaciones y otros relacionados. Tiene a su cargo la instalación de los sistemas de aplicación a los equipos.

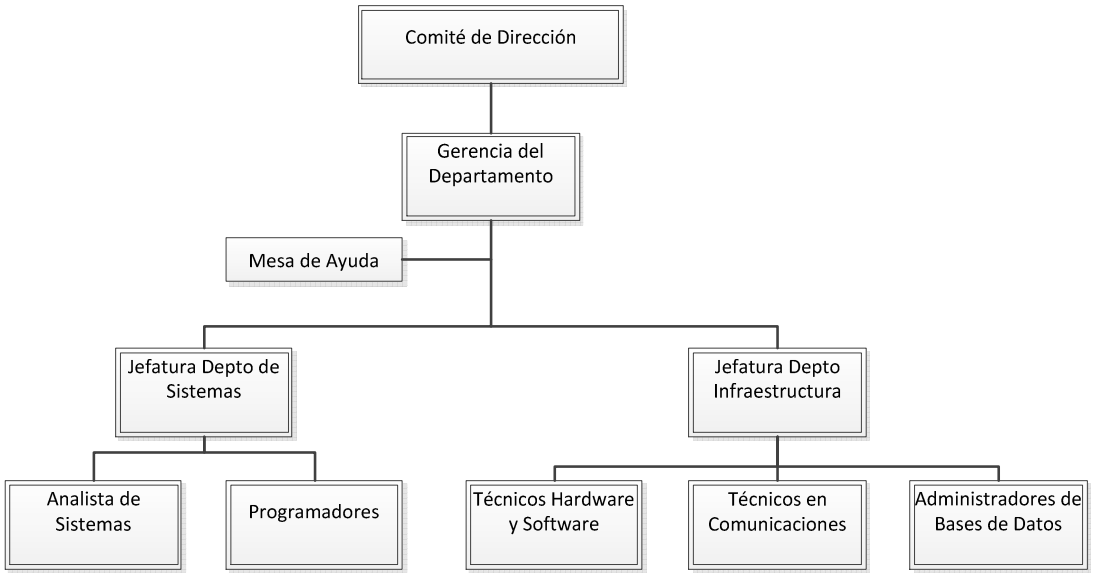
Adicionalmente maneja el presupuesto anual designado para la adquisición de hardware y software, necesario para mantener el servicio y apoyar las áreas operativas y de negocios de una empresa.

Este departamento puede subdividirse en tres secciones:

- Sección de técnicos especializados en manejo de software y hardware.
- Sección de comunicaciones, que se ocupa de administrar el correo electrónico, redes, comunicaciones, internet, antivirus, etc.

- Sección de administración de la información y operaciones relacionadas con el procesamiento electrónico de datos, back-up del sistema e información, inventarios de equipos y medidas de seguridad.

ORGANIGRAMA DEL DEPARTAMENTO DE INFORMÁTICA



Fuente: Muñoz Razo, Carlos. Auditoría de Sistemas Computacionales

2.4 Administración del personal del departamento de informática

La gerencia del departamento de informática es el encargado de establecer políticas y procedimientos para la contratación, promoción, capacitación, evaluación de atribuciones, entrenamiento, goce de vacaciones y culminación de la relación laboral de alguno de los colaboradores.

2.5 Infraestructura necesaria para el funcionamiento del departamento de informática

Además del personal que administra el departamento de informática, es necesario que se cuente con el hardware, software, sistemas de comunicación y manuales de uso de los sistemas y equipos.

2.5.1 El Hardware

Son todos los dispositivos y componentes físicos que realizan las tareas de entrada y salida de información, también se le conoce como la parte dura o física del computador.

2.5.2 Manuales de usuario

Son los documentos que contienen la información descriptiva que detalla o da instrucciones al usuario sobre la utilización u operación del software o hardware.

Incluye también las guías de operación, los términos comúnmente utilizados en el medio y las operaciones básicas del sistema.

2.5.3 El Software

"Es una colección de instrucciones ordenadas lógicamente, que permiten la ejecución de tareas específicas previamente definidas, utilizando el hardware de una computadora."(3:242)

El software tiene algunas funciones específicas, entre ellas:

- Administrar los recursos de un sistema de cómputo.
- Proporcionar las herramientas necesarias para administrar adecuadamente los recursos de un sistema de cómputo.
- Actuar como intermediario entre el usuario, el hardware y la información almacenada internamente o en dispositivos externos.

Con la finalidad de contar con un detalle comprensible para otro programador o usuario, el software deberá contar con la debida documentación, la cual puede definirse como:

"Es un documento especializado en el cual se indican todos los aspectos técnicos que se deben considerar para el adecuado manejo del sistema; estos aspectos suelen ser muy sofisticados y con características especiales sobre el funcionamiento técnico de los sistemas computacionales, no sólo en cuanto al software o hardware, sino también en cuanto a sus instalaciones, equipos y manejo de información."(3:146)

Existen tres tipos de software:

- Software del sistema:
  "Es una colección de programas de computadora usados en el diseño, procesamiento y control de todas las operaciones de computadora y sus dispositivos, como la unidad central de proceso, dispositivos de comunicaciones y dispositivos periféricos, el software del sistema administra y controla el acceso del hardware." (3:368)

- Software de aplicaciones:
  "Son programas escritos para realizar una tarea específica en la computadora y deben ser compatibles con el software del sistema (SO), ejemplo: software para procesar un texto, software para generar una hoja de cálculo; el software de aplicación debe instalarse sobre el software del sistema para poder trabajar."(3:368)

- Software de usuario final:
  "Es el que permite el desarrollo de algunas aplicaciones directamente por los usuarios finales, este software con frecuencia tiene que trabajar a través del software de aplicación y finalmente a través del software del sistema."(3:368)

"El desarrollo de software de aplicaciones para los negocios se efectúa por medio del uso de las etapas tradicionales del ciclo de vida del desarrollo de sistemas (SDLC, por sus siglas en inglés). Este enfoque es el más antiguo y mayormente utilizado para desarrollar aplicaciones de negocio y consta de las siguientes etapas:

- Viabilidad
  Determinar los beneficios estratégicos de implementar el sistema, factores intangibles como la capacitación de los usuarios y la madurez de los procesos del negocio, también deben evaluarse. Este estudio provee la debida justificación para proceder con la siguiente etapa.

- Requerimientos
  Definir el problema o la necesidad que requiere solución y definir los requerimientos de funcionalidad y calidad del sistema a desarrollar. Este puede ser un enfoque personalizado o un paquete suministrado por un proveedor, que conlleva a un proceso definido y documentado de adquisición. En cualquiera de los casos el usuario necesita participar activamente.

- Diseño
  Basándose en los requerimientos definidos, se establecen las especificaciones básicas del sistema y del subsistema, cómo interactúan éstas, y como será implementado usando el hardware, software y la red. Generalmente el diseño incluye tanto las especificaciones de programas como de la base de datos y un plan de seguridad y control de cambios para prevenir la inclusión incontrolada de requerimientos durante el proceso de desarrollo.

- Desarrollo

  Utilizar las especificaciones del diseño para empezar a programar y formalizar los procesos operativos que soportan el sistema. En esta fase tienen lugar diversos niveles de prueba para validar y verificar lo que se ha desarrollado.

- Implementación

  Se establece la operación real del nuevo sistema con la prueba de aceptación del usuario final, realizada en esta etapa. También se puede pasar por un proceso de certificación y acreditación del sistema para determinar su efectividad en mitigar los riesgos hasta un nivel aceptable y brindar informes sobre el cumplimiento de los objetivos previstos y un nivel apropiado de control interno.

- Post Implementación

  Es conveniente realizar un proceso formal para evaluar y monitorear la adecuación del sistema y las medidas del costo-beneficio previstos o el retorno de la inversión, frente a los hallazgos determinados en la etapa de viabilidad y las desviaciones de la misma.” (3:192)

2.5.4 Sistemas de comunicación

Es necesario contar con un sistema de comunicaciones adecuado y seguro que permita realizar enlaces entre el sistema principal y las terminales de los usuarios, así como entre las mismas terminales de la red.

2.5.5 Descripción de procesos

Un departamento de informática debe contar con una apropiada documentación de sus procesos. En esta documentación deberá constar la secuencia de las operaciones y sus procesos, su importancia, horarios de ejecución, personal responsable, posibles contingencias, etc.

2.5.6 Bases de datos

Las bases de datos son una colección de información organizada y enlazada al sistema y las comunicaciones, se puede tener acceso a ella por medio del software y los sistemas de redes.

2.6 Políticas y Procedimientos aplicables a un departamento de informática

"Las políticas y los procedimientos reflejan la guía y la orientación de la gerencia para desarrollar controles sobre los sistemas de información y recursos relacionados." (3:106)

2.6.1 Políticas

"Las políticas representan los estándares definidos por la Alta Gerencia de una organización. Definen las medidas y procedimientos que deben observar los usuarios al utilizar los activos y la información, con el objetivo de asegurar su salvaguarda." (3:106)

Es recomendable que se actualicen por lo menos una vez al año o cuando existan cambios significativos, y deberán darse a conocer a todo el personal del departamento.

Dentro de las políticas de informática se encuentran la asignación y uso de claves de acceso al sistema, el reglamento para el uso del correo electrónico, restricciones de acceso al departamento de informática, manejo de servidores, backup y recuperación de información, etc.

"Las políticas de seguridad para tecnología de información son parte fundamental de las organizaciones impulsadas por la tecnología, como primer paso para construir una estructura de seguridad y control de riesgos, además de los siguientes beneficios:

- Proporciona una base uniforme, estable y formal a seguir por parte del personal.
- Se crea conciencia de los riesgos.
- Contienen reglas y lineamientos a seguir en las actividades y se evitan especulaciones, especialmente para el personal de nuevo ingreso." (3:107)

2.6.2 Procedimientos

"Los procedimientos son el detalle que contiene la documentación de los procesos y los controles integrados en los mismos.

Los procedimientos se derivan de las políticas y están creados para guiar a los usuarios, por lo que estos deben conocerlos a fondo. Así mismo, deberán actualizarse cuando existan cambios significativos." (3:109)

2.7 Administración de la Seguridad Informática

"La administración de la seguridad informática es responsabilidad del departamento de informática y tiene como objetivo proteger la integridad, exactitud, disponibilidad, continuidad y confidencialidad de los sistemas de información. Así como el cumplimiento de las leyes y regulaciones internas y externas aplicables." (3:191)

La seguridad necesaria en un departamento de informática puede clasificarse en: seguridad lógica, seguridad física, del personal, de las bases de datos y de los sistemas de comunicación, como se describen a continuación:

2.7.1 Seguridad Lógica

"Son los controles de acceso de datos a una computadora, para salvaguardar la información ahí almacenada. Así mismo controla las modificaciones realizadas a los códigos de programación del sistema." (3:192)

La identificación y autorización son procesos necesarios para establecer y probar la identidad de un usuario, en el caso del acceso al sistema, los permisos.

Existen varios elementos para fortalecer la seguridad lógica:

- Software de control de acceso

  "Está diseñado para impedir el ingreso, modificación o extracción de datos no autorizados, en un programa o sistema de información." (3:199)

  "Los accesos deberán ser asignados por medio de códigos personalizados, denominados "password" o clave. Para la asignación de estos códigos es necesario que se cuente con perfiles de usuario, que deberán dar acceso al sistema de acuerdo a las funciones asignadas a cada persona de acuerdo al puesto desempeñado dentro de la organización, tomando en consideración los manuales de puestos." (3:199)

  El historial de accesos de cada usuario deberá ser almacenado en una bitácora de operaciones, para futuras consultas.

Se deberán monitorear las actividades realizadas por los usuarios de forma continua. Este seguimiento se puede apoyar en programas especializados disponibles en el mercado, con los cuales se pueden programar alarmas en tiempo real de acuerdo a eventos que se definan en los parámetros del programa, para poder detectar cualquier acceso no autorizado, sustracción o modificación de información.

"El software que se adquiera deberá poder monitorear como mínimo los accesos a:

- Librerías
- Archivos de datos
- Reportes
- Red de comunicación.
- Programas de aplicación.
- Diccionario de datos.
- Intentos de accesos externos."(7:199)

- Firewall

"El Firewall (Cortafuegos) es un software que permite la administración centralizada de los accesos a la información, desde canales externos, principalmente desde internet o canales VPN (virtual protocol network).

Funciona programando o asignando los permisos que tendrán los usuarios, así como los privilegios para el uso de la información. Bloquean el acceso a sitios particulares de internet.

También impiden que determinados usuarios tengan acceso a servidores o servicios. Monitorean las comunicaciones entre una red interna y una externa. Pueden encriptar o cifrar paquetes que son enviados entre diferentes ubicaciones físicas dentro de una organización creando una red virtual de internet.

Son dispositivos que ayudan a administrar políticas de seguridad para el tráfico de información que ingresa a la organización y se transmite desde diferentes segmentos de una red.

Un firewall proporciona un buen porcentaje de seguridad, sin embargo, es importante que se analicen detalladamente algunos posibles problemas o debilidades importantes:

- El tráfico interno de comunicaciones en la red no es analizado.
- Malas configuraciones.
- Falta de monitoreo de las actividades de los usuarios.
- Falta de actualización de las políticas.” (3:532)

- Software para prevención y detección de intrusos

  Estos programas funcionan brindando alertas ante la realización de ataques con éxito e incluso ante ataques en progreso.

  Estos programas deberán ser parametrizados con eficacia identificando plenamente las posibles situaciones de riesgo, en el sentido de que no ofrezcan ni falsos positivos (calificar de ataque una situación que no es tal), ni falsos negativos (no considerar como ataque una situación que en realidad si lo era).

  La efectividad de un programa de prevención y detección de intrusos será mayor cuanto más corto es el tiempo de respuesta de la alerta, para permitir actuar oportunamente y en consecuencia poder detener el ataque en curso.

  Estás características deben considerarse siempre para que el software sea de verdadera utilidad en la detección de intrusiones al sistema informático de la organización.

  Prevención, detección y reacción constituyen tres conceptos clave en todo sistema de protección que pretenda ofrecer soluciones integrales de seguridad.

  Hoy en día, prácticamente la totalidad de productos de seguridad en el mercado, se centran en la primera de esas acciones, la prevención del ataque, utilizando cortafuegos y criptografía. Aunque ningún programa de este tipo será nunca cien por ciento infalible, lo cierto es que disminuirá la probabilidad de éxito de un ataque.

  El beneficio de un software para prevención y detección de intrusos, es proveer una solución proactiva, bloqueando amenazas antes de que ocurra el daño a través de inteligencia de seguridad en tiempo real, control de cambio y administración de dispositivos.

  El software para prevención y detección de intrusos tiene como finalidad permitir y controlar el acceso a los siguientes recursos:

- Programas de librerías.
- Archivos de datos.
- Programas de aplicación.
- Diccionarios de datos.
- Sistemas de comunicación.

"Los programas para detección de intrusos permiten detectar ataques que pasan inadvertidos a un firewall (cortafuegos) y avisan antes o justo después de que se produzcan esos ataques." (3:537)

- Antivirus

"Un departamento de informática debe contar con un antivirus, que es un programa para detectar y eliminar los virus." (3:549)

Los virus son programas computacionales avanzados que tienen como objetivo principal la destrucción de la información almacenada en las computadoras o la saturación de los sistemas, así como la obtención no autorizada de información.

2.7.2 Seguridad Física

Para proteger adecuadamente el software, el hardware y la información, es necesario que las instalaciones del departamento de informática cuenten con las debidas medidas de seguridad.

Las principales medidas de seguridad que deben existir sobre las instalaciones físicas del departamento de informática son:

- Accesos

Se deben restringir los accesos para que únicamente el personal autorizado ingrese a las instalaciones del departamento de informática. El acceso puede ser controlado por medio del uso de un dispositivo electrónico activado por una tarjeta y códigos que se asignan al personal que tendrá libre acceso.

- Cámaras de vigilancia

  Es recomendable que existan cámaras de vigilancia en el departamento de informática para monitorear las actividades del personal que labora en el departamento, así como verificar el control de los accesos.

- Bitácoras de operación

  Un departamento de informática debe contar con bitácoras de operación (pistas de auditoría), que contengan como mínimo la fecha, nombre del usuario operador o consultor de la información, datos anteriores, datos nuevos, etc. Todo esto para permitir monitorear posteriormente y en tiempo real el acceso a la información.

- Aire acondicionado

  Los equipos de computación concentrados dentro del departamento de informática generan calor que puede dañarlos, por lo que es necesario que se cuente con equipo adecuado de aire acondicionado que evite el sobrecalentamiento, generalmente la temperatura ideal para los equipos de cómputo oscila entre 14 y 17 grados centígrados.

- Suministros de energía eléctrica

  El servicio de energía eléctrica se considera uno de los servicios críticos, se debe garantizar que en ausencia del servicio público se cuente con una fuente de corriente alterna o servicio propio.

  Esta corriente alterna puede ser provista mediante UPS (uninterruptible power supply), o plantas generadoras de electricidad. Así mismo es necesario contar con reguladores de voltaje, que protejan los equipos de sobrecargas de electricidad.

- Detección de humo e inundaciones

  Se deberá contar con alarmas detectoras de humo e inundaciones para salvaguardar el equipo y el personal de los daños causados por fuego y agua.

- Seguros

  Se deberá contar con seguros que contemplen el resarcimiento de los daños provocados por incendios, terremotos, sabotaje, hurto, robo, daños al personal y otros que puedan afectar al software, hardware, información y al personal del departamento de informática.

2.7.3 Seguridad del Personal

La seguridad del personal debe ser uno de los principales objetivos de seguridad en un departamento de informática. Se deberán monitorear sus actividades.

Es importante contar con políticas de incentivos y reconocimientos, para garantizar la constante motivación del personal.

Se deberá contar con políticas de rotación de puestos, para evitar tener personal insustituible y además detectar posibles errores y/o fraudes, además implementar estándares de calidad y de control interno en el desarrollo del software para evitar actos dolosos, realizados por los usuarios o los mismos programadores.

2.7.4 Seguridad de la Base de Datos

Las bases de datos son la colección resultante del proceso electrónico de datos. La seguridad deberá orientarse a prevención de la manipulación no autorizada de la información que contengan.

2.7.5 Seguridad de los Sistemas de Comunicación

Los sistemas de comunicación permiten recibir, enviar y procesar la información entre las computadoras de la organización. Se deberá asegurar su utilización mediante accesos definidos por niveles, controlando el envío y recepción de información mediante estos sistemas.

2.7.6 Seguridad en la programación de los sistemas

Su objetivo es constatar que los sistemas estarán programados para satisfacer los objetivos de la organización de acuerdo a las necesidades y funciones de los usuarios finales.

2.8 Presupuestos para adquisición y mantenimiento de tecnología de información

Un departamento de informática deberá contar con un presupuesto que le permita realizar la adquisición oportuna de los diferentes recursos necesarios para el desarrollo de sus actividades. Generalmente este presupuesto se elabora para periodos anuales.

Un presupuesto permite el pronóstico, monitoreo y análisis de la adquisición de recursos informáticos. Permite la asignación adecuada de los recursos tomando en consideración los planes a corto y largo plazo.

Los presupuestos deberán ser elaborados por la gerencia del departamento, y autorizados anualmente por el comité de dirección, derivado de la fluctuación constante en los precios y la constante actualización de los recursos tecnológicos.

La aprobación de la adquisición de software y hardware será conforme este presupuesto, sin embargo éste deberá ser flexible para cumplir con compras que se requieran por casos de emergencia que deberán ser autorizados por medio de una reunión extraordinaria del comité de dirección.

CAPÍTULO III

AUDITORÍA INTERNA DE SISTEMAS INFORMÁTICOS

Para una mejor comprensión de la función de auditoría interna aplicada a los sistemas informáticos, se hace necesario conocer algunas definiciones generales de auditoría:

“Auditar es el proceso de acumular y evaluar evidencia, realizado por una persona independiente y competente, acerca de la información cuantificable de una entidad económica específica, con el propósito de determinar e informar sobre al grado de correspondencia existente entre la información cuantificable y los criterios establecidos.” (7:4)

“Es la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoria, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones.” (11:11)

Tomando en consideración estas definiciones se puede indicar que Auditoría es el proceso independiente de revisión de actividades, funciones específicas, resultados u operaciones de una entidad, mediante la acumulación y evaluación de evidencia, con el propósito de determinar e informar sobre el grado de correspondencia entre la información cuantificable y los criterios establecidos.

De lo anterior se destaca la amplitud del alcance de Auditoría, ya que sus técnicas y procedimientos se consideran aplicables a cualquier revisión donde existan criterios preestablecidos para la comparación y/o evaluación de información cuantificable y no se limita a revisiones acerca de la razonabilidad de las cifras en los estados financieros.

La definición de Auditoría Interna la establece en diciembre del 2000 el instituto de Auditores Internos de los Estados Unidos de América (IIA) de la siguiente forma: “La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno” (13:1)

Aunque el enfoque tradicional de auditoría interna de hasta hace algunos años, consideraba a la auditoría interna como un elemento operativo, aquel que aprobaba las transacciones, ponía el visto

bueno en los asientos contable, liquidaciones, etc. El enfoque moderno pretende enfatizar su función de control, mayormente como elemento de la misma, modificando, rectificando y cambiando las funciones de auditoría interna, de una acción de control previo, hacia una acción más positiva orientada a la evaluación de sistemas, procesos y resultados, dentro de los cuales cobra cada vez más importancia la evaluación de sistemas informáticos para el aseguramiento de información confiable y oportuna, como consecuencia del auge de la tecnología en las empresas modernas.

3.1 Auditoría Interna de Sistemas Informáticos

A continuación se presentan algunas definiciones de Auditoría de Sistemas Informáticos:

"Es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa" (11:19)

"La auditoría en informática es la revisión y evaluación de los controles, sistemas y procedimientos de Informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones." (6:18)

"La Auditoría de Sistemas Informáticos puede definirse como cualquier auditoría que abarca la revisión y evaluación (parcial o total) de los sistemas automatizados de procesamiento de información, procesos relacionados no automatizados y las interfaces entre ellos" (3:34)

Las anteriores definiciones destacan características importantes del trabajo que realiza la auditoría de sistemas informáticos, pero a nivel internacional se acepta de forma general el establecido por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés), que también publicó los Objetivos de Control de Información y Tecnología Relacionada (COBIT, por sus siglas en inglés) en que se basa el presente trabajo, por lo que deberá ser el concepto a considerar y dicta de la siguiente manera: "Auditoría de Sistemas es cualquier auditoría que abarca la revisión y

evaluación de todos los aspectos (o de cualquier porción de ellos), de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.” (12:1)

La importancia de la Auditoría Interna en la revisión de controles informáticos es la evaluación continuada que se realiza de acuerdo al plan anual de trabajo, donde el Gerente de Auditoría Interna debe considerar el tipo de revisión que la administración necesita para asegurar su inversión en tecnología informática, ya sea que los sistemas se encuentren completamente establecidos y Auditoría Interna se limite a aplicar evaluaciones de monitoreo, que la empresa se encuentre en proceso de análisis para la adquisición de nueva tecnología informática, o se haya tomado la decisión de adaptar el software existente a las nuevas necesidades de la empresa y por ello se encuentre en proceso de mantenimiento e implementación de cambios importantes que puedan afectar directamente la información financiera, donde Auditoría Interna deberá aplicar pruebas específicas para determinar su efecto.

Tomando como base que la Auditoría Interna es el departamento asesor de la gerencia en materia de sistemas de información, control y operación, se puede apreciar que debe concentrarse en controles que minimicen los riesgos y que sirvan como base para la acción de los niveles gerenciales. Con mayor razón si se toma en cuenta que los sistemas informáticos son sistemas rápidos de proceso y manejo de datos, lo cual representa también un gran peligro al momento que existan fallas no detectadas en el procesamiento.

Por lo anterior, las razones básicas por las que Auditoría Interna debe intervenir en la evaluación de sistemas informáticos, son las siguientes:

- “La gran dependencia de la organización como usuaria de la unidad encargada del desarrollo y manejo de la tecnología.

- La falta de una clara comprensión del uso de la tecnología por parte de las unidades usuarias.
- La falta de conciencia sobre el alcance y control de la tecnología dentro de la organización.
- El permanente avance tecnológico.

- El costo representativo de equipos y aplicaciones existentes.

- Limitación en el conocimiento de los objetivos de la organización y de las unidades usuarias, por parte de la unidad encargada del desarrollo y manejo de la tecnología.

- Mayor número de equipos y terminales repartidos dentro de la organización y el país.

- La necesidad de evaluar las accione que lleva cabo la unidad encargada del desarrollo y manejo de la tecnología.

- Mayor vulnerabilidad de la organización por el avance tecnológico.

- Ausencia de programas formales de mantenimiento y sostenibilidad de los sistemas y tecnología en uso.

- Riesgos permanentes que pueden dañar la información a través de virus u otros aspectos en las redes o Internet."(8:539)

3.2 Normas y Procedimientos para auditar sistemas informáticos

La Auditoría de Sistemas de Información es un trabajo de naturaleza especializada y las habilidades necesarias para llevar a cabo este tipo de auditorías requieren el desarrollo y la promulgación de normas específicas para la práctica profesional como las emitidas por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) las cuales son aplicables para el trabajo de auditoría realizado por miembros de la asociación y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información (CISA, por sus siglas en inglés), aunque a criterio personal pueden servir de base para cualquier auditor que cuente con las habilidades y destrezas suficientes y necesite apoyarse en una normativa específica para realizar su trabajo, debido a que el planteamiento a nivel general es similar a la normativa para la realización del trabajo de cualquier auditoría por lo que en el presente trabajo se considera la más adecuadas para una auditoría de sistemas de información.

Antes de describir las normas de ISACA para la Auditoría de Sistemas Informáticos se hace necesario desarrollar la normativa internacional aplicable a nivel nacional que todo auditor debe observar en la realización de su auditoría, específicamente en una auditoría de sistemas informáticos actuando como auditor interno.

3.3 Normas Internacionales de Auditoría

Para su desarrollo ordenado el presente tema se divide en Normas Ético Morales y Normas Profesionales.

3.3.1 Normas Ético Morales

Desde el punto de vista del auditor interno como profesional en la evaluación de sistemas, se hace necesario contar con un código de ética para la profesión de auditoría interna debido a que esta se basa en la confianza que se imparte a su aseguramiento objetivo sobre la gestión de riesgos, control y dirección.

El Código de Ética del Instituto Internacional de Auditoría Interna, además de la definición de auditoría interna, incluye dos componentes esenciales:

- Principios que son relevantes para la profesión y práctica de la auditoría interna.
- Reglas de conducta que describen las normas de comportamiento que se espera sean observadas por los auditores internos.

Estas reglas son una ayuda para la interpretación de los principios en aplicaciones prácticas. Su intención es guiar la conducta ética de los auditores internos. Es aplicable tanto a las personas como a las entidades que proveen servicios de auditoría interna.

Se espera que los auditores internos apliquen y cumplan con los siguientes principios:

- Integridad:

  La integridad de los auditores internos establece confianza y, consiguientemente, provee la base para confiar en su juicio.

- Objetividad:

  Los auditores internos exhiben el más alto nivel de objetividad profesional al reunir, evaluar y comunicar información sobre la actividad o proceso a ser examinado. Los auditores internos hacen una evaluación equilibrada de todas las circunstancias relevantes y forman sus juicios sin dejarse influir indebidamente por sus propios intereses o por terceras personas.

- Confidencialidad:

  Los auditores internos respetan el valor y la propiedad de la información que reciben y no divulgan información sin la debida autorización a menos que exista una obligación legal o profesional para hacerlo.

- Competencia:

  Los auditores internos aplican el conocimiento, aptitudes y experiencia necesarios al desempeñar los servicios de auditoría interna.

Además se espera que realicen su trabajo respetando las siguientes reglas de conducta relacionadas con los principios anteriores:

- Integridad:

  - Desempeñar su trabajo con honestidad, diligencia y responsabilidad.
  - Respetar las leyes y divulgar lo que corresponda de acuerdo con la ley y la profesión.
  - No participar a sabiendas de una actividad ilegal o de actos que vayan en detrimento de la profesión de auditoría interna o de la organización.
  - Respetar y contribuir a los objetivos legítimos y éticos de la organización.

- Objetividad:

  - No participar en actividades o relaciones que puedan perjudicar o que aparenten que puedan perjudicar su evaluación imparcial. Esta participación incluye aquellas actividades o relaciones que puedan estar en conflicto con los intereses de la organización.
  - No aceptar nada que pueda perjudicar o que aparente que pueda perjudicar su juicio profesional.
  - Divulgar todos los hechos materiales que conozcan y que, de no ser divulgados, pudieran distorsionar el informe de las actividades sujetas a revisión.

- Confidencialidad:

  - Ser prudentes en el uso y protección de la información adquirida en el transcurso de su trabajo.

- No utilizar información para lucro personal o de alguna manera que fuera contraria a la ley o en detrimento de los objetivos legítimos y éticos de la organización.

- Competencia:

  - Participar solo en aquellos servicios para los cuales tengan los suficientes conocimientos, aptitudes o experiencia.
  - Desempeñar todos los servicios de auditoría interna de acuerdo con las normas para la práctica profesional de la auditoría interna.
  - Mejorar continuamente sus aptitudes y la efectividad y calidad de sus servicios.

3.3.2 Normas Profesionales

Para normar las actividades de Auditoría Interna existe el Instituto Internacional de Auditoría Interna (IIA, por sus siglas en inglés) donde se han emitido un conjunto de normas denominadas “Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (NIEPAI)” las cuales están conformadas por Normas sobre Atributos, Normas sobre Desempeño, y Normas sobre Implantación.

Las Normas sobre Atributos definen las características de las organizaciones y los individuos que desarrollan actividades de auditoría interna. Las Normas sobre desempeño describen la naturaleza de las actividades de auditoría interna y proveen criterios de calidad con los cuales puede evaluarse el desempeño de estos servicios. Las Normas sobre Atributos y sobre Desempeño se aplican a todos los servicios de auditoría interna en general, mientras que las Normas sobre Implantación se aplican a determinados tipos de trabajos.

El auditor interno en el medio guatemalteco deberá observar principalmente la normativa vigente para auditorías de estados financieros emitida por el Consejo de Normas de Auditoría y Atestiguamiento (IAASB, por sus siglas en inglés) de la Federación Internacional de Contadores (IFAC, por sus siglas en inglés), las cuales fueron adoptadas por el Instituto Guatemalteco de Contadores Públicos y Auditores (IGCPA) como la normativa vigente para la práctica de la profesión de auditoría en la República de Guatemala a partir de enero del 2008, las que se denominan “Normas Internacionales sobre Control de Calidad, Auditoría y Atestiguamiento y Servicios Relacionados (Normas Internacionales o Normas del IAASB), donde la evaluación del control interno, ya sea a nivel de controles administrativos o de controles de los sistemas informáticos, influyen en la extensión y alcance de las pruebas sustantivas que deben aplicarse durante la revisión por el grado de confianza que el auditor considera depositar en las cifras de los estados financieros.

La norma internacional de auditoría No. 315 “Entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa” establece y proporciona guías para conocer la entidad y su entorno, incluyendo su control interno, y para evaluar los riesgos de representación errónea en un auditoría de estados financieros.
En resumen esta norma plantea los siguientes requisitos:

- Procedimientos de evaluación del riesgo y fuentes de información sobre la entidad y su entorno, incluyendo su control interno:

  Explica los procedimientos de auditoría que se requiere al auditor realizar para obtener el entendimiento de la entidad y su entorno, incluyendo su control interno (procedimientos de evaluación de riesgo). También requiere la discusión entre el equipo de trabajo sobre la susceptibilidad de los estados financieros a representación errónea de importancia relativa.

- Entendimiento de la entidad y su entorno, incluyendo su control interno:

  Requiere que el auditor entienda aspectos específicos de la entidad y su entorno, y componentes de su control interno, para identificar y evaluar los riesgos de representación errónea de importancia relativa.

- Evaluación de los riesgos de representación errónea de importancia relativa:

  Requiere que el auditor identifique y evalúe estos riesgos a nivel de estados financieros y de aseveración. Se indica que el auditor deberá:

  - Identificar los riesgos al considerar la entidad y su entorno, incluyendo controles relevantes, y al considerar las clases de transacciones, saldos de cuentas y revelaciones en los estados financieros.
  - Relacionar los riegos identificados con los que puedan estar mal a nivel de aseveración; y
  - Considerar la importancia y probabilidad de los riesgos.
  - Además requiere que el auditor determine si cualquiera de los riesgos evaluados son riesgos importantes que requieran consideración especial de auditoría o riesgos para los que los procedimientos sustantivos por si solos no proporcionen suficiente evidencia apropiada de auditoría. Se requiere que el auditor evalúe el diseño de los controles de la entidad, incluyendo actividades de control relevantes, sobre dichos riesgos y que determine si se han implantado.

- Comunicación con los encargados del mando (gobierno corporativo) y con la administración:

  Se tratan asuntos relativos al control interno que el auditor comunica a los encargados del mando y la administración.

- Documentación:

  Se establecen los requisitos mínimos de documentación relacionados.

Para que el auditor logre un entendimiento de la entidad y su entorno, deberá considerar y comprender los siguientes aspectos:

- Factores de la industria, de regulación y otros factores externos, incluyendo el marco de referencia de información financiera aplicable.
- Naturaleza de la entidad, incluyendo la selección y aplicación de políticas contables.
- Objetivos y estrategias y los riesgos de negocio relacionados que puedan dar como resultado una representación errónea de importancia relativa de los estados financieros.
- Medición y revisión del desempeño financiero de la entidad.
- Control Interno.

De los anteriores aspectos, es el entendimiento y evaluación del control interno el que se relaciona directamente con el presente trabajo por lo que a continuación se desarrolla lo que la norma establece al respecto:

El auditor utiliza la evaluación y el entendimiento del control interno para identificar los tipos de representaciones erróneas potenciales, considerar factores que afectan a los riesgos de representación errónea de importancia relativa, y diseñar la naturaleza, oportunidad y extensión de procedimientos adicionales de auditoría.

El Control Interno es el proceso diseñado y efectuado por los encargados del mando (gobierno corporativo), la administración y otro personal para proporcionar certeza razonable sobre el logro de los objetivos de la entidad respecto de la confiabilidad de la información financiera, efectividad y eficiencia de las operaciones y cumplimiento con leyes y regulaciones aplicables. El control interno se diseña e implementa para atender a riesgos de negocio identificados que amenazan el logro de cualquiera de esos objetivos.

Los componentes del control interno, según la norma, son los siguientes:

- El ambiente de control
- El proceso de evaluación de riesgo
- El sistema de información, incluyendo los procesos del negocio relacionados, relevantes a la información financiera y la comunicación.
- Actividades de control
- Monitoreo de controles.

Para fines de la norma, el término “control interno” abarca los anteriores cinco componentes. Además el término “controles” se refiere a uno o más de los componentes, o cualquiera de sus aspectos.

Con relación a ambientes de tecnología informática (TI) la norma define los beneficios potenciales de efectividad y eficiencia para el control interno de una entidad porque hace posible que la misma:

- Aplique de manera consistente reglas de negocios predefinidas y realice cálculos complejos al procesar grandes volúmenes de transacciones o datos.
- Mejore la oportunidad, disponibilidad y exactitud de la información.
- Facilite el análisis adicional de información
- Amplíe la capacidad de monitorear el desempeño de las actividades de la entidad y sus políticas y procedimientos.
- Reduzca el riesgo de que se burlen los controles; y
- Aumente la capacidad de lograr una efectiva segregación de funciones al implementar controles de seguridad en aplicaciones, bases de datos y sistemas de operación.

A su vez la tecnología informática presenta riesgos específicos de control interno que incluyen lo siguiente:

- Dependencia de sistemas o programas que procesen los datos de una manera no exacta o que procesen datos no exactos, o ambas cosas.
- Acceso no autorizado a datos que puedan dar como resultado destrucción de datos o cambios no apropiados a los mismos, incluyendo el registro de transacciones no autorizadas o inexistentes, o registro inexacto de transacciones. Pueden surgir riesgos particulares cuando múltiples usuarios tienen acceso a una base común de datos.

- La posibilidad de que personal de TI obtenga privilegios de acceso más allá de los necesarios para desempeñar sus deberes asignados, faltando, por lo tanto, a la segregación apropiada de funciones.
- Cambios no autorizados a datos en los archivos maestros.
- Cambios no autorizados a sistemas o programas.
- Dejar de hacer los cambios necesarios a sistemas o programas.
- Intervención manual inapropiada.
- Potencial pérdida de datos o incapacidad de acceder a los datos según se requiere.

El auditor deberá obtener un entendimiento del sistema de información, incluyendo los procesos de negocios relacionados, relevantes para la información financiera, incluyendo las áreas siguientes:

- Las clases de transacciones en las operaciones de la entidad que sean importantes para la los estados financieros.
- Los procedimientos, tanto en sistemas de tecnología informática como manuales, por los que se inician, registran, procesan e informan dichas transacciones en los estados financieros.
- Los registros contable relacionados, ya sea electrónicos o manuales, que soportan información y cuentas especificas en los estados financieros, respecto de iniciar, registrar, procesar e informar las transacciones.
- Cómo captura el sistema de información los hechos y condiciones, distintos de clases de transacciones, que son importantes para los estados financieros.
- El proceso de información financiera utilizado para preparar los estados financieros de la entidad, incluyendo estimaciones contables y revelaciones importantes.

El auditor deberá obtener un entendimiento suficiente de las actividades de control para evaluar los riesgos de representación errónea de importancia relativa al nivel de aseveración y para diseñar procedimientos adicionales de auditoría que respondan a los riesgos evaluados. Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las directrices de la administración; por ejemplo, que se toman las acciones necesarias para atender los riesgos que amenazan el logro de los objetivos de la entidad. Las actividades de control, sean dentro de sistemas de tecnología informática o manuales, tienen diversos objetivos y se aplican a diversos niveles organizacionales y funcionales. Ejemplos de actividades de control específicas incluyen las relativas a:

- Autorización
- Revisiones de desempeño

- Procesamiento de información.
- Controles físicos
- Segregación de funciones

El auditor deberá obtener un entendimiento de cómo ha respondido la entidad a los riesgos que se originan de la tecnología informática (TI) estableciendo controles generales efectivos de TI y controles de aplicación. Desde la perspectiva del auditor, los controles sobre los sistemas de TI son efectivos cuando mantienen la integridad de la información y la seguridad de los datos que procesan.

Los controles generales de TI son políticas y procedimientos que se relacionan con muchas aplicaciones y soportan el funcionamiento efectivo de los controles de aplicación al colaborar con el aseguramiento de la operación continua apropiada de los sistemas de información. Los controles generales de TI que mantienen la integridad de la información y seguridad de los datos comúnmente incluyen controles sobre lo siguiente:

- Operaciones de centros de datos y redes.
- Adquisición, cambio y mantenimiento de software del sistema.
- Seguridad de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de aplicación.

Los controles de aplicación son procedimientos manuales o automatizados que típicamente operan en el ámbito del proceso del negocio. Los controles de aplicación pueden ser de naturaleza preventiva o detectiva y se diseñan para asegurar la integridad de los registros contables. Consecuentemente, los controles de aplicación se relacionan con procedimientos que se usan para iniciar, registrar, procesar e informar transacciones u otros datos financieros. Estos controles ayudan a asegurar que las transacciones ocurrieron, que están autorizadas y que son registras y procesadas de manera completa y exacta. Los ejemplos incluyen verificaciones de emisión de cheques de datos de entrada, y verificaciones de secuencia numérica de los cheques con seguimiento manual de informes de excepción o corrección en el punto de entrada de los datos.

El auditor deberá identificar y evaluar los riesgos de representación errónea de importancia relativa al nivel de estados financieros y al nivel de aseveración para clases de transacciones, saldos de cuentas y revelaciones. Para este fin el auditor:

- Identifica los riesgos a lo largo del proceso de obtención de entendimiento de la entidad y su entorno, incluyendo los controles relevantes que se relacionan con los riesgos, y al

considerar las clases de transacciones, saldos de cuentas y revelaciones en los estados financieros;

- Relaciona los riesgos identificados con lo que pueda estar mal al nivel de aseveraciones;
- Considera si los riesgos son de una magnitud que pudiera dar como resultado una representación errónea de importancia relativa de los estados financieros; y
- Considera la probabilidad de que los riesgos pudieran dar como resultado representación errónea de importancia relativa de los estados financieros.

En cuanto a la comunicación con los encargados del mando (gobierno corporativo) o con la administración, el auditor deberá informarles, oportuna y apropiadamente, acerca de las debilidades de importancia relativa en el diseño o implementación del control interno que hayan llegado a la atención del auditor.

Si el auditor identifica riesgos de representación errónea de importancia relativa que la entidad no ha controlado, o cuyo control relevante es inadecuado, o si a juicio del auditor hay una debilidad de importancia relativa en el proceso de evaluación del riesgo por la entidad, entonces el auditor incluye estas debilidades del control interno en la comunicación de asuntos de auditoría del interés de la administración.

La documentación mínima requerida para respaldar la evaluación del auditor es:

- La discusión entre el equipo del trabajo respecto de la susceptibilidad de los estados financieros a representación errónea de importancia relativa, debida a error o fraude, y las decisiones importantes que se alcancen;
- Elementos clave del entendimiento que se obtiene respecto de cada una de los aspectos de la entidad y su entorno, incluyendo cada uno de los componentes del control, para evaluar los riesgos de representación errónea de importancia relativa de los estados financieros; las fuentes de información de las que se obtuvo el entendimiento; y los procedimientos de evaluación de riesgo;
- Los riesgos identificados y evaluados de representación errónea de importancia relativa al nivel de estado financiero y al nivel de aseveración; y
- Los riesgos identificados y los controles relacionados evaluados.

3.4 Normas de la Asociación de Auditoría y Control de Sistemas Informáticos (ISACA)

La Asociación de Auditoría y Control de Sistemas de Información, (ISACA, por sus siglas en inglés), fue fundada en 1969 con el objetivo de brindar bases uniformes a los profesionales dedicados a la realizar auditorías de sistemas informáticos. Derivado de este trabajo ha implementado estándares, directrices y procedimientos para el desarrollo del trabajo de Auditoría de Sistemas Informáticos.

- Los Estándares:

  Definen los requerimientos obligatorios para la auditoría y para los informes de auditoría de sistemas informáticos.

- Las Directrices:

  Brindan una guía para aplicar los estándares de auditoría de sistemas informáticos.

- Los Procedimientos:

  Ofrecen ejemplos de procedimientos que debe seguir un auditor de sistemas informáticos en una asignación de auditoría.

Los estándares de ISACA aplicables para la auditoría de sistemas informáticos son:

- Estatuto de Auditoría:

  El propósito, responsabilidad, autoridad de la auditoría de sistemas informáticos deberían estar debidamente documentados en un estatuto de auditoría o en un contrato.

- Independencia profesional:

  En todos los asuntos relacionados con la auditoría, el auditor de sistemas informáticos debería ser independiente del auditado tanto en actitud como en apariencia.

- Independencia organizacional:

  La función de auditoría de sistemas deberá ser independiente del área o actividad que se esté revisando.

- Ética y Estándares Procesionales:

  Estipula la observancia del auditor de sistemas hacia el código de ética profesional de ISACA y el debido cuidado profesional mediante los estándares profesionales aplicables.

- Competencia Profesional:

  Hace énfasis en que el auditor de sistemas debe ser profesionalmente competente, contar con las habilidades y conocimientos suficientes para realizar el trabajo de auditoría asignado y debe mantener esa competencia mediante la educación continuada.

- Planeación:

  El auditor debería planear adecuadamente la auditoría de sistemas de información, tomando en cuenta aspectos como el alcance en base a los objetivos, el cumplimiento de las leyes y estándares profesionales aplicables, tomar en cuenta el enfoque basado en riesgos, desarrollar y documentar el plan de auditoria detallando la naturaleza, los objetivos, el alcance y los recursos requeridos y desarrollar el programa y los procedimientos de auditoría a aplicar.

- Ejecución del Trabajo de Auditoría:

  Estipula la debida supervisión del trabajo de auditoría, las características de la evidencia y la debida documentación de todo el proceso de auditoría.

- Informe:

  Establece que el auditor de sistemas de información debería proveer un informe, en formato apropiado, al terminar la revisión. Además establece los requisitos mínimos que deberían incluirse en el mismo, como la identificación de la organización, los destinatarios, y cualquier restricción sobre su publicación, entre otros.

- Actividades de Seguimiento:

  Establece que el auditor de sistemas de información debería solicitar y evaluar la información relevante para determinar si la dirección ha tomado las acciones apropiadas de acuerdo a sus recomendaciones de manera oportuna.

- Irregularidades y Actos Ilícitos:

  Establece criterios importantes para reducir el riesgo a un nivel mínimo aceptable, mediante la consideración del riesgo de irregularidades y actos ilícitos, y manteniendo una actitud de escepticismo profesional, entre otros.

- Gobierno de TI:

  El auditor de sistemas de información debería revisar y evaluar si la función de sistemas informáticos está alineada con la visión, misión, valores, objetivos y estrategias de la organización.

- Uso de la evaluación de riesgos en la planeación de auditoría:

  Establece que el auditor debería utilizar una técnica apropiada de evaluación de riesgos al desarrollar el plan general de auditoría de sistemas y determinar las prioridades para la asignación efectiva de recursos de auditoría.

- Materialidad de la Auditoría:

  Mientras determina la naturaleza, duración y extensión de los procedimientos de auditoría, el auditor de sistemas debería considerar la materialidad de la auditoría y su relación con el riesgo.

- Uso del trabajo de otros expertos:

  Establece que el auditor de sistemas debería, donde considere apropiado, apoyarse en el trabajo de otros expertos para la realización de la auditoría.

3.5 Metodología de la Auditoría de Sistemas

Puede definirse como “una serie ordenada de acciones, tareas y procedimientos, los cuales serán utilizados conforme a un método minucioso, previamente establecido, a fin de utilizar una serie de herramientas, métodos e instrumentos necesarios en la evaluación del área de sistemas.”(11:185)

A continuación se establecen las fases aplicables de forma general a cualquier tipo de auditoría dentro del campo de los sistemas:

- Planeación:

  Se identifican las razones de la auditoría y se determinan los objetivos de la misma, así como el diseño de los métodos, técnicas y procedimientos necesarios para llevarla a cabo y los documentos que servirán de apoyo para su ejecución.

- Ejecución:

  Es el paso siguiente de la planeación, el cual se determina por las características concretas, los puntos y requerimientos que se estimaron en esa etapa. En esta fase se realizan las acciones programadas para la auditoría, se aplican los instrumentos y herramientas, se identifican y elaboran los documentos de desviaciones, se elabora el dictamen preliminar y se presenta a discusión, y se integra el legajo de papeles de trabajo de la auditoría.

- Informe:

  Se considera el último paso de la metodología de auditoría de sistemas y consiste en emitir un dictamen como resultado final. Los puntos a considerar incluyen la elaboración de un informe de situaciones detectadas, la elaboración del dictamen final y la presentación del informe de auditoría.

CAPÍTULO IV

OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT)

4.1 Antecedentes

El modelo de los Objetivos de Control para Información y Tecnología Relacionada, de aquí en adelante "COBIT", por sus siglas en inglés, es una iniciativa desarrollada por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés) y el Instituto de Gobierno de Tecnología de Información (ITGI, por sus siglas en inglés).

La Asociación de Auditoría y Control de Sistemas de Información (ISACA), fue fundada en 1969 en los Estados Unidos de América y es una organización líder en Gobernabilidad, Control, Aseguramiento y Auditoría de Tecnología de Información, con sede en Chicago, Illinois, Estados Unidos de América, cuenta con más de sesenta mil miembros en más de 100 países. Realiza eventos, conferencias, desarrolla estándares de gobierno de tecnología de información, aseguramiento, auditoría y seguridad.

El Instituto de Gobierno de Tecnología de Información se estableció en 1998 en los Estados Unidos de América, buscando evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. Un gobierno de tecnología de información efectivo, ayuda a garantizar que esa tecnología de información brinde soporte al logro de las metas del negocio, optimice el retorno de la inversión en tecnología de información, y administre de forma adecuada los riesgos y oportunidades asociados a la tecnología de información.

COBIT fue desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad y control en Tecnología de Información, partiendo de la premisa de que los recursos de Tecnología de Información se deben gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos.

A continuación una reseña de la evolución del modelo COBIT:

1992 Comienza la actualización de los objetivos de control de ISACA

1996 ISACA proporciona a los profesionales de tecnologías de información un marco de mejores prácticas de control generalmente aplicables y aceptadas.

1998 Se actualiza y se publica una segunda versión a la que se le incorporan las "Herramientas de implantación" y un CD

2000 Se publica la 3ª Edición

2004 Ante las regulaciones internacionales, ISACA publica COBIT para el cumplimiento con la ley Sarbanes-Oxley de los Estados Unidos de América.

2005 Se publica COBIT 4.0, fortaleciendo el enfoque de Marco de Gobernabilidad de Tecnología de Información.

2007 Se publica COBIT 4.1, incluyendo mejoras en cuadros y guías para la medición del desempeño, los objetivos de control y mejoras en la alineación de objetivos de negocio y de TI.

Esta evolución hasta COBIT 4 responde a las necesidades actuales, con lo cual ha pasado de ser una herramienta para auditoría, a un marco de gobernabilidad de tecnologías de información.

4.2 Resumen Ejecutivo

Es un documento que presenta la metodología de los objetivos de control bajo un enfoque ejecutivo o de alto nivel y busca proveer a la administración un entendimiento de los principios y conceptos claves de COBIT.

Considera que un elemento crítico para el éxito y la supervivencia de las organizaciones es la administración efectiva de la información y de la tecnología de información (TI) relacionada con ella. Debido a que en esta sociedad cada vez más globalizada, la información puede viajar a través del ciberespacio sin las restricciones de tiempo, distancia y velocidad, busca enfatizar este aspecto crítico en base a:

- La creciente dependencia en la información y en los sistemas que proporcionan esa información.
- La creciente vulnerabilidad y un amplio espectro de amenazas sobre la información.
- La escala y el costo de las inversiones actuales y futuras en tecnología de información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Por lo que en la actualidad muchas organizaciones pueden considerar a la información y la tecnología que la soporta, como sus más valiosos activos.

El ámbito empresarial se desarrolla mediante la competitividad y el dinamismo, propiciando que la

gerencia generalmente incremente sus expectativas relacionadas con la entrega de servicios de tecnología de información. Ciertamente, la información y los sistemas de información pueden llegar a ser penetrantes en las organizaciones, desde las plataformas del usuario hasta las redes locales, estructuras cliente servidor y equipos mainframe. Derivado de esto, la administración requiere niveles de servicio que presenten incrementos de calidad, funcionalidad y facilidad de uso, así como un mejoramiento continuo y una disminución de los tiempos de entrega, al tiempo que demanda que esto se realice a un costo más bajo.

Muchas organizaciones reconocen los potenciales beneficios que puede proporcionarle la tecnología de información, sin embargo, si desean ser exitosas, también deben comprender y administrar los riesgos asociados con la implementación de nueva tecnología. Por lo tanto, la administración debe tener una apreciación y un entendimiento básico de los riesgos y limitantes de la utilización de tecnología de información para proporcionarle una dirección efectiva y controles adecuados. COBIT ayuda a salvar la brecha existente entre riesgos de negocio, necesidades de control y aspectos técnicos al proporcionar las mejores prácticas a través de un marco de trabajo de dominios y procesos y presentar un detalle de actividades en una estructura manejable y lógica. Las mejores prácticas de COBIT representan el consenso de los expertos, ayudan a la administración a optimizar la inversión en tecnología de información, pero aún más importante, representan aquello sobre lo que serán evaluados al momento de surgir eventualidades importantes.

Las organizaciones deben cumplir con requerimientos de calidad, regulatorios y de seguridad, tanto para su información, como para sus activos. La administración debe obtener un balance adecuado en el empleo de los siguientes recursos informáticos:

- Personas
- Instalaciones
- Tecnología
- Sistemas de aplicación, y
- Datos.

Para cumplir con esa responsabilidad, así como para alcanzar sus expectativas, la administración debe establecer un sistema adecuado de control interno. Por lo tanto, ese sistema debe existir de modo que brinde soporte a los procesos de negocio y debe ser preciso en la forma en que cada actividad individual de control satisface los requerimientos de información y puede impactar en los recursos de tecnología de información. El impacto en los recursos de tecnología de información se enfatiza en el Marco de Trabajo de COBIT, conjuntamente al logro de los siguientes requisitos indispensables para la información del negocio:

- Efectividad.
- Eficiencia.
- Confidencialidad.
- Integridad.
- Disponibilidad.
- Cumplimiento.
- Confiabilidad.

La Administración por medio del Gobierno Corporativo (Corporate Governance, en inglés), debe asegurar que la debida diligencia (due dilligence, en inglés) sea ejercitada por todos los individuos involucrados en la administración, utilización, diseño, desarrollo, mantenimiento u operación de los sistemas de información.

Un Objetivo de Control de Tecnología de Información es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología de información.

La orientación a negocios es el tema principal de COBIT. Está diseñado no solo para ser utilizado por usuarios y auditores, sino también para ser utilizado como una lista de verificación (check list) detallada para los propietarios de los procesos del negocio. En forma creciente, las prácticas del negocio requieren de una mayor delegación y otorgamiento de autoridad de los dueños de procesos para que estos posean total responsabilidad de todos los aspectos relacionados con dichos procesos de negocio. En forma particular, esto incluye el proporcionar controles adecuados. El Marco de Trabajo de COBIT, proporciona herramientas al propietario del proceso para facilitarle el cumplimiento de esa responsabilidad.

La administración de una empresa requiere de prácticas generalmente aplicables y aceptadas de control y gobierno de tecnología de información para medir comparativamente, tanto su ambiente de tecnología de información existente, como su ambiente planeado. COBIT habilita el desarrollo de una política clara y de mejores prácticas de control de tecnología de información a través de organizaciones a nivel mundial. El objetivo de COBIT es proporcionar estos objetivos de control, dentro de un marco de trabajo definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales del mundo.

Por lo tanto, COBIT está orientado a ser la herramienta de Gobierno de Tecnología de Información que ayude al entendimiento y la administración de riesgos asociados a la tecnología de información y tecnologías relacionadas.

4.3 Marco de Trabajo

4.3.1 Razones para utilizarlo

El Marco de Trabajo para el Control y Gobierno de Tecnología de Información, responde a la percepción de la alta dirección de las empresas acerca del creciente impacto de la información sobre el éxito o fracaso de una empresa. Por lo tanto la dirección espera comprender mejor la forma en que la tecnología de información es operada y la posibilidad de que sea aprovechada con éxito para lograr una ventaja competitiva.

La alta dirección necesita saber si con la información administrada en la empresa, es posible que:

- Se garantice el logro de sus objetivos,
- Se tenga la suficiente flexibilidad para aprender y adaptarse,
- Se cuente con un manejo juicioso de los riesgos que enfrenta la información, y
- Se reconozcan de forma apropiada las oportunidades y se actúe de acuerdo a ellas.

Además la alta dirección necesita comprender los riesgos y beneficios de la tecnología de información, ya que el éxito de las empresas depende de encontrar las maneras de:

- Sincronizar las estrategias de tecnología informática con las estrategias del negocio,
- Lograr que toda la estrategia de tecnología informática, así como las metas planteadas, fluyan gradualmente hacia toda la empresa,
- Proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas,
- Crear relaciones constructivas y comunicaciones efectivas entre la tecnología informática y el negocio, además de los interesados externos, y
- Medir el desempeño de la tecnología informática.

Por otro lado, para que las empresas puedan responder de forma efectiva a los anteriores requerimientos de negocio y gobierno, deben adoptar e implementar un marco de referencia de gobierno y control de tecnologías de información, de tal manera que:

- Se forme un vínculo con los requerimientos del negocio,
- El desempeño real frente a los requerimientos sea transparente,
- Se organicen sus actividades en un modelo de procesos de aceptación general,
- Se identifiquen los principales recursos a ser aprovechados, y
- Se definan los objetivos de control gerenciales a ser considerados.

4.3.2 Beneficios a Usuarios

Debido a que cada uno de los posibles interesados tiene necesidades específicas de información, a continuación se mencionan los tipos de personal que pueden apoyarse en un marco de trabajo de control sobre tecnología de información:

- Interesados dentro de la empresa que busquen generar valor de las inversiones en tecnología informática:
    - Aquellos que tomen decisiones de inversiones.
    - Aquellos que deciden respecto a los requerimientos.
    - Aquellos que utilicen los servicios de tecnología informática.
- Interesados internos y externos que presten servicios de tecnología informática:
    - Aquellos que administren la organización y los procesos de tecnología informática.
    - Aquellos que desarrollen soluciones.
    - Aquellos que operen los servicios.
- Interesados internos y externos con responsabilidades de control y riesgo:
    - Aquellos con responsabilidades de seguridad, privacidad y/o riesgo.
    - Aquellos que realicen funciones de cumplimiento.
    - Aquellos que requieran o proporcionen servicios de aseguramiento.

En resumen, COBIT está diseñado para ser utilizado por tres audiencias distintas:

- Administración:

  Para ayudarlos a lograr un balance entre los riesgos y las inversiones en control en un ambiente de tecnología de información.

- Usuarios:

  Para obtener una garantía en cuanto a la seguridad y controles de los servicios de información proporcionados internamente o por terceras personas.

- Auditores:

  Para dar soporte a las opiniones mostradas a la administración sobre los controles internos en tecnología informática.

4.3.3 Nivel de Cobertura

Los requerimientos mencionados anteriormente conllevan a un marco de trabajo de gobierno y control de tecnología de información que satisfaga las siguientes especificaciones generales:

- Brindar un enfoque de negocios que permita la alineación entre los objetivos de negocio y los objetivos de tecnología informática.

- Estar orientado a procesos para definir el alcance y el grado de cobertura, con una estructura definida que permita una fácil navegación en el contenido.

- Ser de aceptación general a nivel internacional al ser consistente con las mejores prácticas y estándares de tecnología informática mundiales, además debe ser independiente de tecnologías específicas.

- Proporcionar un lenguaje común, con un conjunto de términos y definiciones que sean comprensibles para todos los interesados.

- Ayudar a satisfacer requerimientos legales y regulatorios, al ser consistente con estándares de gobierno corporativo generalmente aceptados y con controles de tecnología informática esperados por agentes reguladores y auditores externos.

El Marco de Trabajo de COBIT puede satisfacer estas necesidades por ser orientado al negocio, orientado a procesos, basado en controles e impulsado por mediciones.

4.3.4 Orientado al Negocio

La característica principal de COBIT es que está orientado a apoyar los requerimientos de información del negocio. Está diseñado para ser utilizado por proveedores de servicio, usuarios y auditores de tecnología informática, pero principalmente busca servir de guía integral para la gerencia y los propietarios de los procesos del negocio, ya que pueden utilizarlo para autoevaluar su inversión o la eficacia de sus procesos.

El principio general en que se basa COBIT es el siguiente:
(Para) “proporcionar la información que la empresa requiere para el logro de sus objetivos, la empresa necesita administrar y controlar sus recursos de tecnología informática usando un conjunto estructurado de procesos que ofrezcan los servicios requeridos de información.” (1:13)

Es por eso que el marco de trabajo de COBIT al estar implementado correctamente, ofrece herramientas que garantizan la alineación de la tecnología informática con los requerimientos de información del negocio, hasta un grado de certidumbre suficiente que asegure el cumplimiento de las metas del negocio.

COBIT define siete criterios de información basados en los requerimientos generales de calidad, regulación y seguridad, como lo son:

- Efectividad: Implica que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consistente y utilizable.

- Eficiencia: Consiste en que la información sea generada optimizando los recursos para lograr mayor productividad y economía.

- Confidencialidad: Se refiere a la protección de la información sensitiva contra revelaciones no autorizadas.

- Integridad: Está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a valores y expectativas del negocio.

- Disponibilidad. Se refiere a que la información esté disponible en el momento en que sea requerida por los procesos del negocio. También concierne a la capacidad necesaria para la protección de los recursos.

- Cumplimiento: Se refiere al acatamiento de aquellas leyes, reglamentos y acuerdos contractuales a los que está sujeto el proceso de negocio, en otras palabras, criterios de negocio impuestos externamente, así como políticas internas.

- Confiabilidad: Significa proporcionar la información apropiada para que la gerencia administre la entidad y ejercite sus responsabilidades regulatorias y administrativas.

Definir un conjunto de metas generales de negocio y de tecnología informática ofrece una base más depurada y relacionada con el negocio para el establecimiento de sus requerimientos y para el desarrollo de unidades cuantificables denominadas métricas, que permitan la medición con respecto a las metas establecidas.

4.3.5 Orientado a procesos

Las actividades de tecnología de información están definidas en COBIT dentro de un modelo genérico de procesos dividido en cuatro dominios: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte, y Monitorear y Evaluar. Estos dominios se pueden comparar con las áreas tradicionales de tecnología de información de planear, construir, ejecutar y monitorear.

Para gobernar efectivamente la tecnología informática, COBIT define cuatro dominios que requieren ser administrados, resumidos de la siguiente manera:

- Planear y Organizar:

  Cubre las estrategias y las tácticas de la empresa en materia de tecnología informática, relacionadas con la identificación de las distintas formas en que esa tecnología puede contribuir de la mejor manera al logro de los objetivos del negocio.

- Adquirir e Implementar:

  Cubre la identificación, desarrollo y adquisición, así como la implementación e integración de las soluciones de tecnología informática en los procesos del negocio, que son necesarias para llevar a cabo la estrategia de tecnología establecida en los procesos incluidos en el dominio anterior. Además, cubre el cambio y el mantenimiento de los sistemas existentes para garantizar que continúen satisfaciendo los objetivos del negocio.

- Entregar y Dar Soporte:

  Cubre la propia entrega de los servicios de tecnología informática requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte a los usuarios, la administración de los datos y de las instalaciones operacionales.

- Monitorear y Evaluar:

  Debido a que los procesos de tecnología informática deben evaluarse regularmente en cuanto al cumplimiento de los requerimientos de control y respecto a su calidad, en este dominio se cubren aspectos relacionados con la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno de TI.

4.3.6 Basado en controles

Para una mejor comprensión primero se hace necesario definir lo que se debe entender como control según COBIT: “Control se define como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable que los objetivos de negocio se alcanzarán, y los eventos no deseados serán prevenidos o detectados y corregidos” (1:16)

Además lo que COBIT establece como objetivo de control de tecnología informática queda definido de la siguiente manera: “Un objetivo de control de TI es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular. Los objetivos de control de COBIT son los requerimientos mínimos para un control efectivo de cada proceso de IT.” (1:16)

De acuerdo a lo anterior para que una entidad obtenga una seguridad razonable de que sus objetivos de negocio se alcanzarán, es necesario que la administración defina políticas, prácticas, procedimientos y una estructura organizacional que se traduzca en controles, pero también se hace

necesario que al establecer controles en los procesos de tecnología informática, estos cumplan con los requerimientos mínimos que establece COBIT para considerarse efectivos.

En COBIT cada uno de los procesos de tecnología de información cuenta con un objetivo de control de alto nivel (principal) y un determinado número de objetivos de control detallados, que en conjunto representan las características de un proceso de tecnología de información bien administrado.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio más un número que identifica el proceso, un punto, para luego agregar un número que identifica al objetivo de control dentro de ese proceso, a continuación un ejemplo:

Dominio AI: Adquirir e Implementar
Proceso AI1: Identificar soluciones automatizadas
Objetivo de control AI1.2: Reporte de análisis de riesgo
Identificación de COBIT: **AI1.2**

Para obtener una visión completa de los requerimientos de control, COBIT define para cada proceso los siguientes controles generales, los cuales deben manejarse como un todo conjuntamente con los objetivos de control:

- Dueño del proceso:

  Para que la responsabilidad sea clara, se debe asignar un dueño para cada proceso.

- Reiterativo:

  Cada proceso debe definirse de tal forma que sea repetitivo.

- Metas y objetivos:

  Para una ejecución efectiva, deben establecerse metas y objetivos claros para cada proceso.

- Roles y responsabilidades:

  Para una ejecución eficiente, se deben definir roles, actividades y responsabilidades claras en cada proceso.

- Desempeño del proceso:

  La medición del desempeño de cada proceso se realiza comparándolo con sus metas.

- Políticas, planes y procedimientos:

  Cualquier política, plan o procedimiento impulsado por un proceso COBIT, Debe ser documentado, revisado, actualizado, formalizado y comunicado adecuadamente a todas las partes involucradas.

"Los controles efectivos reducen el riesgo, aumentan la probabilidad de la entrega de valor y aumentan la eficiencia debido a que habrá menos errores y un enfoque administrativo más consistente" (1:17)

Para un mejor entendimiento de como los controles del negocio se relacionan con los controles de tecnología informática, se describe a continuación la forma en que el sistema empresarial de controles internos impacta a la tecnología informática en tres niveles:

- Controles de alto nivel (Empresa): Basados en políticas generales de negocio que deben aplicarse sobre el ambiente de TI, por ejemplo, estilo de operación, información compartida, etc.

- Controles Generales de TI: Relacionados con la función general de TI, por ejemplo: administración de cambios, acceso a programas y datos, etc.

- Controles de Aplicación: Integrados en las aplicaciones que soportan los procesos de negocio, por ejemplo, completitud, validez, autorización, segregación de funciones, etc.

Los controles de tecnología de información se pueden clasificar de la siguiente manera:

- Controles Generales:

  Se pueden definir como los que están inmersos en los procesos y servicios de tecnología informática. Por ejemplo:

  - Controles en el desarrollo de sistemas
  - Controles en la administración de cambios

- Controles de seguridad informática
- Controles en la operación del computador

- Controles de Aplicación:

  Son los que están incluidos en las aplicaciones (programas) del proceso de negocio. Por ejemplo:

  - Integridad
  - Precisión
  - Validez
  - Autorización
  - Segregación de funciones

Los procesos de tecnología informática de COBIT abarcan los controles generales de TI, pero no los controles de las aplicaciones, porque ellos son responsabilidad del propietario del proceso de negocio y deberían estar integrados en los procesos de negocio.

4.3.7 Impulsado por mediciones

Las empresas necesitan medir su posición con respecto al estado de sus propios sistemas informáticos, para saber dónde se requieren mejoras, implementarlas y luego diseñar una serie de herramientas gerenciales que les permitan monitorear esas mejoras, buscando siempre justificar el alcance mediante un equilibrio entre el beneficio y el costo.

COBIT impulsa estas mediciones por medio de:

- Modelo de madurez
- Metas y mediciones de desempeño para los procesos de TI
- Metas de actividades

Modelo de Madurez

El modelado de madurez para la administración y el control de los procesos de tecnología de información se basa en un método de evaluación de la organización, mediante el cual se puede evaluar a sí misma desde un nivel de no-existente (0) hasta un nivel óptimo (5). Este enfoque se basa en el modelo de madurez diseñado por el Instituto de Ingeniería de Software (Software

Engineering Institute, en inglés), instituto federal estadounidense de investigación y desarrollo fundado por el Congreso de los Estados Unidos en 1984, por medio del cual se define la madurez de la capacidad del desarrollo de software.

Los niveles de madurez están diseñados como perfiles de control de los procesos de tecnología de información que una empresa debería reconocer como descripciones de estados posibles actuales y futuros.

Al utilizar los modelos de madurez para cada uno de los 34 procesos de tecnología de información de COBIT, la administración podrá identificar:

- El desempeño real de la empresa (Situación actual)
- El estatus actual de la industria (Comparación externa o benchmarking)
- El objetivo de mejora de la empresa (Proyección a futuro)

Debido a que COBIT es un marco de referencia para la administración de procesos de tecnología informática que se enfoca fuertemente en el control, se recomienda que las escalas del modelo de madurez sean prácticas en su aplicación y razonablemente fáciles de comprender. En algunos casos, el tema de procesos de tecnología de información puede hacerse complejo y subjetivo, por lo que se puede facilitar su análisis mediante evaluaciones sencillas que aumenten el conocimiento, que logren un consenso amplio y que motiven su mejora. Estas evaluaciones pueden realizarse contra las descripciones del modelo de madurez como un todo o abarcando cada una de las afirmaciones individuales de las descripciones. De cualquier forma, es recomendable contar con experiencia en los procesos de la empresa revisada.

Para cada uno de los 34 procesos de COBIT se define un modelo de madurez con una escala de medición de 0 a 5, basado en el siguiente modelo general:

“0 No existente:

Carencia de cualquier control reconocible. La empresa no reconoce siquiera que existe un problema a resolver.

1 Inicial:

Existe evidencia de que la empresa ha reconocido que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques ad hoc que

tienden a ser aplicados en forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

2 Repetible:

Se han desarrollado los procesos hasta el punto que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento y comunicación formal de los procedimientos estándar, y se deja a la responsabilidad del individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

3 Definido:

Los procedimientos se han estandarizado y documentado, y se han difundido a través del entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.

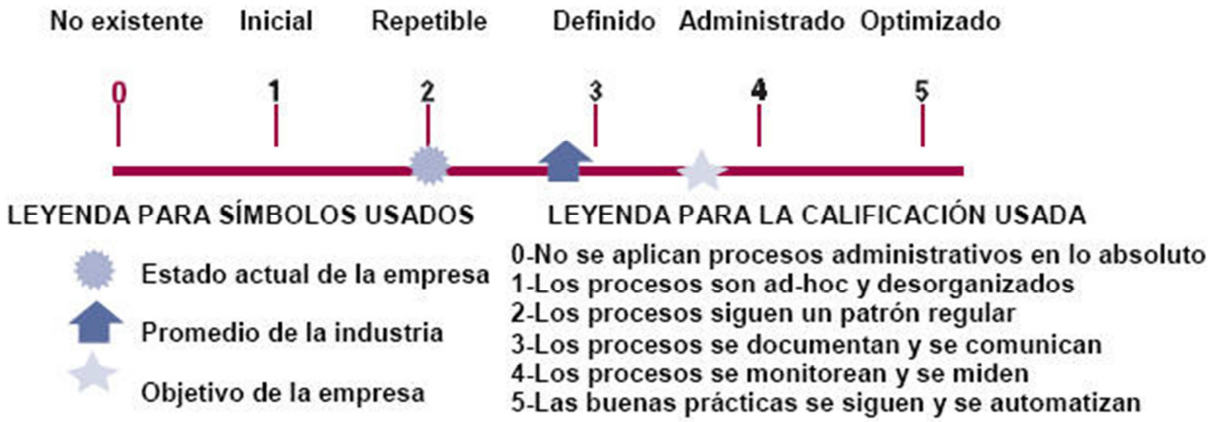
4 Administrado:

Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se usa la automatización y herramientas de una manera limitada y fragmentada.

5 Optimizado:

Los procesos se han refinado hasta un nivel de mejora práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas. TI se usa de forma integrada para automatizar el trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la empresa se adapte de manera rápida.” (1:20)

Los modelos de madurez miden la capacidad de administrar controles en los procesos de tecnología informática y su ventaja radica en que por medio de ellos se le hace relativamente fácil a la administración ubicarse en la escala de medición y evaluar que debe hacerse para desarrollar una mejora.



Fuente: Cobit 4.0

La grafica anterior muestra las escalas del modelo de madurez, las cuales permiten que los profesionales de la auditoría puedan explicar a la administración dónde se encuentran los defectos en la administración de controles en los procesos de tecnología informática y puedan establecer objetivos de control donde sean requeridos. Específicamente, el nivel de madurez en la administración se basará en el grado de dependencia de la empresa en la tecnología informática, en lo sofisticado de su tecnológica y, más importante, en el valor de su información.

Es por esto que se considera al modelado de madurez como el que posibilita que los procesos que establece COBIT sean auditables.

Para que un ambiente de control pueda considerarse como implantado de forma adecuada, es necesario que el negocio logre alcanzar los tres aspectos de la madurez, estos son capacidad, desempeño y control. La primera se refiere a la capacidad de administrar los procesos y desempeño es la forma en que se usa o se implanta esa capacidad.

Un incremento de la madurez reduce el riesgo y mejora la eficiencia, reduciendo los errores, logrando más procesos predecibles y rentabilizando el uso de los recursos.

Método de determinación del nivel de madurez

“El modelado de madurez para la administración y control sobre los procesos de tecnología informática está basado en un método de evaluar donde se encuentra la organización, por medio de la asignación de un valor nominal de madurez a cada proceso, iniciando en no existente (0) hasta optimizado (5).

Los resultados del modelo de madurez son obtenidos en base a COBIT 4.0, el cual contiene declaraciones concernientes al desempeño de la tecnología informática en áreas específicas de los procesos de COBIT. El auditado deberá analizar y manifestar su nivel de conformidad con cada declaración dentro de cuatro posibles repuestas que a su vez representan valores:

- Nada = 0
- Un poco = 0.33
- Bastante = 0.66
- Totalmente = 1.00

Para obtener valores sobre cada una de las respuestas a las declaraciones de COBIT, se necesita multiplicar “Peso” y “Respuesta”, a través de la siguiente formula:

$$V = P \times R$$

Donde V es el valor de puntuación de la declaración de madurez, P es el peso de cada declaración de madurez, y R es el valor de la respuesta de cada declaración.

Para obtener la puntuación del nivel de madurez, lo primero que el auditor necesita es calcular el Cumplimiento para cada nivel de madurez, el cual se obtiene al sumar los valores de cada nivel y luego dividirlos dentro del peso total para cada nivel.

$$C = \sum V / \sum P$$

Donde C es cumplimiento, V es el valor de las respuestas para cada declaración de madurez, y P es el peso de cada declaración.

El siguiente paso es la Normalización, la cual se puede obtener mediante dividir el valor de Cumplimiento de cada nivel dentro del valor de Cumplimiento de todos los niveles de cada proceso de TI.

$$N = C / \sum C$$

Donde N es el valor normalizado y C el valor de cumplimiento de cada nivel.

La contribución se determina mediante la multiplicación del Nivel (0 a 5) por el valor normalizado de cada nivel. Con la contribución total para todos los niveles de un proceso de tecnología informática, el auditor obtendrá la puntuación del nivel de madurez de la empresa.

$$Co = Nv \times N$$

Donde Co es la contribución, Nv es el nivel de madurez y N es el valor normalizado de las respuestas a las declaraciones.

El nivel de madurez se obtiene sumando los valores de contribución del proceso de tecnología informática evaluado.

$$NM = \sum Co$$

Donde NM es el nivel de madurez y Co es la contribución para cada declaración del nivel de madurez."(18:1)

Medición del Desempeño

COBIT define metas y métricas, agrupadas en los siguientes tres niveles:

1. Metas y métricas de TI:

   Definen lo que el negocio espera de la tecnología informática (TI). Lo que el negocio utiliza para medir a TI.

2. Metas y métricas de Proceso:

   Definen lo que el proceso de tecnología informática debe generar para dar soporte a los objetivos de tecnología informática (TI). Lo que se utiliza para medir al propietario del proceso de TI.

3. Métricas de desempeño de los procesos:

   Definen el nivel de desempeño del proceso que indique si es posible alcanzar las metas.

Un ejemplo para ilustrar lo anterior, es tomar una meta de negocio como “Mantener la reputación y liderazgo de la empresa”, donde para cumplir con ese objetivo de negocio la tecnología informática debe alinearse y también tener metas y sus correspondientes mediciones que deberán ser “Garantizar que los servicios de tecnología informática puedan resistir y recuperarse de ataques externos”, lo cual podrá alcanzarse si a nivel de procesos se logra “Detectar y resolver accesos no autorizados a la información, aplicaciones e infraestructura”, que incluye realizar la actividad de “Entender requerimientos de seguridad, vulnerabilidades y amenazas”.

COBIT utiliza dos tipos de métricas o mediciones: Indicadores de metas e indicadores de desempeño. Los indicadores de metas de bajo nivel pasan a ser indicadores de desempeño para los niveles más altos.

Los indicadores de metas (KGI, key goal indicator en inglés) definen mediciones que informan a la administración si un proceso alcanzó sus requerimientos de negocio, y por lo regular se expresan en términos de criterios de información, como los siguientes:

- Disponibilidad de información necesaria para dar soporte a las necesidades del negocio.
- Ausencia de riesgos de integridad y de confiabilidad.
- Rentabilidad de procesos y operaciones.
- Confirmación de confiabilidad, efectividad y cumplimiento.

Los indicadores clave de desempeño (KPI, key performance indicator en inglés) son mediciones que definen el nivel de desempeño del proceso de tecnología informática para alcanzar una determinada meta. Son los indicadores principales para saber si es factible alcanzar la meta, y con buenos indicadores de las capacidades, prácticas y habilidades. Miden las metas de las actividades, las cuales son acciones que el propietario del proceso debe seguir para lograr un efectivo desempeño del proceso.

Las siguientes son las características sugeridas para lograr métricas efectivas:

- Un elevado balance entre entendimiento-esfuerzo. (entendimiento del desempeño y del logro de metas en contraste con el esfuerzo de lograrlos)
- Deben ser comparables internamente. (un porcentaje relativo a una base establecida o números en el tiempo)
- Deben ser comparables externamente.
- Es mejor tener pocas métricas pero bien definidas, que una larga lista de menor calidad.

- Deben ser fáciles de medir y no se deben confundir con las metas.

El marco de trabajo de COBIT relaciona los requerimientos de información y de gobierno del negocio con los objetivos de la función de servicios de tecnología informática. Su modelo de procesos permite administrar y controlar las actividades de tecnología informática y los recursos que la soportan, en base a los objetivos de control de COBIT, y los alinea y monitorea por medio de los indicadores de metas (KGI) y los indicadores de desempeño (KPI) de COBIT.

En resumen, los recursos de tecnología informática son manejados por procesos de tecnología informática para lograr las metas de tecnología informática que respondan a los requerimientos de información y administración del negocio. Lo cual puede definirse como el principio básico del modelo de control de COBIT.

4.4 Directrices de Auditoría

Las Directrices de Auditoría ofrecen una herramienta complementaria para aplicar fácilmente el Marco Referencial y los Objetivos de Control COBIT dentro de las actividades de auditoría y evaluación. El propósito de las Directrices de Auditoría es contar con una estructura sencilla para auditar y evaluar controles, con base en prácticas de auditoría generalmente aceptadas y compatibles con el esquema global COBIT.

La segunda edición de estas directrices y única traducida al español, fue emitida en el año 1998 por el Comité Directivo de COBIT en conjunto con la que en ese tiempo se denominaba Fundación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Foundation), que actualmente se conoce como Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés). Estas directrices de auditoría se mantuvieron vigentes hasta el año 2007 en que pasaron a ser Guías de Aseguramiento de Tecnología de Información utilizando COBIT (IT Assurance Guide Using Cobit), del cual no existe traducción al español, por lo que en el presente trabajo solo se mencionan.

Debido a que los objetivos y prácticas individuales de auditoría varían considerablemente entre las empresas y que existen distintas prácticas entre los profesionales dedicados a actividades relacionadas con la auditoría de sistemas, las Directrices de Auditoría se desarrollan bajo una estructura genérica al estar de acuerdo a criterios de aceptación general a nivel internacional y de alto nivel por el detalle en que son desarrollados.

Los auditores deben cumplir con algunos requerimientos generales para proporcionar a los directivos y a los poseedores de los procesos de negocios, seguridad y asesoría respecto a los controles en una organización a fin de: ofrecer una seguridad razonable de que se está cumpliendo con los objetivos de control correspondientes; identificar dónde se encuentran las debilidades significativas en dichos controles; justificar los riesgos que pueden estar asociados con tales debilidades, y finalmente aconsejar a estos ejecutivos sobre las medidas correctivas que deben adoptarse. COBIT ofrece políticas claras y prácticas eficaces en materia de seguridad y control de información, así como tecnología asociada.

Estas Directrices de Auditoría proporcionan orientación para preparar planes de auditoría que se integran al Marco COBIT y a los Objetivos de Control detallados. Deben ser usados conjuntamente con estos dos últimos, y a partir de ahí pueden desarrollarse programas específicos de auditoría, aunque no son exhaustivas ni definitivas para la aplicación de auditorías de sistemas o evaluaciones de controles donde se necesite realizar ajustes según las condiciones específicas de cada evaluación.

“No obstante lo anterior, se necesita aclarar que hay cuatro cosas que las Directrices de Auditoría COBIT no son:

- Las Directrices de Auditoría no pretenden ser una herramienta para crear el plan y cobertura general de auditoría que considera una amplia gama de factores, incluyendo debilidades anteriores, riesgo a la organización, incidentes conocidos, nuevos acontecimientos, y selección de estrategias.

  Aun cuando el Marco y los Objetivos de Control ofrecen algunas orientaciones, los alcances de las Directrices no incluyen una guía precisa para actividades específicas.

- Las Directrices de Auditoría no están diseñadas como instrumento para enseñar las bases de la auditoría, aun cuando incorporen los elementos normalmente aceptados de la auditoría general y de TI.

- Las Directrices de Auditoría no pretenden explicar en detalle la forma en que pueden utilizarse las herramientas computarizadas para apoyar y automatizar los procesos de auditoría de TI, en materia de planeación, evaluación, análisis y documentación (que incluyen las Técnicas de Auditoría Asistidas por Computadora, pero no se limitan a ellas).

Existe un enorme potencial para usar la tecnología de información dirigida a aumentar la eficiencia y efectividad de las auditorías, pero una orientación en este sentido, tampoco está dentro de los alcances de las Directrices.

- Las Directrices de Auditoría no son exhaustivas ni definitivas, pero se desarrollarán conjuntamente con COBIT y sus Objetivos de Control detallados.” (2:23)

“Las Directrices de Auditoría COBIT permiten al auditor cotejar los procesos específicos de TI con los Objetivos de Control COBIT recomendados, de forma que puedan:

- Asesorar a los directivos identificando en qué casos los controles son suficientes, o
- Asesorarlos respecto a los procesos que requieren ser mejorados.”(2:23)

CAPÍTULO V

CASO PRÁCTICO DE EVALUACIÓN DE CONTROLES PARA LA ADQUISICIÓN E IMPLEMENTACIÓN DE SOLUCIONES INFORMÁTICAS POR PARTE DEL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA DISTRIBUIDORA DE VEHÍCULOS AUTOMOTORES SEGÚN EL MODELO COBIT DE CONTROL INTERNO INFORMÁTICO

Con el objetivo de dar a conocer la forma de evaluar la capacidad de administrar los controles informáticos en la adquisición e implementación de software según los objetivos de control para información y tecnología relacionada (COBIT, por sus siglas en inglés), mediante las escalas de madurez que este modelo define para cada proceso, se presentan a continuación los aspectos fundamentales que debe considerar el auditor de sistemas:

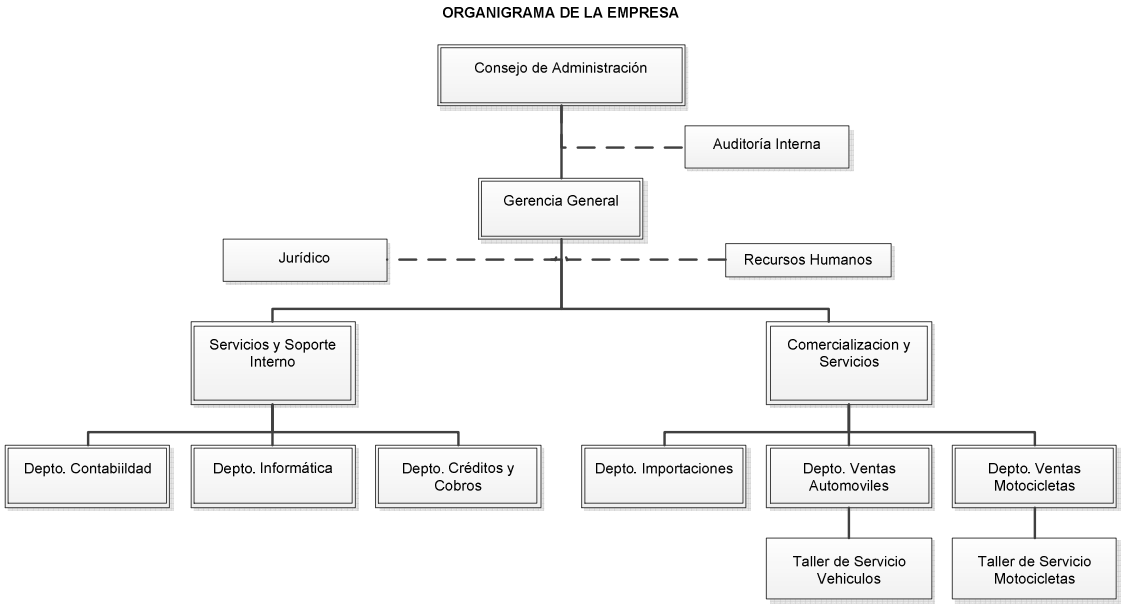
5.1 Antecedentes del caso práctico

La evaluación se realizó en la empresa Ruedas Mágicas, S.A. que inició sus operaciones en el año 1970 dedicándose a la importación, distribución y venta de vehículos automotores especializándose en automóviles y motocicletas, repuestos y accesorios; su actividad abarca todo el territorio de Guatemala con sede central en la zona 1 de la Ciudad de Guatemala y cuenta con una sucursal en el Boulevard Revolución, además de un taller de servicio para vehículos y otro para motocicletas.

La empresa se encuentra organizada de la siguiente manera:

- Consejo de Administración
- Gerencia General
- Departamento de Contabilidad
- Departamento de Auditoría Interna
- Departamento de Informática
- Departamento de Créditos y Cobros
- Departamento de Recursos Humanos
- Departamento Jurídico
- Departamento de Importaciones
- Departamento de Ventas de Automóviles, repuestos y accesorios
- Departamento de Ventas de Motocicletas, repuestos y accesorios
- Taller Automotriz
- Taller de Motocicletas

A continuación se presenta una gráfica de la estructura organizacional de la empresa evaluada:



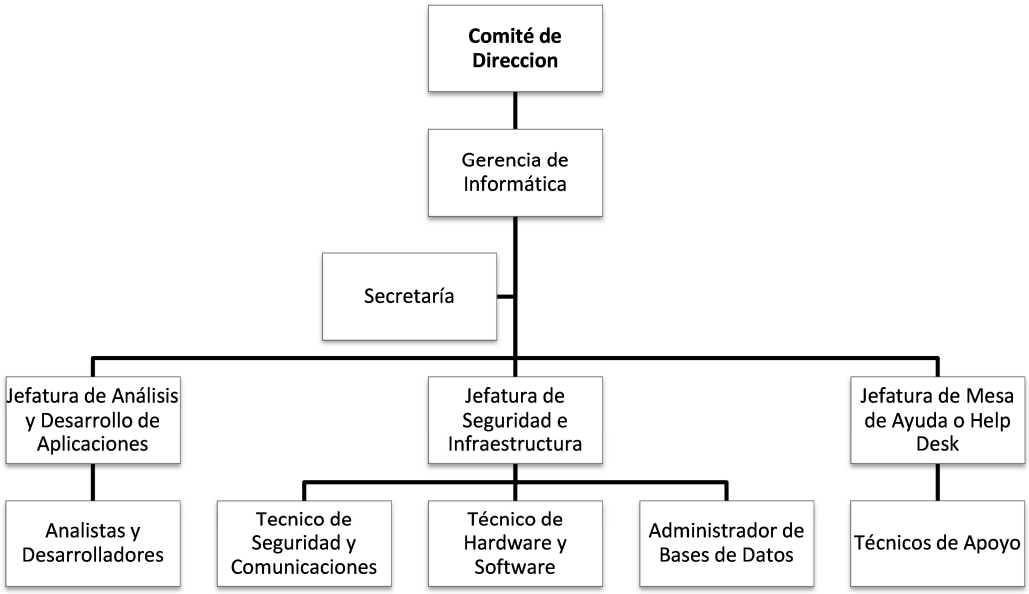
Fuente: Empresa evaluada.

La organización del departamento de informática presenta la siguiente estructura:

- Comité de Dirección
- Gerencia del Departamento
- Gerencia de Análisis y Desarrollo
- Analistas y desarrolladores de software
- Gerencia de Seguridad e Infraestructura
- Jefatura de Mesa de Ayuda
- Técnicos de soporte interno
- Secretaria del departamento

A continuación se presenta una gráfica de esta estructura organizacional:

ORGANIGRAMA DEL DEPARTAMENTO DE INFORMÁTICA



Fuente: Departamento de informática de empresa evaluada.

5.2 Desarrollo del Caso Práctico

La empresa Ruedas Mágicas, S.A. ha experimentado un notable crecimiento económico y de operaciones durante los últimos cinco años, por lo que actualmente se encuentra en un proceso de evaluación de soluciones informáticas que le permitan gestionar su crecimiento de forma transparente para los usuarios internos y externos de su información.

La administración de la empresa ha solicitado la opinión del departamento de Auditoría Interna sobre el nivel de control aplicado por el departamento de informática de la empresa en los procesos de adquisición, implementación y mantenimiento de tecnología informática, con el objetivo de conocer de forma objetiva la forma en que las inversiones en tecnología son gestionadas por ese departamento.

Para dar soporte a la opinión de los auditores internos sobre los controles informáticos, el trabajo de auditoría deberá basarse en los Objetivos de Control para Información y Tecnología Relacionada (COBIT) por ser considerados como las mejores prácticas de control y gobierno de tecnología de información a nivel mundial. Los Objetivos de Control para Información y Tecnología Relacionada, de aquí adelante COBIT, permiten evaluar los controles desde tres perspectivas diferentes como lo son los recursos de tecnología informática, los criterios de información y los procesos de tecnología informática.

De los anteriores tres enfoques, la gerencia de auditoría interna ha decido realizar la evaluación desde el punto de vista de los procesos de tecnología informática, tomando como base los criterios de evaluación establecidos en uno de los cuatro dominios que conforman la metodología COBIT, denominado “Adquisición e Implementación de Soluciones Informáticas (AI)”.

5.2.1 Contenido del Caso Práctico

Descripción	PT No.
Fase de Planeación	
Carta de notificación para la iniciación de la Auditoría	MM01
Nombramiento del auditor que realizará la auditoría	MM02
Programa de Auditoría para realizar la evaluación de controles de acuerdo al modelo de madurez de COBIT	MM03
Fase de Ejecución	
Evaluación del proceso de Identificar Soluciones Automatizadas (AI1)	MM04
Cuestionarios a Función: Gerencia de Departamento	MM04-01
Cuestionarios a Función: Gerencia de Seguridad	MM04-02
Evaluación del proceso de Adquirir e implementar Software Aplicativo (AI2)	MM05
Cuestionarios a Función: Gerencia de Departamento	MM05-01
Cuestionarios a Función: Gerencia de Seguridad	MM05-02
Evaluación del proceso de Adquirir e implementar Infraestructura tecnológica (AI3)	MM06
Cuestionarios a Función: Gerencia de Departamento	MM06-01
Cuestionarios a Función: Gerencia de Seguridad	MM06-02
Evaluación del proceso de Facilitar la operación y el uso (AI4)	MM07
Cuestionarios a Función: Gerencia de Departamento	MM07-01
Cuestionarios a Función: Gerencia de Desarrollo	MM07-02
Evaluación del proceso de Adquirir recursos de tecnología Informática (AI5)	MM08
Cuestionarios a Función: Gerencia de Departamento	MM08-01
Cuestionarios a Función: Gerencia de Seguridad	MM08-02
Cuestionarios a Función: Gerencia de Desarrollo	MM08-03
Evaluación del proceso de Administrar Cambios (AI6)	MM09
Cuestionarios a Función: Gerencia de Departamento	MM09-01
Cuestionarios a Función: Gerencia de Seguridad	MM09-02
Cuestionarios a Función: Gerencia de Desarrollo	MM09-03
Evaluación del proceso de Instalar y acreditar soluciones y cambios (AI7)	MM10
Cuestionarios a Función: Gerencia de Departamento	MM10-01
Cuestionarios a Función: Gerencia de Seguridad	MM10-02
Cuestionarios a Función: Gerencia de Desarrollo	MM10-03
Resumen de niveles de madurez	MM11
Fase de Informe	
Informe de Auditoría	

Papel de Trabajo	MM01
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	15-01-2009
FECHA FIN:	16-01-2009

5.2.2 Papeles de trabajo del caso práctico

Ruedas mágicas, S.A.

Auditoría Interna

CARTA DE NOTIFICACIÓN DE LA REALIZACIÓN DE LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO EN LA ADQUISICIÓN E IMPLEMENTACIÓN DE SOLUCIONES INFORMÁTICAS EN EL DEPARTAMENTO DE INFORMÁTICA

Sr. Rodrigo Juárez
Gerente del Departamento de Informática
Presente

Respetable Sr. Juárez

Por este medio se le comunica que conforme nuestro plan de trabajo, se iniciará la revisión del control interno sobre los procesos de adquisición e implementación de soluciones informáticas que realiza la unidad a su cargo. La actividad ha sido asignada al Sr. Estuardo Díaz, asistente de auditoría interna y supervisada por su servidor.

Al final de la evaluación se le estarán enviando los resultados detallando los hallazgos y recomendaciones.

Se le agradece su colaboración.
Atentamente,

Lic. Luis Dionicio
Auditor Interno
C.C. Archivo

Papel de Trabajo	MM02
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	15-01-2009
FECHA FIN:	16-01-2009

Ruedas mágicas, S.A.

Auditoría Interna

NOMBRAMIENTO PARA REALIZAR LA EVALUACIÓN DEL CONTROL INTERNO EN LOS PROCESOS DE ADQUIRIR E IMPLEMENTAR SOLUCIONES INFORMÁTICAS EN EL DEPARTAMENTO DE INFORMÁTICA

Sr. Estuardo Díaz
Asistente de Auditoría
Presente

Estimado Sr. Díaz:

Se le comunica que ha sido nombrado para realizar la revisión del control interno informático en los procesos de adquisición e implementación de soluciones informáticas en el departamento de informática de la empresa. Para llevar a cabo esta evaluación deberá basarse en el correspondiente dominio contenido en el modelo de los Objetivos de Control para Información y Tecnología Relacionada (COBIT).

El tiempo asignado para esta actividad es de 15 días, iniciando el 15 de enero del presente año.

Atentamente

Lic. Luis Dionicio
Auditor Interno

Ruedas mágicas, S.A.
Auditoría Interna

Papel de Trabajo	MM03
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	15-01-2009
FECHA FIN:	16-01-2009

PROGRAMA DE AUDITORÍA INTERNA PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO DE LOS PROCESOS DE ADQUISICIÓN E IMPLEMENTACIÓN DE SOLUCIONES INFORMÁTICAS SEGÚN EL MODELO COBIT DE CONTROL INTERNO

I. INTRODUCCIÓN

Para llevar a cabo la estrategia de tecnología informática es necesario que las soluciones tecnológicas sean identificadas, desarrolladas o adquiridas, así también sean implementadas e integradas a los procesos del negocio. Además, es necesario que el cambio y el mantenimiento de los sistemas existentes sean controlados para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

II. OBJETIVOS

Evaluar el nivel de madurez de los controles informáticos en la administración de los procesos de adquisición e implementación de soluciones informáticas establecida por el departamento de informática de la empresa Ruedas Mágicas, S.A.

III. ALCANCE

El trabajo de auditoría deberá proveer una opinión de alto nivel enmarcada en la determinación del nivel de madurez de la administración de controles informáticos para los procesos incluidos en el dominio COBIT de Adquisición e Implementación (AI), mediante las siguientes técnicas de evaluación:

- Cuestionarios elaborados en base a las declaraciones de los niveles de madurez para cada proceso de COBIT.
- Verificación física de documentación requerida por el modelo.
- Informe de resultados.
- Resumen de resultados.

IV. PROCEDIMIENTO

Para la evaluación del control interno en los procesos de adquisición e implementación de soluciones informáticas en base al modelo COBIT, se aplicará lo siguiente:

EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO

Para cada objetivo de control de alto nivel se aplicarán cuestionarios elaborados en base a las declaraciones de los niveles de madurez de COBIT y se revisará la documentación necesaria para determinar el nivel de madurez de cada proceso y sus actividades detalladas.

Los procesos y actividades que deberán evaluarse son los siguientes:

- **Identificar soluciones automatizadas (AI1):**
    - Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.
    - Reporte de análisis de riesgos.
    - Estudio de factibilidad y formulación de cursos alternativos de acción.
    - Requerimientos, decisión de factibilidad y aprobación.

- **Adquirir y mantener software aplicativo (AI2):**
    - Diseño de alto nivel.
    - Diseño detallado.
    - Control y auditabilidad de aplicaciones.
    - Seguridad y disponibilidad de aplicaciones.
    - Configuración e implantación de software aplicativo adquirido.
    - Actualizaciones importantes en sistemas existentes.
    - Desarrollo de software aplicativo.
    - Aseguramiento de la calidad del software.
    - Administración de los requerimientos de aplicaciones.
    - Mantenimiento de software aplicativo.

- **Adquirir y mantener infraestructura tecnológica (AI3):**

    - Plan de adquisición de infraestructura tecnológica.
    - Protección y disponibilidad del recurso de infraestructura.
    - Mantenimiento de la infraestructura.
    - Ambiente de prueba de factibilidad.

- **Facilitar la operación y el uso (AI4):**

    - Plan para soluciones de operación.
    - Transferencia de conocimiento a la gerencia del negocio.
    - Transferencia de conocimiento a los usuarios finales.
    - Transferencia de conocimiento al personal de operaciones y soporte.

- **Adquirir recursos de TI (AI5):**

    - Control de adquisición.
    - Administración de contratos con proveedores.
    - Selección de proveedores.
    - Adquisición de software.
    - Adquisición de recursos de desarrollo.
    - Adquisición de infraestructura, instalaciones y servicios relacionados.

- **Administrar cambios (AI6):**

    - Estándares y procedimientos para cambios.
    - Evaluación de impacto, priorización y autorización.
    - Cambios de emergencia.
    - Seguimiento y reporte del estatus de cambio.
    - Cierre y documentación del cambio.

- **Instalar y acreditar soluciones y cambios (AI7):**

    - Entrenamiento.
    - Plan de prueba.
    - Plan de implantación.
    - Ambiente de prueba.

- Conversión de sistema y datos.
- Prueba de cambios.
- Prueba final y aceptación.
- Transferencia a producción.
- Liberación de software.
- Distribución del sistema.
- Registro y rastreo de cambios.
- Revisión posterior a la implantación.

V. INFORME

- **Elaboración del informe.**

Se deberá elaborar un informe por cada proceso incluido en el dominio COBIT objeto de evaluación, indicando los resultados y comparando contra el nivel de control deseado por la administración.

- **Normativa:**

Objetivos de control para información y tecnología relacionada versión 4.0 (COBIT 4.0, por sus siglas en inglés).

- **Cronograma:**

Para realizar esta revisión se asignan 15 días para la recolección de información, cuestionarios y presentación del informe. Se establece como fecha de inicio el 15 de enero de 2009 y como fecha de entrega del informe resumido y los informes detallados el día 31 de enero.

- **Presentación del informe:**

Los resultados del trabajo realizado deberán presentarse por medio de un informe gerencial sobre la madurez de los procesos incluidos en el dominio de COBIT que se evalúa. El informe en borrador deberá presentarse previamente al gerente del departamento de informática conteniendo los hallazgos y recomendaciones considerados como relevantes para el mejoramiento y fortalecimiento del entorno de control de esa unidad administrativa, mediante lo cual se deberá obtener el compromiso para la implementación de las recomendaciones.

- **Distribución del informe:**

Después de la entrega definitiva de los resultados se deberá enviar una copia del informe al gerente del departamento de informática. Además se deberá distribuir una copia del informe a los siguientes interesados: Gerente general.

Atentamente,

Lic. Luis Dionicio
Auditor Interno

Papel de Trabajo	MM04
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Evaluación del proceso de Identificar Soluciones Automatizadas (AI1)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI1 Identificar soluciones automatizadas					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	2	0.000	0.000	0.000
1	1.00	3	0.333	0.105	0.105
2	0.00	4	0.000	0.000	0.000
3	4.00	4	1.000	0.316	0.948
4	6.00	6	1.000	0.316	1.264
5	5.00	6	0.833	0.263	1.315
TOTAL	**16.00**	**25**	**3.166**	**1.00**	**3.632**
PRUEBA	16.00	25			**72.6%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Gerencia de Seguridad					
0	0.00	2	0.00	0.000	0.000
1	2.33	3	0.78	0.260	0.260
2	0.33	4	0.08	0.028	0.056
3	2.99	4	0.75	0.250	0.750
4	4.98	6	0.83	0.277	1.108
5	3.32	6	0.55	0.185	0.925
TOTAL	**13.95**	**25**	**2.99**	**1.00**	**3.099**
PRUEBA	13.95	25			**62.0%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Consolidación de resultados					
0	0.00	2	0.000	0.000	0.000
1	3.33	3	1.110	0.180	0.180
2	0.33	4	0.083	0.013	0.026
3	6.99	4	1.748	0.284	0.852
4	10.98	6	1.830	0.297	1.188
5	8.32	6	1.387	0.225	1.125
TOTAL	**29.95**	**25**	**6.158**	**1.00**	**3.371**
PRUEBA	29.95	25			**67.4%**
DIFERENCIA	0	0			**NIVEL ACTUAL**

PROCESO: AI1 Identificar soluciones automatizadas			Que tanto está de acuerdo?				P/T: MM04-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**No.**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	La organización no requiere la identificación de requerimientos funcionales y operativos para el desarrollo, implementación o modificación de soluciones, como por ejemplo soluciones de sistema, de servicio, de infraestructura, de software y de datos.	X				0.00
0	2	La organización no mantiene una conciencia sobre las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	X				0.00
1	3	Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas.				X	1.00
1	4	Los grupos individuales tienden a reunirse para discutir necesidades de manera informal y los requerimientos por lo general no están documentados.	X				0.00
1	5	Las soluciones son identificadas por personas basadas en una conciencia limitada del mercado, o en respuesta a ofertas de proveedores. Hay poco o ningún análisis estructurado o investigación acerca de la tecnología disponible.	X				0.00
2	6	Hay algunos enfoques intuitivos para identificar las soluciones de TI y los mismos varían en todo el negocio.	X				0.00
2	7	Las soluciones son identificadas de manera informal sobre la base de la experiencia interna y de los conocimientos de la función de TI. El éxito de cada proyecto depende de la experiencia de unas pocas personas claves de TI.	X				0.00
2	8	La calidad de la documentación y de la toma de decisiones varía considerablemente.	X				0
2	9	Se emplean enfoques sin estructura para definir los requerimientos e identificar las soluciones de tecnología.	X				0
3	10	Se usan métodos claros y estructurados para determinar las soluciones de TI.				X	1
3	11	El método para la determinación de soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del usuario o del negocio, las oportunidades tecnológicas, la factibilidad económica, los análisis de riesgos y otros factores.				X	1.00
3	12	El proceso para la determinación de soluciones de TI se aplica a algunos proyectos basándose en factores como las decisiones hechas por el personal involucrado, la cantidad de tiempo de administración dedicado y el tamaño y la prioridad del requerimiento original del negocio.				X	1.00
3	13	Se emplean métodos estructurados para definir los requerimientos e identificar las soluciones de TI.				X	1.00
4	14	Existe una metodología establecida para la identificación y evaluación de soluciones de TI y la misma se emplea para la mayoría de proyectos.				X	1.00
4	15	La documentación de proyectos es de buena calidad y cada etapa es debidamente aprobada.				X	1.00
4	16	Los requerimientos son bien articulados y están en conformidad con estructuras predefinidas.				X	1.00
4	17	Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias.				X	1.00
4	18	La metodología es clara, definida, generalmente comprendida y medible.				X	1.00
4	19	Hay una interfaz claramente definida entre la gerencia de TI y de negocio respecto a la identificación y evaluación de soluciones de TI.				X	1.00
5	20	La metodología para la identificación y evaluación de soluciones de TI se mejora continuamente.				X	1.00
5	21	La metodología de adquisición e implementación es lo suficientemente flexible para acomodar proyectos de pequeña y gran escala.				X	1.00
5	22	La metodología es apoyada por bases de datos de conocimientos internas y externas que contienen materiales de referencia sobre soluciones tecnológicas.				X	1.00
5	23	La metodología misma produce documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.				X	1.00
5	24	La organización puede a menudo identificar nuevas oportunidades para utilizar la tecnología para ganar ventaja competitiva, influir en el proceso de reingeniería del negocio y mejorar la eficiencia general.				X	1.00
5	25	La gerencia detecta y actúa en consecuencia si las soluciones de TI son aprobadas sin considerar tecnologías alternativas o requerimientos funcionales de negocio.	X				0.00
	25		TOTAL DEL NIVEL				16

PROCESO: AI1 Identificar soluciones automatizadas			Que tanto está de acuerdo?				P/T: MM04-02
Función: Gerencia de Seguridad			**Fecha: 20/01/2009**				
NV	**No.**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	La organización no requiere la identificación de requerimientos funcionales y operativos para el desarrollo, implementación o modificación de soluciones, como por ejemplo soluciones de sistema, de servicio, de infraestructura, de software y de datos.	X				0.00
0	2	La organización no mantiene una conciencia sobre las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	X				0.00
1	3	Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas.				X	1.00
1	4	Los grupos individuales tienden a reunirse para discutir necesidades de manera informal y los requerimientos por lo general no están documentados.				X	1.00
1	5	Las soluciones son identificadas por personas basadas en una conciencia limitada del mercado, o en respuesta a ofertas de proveedores. Hay poco o ningún análisis estructurado o investigación acerca de la tecnología disponible.		X			0.33
2	6	Hay algunos enfoques intuitivos para identificar las soluciones de TI y los mismos varían en todo el negocio.		X			0.33
2	7	Las soluciones son identificadas de manera informal sobre la base de la experiencia interna y de los conocimientos de la función de TI. El éxito de cada proyecto depende de la experiencia de unas pocas personas claves de TI.	X				0.00
2	8	La calidad de la documentación y de la toma de decisiones varía considerablemente.	X				0
2	9	Se emplean enfoques sin estructura para definir los requerimientos e identificar las soluciones de tecnología.	X				0
3	10	Se usan métodos claros y estructurados para determinar las soluciones de TI.				X	1
3	11	El método para la determinación de soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del usuario o del negocio, las oportunidades tecnológicas, la factibilidad económica, los análisis de riesgos y otros factores.			X		0.66
3	12	El proceso para la determinación de soluciones de TI se aplica a algunos proyectos basándose en factores como las decisiones hechas por el personal involucrado, la cantidad de tiempo de administración dedicado y el tamaño y la prioridad del requerimiento original del negocio.		X			0.33
3	13	Se emplean métodos estructurados para definir los requerimientos e identificar las soluciones de TI.				X	1.00
4	14	Existe una metodología establecida para la identificación y evaluación de soluciones de TI y la misma se emplea para la mayoría de proyectos.			X		0.66
4	15	La documentación de proyectos es de buena calidad y cada etapa es debidamente aprobada.				X	1.00
4	16	Los requerimientos son bien articulados y están en conformidad con estructuras predefinidas.			X		0.66
4	17	Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias.			X		0.66
4	18	La metodología es clara, definida, generalmente comprendida y medible.				X	1.00
4	19	Hay una interfaz claramente definida entre la gerencia de TI y de negocio respecto a la identificación y evaluación de soluciones de TI.				X	1.00
5	20	La metodología para la identificación y evaluación de soluciones de TI se mejora continuamente.			X		0.66
5	21	La metodología de adquisición e implementación es lo suficientemente flexible para acomodar proyectos de pequeña y gran escala.		X			0.33
5	22	La metodología es apoyada por bases de datos de conocimientos internas y externas que contienen materiales de referencia sobre soluciones tecnológicas.				X	1.00
5	23	La metodología misma produce documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.				X	1.00
5	24	La organización puede a menudo identificar nuevas oportunidades para utilizar la tecnología para ganar ventaja competitiva, influir en el proceso de reingeniería del negocio y mejorar la eficiencia general.		X			0.33
5	25	La gerencia detecta y actúa en consecuencia si las soluciones de TI son aprobadas sin considerar tecnologías alternativas o requerimientos funcionales de negocio.	X				0.00
	25		TOTAL DEL NIVEL				13.95

Papel de Trabajo	MM05
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Evaluación del proceso de Adquirir e Implementar Software Aplicativo (AI2)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI2 Adquirir e implementar software aplicativo					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	2	0.000	0.000	0.000
1	1.33	4	0.333	0.104	0.104
2	0.33	4	0.083	0.026	0.052
3	4.00	5	0.800	0.249	0.747
4	3.00	3	1.000	0.311	1.244
5	5.00	5	1.000	0.311	1.555
TOTAL	**13.66**	**23**	**3.216**	**1.00**	**3.702**
PRUEBA	13.66	23			**74.0%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Gerencia de Seguridad					
0	0.33	2	0.165	0.060	0.000
1	1.65	4	0.413	0.150	0.150
2	1.32	4	0.330	0.120	0.240
3	3.31	5	0.662	0.240	0.720
4	1.98	3	0.660	0.239	0.956
5	2.64	5	0.528	0.191	0.955
TOTAL	**11.23**	**23**	**2.760**	**1.00**	**3.021**
PRUEBA	11.23	23			**60.4%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Consolidación de resultados					
0	0.33	2	0.165	0.028	0.000
1	2.98	4	0.745	0.125	0.125
2	1.65	4	0.413	0.069	0.138
3	7.31	5	1.462	0.245	0.735
4	4.98	3	1.660	0.278	1.112
5	7.64	5	1.528	0.256	1.280
TOTAL	**24.89**	**23**	**5.973**	**1.00**	**3.390**
PRUEBA	24.89	23			**67.8%**
DIFERENCIA	0	0			**NIVEL ACTUAL**

PROCESO: AI2 Adquirir e implementar software aplicativo			Que tanto está de acuerdo?				P/T: MM05-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No existe un diseño y especificacion de aplicaciones.	x				0
0	2	Generalmente las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos especificos, considerando poco o nada los requerimientos actuales.	x				0
1	3	Existe conciencia de la necesidad de contar con un proceso de adquisicion y mantenimiento de aplicaciones.				x	1
1	4	Los enfoques para adquisicion y mantenimiento de software aplicativo varian de un proyecto a otro.		x			0.33
1	5	Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte.	x				0
1	6	Se tiene poca consideracion hacia la seguridad y disponibilidad de la aplicación en el diseño y adquisicion de software aplicativo.	x				0
2	7	Hay procesos diferentes pero similares para adquirir y mantener aplicaciones basados en la experiencia dentro de la función de TI.	x				0
2	8	La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y de los niveles de experiencia dentro de la TI.		x			0.33
2	9	El mantenimiento es usualmente problemático y sufre cuando se perdieron conocimientos internos de la organización.	x				0
2	10	Al diseñar o adquirir el software de aplicación se presta poca o ninguna consideración a la seguridad y disponibilidad de la aplicación.	x				0
3	11	Hay un proceso claro, definido y generalmente comprendido para la adquisición e implementación de software de aplicación.				x	1
3	12	Este proceso está en concordancia con la estrategia de TI y la del negocio.				x	1
3	13	Se intentan aplicar coherentemente los procesos documentados en todos los proyectos y aplicaciones diferentes.				x	1
3	14	Las metodologías son generalmente inflexibles y difíciles de aplicar a todos los casos, de modo que los pasos son frecuentemente omitidos.	x				0
3	15	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				x	1
4	16	Hay una metodología formal, clara y bien entendida que incluye un proceso de diseño y especificación, criterios para la adquisición de software de aplicación, un proceso para realizar pruebas y requerimientos para la documentación.				x	1
4	17	Existen mecanismos de aprobación documentados y acordados para asegurar que se sigan todos los pasos y que se autoricen las excepciones.				x	1
4	18	Las prácticas y procedimientos evolucionaron y se adecuan a la organización, son usados por todo el personal, y se aplican a la mayoría de los requerimientos de aplicación.				x	1
5	19	Las prácticas de adquisición y mantenimiento de software de aplicación están alineadas con los procesos definidos.				x	1
5	20	El método está basado en componentes, con aplicaciones predefinidas y estandarizadas adaptadas a las necesidades del negocio. Este método se aplica a nivel de toda la organización.				x	1
5	21	La metodología de adquisición y mantenimiento es avanzada, posibilita una rápida implementación y permite una alta capacidad de respuesta y flexibilidad para responder a los requerimientos cambiantes del negocio.				x	1
5	22	La metodología de adquisición e implementación de software de aplicación está sujeta a una mejora continua y es respaldada por bases de datos de conocimientos internas y externas que contienen materiales de referencia y buenas prácticas.				x	1
5	23	La metodología genera documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.				x	1
			TOTAL DEL NIVEL				13.66

PROCESO: AI2 Adquirir e implementar software aplicativo			Que tanto está de acuerdo?				P/T: MM05-02
Función: Gerencia de Seguridad			**Fecha: 20/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No existe un diseño y especificacion de aplicaciones.	X				0
0	2	Generalmente las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos especificos, considerando poco o nada los requerimientos actuales.		X			0.33
1	3	Existe conciencia de la necesidad de contar con un proceso de adquisicion y mantenimiento de aplicaciones.			X		0.66
1	4	Los enfoques para adquisicion y mantenimiento de software aplicativo varian de un proyecto a otro.			X		0.66
1	5	Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte.		X			0.33
1	6	Se tiene poca consideracion hacia la seguridad y disponibilidad de la aplicación en el diseño y adquisicion de software aplicativo.	X				0
2	7	Hay procesos diferentes pero similares para adquirir y mantener aplicaciones basados en la experiencia dentro de la función de TI.			X		0.66
2	8	La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y de los niveles de experiencia dentro de la TI.			X		0.66
2	9	El mantenimiento es usualmente problemático y sufre cuando se perdieron conocimientos internos de la organización.	X				0
2	10	Al diseñar o adquirir el software de aplicación se presta poca o ninguna consideración a la seguridad y disponibilidad de la aplicación.	X				0
3	11	Hay un proceso claro, definido y generalmente comprendido para la adquisición e implementación de software de aplicación.			X		0.66
3	12	Este proceso está en concordancia con la estrategia de TI y la del negocio.			X		0.66
3	13	Se intentan aplicar coherentemente los procesos documentados en todos los proyectos y aplicaciones diferentes.			X		0.66
3	14	Las metodologías son generalmente inflexibles y difíciles de aplicar a todos los casos, de modo que los pasos son frecuentemente omitidos.		X			0.33
3	15	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1
4	16	Hay una metodología formal, clara y bien entendida que incluye un proceso de diseño y especificación, criterios para la adquisición de software de aplicación, un proceso para realizar pruebas y requerimientos para la documentación.			X		0.66
4	17	Existen mecanismos de aprobación documentados y acordados para asegurar que se sigan todos los pasos y que se autoricen las excepciones.			X		0.66
4	18	Las prácticas y procedimientos evolucionaron y se adecuan a la organización, son usados por todo el personal, y se aplican a la mayoría de los requerimientos de aplicación.			X		0.66
5	19	Las prácticas de adquisición y mantenimiento de software de aplicación están alineadas con los procesos definidos.			X		0.66
5	20	El método está basado en componentes, con aplicaciones predefinidas y estandarizadas adaptadas a las necesidades del negocio. Este método se aplica a nivel de toda la organización.		X			0.33
5	21	La metodología de adquisición y mantenimiento es avanzada, posibilita una rápida implementación y permite una alta capacidad de respuesta y flexibilidad para responder a los requerimientos cambiantes del negocio.			X		0.66
5	22	La metodología de adquisición e implementación de software de aplicación está sujeta a una mejora continua y es respaldada por bases de datos de conocimientos internas y externas que contienen materiales de referencia y buenas prácticas.			X		0.66
5	23	La metodología genera documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.		X			0.33
			TOTAL DEL NIVEL				11.23

Papel de Trabajo	MM06
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Evaluación del proceso de adquirir y mantener infraestructura tecnológica (AI3)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI3 Adquirir e implementar infraestructura tecnologica					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	1	0.000	0.000	0.000
1	0.00	3	0.000	0.000	0.000
2	2.98	5	0.596	0.178	0.356
3	3.33	4	0.833	0.249	0.747
4	3.66	4	0.915	0.274	1.096
5	5.00	5	1.000	0.299	1.495
TOTAL	**14.97**	**22**	**3.344**	**1.00**	**3.694**
PRUEBA	14.97	22			**73.9%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Gerencia de Seguridad					
0	0.33	1	0.330	0.102	0.000
1	0.33	3	0.110	0.034	0.034
2	1.32	5	0.264	0.081	0.162
3	3.66	4	0.915	0.282	0.846
4	3.32	4	0.830	0.256	1.024
5	3.99	5	0.798	0.246	1.230
TOTAL	**12.95**	**22**	**3.247**	**1.00**	**3.296**
PRUEBA	12.95	22			**65.9%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Consolidación de resultados					
0	0.33	1	0.330	0.050	0.000
1	0.33	3	0.110	0.017	0.017
2	4.30	5	0.860	0.130	0.260
3	6.99	4	1.748	0.265	0.795
4	6.98	4	1.745	0.265	1.060
5	8.99	5	1.798	0.273	1.365
TOTAL	**27.92**	**22**	**6.591**	**1.00**	**3.497**
PRUEBA	27.92	22			**69.9%**
DIFERENCIA	0	0			**NIVEL ACTUAL**

PROCESO: AI3 Adquirir e implementar infraestructura tecnologica			Que tanto está de acuerdo?				P/T: MM06-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	La arquitectura de la tecnología no es considerada un tema lo suficientemente importante como para ser tratado.	x				0
1	2	Se hacen cambios a la infraestructura para cada nueva aplicación sin un plan general.	x				0
1	3	A pesar de que hay conciencia de que la infraestructura de TI es importante, no hay un método general coherente.	x				0
1	4	Las actividades de mantenimiento reaccionan a las necesidades a corto plazo. El entorno de producción es el entorno de pruebas.	x				0
2	5	Hay coherencia entre los métodos tácticos, cuando se adquiere y se mantiene la infraestructura de TI.				x	1
2	6	La adquisición y el mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que deben ser apoyadas.	x				0
2	7	Hay una comprensión de que la infraestructura de TI es importante, y dicha comprensión es apoyada por algunas prácticas formales.			x		0.66
2	8	Se programa algún mantenimiento, pero el mismo no es programado y coordinado completamente.			x		0.66
2	9	Para algunos entornos existe un entorno de pruebas separado.			x		0.66
3	10	Existe un proceso claro, definido y generalmente entendido para adquirir y mantener la infraestructura de TI.				x	1
3	11	El proceso apoya las necesidades de las aplicaciones críticas del negocio y está alineado con la estrategia de TI y del negocio aunque no se aplique de forma coherente.		x			0.33
3	12	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				x	1
3	13	Existen entornos separados para pruebas y producción.				x	1
4	14	El proceso de adquisición y mantenimiento para la infraestructura tecnológica se ha desarrollado hasta el punto que funciona bien para la mayoría de las situaciones, es seguido coherentemente y se concentra en la reutilización.				x	1
4	15	La infraestructura de TI soporta de manera adecuada las aplicaciones de negocio.				x	1
4	16	El proceso de adquisicion y mantenimiento para la infraestructura tecnologia está bien organizado y es proactivo.				x	1
4	17	El costo y el tiempo para alcanzar el nivel esperado de escalabilidad, flexibilidad e integración está parcialmente optimizado.			x		0.66
5	18	El proceso de adquisición y mantenimiento para la infraestructura tecnológica es proactivo y está estrechamente alineado con aplicaciones críticas del negocio y con la arquitectura de la tecnología.				x	1
5	19	Se siguen las mejores prácticas respecto a soluciones de tecnología y la organización está al tanto de los últimos desarrollos en plataformas y herramientas de administración.				x	1
5	20	Los costos son reducidos racionalizando y estandarizando los componentes de la infraestructura y usando la automatización.				x	1
5	21	El alto nivel de conocimientos técnicos puede identificar las mejores formas de mejorar proactivamente el desempeño, incluyendo la consideración de opciones de tercerización.				x	1
5	22	La infraestructura de TI es vista como el posibilitador clave para aprovechar el uso de la TI.				x	1
			TOTAL DEL NIVEL				14.97

PROCESO: AI3 Adquirir e implementar infraestructura tecnologica			Que tanto está de acuerdo?				P/T: MM06-02
Función: Gerencia de Seguridad			**Fecha: 20/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	La arquitectura de la tecnología no es considerada un tema lo suficientemente importante como para ser tratado.		X			0.33
1	2	Se hacen cambios a la infraestructura para cada nueva aplicación sin un plan general.	X				0
1	3	A pesar de que hay conciencia de que la infraestructura de TI es importante, no hay un método general coherente.		X			0.33
1	4	Las actividades de mantenimiento reaccionan a las necesidades a corto plazo. El entorno de producción es el entorno de pruebas.	X				0
2	5	Hay coherencia entre los métodos tácticos, cuando se adquiere y se mantiene la infraestructura de TI.			X		0.66
2	6	La adquisición y el mantenimiento de la infraestructura de TI no se basa en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que deben ser apoyadas.	X				0
2	7	Hay una comprensión de que la infraestructura de TI es importante, y dicha comprensión es apoyada por algunas prácticas formales.			X		0.66
2	8	Se programa algún mantenimiento, pero el mismo no es programado y coordinado completamente.	X				0
2	9	Para algunos entornos existe un entorno de pruebas separado.	X				0
3	10	Existe un proceso claro, definido y generalmente entendido para adquirir y mantener la infraestructura de TI.				X	1
3	11	El proceso apoya las necesidades de las aplicaciones críticas del negocio y está alineado con la estrategia de TI y del negocio aunque no se aplique de forma coherente.			X		0.66
3	12	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1
3	13	Existen entornos separados para pruebas y producción.				X	1
4	14	El proceso de adquisición y mantenimiento para la infraestructura tecnológica se ha desarrollado hasta el punto que funciona bien para la mayoría de las situaciones, es seguido coherentemente y se concentra en la reutilización.			X		0.66
4	15	La infraestructura de TI soporta de manera adecuada las aplicaciones de negocio.				X	1
4	16	El proceso de adquisicion y mantenimiento para la infraestructura tecnologia está bien organizado y es proactivo.				X	1
4	17	El costo y el tiempo para alcanzar el nivel esperado de escalabilidad, flexibilidad e integración está parcialmente optimizado.			X		0.66
5	18	El proceso de adquisición y mantenimiento para la infraestructura tecnológica es proactivo y está estrechamente alineado con aplicaciones críticas del negocio y con la arquitectura de la tecnología.				X	1
5	19	Se siguen las mejores prácticas respecto a soluciones de tecnología y la organización está al tanto de los últimos desarrollos en plataformas y herramientas de administración.				X	1
5	20	Los costos son reducidos racionalizando y estandarizando los componentes de la infraestructura y usando la automatización.		X			0.33
5	21	El alto nivel de conocimientos técnicos puede identificar las mejores formas de mejorar proactivamente el desempeño, incluyendo la consideración de opciones de tercerización.				X	1
5	22	La infraestructura de TI es vista como el posibilitador clave para aprovechar el uso de la TI.			X		0.66
			TOTAL DEL NIVEL				12.95

Papel de Trabajo	MM07
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Evaluación del proceso de facilitar la ejecución y el uso (AI4)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI4 Facilitar la operación y el uso					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	2	0.000	0.000	0.000
1	1.00	6	0.167	0.053	0.053
2	1.00	5	0.200	0.064	0.128
3	7.00	9	0.778	0.247	0.741
4	10.00	10	1.000	0.318	1.272
5	4.00	4	1.000	0.318	1.590
TOTAL	**23**	**36**	**3.145**	**1.00**	**3.784**
PRUEBA	23	36			**75.7%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Gerencia de Desarrollo					
0	2.00	2	1.000	0.325	0.000
1	3.65	6	0.608	0.198	0.198
2	2.97	5	0.594	0.193	0.386
3	4.30	9	0.478	0.155	0.465
4	2.31	10	0.231	0.075	0.300
5	0.66	4	0.165	0.054	0.270
TOTAL	**15.89**	**36**	**3.076**	**1.00**	**1.619**
PRUEBA	15.89	36			**32.4%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Consolidación de resultados					
0	2.00	2	1.000	0.161	0.000
1	4.65	6	0.775	0.125	0.125
2	3.97	5	0.794	0.128	0.256
3	11.30	9	1.256	0.202	0.606
4	12.31	10	1.231	0.198	0.792
5	4.66	4	1.165	0.187	0.935
TOTAL	**38.89**	**36**	**6.221**	**1.00**	**2.714**
PRUEBA	38.89	36			**54.3%**
DIFERENCIA	0	0			**NIVEL ACTUAL**

PROCESO: AI4 Facilitar la operación y el uso			Que tanto está de acuerdo?				P/T: MM07-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No hay ningún proceso establecido respecto a la producción de documentación de usuario, manuales de operaciones y material de capacitación.	x				0
0	2	Los únicos materiales que existen son los suministrados con los productos comprados.	x				0
1	3	La organización está conciente de que se necesita un proceso que resuelva la documentación.				x	1
1	4	La documentación se produce ocasionalmente y está distribuida desigualmente entre grupos limitados.	x				0
1	5	Gran parte de la documentación y de los procedimientos son obsoletos. .	x				0
1	6	Los materiales de capacitación tienden a ser esquemas que se usan una sola vez con calidad variable.	x				0
1	7	Prácticamente no hay integración de los procedimientos en todos los diferentes sistemas y unidades de negocio.	x				0
1	8	No hay colaboración por parte de las unidades de negocio en el diseño de programas de capacitación	x				0
2	9	Se usan enfoques similares para producir procedimientos y documentación, pero los mismos no están basados en un enfoque o marco estructurado.	x				0
2	10	No hay un enfoque uniforme para el desarrollo de procedimientos operativos y de usuario.	x				0
2	11	El material de capacitación es producido individualmente o por grupos de proyectos y su calidad depende de las personas involucradas.				x	1
2	12	Los procedimientos y la calidad del soporte de usuario varían de pobre a muy bueno, con muy poca coherencia e integración en toda la organización.	x				0
2	13	Se proveen o facilitan los programas de capacitación para el negocio y los usuarios, pero no hay un plan general para la entrega e implementación de capacitación.	x				0
3	14	Hay un marco claramente definido, aceptado y entendido para la documentación del usuario, los manuales de operaciones y los materiales de capacitación.				x	1
3	15	Los procedimientos son almacenados y mantenidos en una biblioteca formal y pueden ser accedidos por cualquiera que necesite saber.				x	1
3	16	Se hacen correcciones a la documentación y los procedimientos de manera reactiva.	x				0
3	17	Se cuenta con procedimientos fuera de línea y éstos pueden ser accedidos y mantenidos en caso de desastre.				x	1
3	18	Existe un proceso que especifica que las actualizaciones de procedimientos y materiales de capacitación son un producto explícito de un proyecto de cambio.				x	1
3	19	A pesar de la existencia de enfoques definidos, el contenido real varía porque no hay control para hacer cumplir las normas.	x				0
3	20	Los usuarios están formalmente involucrados en este proceso.				x	1
3	21	Se usan cada vez más herramientas automatizadas para la generación y distribución de procedimientos.				x	1
3	22	La capacitación de usuarios y de negocio es planificada y programada.				x	1
4	23	Hay un marco de trabajo definido para mantener los procedimientos y los materiales de capacitación que cuenta con el apoyo de la gerencia de TI.				x	1
4	24	El enfoque adoptado para mantener los procedimientos y los manuales de capacitación cubre todos los sistemas y unidades de negocio, a fin de que los procesos puedan ser vistos desde una perspectiva de negocios.				x	1
4	25	Los procedimientos y los materiales de capacitación están integrados para incluir interdependencias e interfaces.				x	1
4	26	Existen controles para asegurar que las normas se cumplen y que los procedimientos se desarrollen y se mantengan para todos los procesos.				x	1
4	27	La realimentación del negocio y de los usuarios acerca de la documentación y la capacitación se recopila y evalúa como parte de un proceso de mejora continua.				x	1
4	28	La documentación y los materiales de capacitación están por lo general a un buen nivel predecible de confiabilidad y disponibilidad.				x	1
4	29	Está emergiendo un proceso para documentar y administrar procedimientos de forma automática.				x	1
4	30	El desarrollo de procedimientos automatizados está cada vez más integrado con el desarrollo de sistemas de aplicación, facilitando la coherencia y el acceso de los usuarios.				x	1
4	31	La capacitación de negocios y de usuarios tiene una gran capacidad de respuesta respecto a las necesidades del negocio.				x	1
4	32	La gerencia de TI está desarrollando métricas para el desarrollo y la entrega de documentación, materiales de capacitación y programas de capacitación.				x	1
5	33	El proceso para la documentación operativa y de usuarios es mejorado continuamente a través de la adopción de nuevas herramientas o métodos.				x	1
5	34	Los materiales de procedimiento y capacitación son tratados como una base de conocimientos que evoluciona constantemente y es mantenida electrónicamente usando una administración de conocimientos actualizada y tecnologías de flujo de trabajo y distribución, lo cual la hace accesible y fácil de mantener.				x	1
5	35	El material está actualizado para reflejar cambios organizacionales, operativos y de software.				x	1
5	36	El desarrollo de documentación y materiales de capacitación, así como la entrega de los programas de capacitación, están totalmente integrados con el negocio y con las definiciones de procesos de negocios, apoyando así a los requerimientos a nivel de toda la organización en lugar de solo a los procedimientos orientados a TI.				x	1
	36		TOTAL DEL NIVEL				23

PROCESO: AI4 Facilitar la operación y el uso			Que tanto está de acuerdo?				P/T: MM07-02
Función: Gerencia de Desarrollo			**Fecha: 23/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No hay ningún proceso establecido respecto a la producción de documentación de usuario, manuales de operaciones y material de capacitación.				X	1
0	2	Los únicos materiales que existen son los suministrados con los productos comprados.				X	1
1	3	La organización está conciente de que se necesita un proceso que resuelva la documentación.				X	1
1	4	La documentación se produce ocasionalmente y está distribuida desigualmente entre grupos limitados.				X	1
1	5	Gran parte de la documentación y de los procedimientos son obsoletos. .		X			0.33
1	6	Los materiales de capacitación tienden a ser esquemas que se usan una sola vez con calidad variable.			X		0.66
1	7	Prácticamente no hay integración de los procedimientos en todos los diferentes sistemas y unidades de negocio.			X		0.66
1	8	No hay colaboración por parte de las unidades de negocio en el diseño de programas de capacitación	X				0
2	9	Se usan enfoques similares para producir procedimientos y documentación, pero los mismos no están basados en un enfoque o marco estructurado.			X		0.66
2	10	No hay un enfoque uniforme para el desarrollo de procedimientos operativos y de usuario.			X		0.66
2	11	El material de capacitación es producido individualmente o por grupos de proyectos y su calidad depende de las personas involucradas.			X		0.66
2	12	Los procedimientos y la calidad del soporte de usuario varían de pobre a muy bueno, con muy poca coherencia e integración en toda la organización.		X			0.33
2	13	Se proveen o facilitan los programas de capacitación para el negocio y los usuarios, pero no hay un plan general para la entrega e implementación de capacitación.			X		0.66
3	14	Hay un marco claramente definido, aceptado y entendido para la documentación del usuario, los manuales de operaciones y los materiales de capacitación.		X			0.33
3	15	Los procedimientos son almacenados y mantenidos en una biblioteca formal y pueden ser accedidos por cualquiera que necesite saber.	X				0
3	16	Se hacen correcciones a la documentación y los procedimientos de manera reactiva.			X		0.66
3	17	Se cuenta con procedimientos fuera de línea y éstos pueden ser accedidos y mantenidos en caso de desastre.				X	1
3	18	Existe un proceso que especifica que las actualizaciones de procedimientos y materiales de capacitación son un producto explícito de un proyecto de cambio.	X				0
3	19	A pesar de la existencia de enfoques definidos, el contenido real varía porque no hay control para hacer cumplir las normas.			X		0.66
3	20	Los usuarios están formalmente involucrados en este proceso.			X		0.66
3	21	Se usan cada vez más herramientas automatizadas para la generación y distribución de procedimientos.			X		0.66
3	22	La capacitación de usuarios y de negocio es planificada y programada.		X			0.33
4	23	Hay un marco de trabajo definido para mantener los procedimientos y los materiales de capacitación que cuenta con el apoyo de la gerencia de TI.		X			0.33
4	24	El enfoque adoptado para mantener los procedimientos y los manuales de capacitación cubre todos los sistemas y unidades de negocio, a fin de que los procesos puedan ser vistos desde una perspectiva de negocios.	X				0
4	25	Los procedimientos y los materiales de capacitación están integrados para incluir interdependencias e interfaces.	X				0
4	26	Existen controles para asegurar que las normas se cumplen y que los procedimientos se desarrollen y se mantengan para todos los procesos.		X			0.33
4	27	La realimentación del negocio y de los usuarios acerca de la documentación y la capacitación se recopila y evalúa como parte de un proceso de mejora continua.	X				0
4	28	La documentación y los materiales de capacitación están por lo general a un buen nivel predecible de confiabilidad y disponibilidad.	X				0
4	29	Está emergiendo un proceso para documentar y administrar procedimientos de forma automática.		X			0.33
4	30	El desarrollo de procedimientos automatizados está cada vez más integrado con el desarrollo de sistemas de aplicación, facilitando la coherencia y el acceso de los usuarios.			X		0.66
4	31	La capacitación de negocios y de usuarios tiene una gran capacidad de respuesta respecto a las necesidades del negocio.		X			0.33
4	32	La gerencia de TI está desarrollando métricas para el desarrollo y la entrega de documentación, materiales de capacitación y programas de capacitación.		X			0.33
5	33	El proceso para la documentación operativa y de usuarios es mejorado continuamente a través de la adopción de nuevas herramientas o métodos.		X			0.33
5	34	Los materiales de procedimiento y capacitación son tratados como una base de conocimientos que evoluciona constantemente y es mantenida electrónicamente usando una administración de conocimientos actualizada y tecnologías de flujo de trabajo y distribución, lo cual la hace accesible y fácil de mantener.	X				0
5	35	El material está actualizado para reflejar cambios organizacionales, operativos y de software.	X				0
5	36	El desarrollo de documentación y materiales de capacitación, así como la entrega de los programas de capacitación, están totalmente integrados con el negocio y con las definiciones de procesos de negocios, apoyando así a los requerimientos a nivel de toda la organización en lugar de solo a los procedimientos orientados a TI.		X			0.33
	36		TOTAL DEL NIVEL				15.89

Papel de Trabajo	MM08
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Ruedas mágicas, S.A.

Auditoría Interna

Evaluación del proceso de adquirir recursos de tecnología informática (AI5)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI5 Adquirir recursos de tecnología informática					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	2	0.000	0.000	0.000
1	3.00	4	0.750	0.184	0.184
2	1.99	6	0.332	0.081	0.162
3	6.00	6	1.000	0.245	0.735
4	7.00	7	1.000	0.245	0.980
5	6.00	6	1.000	0.245	1.225
TOTAL	**23.99**	**31**	**4.082**	**1.00**	**3.286**
PRUEBA	23.99	31			**65.7%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Gerencia de Seguridad					
0	0.00	2	0.000	0.000	0.000
1	2.66	4	0.665	0.187	0.187
2	2.32	6	0.387	0.109	0.218
3	4.31	6	0.718	0.202	0.606
4	6.32	7	0.903	0.254	1.016
5	5.32	6	0.887	0.249	1.245
TOTAL	**20.93**	**31**	**3.560**	**1.00**	**3.272**
PRUEBA	20.93	31			**65.4%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Gerencia de Desarrollo					
0	0.00	2	0.000	0.000	0.000
1	1.98	4	0.495	0.139	0.139
2	1.33	6	0.222	0.062	0.124
3	6.00	6	1.000	0.281	0.843
4	6.32	7	0.903	0.253	1.012
5	5.66	6	0.943	0.265	1.325
TOTAL	**21.29**	**31**	**3.563**	**1.00**	**3.443**
PRUEBA	21.29	31			**68.9%**
DIFERENCIA	0	0			**NIVEL ACTUAL**
FUNCIÓN: Consolidación de resultados					
0	0.00	2	0.000	0.000	0.000
1	7.64	4	1.910	0.170	0.170
2	5.64	6	0.940	0.084	0.168
3	16.31	6	2.718	0.243	0.729
4	19.64	7	2.806	0.250	1.000
5	16.98	6	2.830	0.253	1.265
TOTAL	**66.21**	**31**	**11.204**	**1.00**	**3.332**
PRUEBA	66.21	31			**66.6%**
DIFERENCIA	0	0			**NIVEL ACTUAL**

PROCESO: AI5 Adquirir recursos de tecnología informática			Que tanto está de acuerdo?				P/T: MM08-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**#**	**DECLARACIÓN**	Nada	Un Poco	Bastante	Completamente	**Valor de cumplimiento**
0	1	No está definido un proceso de abastecimiento de TI.	x				0
0	2	La organización no reconoce la necesidad de contar con políticas y procedimientos de abastecimiento claros para asegurar que todos los recursos de TI estén disponibles de forma oportuna y costo-eficiente.	x				0
1	3	La organización reconoce la necesidad de contar con políticas y procedimientos documentados que vinculen la adquisición de TI con el proceso general de abastecimiento de negocio de la organización.				x	1
1	4	Se desarrollan y administran contratos para la adquisición de los recursos de TI por parte de los administradores de proyecto y otras personas que emplean su juicio profesional en lugar de políticas y procedimientos formales.				x	1
1	5	Existe una relación ad hoc entre la TI y los procesos de adquisición corporativa y de administración de contratos.				x	1
1	6	Los contratos de adquisición se administran al finalizar los proyectos en lugar de hacerlo de forma continua.	x				0
2	7	Hay conciencia en la organización acerca de la necesidad de contar con políticas y procedimientos para la adquisición de TI.				x	1
2	8	Las políticas y los procedimientos están parcialmente integrados con el proceso de abastecimiento general de negocios de la organización.		x			0.33
2	9	Los procesos de abastecimiento se emplean mayormente para proyectos de gran porte y visibilidad.		x			0.33
2	10	Las responsabilidades y la rendición de cuentas por el abastecimiento de TI y la administración de contratos se determina por la experiencia individual del administrador del contrato.		x			0.33
2	11	Se reconoce la importancia de la administración y el relacionamiento con los proveedores; sin embargo los mismos se atienden basándose en iniciativas individuales.	x				0
2	12	Los procesos de contratos se utilizan mayormente para proyectos de gran porte y visibilidad.	x				0
3	13	La gerencia establece políticas y procedimientos para la adquisición de TI.				x	1
3	14	Las políticas y los procedimientos están guiados por el proceso de abastecimiento general de negocios de la organización.				x	1
3	15	La adquisición de TI está mayormente integrada con los sistemas de abastecimiento generales del negocio.				x	1
3	16	Existen estándares de TI para la adquisición de recursos de TI.				x	1
3	17	Los proveedores de recursos de TI están integrados en los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.				x	1
3	18	La gerencia de TI comunica la necesidad de una administración de adquisiciones y contratos adecuada en toda la función de TI.				x	1
4	19	La adquisición de TI está completamente integrada con los sistemas de abastecimiento generales del negocio.				x	1
4	20	Los estándares de TI para la adquisición de recursos de TI se usan para todos los abastecimientos.				x	1
4	21	Se toman mediciones relativas a los casos de negocio para la adquisición de TI en los contratos y en la administración del abastecimiento.				x	1
4	22	Se encuentra disponible una emisión de informes sobre la actividad de adquisición de TI que apoya los objetivos de negocio.				x	1
4	23	La gerencia generalmente es conciente de las excepciones a las políticas y procedimientos para la adquisición de TI.				x	1
4	24	Comienza a desarrollarse una administración estratégica de relacionamiento.				x	1
4	25	La gerencia de TI exige el uso del proceso de adquisición y administración de contratos para todas las adquisiciones al revisar las mediciones de desempeño.				x	1
5	26	La gerencia establece recursos de adquisiciones a procesos exhaustivos para la adquisición de TI.				x	1
5	27	La gerencia exige el cumplimiento de las políticas y procedimientos para la adquisición de TI.				x	1
5	28	Se toman mediciones que son relevantes a los casos de negocio para las adquisiciones de TI en los contratos y en la administración del abastecimiento.				x	1
5	29	Se establecen buenas relaciones con los proveedores y socios a lo largo del tiempo y la calidad de dichas relaciones es medida y monitoreada. Las relaciones se administran estratégicamente.				x	1
5	30	Los estándares, políticas y procedimientos de TI para la adquisición de recursos de TI se administran estratégicamente y responden a las medidas del proceso.				x	1
5	31	La gerencia de TI comunica la importancia estratégica de una administración de adquisiciones y contratos adecuada en toda la función de TI.				x	1
	31		TOTAL DEL NIVEL				23.99

PROCESO: AI5 Adquirir recursos de tecnología informática			Que tanto está de acuerdo?				P/T: MM08-02
Función: Gerencia de Seguridad			**Fecha: 20/01/2009**				
NV	**#**	**DECLARACIÓN**	Nada	Un Poco	Bastante	Completamente	**Valor de cumplimiento**
0	1	No está definido un proceso de abastecimiento de TI.	X				0
0	2	La organización no reconoce la necesidad de contar con políticas y procedimientos de abastecimiento claros para asegurar que todos los recursos de TI estén disponibles de forma oportuna y costo-eficiente.	X				0
1	3	La organización reconoce la necesidad de contar con políticas y procedimientos documentados que vinculen la adquisición de TI con el proceso general de abastecimiento de negocio de la organización.				X	1
1	4	Se desarrollan y administran contratos para la adquisición de los recursos de TI por parte de los administradores de proyecto y otras personas que emplean su juicio profesional en lugar de políticas y procedimientos formales.				X	1
1	5	Existe una relación ad hoc entre la TI y los procesos de adquisición corporativa y de administración de contratos.			X		0.66
1	6	Los contratos de adquisición se administran al finalizar los proyectos en lugar de hacerlo de forma continua.	X				0
2	7	Hay conciencia en la organización acerca de la necesidad de contar con políticas y procedimientos para la adquisición de TI.			X		0.66
2	8	Las políticas y los procedimientos están parcialmente integrados con el proceso de abastecimiento general de negocios de la organización.			X		0.66
2	9	Los procesos de abastecimiento se emplean mayormente para proyectos de gran porte y visibilidad.	X				0
2	10	Las responsabilidades y la rendición de cuentas por el abastecimiento de TI y la administración de contratos se determina por la experiencia individual del administrador del contrato.	X				0
2	11	Se reconoce la importancia de la administración y el relacionamiento con los proveedores; sin embargo los mismos se atienden basándose en iniciativas individuales.	X				0
2	12	Los procesos de contratos se utilizan mayormente para proyectos de gran porte y visibilidad.				X	1
3	13	La gerencia establece políticas y procedimientos para la adquisición de TI.				X	1
3	14	Las políticas y los procedimientos están guiados por el proceso de abastecimiento general de negocios de la organización.			X		0.66
3	15	La adquisición de TI está mayormente integrada con los sistemas de abastecimiento generales del negocio.		X			0.33
3	16	Existen estándares de TI para la adquisición de recursos de TI.				X	1
3	17	Los proveedores de recursos de TI están integrados en los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.			X		0.66
3	18	La gerencia de TI comunica la necesidad de una administración de adquisiciones y contratos adecuada en toda la función de TI.			X		0.66
4	19	La adquisición de TI está completamente integrada con los sistemas de abastecimiento generales del negocio.			X		0.66
4	20	Los estándares de TI para la adquisición de recursos de TI se usan para todos los abastecimientos.				X	1
4	21	Se toman mediciones relativas a los casos de negocio para la adquisición de TI en los contratos y en la administración del abastecimiento.				X	1
4	22	Se encuentra disponible una emisión de informes sobre la actividad de adquisición de TI que apoya los objetivos de negocio.				X	1
4	23	La gerencia generalmente es conciente de las excepciones a las políticas y procedimientos para la adquisición de TI.			X		0.66
4	24	Comienza a desarrollarse una administración estratégica de relacionamiento.				X	1
4	25	La gerencia de TI exige el uso del proceso de adquisición y administración de contratos para todas las adquisiciones al revisar las mediciones de desempeño.				X	1
5	26	La gerencia establece recursos de adquisiciones a procesos exhaustivos para la adquisición de TI.			X		0.66
5	27	La gerencia exige el cumplimiento de las políticas y procedimientos para la adquisición de TI.				X	1
5	28	Se toman mediciones que son relevantes a los casos de negocio para las adquisiciones de TI en los contratos y en la administración del abastecimiento.				X	1
5	29	Se establecen buenas relaciones con los proveedores y socios a lo largo del tiempo y la calidad de dichas relaciones es medida y monitoreada. Las relaciones se administran estratégicamente.				X	1
5	30	Los estándares, políticas y procedimientos de TI para la adquisición de recursos de TI se administran estratégicamente y responden a las medidas del proceso.			X		0.66
5	31	La gerencia de TI comunica la importancia estratégica de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1
	31		TOTAL DEL NIVEL				20.93

PROCESO: AI5 Adquirir recursos de tecnología informática			Que tanto está de acuerdo?				P/T: MM08-03
Función: Gerencia de Desarrollo			**Fecha: 23/01/2009**				
NV	**#**	**DECLARACIÓN**	Nada	Un Poco	Bastante	Completamente	**Valor de cumplimiento**
0	1	No está definido un proceso de abastecimiento de TI.	X				0
0	2	La organización no reconoce la necesidad de contar con políticas y procedimientos de abastecimiento claros para asegurar que todos los recursos de TI estén disponibles de forma oportuna y costo-eficiente.	X				0
1	3	La organización reconoce la necesidad de contar con políticas y procedimientos documentados que vinculen la adquisición de TI con el proceso general de abastecimiento de negocio de la organización.			X		0.66
1	4	Se desarrollan y administran contratos para la adquisición de los recursos de TI por parte de los administradores de proyecto y otras personas que emplean su juicio profesional en lugar de políticas y procedimientos formales.			X		0.66
1	5	Existe una relación ad hoc entre la TI y los procesos de adquisición corporativa y de administración de contratos.			X		0.66
1	6	Los contratos de adquisición se administran al finalizar los proyectos en lugar de hacerlo de forma continua.	X				0
2	7	Hay conciencia en la organización acerca de la necesidad de contar con políticas y procedimientos para la adquisición de TI.				X	1
2	8	Las políticas y los procedimientos están parcialmente integrados con el proceso de abastecimiento general de negocios de la organización.		X			0.33
2	9	Los procesos de abastecimiento se emplean mayormente para proyectos de gran porte y visibilidad.	X				0
2	10	Las responsabilidades y la rendición de cuentas por el abastecimiento de TI y la administración de contratos se determina por la experiencia individual del administrador del contrato.	X				0
2	11	Se reconoce la importancia de la administración y el relacionamiento con los proveedores; sin embargo los mismos se atienden basándose en iniciativas individuales.	X				0
2	12	Los procesos de contratos se utilizan mayormente para proyectos de gran porte y visibilidad.	X				0
3	13	La gerencia establece políticas y procedimientos para la adquisición de TI.				X	1
3	14	Las políticas y los procedimientos están guiados por el proceso de abastecimiento general de negocios de la organización.				X	1
3	15	La adquisición de TI está mayormente integrada con los sistemas de abastecimiento generales del negocio.				X	1
3	16	Existen estándares de TI para la adquisición de recursos de TI.				X	1
3	17	Los proveedores de recursos de TI están integrados en los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.				X	1
3	18	La gerencia de TI comunica la necesidad de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1
4	19	La adquisición de TI está completamente integrada con los sistemas de abastecimiento generales del negocio.			X		0.66
4	20	Los estándares de TI para la adquisición de recursos de TI se usan para todos los abastecimientos.				X	1
4	21	Se toman mediciones relativas a los casos de negocio para la adquisición de TI en los contratos y en la administración del abastecimiento.				X	1
4	22	Se encuentra disponible una emisión de informes sobre la actividad de adquisición de TI que apoya los objetivos de negocio.				X	1
4	23	La gerencia generalmente es conciente de las excepciones a las políticas y procedimientos para la adquisición de TI.				X	1
4	24	Comienza a desarrollarse una administración estratégica de relacionamiento.			X		0.66
4	25	La gerencia de TI exige el uso del proceso de adquisición y administración de contratos para todas las adquisiciones al revisar las mediciones de desempeño.				X	1
5	26	La gerencia establece recursos de adquisiciones a procesos exhaustivos para la adquisición de TI.				X	1
5	27	La gerencia exige el cumplimiento de las políticas y procedimientos para la adquisición de TI.				X	1
5	28	Se toman mediciones que son relevantes a los casos de negocio para las adquisiciones de TI en los contratos y en la administración del abastecimiento.			X		0.66
5	29	Se establecen buenas relaciones con los proveedores y socios a lo largo del tiempo y la calidad de dichas relaciones es medida y monitoreada. Las relaciones se administran estratégicamente.				X	1
5	30	Los estándares, políticas y procedimientos de TI para la adquisición de recursos de TI se administran estratégicamente y responden a las medidas del proceso.				X	1
5	31	La gerencia de TI comunica la importancia estratégica de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1
	31		TOTAL DEL NIVEL				21.29

Papel de Trabajo	MM09
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Ruedas mágicas, S.A.

Auditoría Interna

Evaluación del proceso de administración de cambios (AI6)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI6 Administrar cambios					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	2	0.000	0.000	0.000
1	0.00	3	0.000	0.000	0.000
2	0.00	2	0.000	0.000	0.000
3	1.33	3	0.443	0.187	0.561
4	8.33	9	0.926	0.391	1.564
5	5.00	5	1.000	0.422	2.110
TOTAL	14.66	24	2.369	1.00	4.235
PRUEBA	14.66	24			84.7%
DIFERENCIA	0	0			NIVEL ACTUAL
FUNCIÓN: Gerencia de Seguridad					
0	0.00	2	0.000	0.000	0.000
1	1.32	3	0.440	0.180	0.180
2	0.00	2	0.000	0.000	0.000
3	1.99	3	0.663	0.271	0.813
4	7.31	9	0.812	0.332	1.328
5	2.64	5	0.528	0.216	1.080
TOTAL	13.26	24	2.443	1.00	3.401
PRUEBA	13.26	24			68.0%
DIFERENCIA	0	0			NIVEL ACTUAL
FUNCIÓN: Gerencia de Desarrollo					
0	0.66	2	0.330	0.131	0.000
1	1.32	3	0.440	0.175	0.175
2	1.32	2	0.660	0.262	0.524
3	1.65	3	0.550	0.219	0.657
4	3.63	9	0.403	0.160	0.640
5	0.66	5	0.132	0.052	0.260
TOTAL	9.24	24	2.515	1.00	2.256
PRUEBA	9.24	24			45.1%
DIFERENCIA	0	0			NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.66	2	0.330	0.045	0.000
1	2.64	3	0.880	0.120	0.120
2	1.32	2	0.660	0.090	0.180
3	4.97	3	1.657	0.226	0.678
4	19.27	9	2.141	0.292	1.168
5	8.30	5	1.660	0.227	1.135
TOTAL	37.16	24	7.328	1.00	3.281
PRUEBA	37.16	24			65.6%
DIFERENCIA	0	0			NIVEL ACTUAL

PROCESO: AI6 Administrar cambios			Que tanto está de acuerdo?				P/T: MM09-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.	x				0
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.	x				0
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.	x				0
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.	x				0
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción causados por una administración deficiente del cambio.	x				0
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.	x				0
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.	x				0
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo.				x	1
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.	x				0
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.		x			0.33
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.				x	1
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.		x			0.33
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.				x	1
4	14	Está establecido un proceso de aprobación para los cambios.				x	1
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.				x	1
4	16	La documentación de configuración generalmente es precisa.				x	1
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.				x	1
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.				x	1
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.				x	1
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.				x	1
5	21	El proceso de revisión refleja los resultados del monitoreo.				x	1
5	22	La información de configuración está automatizada y provee control de versiones.				x	1
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.				x	1
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.				x	1
	24		TOTAL DEL NIVEL				14.66

PROCESO: AI6 Administrar cambios			Que tanto está de acuerdo?				P/T: MM09-02
Función: Gerencia de Seguridad			**Fecha: 20/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.	X				0
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.	X				0
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.			X		0.66
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.			X		0.66
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción causados por una administración deficiente del cambio.	X				0
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.	X				0
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.	X				0
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo.			X		0.66
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.		X			0.33
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.				X	1
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.				X	1
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.			X		0.66
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.				X	1
4	14	Está establecido un proceso de aprobación para los cambios.				X	1
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.		X			0.33
4	16	La documentación de configuración generalmente es precisa.				X	1
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.				X	1
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.			X		0.66
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.			X		0.66
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.			X		0.66
5	21	El proceso de revisión refleja los resultados del monitoreo.			X		0.66
5	22	La información de configuración está automatizada y provee control de versiones.			X		0.66
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.	X				0
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.			X		0.66
	24		TOTAL DEL NIVEL				13.26

PROCESO: AI6 Administrar cambios			Que tanto está de acuerdo?				P/T: MM09-03
Función: Gerencia de Desarrollo			**Fecha: 23/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.		X			0.33
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.		X			0.33
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.		X			0.33
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.			X		0.66
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción causados por una administración deficiente del cambio.		X			0.33
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.			X		0.66
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.			X		0.66
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo.			X		0.66
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.		X			0.33
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.			X		0.66
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.		X			0.33
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.			X		0.66
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.		X			0.33
4	14	Está establecido un proceso de aprobación para los cambios.		X			0.33
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.		X			0.33
4	16	La documentación de configuración generalmente es precisa.		X			0.33
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.		X			0.33
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.			X		0.66
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.		X			0.33
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.		X			0.33
5	21	El proceso de revisión refleja los resultados del monitoreo.		X			0.33
5	22	La información de configuración está automatizada y provee control de versiones.	X				0
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.	X				0
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.	X				0
	24		TOTAL DEL NIVEL				9.24

Ruedas mágicas, S.A.

Auditoría Interna

Papel de Trabajo	MM10
HECHO POR:	E.R.D.M
REVISADO POR:	L.G.D.T
FECHA INICIO:	17-01-2009
FECHA FIN:	25-01-2009

Evaluación del proceso de instalar y acreditar soluciones y cambios (AI7)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de madurez y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D),(E) y (F) se calculan según la fórmula indicada. ∑ (F) = Nivel de Madurez del Proceso.

PROCESO: AI7 Instalar y acreditar soluciones y cambios					
CÓMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE MADUREZ					
FUNCIÓN: Gerencia Departamento de Informática					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE MADUREZ	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/∑D)	NIVEL DE MADUREZ (A*E)
0	0.00	1	0.000	0.000	0.000
1	1.00	3	0.333	0.111	0.111
2	0.00	3	0.000	0.000	0.000
3	2.66	4	0.665	0.222	0.666
4	6.00	6	1.000	0.334	1.336
5	6.00	6	1.000	0.334	1.670
TOTAL	15.66	23	2.998	1.00	3.783
PRUEBA	15.66	23			75.7%
DIFERENCIA	0	0			NIVEL ACTUAL
FUNCIÓN: Gerencia de Seguridad					
0	0.00	1	0.000	0.000	0.000
1	1.00	3	0.333	0.124	0.124
2	0.33	3	0.110	0.041	0.082
3	2.31	4	0.578	0.216	0.648
4	4.98	6	0.830	0.310	1.240
5	4.98	6	0.830	0.310	1.550
TOTAL	13.6	23	2.681	1.00	3.644
PRUEBA	13.6	23			72.9%
DIFERENCIA	0	0			NIVEL ACTUAL
FUNCIÓN: Gerencia de Desarrollo					
0	0.00	1	0.000	0.000	0.000
1	1.99	3	0.663	0.211	0.211
2	1.98	3	0.660	0.210	0.420
3	1.98	4	0.495	0.157	0.471
4	4.31	6	0.718	0.228	0.912
5	3.64	6	0.607	0.193	0.965
TOTAL	13.9	23	3.143	1.00	2.979
PRUEBA	13.9	23			59.6%
DIFERENCIA	0	0			NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.00	1	0.000	0.000	0.000
1	3.99	3	1.330	0.151	0.151
2	2.31	3	0.770	0.087	0.174
3	6.95	4	1.738	0.197	0.591
4	15.29	6	2.548	0.289	1.156
5	14.62	6	2.437	0.276	1.380
TOTAL	43.16	23	8.823	1.00	3.452
PRUEBA	43.16	23			69.0%
DIFERENCIA	0	0			NIVEL ACTUAL

PROCESO: AI7 Instalar y acreditar soluciones y cambios			Que tanto está de acuerdo?				P/T: MM10-01
Función: Gerencia del Departamento			**Fecha: 19/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	Hay una total falta de procesos formales de instalación o acreditación y ni la alta gerencia o el personal de TI reconoce la necesidad de verificar que las soluciones sean adecuadas para el propósito que se pretende.	x				0
1	2	Hay conciencia de la necesidad de verificar y confirmar que las soluciones implementadas sirven para el propósito que se pretende.				x	1
1	3	Se realizan pruebas para algunos proyectos, pero la iniciativa de realizar pruebas es dejada en manos de los equipos individuales de proyecto y los enfoques emprendidos varían.	x				0
1	4	La acreditación y autorización formal es poco frecuente o no existe en absoluto.	x				0
2	5	Hay alguna coherencia entre las pruebas y los enfoques de acreditación, pero típicamente los mismos no se basan en ninguna metodología.	x				0
2	6	Los equipos de desarrollo individual normalmente deciden el método de prueba y hay por lo general ausencia de pruebas de integración.	x				0
2	7	Hay un proceso informal de aprobación.	x				0
3	8	Está establecida una metodología formal relativa a la instalación, migración, conversión y aceptación.				x	1
3	9	Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y están automatizados en cierta medida.				x	1
3	10	Es probable que la capacitación, prueba y transición al estado de producción así como la acreditación varíen en relación al proceso definido, basándose en decisiones puntuales.			x		0.66
3	11	La calidad de los sistemas que entran en producción es desigual, con nuevos sistemas que a menudo generan un nivel significativo de problemas posteriores a la implementación.	x				0
4	12	Los procedimientos son formalizados y desarrollados para que estén bien organizados y sean prácticos, con entornos de prueba y procedimientos de acreditación definidos. En la práctica, todos los grandes cambios a los sistemas siguen este método formal.				x	1
4	13	La evaluación de la satisfacción de los requerimientos de usuario está estandarizada y se puede medir, produciendo métricas que pueden ser revisadas y analizadas efectivamente por la gerencia.				x	1
4	14	La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, con niveles razonables de problemas posteriores a la implementación.				x	1
4	15	La automatización del proceso es ad hoc y depende del proyecto. La gerencia puede estar satisfecha con el nivel actual de eficiencia a pesar de la falta de evaluaciones posteriores a la implementación.				x	1
4	16	El sistema de pruebas refleja adecuadamente el entorno real.				x	1
4	17	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican para los proyectos de gran porte.				x	1
5	18	Los procesos de instalación y acreditación han sido refinados hasta el nivel de la mejor práctica, basados en los resultados del mejoramiento y refinamiento continuo.				x	1
5	19	Los procesos de instalación y acreditación de TI están totalmente integrados en el ciclo de vida del sistema y automatizados donde es conveniente, facilitando la capacitación, prueba y transición al estado de producción de nuevos sistemas de forma más eficiente.				x	1
5	20	Los entornos de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran una transición eficiente y efectiva al entorno de producción.				x	1
5	21	La acreditación tiene lugar por lo general sin reprocesamiento y los problemas posteriores a la implementación están por lo general limitados a correcciones menores.				x	1
5	22	Las revisiones posteriores a la implementación están también estandarizadas, con lecciones aprendidas canalizadas nuevamente al proceso para asegurar una mejora continua de la calidad.				x	1
5	23	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican por igual.				x	1
	23		TOTAL DEL NIVEL				15.66

PROCESO: AI7 Instalar y acreditar soluciones y cambios			Que tanto está de acuerdo?				P/T: MM10-02
Función: Gerencia de Seguridad			**Fecha: 20/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	Hay una total falta de procesos formales de instalación o acreditación y ni la alta gerencia o el personal de TI reconoce la necesidad de verificar que las soluciones sean adecuadas para el propósito que se pretende.	X				0
1	2	Hay conciencia de la necesidad de verificar y confirmar que las soluciones implementadas sirven para el propósito que se pretende.				X	1
1	3	Se realizan pruebas para algunos proyectos, pero la iniciativa de realizar pruebas es dejada en manos de los equipos individuales de proyecto y los enfoques emprendidos varían.	X				0
1	4	La acreditación y autorización formal es poco frecuente o no existe en absoluto.	X				0
2	5	Hay alguna coherencia entre las pruebas y los enfoques de acreditación, pero típicamente los mismos no se basan en ninguna metodología.	X				0
2	6	Los equipos de desarrollo individual normalmente deciden el método de prueba y hay por lo general ausencia de pruebas de integración.		X			0.33
2	7	Hay un proceso informal de aprobación.	X				0
3	8	Está establecida una metodología formal relativa a la instalación, migración, conversión y aceptación.			X		0.66
3	9	Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y están automatizados en cierta medida.			X		0.66
3	10	Es probable que la capacitación, prueba y transición al estado de producción así como la acreditación varíen en relación al proceso definido, basándose en decisiones puntuales.			X		0.66
3	11	La calidad de los sistemas que entran en producción es desigual, con nuevos sistemas que a menudo generan un nivel significativo de problemas posteriores a la implementación.		X			0.33
4	12	Los procedimientos son formalizados y desarrollados para que estén bien organizados y sean prácticos, con entornos de prueba y procedimientos de acreditación definidos. En la práctica, todos los grandes cambios a los sistemas siguen este método formal.				X	1
4	13	La evaluación de la satisfacción de los requerimientos de usuario está estandarizada y se puede medir, produciendo métricas que pueden ser revisadas y analizadas efectivamente por la gerencia.			X		0.66
4	14	La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, con niveles razonables de problemas posteriores a la implementación.			X		0.66
4	15	La automatización del proceso es ad hoc y depende del proyecto. La gerencia puede estar satisfecha con el nivel actual de eficiencia a pesar de la falta de evaluaciones posteriores a la implementación.			X		0.66
4	16	El sistema de pruebas refleja adecuadamente el entorno real.				X	1
4	17	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican para los proyectos de gran porte.				X	1
5	18	Los procesos de instalación y acreditación han sido refinados hasta el nivel de la mejor práctica, basados en los resultados del mejoramiento y refinamiento continuo.				X	1
5	19	Los procesos de instalación y acreditación de TI están totalmente integrados en el ciclo de vida del sistema y automatizados donde es conveniente, facilitando la capacitación, prueba y transición al estado de producción de nuevos sistemas de forma más eficiente.			X		0.66
5	20	Los entornos de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran una transición eficiente y efectiva al entorno de producción.				X	1
5	21	La acreditación tiene lugar por lo general sin reprocesamiento y los problemas posteriores a la implementación están por lo general limitados a correcciones menores.				X	1
5	22	Las revisiones posteriores a la implementación están también estandarizadas, con lecciones aprendidas canalizadas nuevamente al proceso para asegurar una mejora continua de la calidad.			X		0.66
5	23	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican por igual.			X		0.66
	23		TOTAL DEL NIVEL				13.6

PROCESO: AI7 Instalar y acreditar soluciones y cambios			Que tanto está de acuerdo?				P/T: MM10-03
Función: Gerencia de Desarrollo			**Fecha: 23/01/2009**				
NV	**#**	**DECLARACIÓN**	**Nada**	**Un Poco**	**Bastante**	**Completamente**	**Valor de cumplimiento**
0	1	Hay una total falta de procesos formales de instalación o acreditación y ni la alta gerencia o el personal de TI reconoce la necesidad de verificar que las soluciones sean adecuadas para el propósito que se pretende.	X				0
1	2	Hay conciencia de la necesidad de verificar y confirmar que las soluciones implementadas sirven para el propósito que se pretende.				X	1
1	3	Se realizan pruebas para algunos proyectos, pero la iniciativa de realizar pruebas es dejada en manos de los equipos individuales de proyecto y los enfoques emprendidos varían.			X		0.66
1	4	La acreditación y autorización formal es poco frecuente o no existe en absoluto.		X			0.33
2	5	Hay alguna coherencia entre las pruebas y los enfoques de acreditación, pero típicamente los mismos no se basan en ninguna metodología.			X		0.66
2	6	Los equipos de desarrollo individual normalmente deciden el método de prueba y hay por lo general ausencia de pruebas de integración.			X		0.66
2	7	Hay un proceso informal de aprobación.			X		0.66
3	8	Está establecida una metodología formal relativa a la instalación, migración, conversión y aceptación.		X			0.33
3	9	Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y están automatizados en cierta medida.			X		0.66
3	10	Es probable que la capacitación, prueba y transición al estado de producción así como la acreditación varíen en relación al proceso definido, basándose en decisiones puntuales.			X		0.66
3	11	La calidad de los sistemas que entran en producción es desigual, con nuevos sistemas que a menudo generan un nivel significativo de problemas posteriores a la implementación.		X			0.33
4	12	Los procedimientos son formalizados y desarrollados para que estén bien organizados y sean prácticos, con entornos de prueba y procedimientos de acreditación definidos. En la práctica, todos los grandes cambios a los sistemas siguen este método formal.			X		0.66
4	13	La evaluación de la satisfacción de los requerimientos de usuario está estandarizada y se puede medir, produciendo métricas que pueden ser revisadas y analizadas efectivamente por la gerencia.		X			0.33
4	14	La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, con niveles razonables de problemas posteriores a la implementación.			X		0.66
4	15	La automatización del proceso es ad hoc y depende del proyecto. La gerencia puede estar satisfecha con el nivel actual de eficiencia a pesar de la falta de evaluaciones posteriores a la implementación.			X		0.66
4	16	El sistema de pruebas refleja adecuadamente el entorno real.				X	1
4	17	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican para los proyectos de gran porte.				X	1
5	18	Los procesos de instalación y acreditación han sido refinados hasta el nivel de la mejor práctica, basados en los resultados del mejoramiento y refinamiento continuo.		X			0.33
5	19	Los procesos de instalación y acreditación de TI están totalmente integrados en el ciclo de vida del sistema y automatizados donde es conveniente, facilitando la capacitación, prueba y transición al estado de producción de nuevos sistemas de forma más eficiente.			X		0.66
5	20	Los entornos de prueba bien desarrollados, los registros de problemas y los procesos de resolución de fallas aseguran una transición eficiente y efectiva al entorno de producción.				X	1
5	21	La acreditación tiene lugar por lo general sin reprocesamiento y los problemas posteriores a la implementación están por lo general limitados a correcciones menores.			X		0.66
5	22	Las revisiones posteriores a la implementación están también estandarizadas, con lecciones aprendidas canalizadas nuevamente al proceso para asegurar una mejora continua de la calidad.			X		0.66
5	23	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican por igual.		X			0.33
	23		TOTAL DEL NIVEL				13.9

5.2.3 Informe de la evaluación de los controles

Ruedas mágicas, S.A.

Auditoría Interna

Para: **Consejo de Administración**

De: **Auditoría Interna**

Asunto: **Evaluación de controles en los procesos de Adquisición e Implementación de Tecnología Informática**

Fecha: **31/01/2009**

C.C.: **Gerencia General / Gerencia de Informática**

Objetivos

Este informe tiene la finalidad de mostrar los resultados obtenidos en la determinación del nivel de madurez de los controles informáticos aplicados en la adquisición e implementación de tecnología informática y responde a la solicitud de la administración de conocer la situación actual de estos procesos con vista a nuevas inversiones importantes programadas para el futuro cercano.

Alcance

La evaluación fue aplicada a las actividades del departamento de informática realizadas durante el período del 1 de enero al 31 de diciembre de 2008, tomando como base los Objetivos de Control de Información y Tecnología Relacionada, COBIT (por sus siglas en inglés), desde el punto de vista de los procesos incluidos en el dominio de Adquirir e Implementar (AI).

Conclusiones Generales

Los resultados de la evaluación de acuerdo al modelo de madurez establecido por COBIT, muestran que en el departamento de informática de la empresa se administra el control informático en los procesos enmarcados en el dominio de Adquirir e Implementar Tecnología Informática de COBIT, entre los niveles 2-Repetible pero intuitivo y 3-Definido, de una escala máxima de 5, lo cual muestra que se cumplen los objetivos de control de información y tecnología relacionada entre un 50 y 70%.

El dominio de Adquisición e Implementación de Soluciones Informáticas de COBIT agrupa los procesos necesarios para llevar a cabo la estrategia de tecnología informática de la empresa, indicando si los nuevos proyectos generan soluciones que satisfagan las necesidades de información del negocio y son entregados a tiempo y dentro del presupuesto, además indica si los nuevos sistemas trabajarán adecuadamente luego de ser implantados y si los cambios aplicados afectarán las operaciones actuales del negocio.

Conclusiones Específicas

Proceso de Identificar Soluciones Automatizadas

Este proceso muestra la capacidad de la organización para traducir sus requerimientos funcionales y de control a un diseño efectivo y eficiente de soluciones automatizadas técnicamente factibles y rentables.

Los objetivos de control para este proceso incluyen:

1. Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.
2. Reporte de análisis de riesgo.
3. Estudio de factibilidad y formulación de cursos alternativos de acción.
4. Requerimientos, decisión de factibilidad y aprobación.

Conclusiones:
Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Definida”, mostrando un nivel 3 de madurez y un 67% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- Existen enfoques claros y estructurados para determinar las soluciones informáticas.
- El enfoque para la determinación de las soluciones informáticas requiere la consideración de alternativas evaluadas contra los requerimientos del negocio y del usuario, las oportunidades tecnológicas, la factibilidad económica, las evaluaciones de riesgo y otros factores.
- El proceso para determinar las soluciones de tecnología se aplica para algunos proyectos con base en factores tales como las decisiones tomadas por el personal involucrado, la cantidad de tiempo administrativo dedicado, y el tamaño y prioridad del requerimiento original del negocio.
- Se usan enfoques estructurados para definir requerimientos e identificar soluciones de tecnología.

Recomendaciones
Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Establecer la metodología adecuada para la identificación y evaluación de soluciones de tecnología informática y que ésta se aplique a la mayoría de proyectos.
- Mejorar la calidad de la documentación de los proyectos y aprobar adecuadamente cada etapa.

- Articular claramente los requerimientos de acuerdo a las estructuras predefinidas.
- Considerar soluciones tecnológicas alternativas, donde se analicen también los costos y beneficios.
- Clarificar la metodología establecida y que ésta se defina, se entienda y puedan medirse sus los resultados.
- Que exista un enlace claro entre la gerencia de informática y la gerencia general.

Adquirir y mantener software aplicativo

Este proceso muestra la capacidad de la organización para proporcionar soluciones automatizadas que soporten efectivamente al negocio, definiendo claramente sus requerimientos funcionales y operacionales brindando implementaciones estructuradas y con entregables claros.

Los objetivos de control para este proceso incluyen:

1. Diseño de alto nivel.
2. Diseño detallado.
3. Control y auditabilidad de las aplicaciones.
4. Seguridad y disponibilidad de las aplicaciones.
5. Configuración e implantación de software aplicativo.
6. Actualizaciones importantes en sistemas existentes.
7. Desarrollo de software aplicativo.
8. Aseguramiento de la calidad del software.
9. Administración de los requerimientos de aplicaciones.
10. Mantenimiento de software aplicativo.

Conclusiones:
Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Definida”, mostrando un nivel 3 de madurez y un 68% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- Existe un proceso claro, definido y de comprensión general para la adquisición y mantenimiento de software aplicativo.
- Este proceso va de acuerdo con la estrategia de tecnología informática del negocio.
- Se intentan aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos.

- Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que no se cumpla con todos los pasos.
- Las actividades de mantenimiento se planean, programan y coordinan.

Recomendaciones
Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Definir un proceso adecuado para la adquisición y mantenimiento de software aplicativo y alinear las prácticas con el proceso definido.
- Utilizar un enfoque aplicable para toda la empresa, basado en componentes, con aplicaciones predefinidas y estandarizadas que correspondan a las necesidades del negocio.
- Establecer una metodología avanzada que permita un posicionamiento estratégico rápido, un alto grado de reacción y flexibilidad para responder a los requerimientos cambiantes del negocio.
- La metodología establecida debe estar sujeta a mejora continua y respaldada con bases de datos internas y externas que contengan material de referencias y se base en las mejores prácticas.
- La metodología establecida debe producir la documentación necesaria dentro de una estructura predefinida que haga eficiente la producción y el mantenimiento.

Adquirir y mantener infraestructura tecnológica:

Este proceso muestra la capacidad de la organización para proporcionar las plataformas apropiadas de hardware y software del sistema que soporten las aplicaciones del negocio.

Los objetivos de control para este proceso incluyen:

1. Plan de adquisición de infraestructura tecnológica.
2. Protección y seguridad del recurso de infraestructura.
3. Mantenimiento de la infraestructura.
4. Ambiente de prueba y factibilidad.

Conclusiones:
Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Definida”, mostrando un nivel 3 de madurez y un 70% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- Existe un proceso claro, definido y generalmente comprendido para adquirir y dar mantenimiento a la infraestructura tecnológica.
- El proceso respalda las necesidades de aplicaciones críticas del negocio y concuerda con la estrategia de tecnología del negocio, pero no se aplica de forma consistente.
- Se planea, programa y coordina el mantenimiento de la infraestructura tecnológica.
- Existen ambientes separados para prueba y producción.

Recomendaciones
Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Desarrollar este proceso hasta el punto de funcionar bien para la mayoría de situaciones y que permita darle un seguimiento consistente.
- Que la infraestructura de tecnología informática soporte adecuadamente las aplicaciones del negocio mediante su correcta adquisición y mantenimiento.
- Organizar adecuadamente este proceso y aplicarlo de manera preventiva.
- Optimizar parcialmente los tiempos de realización para alcanzar el nivel esperado de escalamiento, flexibilidad e integración.

Facilitar la operación y el uso:

Este proceso muestra la capacidad de la organización para el desarrollo y mantenimiento de procedimientos relacionados con la tecnología informática que garanticen el uso apropiado de las aplicaciones y de las soluciones tecnológicas establecidas.

Los objetivos de control para este proceso incluyen:

1. Plan para soluciones de operación.
2. Transferencia de conocimiento a la gerencia del negocio.
3. Transferencia de conocimiento a los usuarios finales.
4. Transferencia de conocimiento al personal de operaciones y soporte.

Conclusiones:
Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Repetible pero intuitiva”, mostrando un nivel 2 de madurez y un 54% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- Se utilizan enfoques similares para generar procedimientos y documentación, pero no se basan en un enfoque estructural o marco de trabajo.
- No existe un enfoque uniforme para el desarrollo de procedimientos de usuarios y de operación.
- Individuos y equipos de proyectos generan los materiales de entrenamiento, y la calidad depende de los individuos que se involucran.
- Los procedimientos y la calidad del soporte a usuarios van desde pobre a muy buena, con una consistencia e integración muy pequeña a lo largo de la organización.
- Se proporcionan o facilitan programas de entrenamiento para el negocio y los usuarios, pero no hay un plan general para ofrecer o dar entrenamiento.

Recomendaciones

Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Definir un esquema para los procedimientos de mantenimiento y los materiales de entrenamiento que cuenten con el soporte de la administración de tecnología informática.
- Los procedimientos de mantenimiento y los materiales de entrenamiento deben cubrir todos los sistemas y las unidades del negocio, además de estar integrados por medio de interdependencias e interfaces.
- Implementar controles que garanticen el cumplimiento de estándares y que se desarrollan y mantienen procedimientos para todos los procesos.
- Recopilar y evaluar toda la retroalimentación que brindan los funcionarios del negocio y usuarios en general, para mantener un proceso continuo de mejora.
- Generalmente los materiales de documentación y entrenamiento deben encontrarse en buen nivel, predecibles, confiables y disponibles.
- Implementar un proceso de emergencia para el uso de documentación y administración automatizada de los procedimientos.
- Integrar progresivamente el desarrollo automatizado de procedimientos con el desarrollo de sistemas aplicativos, para facilitar la consistencia y el acceso de usuarios.
- El entrenamiento de funcionarios de negocio y usuarios en general debe ir de acuerdo a las necesidades del negocio.
- Se debe desarrollar y entregar documentación, materiales y programación de entrenamiento por parte del departamento de informática.

Adquirir recursos de tecnología informática:

Este proceso muestra la capacidad de la organización para suministrar recursos de tecnología informática, que incluyen personas, hardware, software y servicios. Además la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste a arreglos contractuales y la adquisición en sí, todo con la finalidad de garantizarle a la organización, contar con los recursos te tecnología informática necesarios de manera oportuna y rentable.

Los objetivos de control para este proceso incluyen:

1. Control de adquisición.
2. Administración de contratos con proveedores.
3. Selección de proveedores.
4. Adquisición de software.
5. Adquisición de recursos de desarrollo.
6. Adquisición de infraestructura, instalaciones y servicios relacionados.

Conclusiones:
Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Definida”, mostrando un nivel 3 de madurez y un 67% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- La administración establece políticas y procedimientos para la adquisición de tecnología informática.
- Las políticas y procedimientos toman como guía el proceso general de adquisición de la organización.
- La adquisición de tecnología se integra en gran parte con los sistemas generales de adquisición del negocio.
- Existen estándares de tecnología para la adquisición de recursos de ese tipo.
- Los proveedores se integran dentro de los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.
- La administración de tecnología informática comunica la necesidad de contar con una administración adecuada de adquisiciones y contratos en toda la función de tecnología informática.

Recomendaciones

Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Integrar totalmente la adquisición de tecnología informática con los sistemas generales de adquisición de la empresa.
- Utilizar los estándares de adquisición de recursos de tecnología informática en todos los procesos de adquisición.
- Tomar las medidas necesarias para la administración de contratos y adquisiciones relevantes donde de requiera la compra de tecnología informática.
- Debe disponerse de reportes para sustentar los objetivos de negocio.
- La administración general debe estar generalmente consciente de las excepciones a las políticas y procedimientos para la adquisición de tecnología informática.
- Debe iniciarse el desarrollo de una administración estratégica de relaciones con proveedores de recursos de tecnología.
- La gerencia de informática debe implantar el uso de procesos de administración de adquisiciones y contratos relacionados con la tecnología, en todas las adquisiciones, mediante la revisión periódica de mediciones de desempeño.

Administración de cambios:

Este proceso muestra la capacidad de la organización para la administración de cambios a las aplicaciones, por medio de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura actual de tecnología informática.

Los objetivos de control para este proceso incluyen:

1. Estándares y procedimientos para cambios.
2. Evaluación de impacto, priorización y autorización.
3. Cambios de emergencia.
4. Seguimiento y reporte del estatus del cambio.
5. Cierre y documentación del cambio.

Conclusiones:

Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Definida”, mostrando un nivel 3 de madurez y un 66% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- Existe un proceso formal y definido para la administración de cambios, que incluye categorizar, asignar prioridades, procedimientos de emergencia, autorización de cambios y administración de liberaciones, pero su cumplimiento aun va surgiendo.
- Se dan soluciones temporales a los problemas y los procesos a menudo se omiten.
- Aún pueden darse errores y los cambios no autorizados ocurren ocasionalmente.
- El análisis de impacto de los cambios de tecnología informática y en operaciones de negocio se está volviendo formal, para apoyar la implantación planeada de nuevas aplicaciones y tecnologías.

Recomendaciones

Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Este proceso debe revisarse de forma regular y debe actualizarse para lograr permanecer de acuerdo a las buenas prácticas. Esta revisión debe reflejar los resultados del monitoreo.
- La información de la configuración debe ser computarizada y proporcionar un control confiable de las versiones.
- Sofisticar el rastreo de cambios e incluir herramientas que permitan detectar software no autorizado y sin licencia.
- Integrar la administración de cambios en tecnología informática con la administración de cambios del negocio, para garantizar que la tecnología informática posibilite el incremento de productividad y la creación de nuevas oportunidades de negocio.

Instalar y acreditar soluciones y cambios:

Este proceso muestra la capacidad de la organización para contar con sistemas nuevos o modificados que se desarrollen sin problemas importantes después de la instalación y así garantizar que los sistemas operacionales estén en línea con las expectativas convenidas y con los resultados esperados.

Los objetivos de control para este proceso incluyen:

1. Programas de entrenamiento y capacitación.
2. Establecer un plan de pruebas.
3. Establecer un plan de implementación.
4. Establecer un ambiente separado para pruebas.
5. Conversión de sistema y datos.
6. Pruebas integrales.
7. Prueba final y aceptación.
8. Transferencia a producción.
9. Liberación de software.
10. Distribución del sistema.
11. Registro y rastreo de cambios.
12. Revisión posterior a la implementación.

Conclusiones:

Se determinó que en el departamento de informática se administran los controles sobre este proceso de forma “Definida”, mostrando un nivel 3 de madurez y un 69% de confiabilidad en los objetivos de control informático antes mencionados, de acuerdo a lo siguiente:

- Se cuenta con una metodología formal en relación con la instalación, migración, conversión y aceptación de soluciones informáticas.
- Los procesos de tecnología para la instalación y acreditación están integrados dentro del ciclo de vida del sistema y están automatizados hasta cierto punto.
- El entrenamiento, pruebas y transición y acreditación a producción tienen muy probablemente variaciones respecto al proceso definido, con base en las decisiones individuales.
- La calidad de los sistemas que pasan a producción es inconsistente, y los nuevos sistemas a menudo generan un nivel significativo de problemas posteriores a la implantación.

Recomendaciones

Con la finalidad de cubrir la brecha existente entre el nivel de madurez deseado por la administración para este proceso y el nivel determinado en esta evaluación, se recomienda lo siguiente:

- Deben formalizarse los procedimientos y desarrollarse de forma organizada y práctica con ambientes de prueba definidos y con procedimientos de acreditación. En la práctica todos los cambios mayores de sistemas deben seguir este enfoque formal.

- Estandarizar y hacer medible la evaluación de la satisfacción de los requerimientos del usuario, para producir información que la gerencia pueda revisar y analizar de forma práctica y efectiva.
- Los sistemas que entran en producción deben ser de suficiente calidad para lograr satisfacer a la gerencia, aunque presenten niveles razonables de problemas posteriores a la implantación.
- Los sistemas de prueba deben reflejar adecuadamente el ambiente de producción.
- En proyectos mayores deben aplicarse pruebas de stress para los nuevos sistemas y pruebas de regresión para los sistemas existentes.

Las anteriores conclusiones y recomendaciones fueron discutidas y aceptadas por el Gerente del Departamento de Informática, comprometiéndose a implementar las mejoras en el transcurso de seis meses, sujeto a verificación por parte de Auditoría Interna por medio del monitoreo y la evaluación al finalizar el tiempo propuesto.

Lic. Luis Guillermo Dionicio Teo
Auditor Interno

CONCLUSIONES

1. La falta de conocimiento de la normativa y modelos internacionales de control informático en un departamento de Auditoría Interna de una empresa distribuidora de vehículos automotores, que le permita asesorar a la administración y supervisar el control informático, incide negativamente en el logro de sus objetivos empresariales y no permite obtener el retorno esperado de las inversiones que realice la administración en recursos tecnológicos, debido a la alta dependencia de sus operaciones sobre la tecnología informática.

2. La falta de un Comité de Dirección que guíe y supervise las actividades del Departamento de Informática de una empresa distribuidora de vehículos automotores que procesa su información por medio de sistemas computarizados, no permite alinear los objetivos de la tecnología informática con los objetivos del negocio mediante la transmisión oportuna de los planes estratégicos de la compañía, principalmente en materia de adquisición e implementación de tecnología informática.

3. La Auditoría Interna de la empresa evaluada carece de medios para establecer la situación actual de los controles informáticos de acuerdo a criterios de medición de aceptación general a nivel internacional como COBIT, que le permitan medir el cumplimiento de los objetivos de control y determinar la fiabilidad de la información generada por la tecnología informática después de la implementación de nuevas soluciones o cambios a sistemas existentes.

4. La empresa evaluada no cuenta con un marco de trabajo en base a los Objetivos de Control para Información y Tecnología Relacionada (COBIT) que le permita implantar un gobierno de tecnología informática que proporcione las herramientas de control y monitoreo necesarias para minimizar los riesgos sobre la información.

5. De acuerdo a la evaluación del nivel de madurez de los controles informáticos en la empresa evaluada, Auditoría Interna pudo determinar que en el departamento de informática de la empresa evaluada no se cuenta con el nivel de madurez suficiente en los procesos incluidos en el dominio de adquisición e implementación de tecnología informática de los objetivos de control para información y tecnología relacionada (COBIT), de acuerdo a los requerimientos de confiabilidad definidos por la administración para garantizar razonablemente que las nuevas soluciones informáticas continuarán proporcionando la información confiable y oportuna que necesita para el logro de sus objetivos.

RECOMENDACIONES

1. Que el departamento de Auditoría Interna de las empresas distribuidoras de vehículos automotores que procesen su información por sistemas computarizados, conozca la normativa internacional que rige su actuación y los modelos de control como el de los Objetivos de Control para Información y Tecnología Relacionada (COBIT) que le permitan brindar a la administración la asesoría necesaria y pueda realizar la debida supervisión y monitoreo sobre los controles relacionados con la tecnología informática.

2. Establecer un enlace entre el departamento de informática y la alta administración por medio de un Comité de Dirección que guíe y supervise su actuación, transmitiendo oportunamente las necesidades de información del negocio para alinearlos con los objetivos de la tecnología informática de las empresas distribuidoras de vehículos automotores que procesen su información con sistemas computarizados.

3. Que Auditoría Interna de Sistemas Informáticos utilice criterios de medición como el modelo de madurez establecido por COBIT para la evaluación del cumplimiento de controles y criterios de calidad de la información generada por la tecnología informática, con la finalidad de aportar valor agregado a su trabajo y minimizar los riesgos asociados a la seguridad de la información.

4. Mediante la evaluación del costo/beneficio, se implante el marco de trabajo de los Objetivos de Control y Tecnología Relacionada (COBIT) en una empresa distribuidora de vehículos automotores con el objetivo de garantizar la alineación de la tecnología informática con los requerimientos del negocio y se asegure razonablemente el cumplimiento de las metas del negocio.

5. Que la administración considere las recomendaciones sugeridas por Auditoría Interna en base a la evaluación de controles informáticos de acuerdo a COBIT, ya que son necesarias para alcanzar los niveles de madurez requeridos para los procesos de adquisición e implementación que realiza el departamento de informática de la empresa.

BIBLIOGRAFÍA

1. Asociación de Auditoría y Control de Sistemas Informáticos. COBIT 4.0. Estados Unidos de América. 2005. Pág. 201

2. Asociación de Auditoría y Control de Sistemas Informáticos. DIRECTRICES DE AUDITORÍA COBIT. Estados Unidos de América. 2ª Edición. 1998. Pág. 222

3. Asociación de Auditoría y Control de Sistemas Informáticos. MANUAL DE PREPARACIÓN AL EXAMEN CISA. Estados Unidos de América. 2008. Pág. 693

4. Barrios Pérez, Luis Emilio. PRONTUARIO DE LEYES FISCALES. Ediciones Legales Comercio e Industria. Guatemala 2008.

5. Barrios Pérez, Luis Emilio. CÓDIGO TRIBUTARIO Y ÚLTIMAS REFORMAS INCORPORADAS. Ediciones Legales Comercio e Industria. Guatemala 2007.

6. Echenique García, José Antonio. AUDITORÍA EN INFORMÁTICA. Editorial McGraw Hill. México 2001.

7. ENCICLOPEDIA DE LA AUDITORÍA. España, Océano Grupo Editorial, S.A. 1999 Versión española de la segunda edición de la obra original “Cashin’s Handbook for Auditor”. Pág. 1250

8. Fonseca Borja, Rene Dr. AUDITORÍA INTERNA UN ENFOQUE MODERNO DE PLANIFICACIÓN, EJECUCIÓN Y CONTROL. Editorial Artes Gráficas Acrópolis. Guatemala 2004. Pág. 835

9. Hernández Hernández, Enrique. AUDITORÍA EN INFORMÁTICA: UN ENFOQUE METODOLÓGICO Y PRÁCTICO. Editorial CECSA, México 2000. Pág. 323.

10. Instituto Mexicano de Contadores Públicos, MANUAL DE NORMAS INTERNACIONALES DE AUDITORÍA Y CONTROL DE CALIDAD. México 2009. Pág. 950

11. Muñoz Razo, Carlos. AUDITORÍA EN SISTEMAS COMPUTACIONALES. Editorial Pearson Education. México 2002. Pág. 796

12. Página web, Asociación de Auditoría y Control de Sistemas Informáticos. www.isaca.org/cobit

13. Página web, Instituto de Auditoría Interna. www.theiia.org

14. Página web, Instituto de Gobierno de Tecnología Informática. www.itgi.org

15. Página web, Manual de Auditoría de Sistemas. www.monografías.com

16. Página web, Normas Generales para la Auditoría de los Sistemas de Información. www.isaca.org.pe/normas.htm

17. Página web, Superintendencia de Administración Tributaria (SAT). http://portal.sat.gob.gt/sitio/index

18. Pederiva, Andrea. The Cobit Maturity Model in a Vendor Evaluation Case (El modelo de madurez Cobit en un Caso de Evaluación de Proveedor). Traducción libre. P. 35-38. ISACA: Information Systems Control Journal. Vol. 3. 2003.

19. Ramos Rosales, Edwin Ernesto. AUDITORÍA INTERNA EN EL DEPARTAMENTO DE INFORMÁTICA DE UNA INSTITUCIÓN BANCARIA. Tesis, Facultad de Ciencias Económicas. Universidad de San Carlos de Guatemala. Noviembre 2007. Pág. 179

GLOSARIO

Actividad: Las medidas principales tomadas para operar el proceso COBIT.

Administración del desempeño: La capacidad de administrar cualquier tipo de medición incluyendo mediciones de empleados, equipo, proceso, operativas y financieras. El término denota un control de ciclo cerrado y la vigilancia periódica de la medición.

Arquitectura de la información: Ver arquitectura de TI.

Arquitectura de TI: Un marco integrado para evolucionar o dar mantenimiento a la tecnología informática existente y adquirir nueva, para alcanzar las metas estratégicas y de negocio de la empresa.

Arquitectura empresarial: Mapa de rutas tecnológicas orientado al negocio para el logro de sus metas y objetivos de negocio.

Arquitectura empresarial para TI: Respuesta a la entrega de TI, provista por procesos claramente definidos usando sus recursos (aplicaciones, información, infraestructura y personas).

Autenticación: El acto de verificar la identidad de un usuario y su elegibilidad para acceder a la información computarizada. Está diseñada para proteger contra conexiones de acceso fraudulentas.

Continuidad: Prevenir, mitigar y recuperarse de una interrupción.

Desempeño: La implantación real o el logro de un proceso.

Diccionario de datos: Un conjunto de meta-datos que contiene definiciones y representaciones de elementos de datos.

Directriz: La descripción de un modo particular de lograr algo, la cual es menos prescriptiva que un procedimiento.

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

Estándar: Una práctica de negocio o producto tecnológico que es una práctica aceptada, avalada por la empresa o por el equipo gerencial de TI. Los estándares se pueden implantar para dar soporte a una política o proceso, o como respuesta a una necesidad operativa. Así como políticas, los estándares deben incluir una descripción de la forma en que se detectará el incumplimiento.

Estatuto de Auditoría: Documento que define el propósito, la autoridad y la responsabilidad de la actividad de auditoria interna, aprobado por el consejo.

Gobierno: El método por medio del cual una organización es dirigida, administrada o controlada.

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

Madurez: Indica el grado de confiabilidad o dependencia que el negocio puede tener en un proceso, al alcanzar las metas y objetivos deseados.

Marco de control: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.

Marco de trabajo: Ver marco de control.

Métrica: Un estándar para medir el desempeño contra la meta.

Plan estratégico de TI: Un plan a largo plazo, ej. con un horizonte de tres a cinco años, en el cual la gerencia del negocio de y de TI describen de forma cooperativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).

Propietarios de datos: Individuos, por lo general gerentes o directores, que tienen la responsabilidad de la integridad, el uso y el reporte preciso de los datos computarizados.

Proveedores de servicios: Organización externa que presta servicios a la organización.

Riesgo: El potencial de que una amenaza específica explote las debilidades de un activo o grupo de activos ocasionando pérdida y/o daño. Por lo general se mide por medio de una combinación de probabilidad e impacto.

TI: Tecnología de Información.

Usuario: Una persona que utiliza los sistemas empresariales.