UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

"DESARROLLO DE UNA METODOLOGÍA PARA EL PROCESO DE ASEGURAMIENTO DEL CONTROL INTERNO EN LAS ADQUISICIONES EN TECNOLOGÍAS DE INFORMACIÓN BASADA EN COBIT 4.1 Y EN LAS GUÍAS DE ASEGURAMIENTO DE ISACA, PARA LA DIRECCIÓN DE TECNOLOGÍA DE INFORMACIÓN TRIBUTARIA DE LA DIRECCIÓN GENERAL DE TRIBUTACIÓN DEL MINISTERIO DE HACIENDA".

Trabajo final de investigación aplicada aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas, de la Universidad de Costa Rica, como requisito parcial para optar por el grado de Maestría Profesional en Auditoría de Tecnologías de Información.

MARISOL MADRIGAL CALDERÓN

Carné 946082

Ciudad Universitaria Rodrigo Facio, San José, Costa Rica

Año 2013

DEDICATORIA

Dedico el presente trabajo de graduación a mi madre querida, por su apoyo incondicional y por ser un ejemplo de esfuerzo y superación en mi vida.

AGRADECIMIENTO

En primera instancia agradezco a Dios por darme la salud necesaria para concluir esta etapa en mi vida, por poner en mi camino a las personas que de una u otra forma me han ayudado a lo largo de todo el programa de estudios.

Expreso mi más profundo agradecimiento a Reinier Soto Cordero por confiar en mí y darme el apoyo necesario para poder realizar el presente trabajo en la DTIT de la DGT del Ministerio de Hacienda, a Noily Navarrete Gutiérrez por su ayuda desinteresada, calidad de servicio y atención.

También deseo manifestar mi agradecimiento a don Xiomar Rojas Delgado por el apoyo demostrado a lo largo de toda la Maestría, a don Sergio Espinoza Guido por pronta ayuda en la conclusión del presente trabajo, a los profesores por compartir con nosotros sus conocimientos y experiencias, a Ignacio Salas Segura por su apoyo y servicio en diferentes temas vistos a través de los cursos de la maestría y muy especialmente a mi compañera de estudios Rosibel Ruiz Hernández, por su alto valor de compañerismo, por tantas noches de duro trabajo, motivando constantemente para llevar a buen término la conclusión del programa de estudios.

A todas las personas mencionadas anteriormente y a las que formaron parte de este proceso en forma directa o indirecta, muchas gracias.

El presente trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar por el grado de Maestría Profesional en Auditoría de Tecnologías de Información.

_____	_____
Dr. Aníbal Barquero Chacón **Director Programa de Posgrado en Administración y Dirección de Empresas**	Dr. Sergio Espinoza Guido **Profesor Coordinador**
_____	_____
MSc. Xiomar Delgado Rojas **Profesor Guía**	MCI. Noily Navarrete Gutiérrez **Supervisora Laboral**

_____

Marisol Madrigal Calderón
Sustentante

CONTENIDO

RESUMEN

Esta práctica profesional se realizó como requisito para optar por el grado de Máster en Administración y Dirección de Empresas con énfasis en Auditoría de Tecnologías de Información, y comprende la elaboración de una metodología para las adquisiciones de tecnologías de información que se realizan en la Dirección de Tecnología de Información Tributaria de la Dirección General de Tributación del Ministerio de Hacienda, de acuerdo con el dominio “Adquirir e Implementar” del marco de control COBIT 4.1 y las guías de aseguramiento de ISACA.

Se determinó que este proyecto estaba definido para ser elaborado en seis capítulos, tal como se detalla a continuación:

El capítulo I indica cuáles son los objetivos del trabajo por desarrollar, así como una breve reseña de la Institución donde se realizó el proyecto y la importancia que tiene el tema central en el área de estudio.

El capítulo II brinda conceptos de importancia para el entendimiento del trabajo realizado así como una descripción del significado de las adquisiciones, adquisiciones de TI, mejores prácticas utilizadas en las adquisiciones de TI, así como los beneficios esperados en la aplicación de las mejores prácticas.

El capítulo III plantea un diagnóstico sobre la situación real de la DTIT con respecto al control interno de las adquisiciones de TI, qué normativa se aplica, cuál es la gestión de riesgos utilizada y cuál es el análisis de la situación actual de la DTIT en la materia antes mencionada.

El capítulo IV presenta un análisis de la situación diagnosticada, mostrando cómo debería ser el funcionamiento del Sistema Específico de Valoración de Riesgos Institucional e identificando cuáles son los riesgos asociados a las adquisiciones en tecnologías de información de acuerdo con las mejores prácticas.

La propuesta de la metodología se presenta en el capítulo V, junto con una explicación del uso de las mejores prácticas.

El capítulo VI presenta las conclusiones y recomendaciones del estudio realizado y la importancia que tiene para la DTIT el aplicar la normativa vigente de TI complementada con el uso de las mejores prácticas existentes en la materia.

ÍNDICE DE CUADROS

ÍNDICE DE ABREVIATURAS

DGT	Dirección General de Tributación
DTIT	Dirección de Tecnología de Información Tributaria
TI	Tecnologías de Información
AI	Adquirir e Implementar
CGR	Contraloría General de la República
COBIT	(*Control Objetive for Information and Related Technologies*) Objetivos de Control para la Información y Tecnología Relacionada.
SDLC	(*Systems Development Life Cycle*) Ciclo de Vida del Desarrollo de Sistemas
CMM	Modelo de Madurez de la Capacidad

INTRODUCCIÓN

La tecnología ha venido a modificar la forma de operar de muchas organizaciones, los avances tecnológicos han modificado la percepción que se tenía de hacer negocios, por ello cada vez son más las organizaciones que necesitan adaptarse a estos cambios y en muchas ocasiones esto implica cambiar la estructura organizacional, su forma de hacer las cosas, su método de registrar la información y por ende, cambiar la cultura organizacional.

La información es, en la actualidad, uno de los activos más valiosos de cualquier institución, por lo que contar con adecuadas adquisiciones de tecnologías de información, que brinden a la administración confiabilidad, integridad y disponibilidad de la información, es un aspecto de mucha relevancia.

Toda organización debe velar por la adecuada adquisición de sus tecnologías de información ya que de esto depende el éxito o fracaso de sus proyectos de TI, y el sector gubernamental no escapa a esta situación.

La tecnología avanza a pasos agigantados, el requerimiento de información veraz, confiable y oportuna es una necesidad que las organizaciones han venido a cubrir con la adquisición de tecnologías de información que le brindan las herramientas necesarias para el manejo eficaz y eficiente de la información.

El presente trabajo de graduación pretende desarrollar e implementar una metodología para el proceso de adquisiciones de tecnologías de información (*software y hardware*) basada en las mejores prácticas existentes en el mercado, para ser aplicada en la Dirección de Tecnología de Información Tributaria de la Dirección General de Tributación del Ministerio de Hacienda, con el fin de que dicha área pueda contar con una herramienta actualizada que le sea de utilidad para agilizar el proceso de compras y adquisiciones de TI, así como de garantizar la confiabilidad de que el *hardware y software* adquiridos cumplen con los requerimientos y necesidades de los servicios brindados por la Dirección de Tecnología de Información Tributaria a todos sus usuarios.

Considerando lo descrito anteriormente, es importante recalcar la importancia que tienen las TI para las adquisiciones realizadas por las instituciones gubernamentales, dado que actualmente el Ministerio de Hacienda tramita la mayoría de sus compras por medio del sistema Compra Red, que es un servicio en línea que permite a las instituciones del Sector Público, dar a conocer por medio de Internet, sus demandas de bienes y servicios, a su vez, los proveedores pueden participar con sus ofertas y dar seguimiento a los procesos de la contratación administrativa, además del anterior, también se cuenta con el sistema MerLink, el cual debe implementarse en todas las instituciones estatales a partir del 2014 como única plataforma tecnológica de compras públicas, que permitirá a las proveedurías del sector gubernamental realizar transacciones de compra y venta de bienes y servicios en forma electrónica .

Intereses profesionales

Desarrollar este trabajo final de graduación de Maestría en Auditoría en Tecnologías de Información en la Dirección de Tecnología de Información Tributaria (DTIT), de la Dirección General de Tributación del Ministerio de Hacienda es un gran aporte profesional que consiste en el diseño de una metodología para el proceso de aseguramiento del control interno en las adquisiciones en tecnologías de información, que permitirá poner en práctica los conocimientos adquiridos a lo largo de la maestría.

Justificación

Dada la importancia que tiene para el Ministerio de Hacienda la aplicación de buenas prácticas en tecnologías de información, la Dirección de Tecnología de Información Tributaria está en proceso de capacitar a sus funcionarios en el uso y aplicación de COBIT 4.1, por lo que consideran que una metodología basada en el dominio de “Adquirir e Implementar” de COBIT, sería un trabajo de mucha ayuda para ellos en el desarrollo de sus funciones.

Aporte

El presente trabajo brindará una herramienta mediante el uso del marco de control COBIT 4.1 y las guías de aseguramiento de ISACA para la Dirección de Tecnología de Información Tributaria, de la Dirección General de Tributación del Ministerio de Hacienda, dada la necesidad de contar con una metodología en adquisiciones de TI basada en las mejores prácticas existentes.

Alcance

La presente metodología se desarrollará de setiembre de 2012 a mayo de 2013, tomando como base el dominio “Adquirir e Implementar” del marco de control COBIT 4.1, así como las guías de aseguramiento de ISACA.

Limitaciones y cambios

1. Dado que la metodología elaborada consta de un aproximado de ochocientas preguntas, por limitaciones de tiempo y recurso humano disponible no fue posible su aplicación.
2. Debido a que en el desarrollo del Capítulo III. Diagnóstico de la Situación Actual del Tema, se evidenció la ausencia de una metodología para el control interno de las adquisiciones en TI, la falta de una valoración del riesgo imposibilitó el desarrollo del Capítulo lV Análisis de la Situación Diagnosticada, por lo que, en su lugar se propuso un esquema para identificar los riesgos presentes de acuerdo con la CGR y el uso de las mejores prácticas.
3. Al apartado 2.1 de Definiciones se agregaron más conceptos necesarios para el buen entender del trabajo desarrollado.

CAPÍTULO I. UBICACIÓN DEL TEMA EN EL CONTEXTO

1.1. Título del Proyecto

Desarrollo de una metodología para el proceso de aseguramiento del control interno en las adquisiciones en tecnologías de información basada en COBIT 4.1 y en las guías de aseguramiento de ISACA, para la Dirección de Tecnología de Información Tributaria de la Dirección General de Tributación del Ministerio de Hacienda.

1.2. Objetivo general

Diseñar e implementar, para la Dirección de Tecnología de Información Tributaria de la Dirección General de Tributación del Ministerio de Hacienda, una metodología para el proceso de aseguramiento del control interno de las adquisiciones de tecnologías de información basada en COBIT 4.1 y en las guías de aseguramiento de ISACA, con la finalidad de aplicar el uso de las mejores prácticas existentes sobre el tema.

1.3. Objetivos específicos

1. Revisar el método actual aplicado por la Dirección de Tecnología de Información Tributaria de la Dirección General de Tributación del Ministerio de Hacienda, en lo referente a las adquisiciones en tecnologías de información, con la finalidad de conocer las prácticas utilizadas en cuanto al aseguramiento de su control interno.
2. Analizar los riesgos actuales relacionados con las adquisiciones de tecnologías de información para conocer si existen algunos que puedan ser materializados por falta de control en la Dirección.
3. Desarrollar un procedimiento con base en COBIT 4.1 (dominio: Adquirir e Implementar) y en las guías de aseguramiento de ISACA, para ser

utilizados en las adquisiciones de tecnologías de información que se realicen en la DTIT.

1.4. Ministerio de Hacienda

1.4.1 Reseña Histórica Del Ministerio de Hacienda Costarricense[1]

Siendo Presidente José Rafael de Gallegos, en 1825, se emitió el Decreto LV, mediante el cual se estableció la Tesorería General de Hacienda del Estado y su Caja principal. Allí, se puede afirmar que surge el Ministerio de Hacienda, con la misión de administrar todas las rentas del Estado. Dicho decreto fue emitido el catorce de octubre del año indicado. Posteriormente, la Tesorería General de Hacienda del Estado se convirtió en el Ministerio de Hacienda, dando paso a una entidad pública de suma importancia para el país.

1.4.2 Rol del Ministerio como ente rector del sector financiero[2]

El Sector Financiero, Monetario y Supervisión está integrado por las siguientes instituciones: Ministerio de Hacienda, bancos estatales comerciales, Banco Popular y de Desarrollo Comunal, Instituto Nacional de Seguros (INS), Banco Central de Costa Rica, Autoridad Reguladora de los Servicios Públicos (ARESEP), Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), Superintendencia de Telecomunicaciones

---

[1] Información tomada del Curso Virtual Reinducción General al Ministerio de Hacienda. Primera Edición. Elaborada por el señor Eugenio Redondo Gómez, funcionario del Centro de Investigación y Formación Hacendaria y actualizada por las señoras Celia White Ward y Cynthia Díaz Hernández, Sétima Edición. Agosto 2011.

[2] Redondo Gómez, Eugenio. Centro de Investigación y Formación Hacendaria. Op. Cit.

(SUTEL), Superintendencia de Pensiones (SUPEN), Superintendencia General de Entidades Financieras (SUGEF), la Superintendencia General de Valores (SUGEVAL), Superintendencia de Seguros (SUGESE), además de los órganos adscritos al Ministerio mismo.

Según el artículo 5, inciso f, del Decreto citado, "el Sector Financiero estará bajo la rectoría del Ministro de Hacienda". Entre las atribuciones del Ministro de Hacienda como rector, según el artículo 6 de ese mismo decreto, se encuentran:

a) Aprobar conjuntamente con el Presidente de la República el Plan Sectorial de Gobierno para su respectivo sector, en concordancia con el Plan Nacional de Desarrollo.

b) Dirigir y coordinar las políticas sectoriales en las diversas instituciones que componen el sector.

c) Dirigir y coordinar la respectiva Secretaría Sectorial.

d) Presidir el Consejo Sectorial (…)

e) Velar porque las instituciones del sector respondan adecuadamente a los objetivos sectoriales, así como a las directrices en materia de política sectorial.

f) Autoevaluar la eficiencia y eficacia de los resultados obtenidos por las instituciones en la ejecución de las estrategias y las políticas sectoriales.

g) Establecer mecanismos para integrar de manera participativa, las opiniones de distintos grupos de interés en asuntos de importancia y vinculación sectorial.

h) Visar y presentar ante la o el Ministro de Planificación Nacional y Política Económica las propuestas de modificación al Plan Nacional de Desarrollo

para su aprobación, de acuerdo con las solicitudes presentadas por los jerarcas institucionales.

i) Dirigir y coordinar la elaboración del respectivo Plan Sectorial, supervisar su ejecución y evaluarla. Una vez oficializado el Plan Nacional de Desarrollo, el o los Rectores de cada Sector tendrán un plazo de seis meses para elaborar el respectivo Plan Sectorial, que será de conocimiento de MIDEPLAN y debidamente divulgado.

1.4.3 Visión

El concepto de visión nos define el rumbo o camino que una organización desea seguir al largo plazo, es la meta hacia la cual van dirigidas todas las estrategias para el logro de objetivos institucionales. Responde a la pregunta: ¿Qué es lo que se desea que sea la organización en el futuro?

La visión actual del Ministerio de Hacienda es la siguiente:

Ser un actor estratégico en el desarrollo socioeconómico, con una política hacendaria que impulse el desarrollo económico y social sostenido y la competitividad nacional, en un marco de estabilidad macroeconómica, brindando servicios de calidad, con tecnologías de información y un desempeño transparente y eficiente.[3]

1.4.4 Misión

La definición de misión nos plantea la razón de ser de la organización, cuál es el propósito de su existencia. Responde a la pregunta: ¿Para qué existe la organización?

---

[3] Ministerio de Hacienda. https://www.hacienda.go.cr/NR/rdonlyres/A4C2D1BC-3A7F-4487-BAC7-7B623F3FC129/27838/Misionvisionvalores.pdf

La misión del Ministerio de Hacienda es:

Garantizar a la sociedad costarricense la efectiva y justa recaudación de los impuestos, el uso adecuado del financiamiento del Sector Público y coadyuvar a la asignación de los recursos, con eficiencia, eficiencia y transparencia, mediante una política hacendaria sostenible y la activa rectoría del Sector Financiero, para contribuir al desarrollo económico y social del país.[3]

1.4.5 Valores institucionales[4]

*Los valores ponen de manifiesto aquellas conductas que son consideradas como valiosas dentro de una organización. Los valores, en conjunto con las declaraciones de visión y misión, pretenden ser parte de la filosofía de una institución u organización, entendiendo la palabra "filosofía" como el pensamiento que precede a la acción. El problema de los valores no está en enunciarlos, sino más bien en su "operativización" (**sic**), la cual debe ser diaria y continua a lo largo de los años. En el caso del Ministerio de Hacienda, hay cuatro valores fundamentales y son los siguientes:*

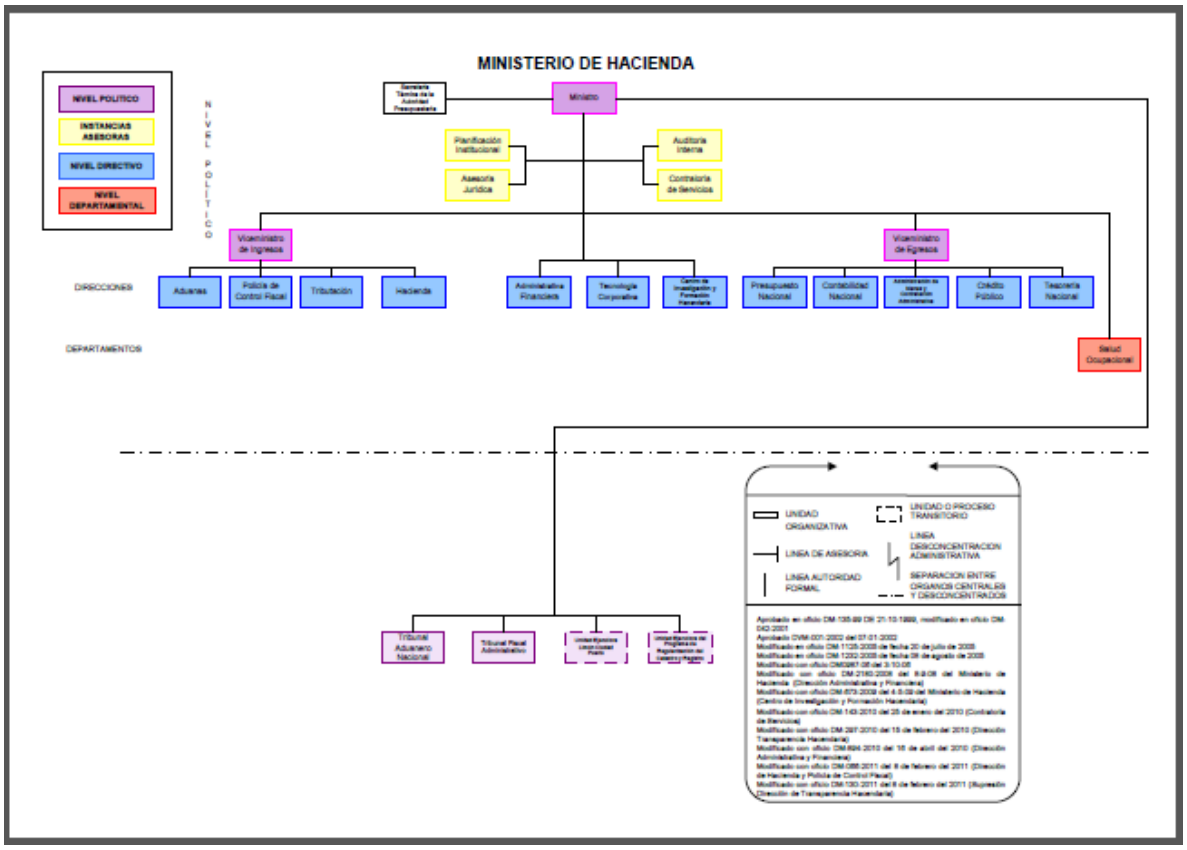
- *Excelencia, la cual se manifiesta en el eficaz y eficiente servicio que se brinda a la sociedad costarricense.*
- *Compromiso, que es la actitud fundamental que se manifiesta en la identificación con la visión y la misión institucional, el esfuerzo realizado para lograrlas y la responsabilidad que nos compete.*
- *Honestidad – Integridad, que se manifiestan en la rectitud y transparencia en el modo de actuar, asumiendo la responsabilidad de los propios actos y siendo coherente en sus actitudes cotidianas,*

[4] Redondo Gómez, Eugenio. Centro de Investigación y Formación Hacendaria. Op. Cit.

con los principios y valores éticos más altos, tales como la verdad, la justicia y el respeto, tanto de las personas, como de los bienes ajenos que se nos han confiado.

- *Trabajo en equipo, unión de los esfuerzos personales y colectivos para el logro de los objetivos de la Institución.*

1.4.6 Organigrama Ministerio de Hacienda



Fuente: Ministerio de Hacienda. “Organigrama del Ministerio de Hacienda”. www.hacienda.go.cr, en https://www.hacienda.go.cr/NR/rdonlyres/A4C2D1BC-3A7F-4487-BAC7-7B623F3FC129/27828/OrganigramaMinisteriodeHacienda.pdf

1.5. Dirección General de Tributación[5]

La Dirección tiene como objeto contribuir con la mejora continua del sistema tributario costarricense, procurando su equilibrio y progresividad, en armonía con los derechos y garantías ciudadanas.

La Dirección es una dependencia del Área de Ingresos del Ministerio que depende directa y jerárquicamente del Viceministro (a) de Ingresos. Es la encargada de la administración y fiscalización general de los tributos que las leyes le encomienden, del desarrollo de todas aquellas otras competencias que le sean atribuidas por las normas, llevando a cabo las actuaciones de información y asistencia a los contribuyentes, la recaudación, la comprobación, auditoría, inspección y valoración que resulten necesarias o convenientes para que los tributos estatales se apliquen con generalidad, equidad y eficacia, promoviendo el cumplimiento voluntario y detectando, corrigiendo y, en su caso, sancionando los incumplimientos.

La Dirección General de Tributación se relaciona con la recaudación de los tributos internos, como el de ventas o el de renta. Todo su desempeño se dirige a la recaudación de éstos y otros más. La declaración de visión indica lo siguiente: "Aspiramos a ser una organización capaz de brindarle a nuestros contribuyentes servicios de alta calidad, al menor costo posible, para el cumplimiento de sus obligaciones tributarias, combatir rápida y efectivamente el incumplimiento y descubrir y procesar el fraude fiscal. Por eso, queremos una organización interna articulada y coherente, que mediante un modelo integral de gestión tributaria, incorpore y utilice modernas tecnologías de

[5] Redondo Gómez, Eugenio. Centro de Investigación y Formación Hacendaria. Op. Cit.

información y comunicación, las mejores prácticas en la especialidad tributaria y un recurso humano motivado, íntegro y en constante desarrollo profesional".

La misión es: "Aplicar las leyes tributarias con generalidad, mediante una gestión efectiva que promueva el cumplimiento voluntario, garantice servicios de información y asistencia al contribuyente y ejerza un control eficaz de los incumplimientos tributarios mediante acciones que se ajusten a los principios y valores institucionales, todo dentro de un marco de respeto a los derechos y garantías ciudadanas".

Los objetivos estratégicos de la Dirección General de Tributación son los siguientes:

a) Mejorar la efectividad del control tributario.

b) Facilitar el cumplimiento voluntario.

c) Fortalecer la eficiencia y eficacia de las operaciones institucionales.

d) Optimizar la administración del capital humano.

1.5.1 Estructura[6]

La Dirección General de Tributación, está constituida por una Dirección General y Subdirección General, de esta última dependen dos áreas:

a. El área de Administración de Acuerdos de Compromisos

b. El área de Comunicación Institucional

---

[6] Redondo Gómez, Eugenio. Centro de Investigación y Formación Hacendaria. Op. Cit.

Asimismo forman parte de la Dirección General trece Direcciones, cuatro Direcciones Regionales y once Administraciones Tributarias Territoriales, incluyendo la segmentación de la Administración Tributaria de San José en Administración Tributaria San José Oeste, Administración Tributaria San José Este y Administración Tributaria San José Sur, así como oficinas de servicio adscritas a Administraciones Tributarias Territoriales.

Las Direcciones que conforman la Dirección General son las siguientes:

1. Dirección de Gestión Integral Tributaria.

2. Área de Control Interno.

3. Dirección de Relaciones Tributarias Inter- Institucionales.

4. Dirección de Normativa, conformada por las Subdirecciones de:

a. Procesos Jurídicos Tributarios Externos.

b. Uniformidad de Criterio y Jurisprudencia.

c. Digesto Tributario.

5. Dirección de Servicio al Contribuyente, conformada por las Subdirecciones de:

a. Información y Asistencia al Contribuyente.

b. Educación y Cultura Fiscal.

c. Administración de Canales.

d. Técnico-Jurídica en Servicio al Contribuyente.

6. Dirección de Recaudación, conformada por las Subdirecciones de Administración del:

a. Registro Único Tributario.

b. Declaraciones, Pagos y Entidades Colaboradoras.

c. Administración de Cuenta Integral Tributaria y Devoluciones.

d. Programación y Seguimiento de Cobro Administrativo.

e. Técnico-Jurídica en Recaudación.

f. Área de Documentación y Archivo.

7. Dirección de Control Tributario Extensivo, conformada por las Subdirecciones de:

a. Control del Cumplimiento Extensivo Formal.

b. Control del Cumplimiento Extensivo Material.

c. Técnico-Jurídica en Control Tributario Extensivo.

8. Dirección de Fiscalización, conformada por las Subdirecciones de:

a. Información y Coordinación Informática.

b. Programación y Selección.

c. Desarrollo Técnico y Control del Proceso de las Actuaciones Fiscalizadoras.

d. Técnico-Jurídica en Fiscalización.

9. Dirección de Tecnología de Información Tributaria, conformada por las Subdirecciones de:

a. Gestión de la Plataforma Tecnológica Tributaria.

b. Aseguramiento del Servicio a Usuarios.

c. Ingeniería de Sistemas.

d. Control de Servicios de Tecnología de Información.

10. Dirección de Inteligencia Tributaria, conformada por las Subdirecciones de:

a. Inteligencia.

b. Centro de Competencias.

11. Dirección de Órgano de Normalización Técnica, conformada por las Subdirecciones de:

a. Valoraciones Municipales.

b. Investigación y Análisis de la Información en Valoraciones Tributaria Municipal.

c. Técnico Jurídico en Valoraciones Municipales.

12. Dirección de Valoraciones Administrativas y Tributarias, conformada por las Subdirecciones de:

a. Valoraciones Administrativas.

b. Valoraciones Tributarias.

c. Técnico Jurídico en Valoraciones Administrativas y Tributarias.

13. Dirección de Tributación Internacional y Técnica Tributaria, conformada por las Subdirecciones de:

a. Negociación y Aplicación de Convenios Tributarios. Internacionales.

b. Coordinación y Actualización de Normas y Procedimientos.

c. Acuerdos Previos sobre Precios de Transferencia.

d. Consulta Tributaria.

14. Dirección de Grandes Contribuyentes Nacionales, conformada por las Subdirecciones de:

a. Investigación de Estudios Económicos y Tributarios de Grandes Contribuyentes.

b. Recaudación, Control y Servicios Tributarios.

c. Fiscalización.

15. Dirección Regional Pacífico, conformada por las Subdirecciones de:

a. Control del Cumplimiento Tributario Regional.

b. Relaciones con el Contribuyente y Entes Locales.

c. La Administración Tributaria Puntarenas.

d. La Administración Tributaria Guanacaste.

16. Dirección Regional Norte, conformada por las Subdirecciones de:

a. Control del Cumplimiento Tributario Regional.

b. Relaciones con el Contribuyente y Entes Locales.

c. La Administración Tributaria Heredia.

d. La Administración Tributaria Zona Norte.

e. La Administración Tributaria Alajuela.

17. Dirección Regional Centro, conformada por las Subdirecciones de:

a. Control del Cumplimiento Tributario Regional.

b. Relaciones con el Contribuyente y Entes Locales.

c. La Administración Tributaria San José Este.

d. La Administración Tributaria San José Oeste.

e. La Administración Tributaria San José Sur.

f. La Administración Tributaria de Limón.

18. Dirección Regional Sur, conformada por las Subdirecciones de:

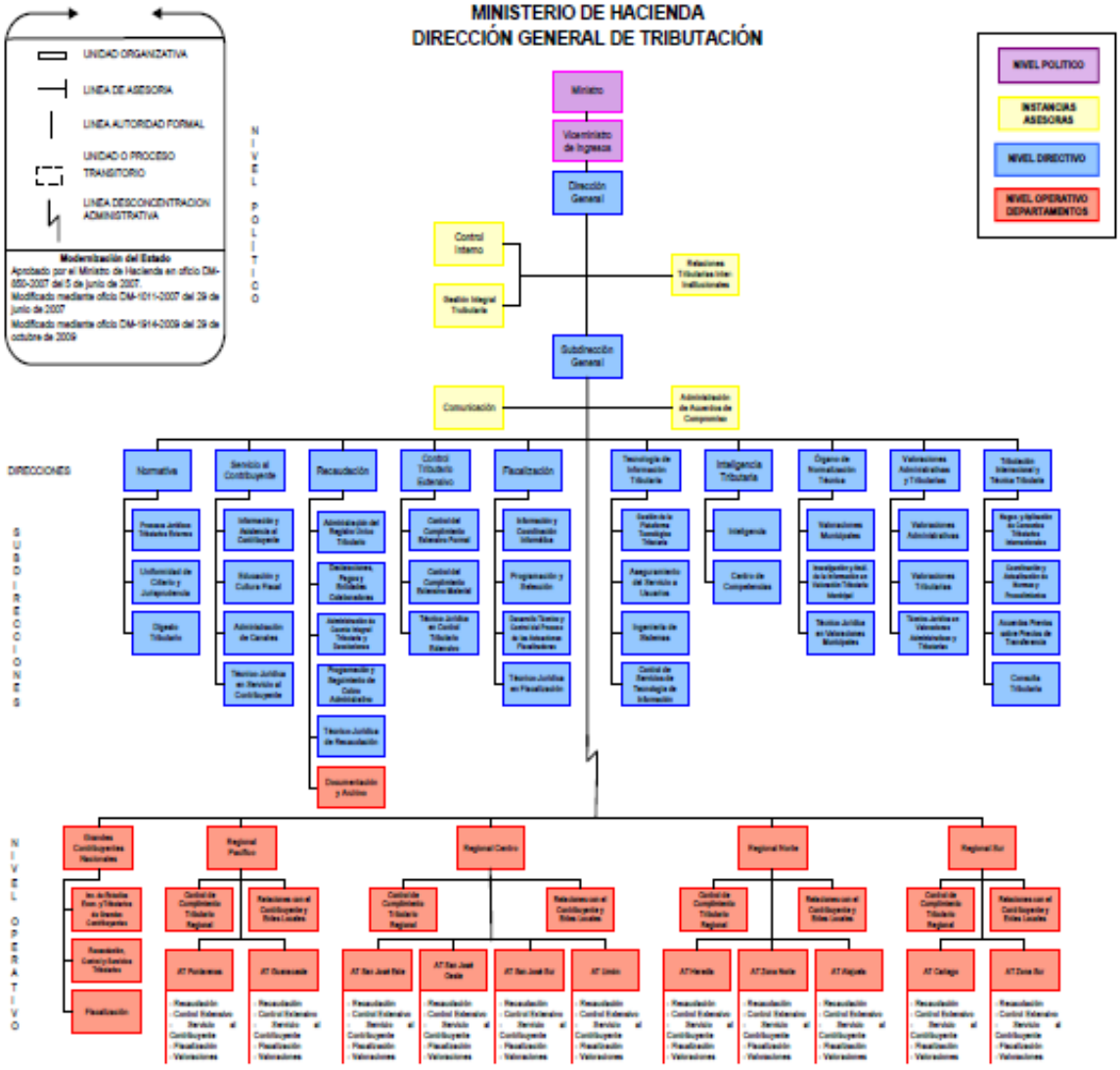
a. Control del Cumplimiento Tributario Regional.

b. Relaciones con el Contribuyente y Entes Locales.

c. La Administración Tributaria Cartago.

d. La Administración Tributaria Zona Sur.

1.5.2 Organigrama de la Dirección General de Tributación



Fuente: Curso Virtual Reinducción General al Ministerio de Hacienda. Sétima edición.

1.6. Dirección de Tecnología de Información Tributaria[7]

Le corresponde a esta Dirección realizar las siguientes funciones:

Traducir las estrategias en materia de Tecnología de Información en prácticas cotidianas de la Dirección General de Tributación, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales.

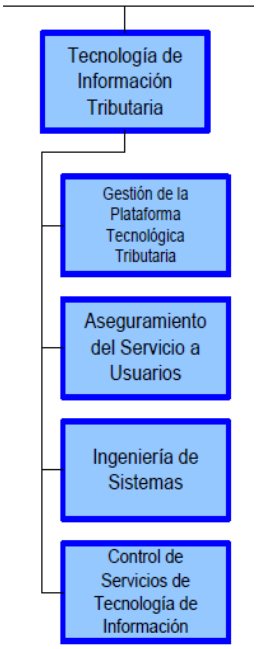
Asegurar que existan los mecanismos necesarios para responder adecuadamente a las amenazas que puedan afectar la gestión de la Tecnología de Información, al servicio de la Administración Tributaria, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.

Asegurar que los productos y servicios de Tecnología de Información sean de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo.

---

[7] Redondo Gómez, Eugenio. Centro de Investigación y Formación Hacendaria. Op. Cit.

1.6.1 Organigrama de la DTIT



Fuente: Curso Virtual Reinducción General al Ministerio de Hacienda. Sétima edición.

1.7. La importancia de las adquisiciones de TI para la DTIT

Dado que a la Dirección de Tecnología de Información Tributaria de la Dirección General de Tributación del Ministerio de Hacienda le compete la promulgación de políticas organizacionales relacionadas con el buen manejo de los datos por parte de diferentes usuarios del Ministerio de Hacienda, contar con mecanismos de control necesarios que eviten la materialización de posibles riesgos y velar para que los productos y servicios estén de acuerdo con las necesidades de los usuarios, entre otras muchas funciones, se hace necesario que existan políticas y

procedimientos claros basados en las mejores prácticas existentes para las adquisiciones de TI.

Contar con un buen método de adquisición en tecnologías de información, que se adapte a las necesidades de la DTIT, es de suma importancia dada la necesidad de un manejo eficaz y eficiente de la información. Las necesidades de TI deben ser identificadas, desarrolladas o adquiridas y luego ser implementadas a los procesos o transacciones ejecutados en la Dirección, pero esto no es suficiente, el mantenimiento, soporte y control también son temas que deben ser considerados para el adecuado manejo de las TI, por lo que la administración debe plantearse las siguientes preguntas:

- ¿Satisface realmente la Dirección de Tecnología de Información Tributaria las necesidades de productos y servicios de TI de los usuarios?
- ¿La adquisición de nuevos productos o servicios, realmente van a satisfacer las necesidades de la Dirección de Tecnología de Información Tributaria?
- ¿Las nuevas adquisiciones en TI se adaptarán realmente al presupuesto y al tiempo establecido?
- ¿Cumplirán realmente las adquisiciones de TI con las especificaciones establecidas?
- ¿Se adaptarán realmente las adquisiciones de TI a las operaciones actuales de la Dirección de Tecnología de Información Tributaria?

Analizar todas estas interrogantes y pensar en las respuestas que se le pueden dar actualmente, en las respuestas que se esperaría fueran las indicadas y sobre todo en las respuestas que se esperan para un futuro, plantea un alto en el camino para la Dirección y vienen a motivar y analizar la importancia que realmente tienen las adquisiciones en tecnología de información para el buen desempeño de las funciones.

CAPÍTULO II. MARCO TEÓRICO

2.1 Definiciones y conceptos.

- Hacienda[8]

Por hacienda se debe entender, entre varias acepciones, el "conjunto de las rentas, impuestos y demás bienes de cualquier índole regidos por el Estado o por otros entes públicos".

- Hacienda Pública[8]

Hacienda pública es el "conjunto de órganos de la administración de un Estado encargados de hacer llegar los recursos económicos a las arcas del mismo, así como los instrumentos con los que dicho Estado gestiona y recauda los tributos; engloba (…) los ingresos y los gastos, lo cual supone tanto la planificación de los tributos y demás ingresos del estado (…) como la elaboración de los Presupuestos Generales del Estado para su aprobación por el órgano correspondiente (Congreso, Parlamento u otro)".

- Administración activa[8]

Por Administración Activa se debe entender, desde un punto de vista funcional, la función decisoria, ejecutoria, resolutoria, directiva u operativa de la Administración.

---

[8] Redondo Gómez, Eugenio. Centro de Investigación y Formación Hacendaria. Op. Cit.

- Administración Pública

Como se indica en la Ley General de la Administración Pública en su artículo 1: *"La Administración Pública estará constituida por el Estado y los demás entes públicos, cada uno con personalidad jurídica y capacidad de derecho público y privado".*

Por su parte el Código Contencioso Administrativo complementa el concepto de la Administración Pública en su artículo 1, in inciso 3), el cual señala: *"… se entenderá por Administración Pública:*

a) La Administración central.
b) Los Poderes Legislativo, Judicial y el Tribunal Supremo de Elecciones, cuando realicen funciones administrativas.
c) La Administración descentralizada, institucional y territorial, y las demás entidades de Derecho público".

- Área de ingresos[9]

Todas aquellas dependencias que conforman el Viceministerio de Ingresos del Ministerio de Hacienda.

- Riesgo [10]

"El potencial que una amenaza determinada explote las vulnerabilidades de un activo (G.3) o grupo de activos y, por consiguiente, ocasione pérdida o daño a la organización". (ISO/IEC PDTR 13335-1).

---

[9] Decreto 35688-H, Gaceta 14 del 21de enero de 2010. Reglamento de Organización y Funciones de la Dirección General de Tributación.

[10] ISACA. Manual de preparación examen CISA 2011. (p. 49)

- Riesgo de TI[11]

"El marco Risk IT de ISACA define el riesgo de TI de este modo:

El riesgo de TI es un riesgo de negocio, específicamente el riesgo de negocio asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de TI dentro de una empresa. Consiste en eventos relacionados con TI que potencialmente podrían impactar al negocio. Incluye una frecuencia y magnitud incierta, y crea retos para cumplir metas y objetivos estratégicos y la incertidumbre en la búsqueda de oportunidades".

- Administración de riesgos[12]

Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales. Es aplicable a cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

- Administración de riesgos de TI[12]

Es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de TI.

---

[11] ISACA. Manual de preparación examen CISA. Op. Cit.

[12] Maxitana Cevallos, Jennifer Dennise y Naranjo Sánchez, Bertha Alice. Administración de riesgos de tecnología de información de una empresa del sector informático. http://www.dspace.espol.edu.ec/bitstream/123456789/15896/3/Resumen%20Cicyt.-%20Administraci%C3%B3n%20de%20Riesgos%20de%20TI%20de%20una%20empresa%20del%20sector%20Inform%C3%A1tico.pdf. Capturado el 21/04/2013

- Control Interno

Según las Normas de Auditoría[13]: Es "*el proceso diseñado, implementado y mantenido por los encargados del gobierno o mando corporativo, la administración y otro personal, para proporcionar seguridad razonable sobre el logro de los objetivos de la entidad respecto a la confiabilidad de la información financiera, efectividad y eficiencia de las operaciones y cumplimiento de las leyes y regulaciones aplicables. El término "controles" se refiere a cualesquiera aspectos de uno o más de los componentes del control interno."*

- Actividades de control[14]

Las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las directrices de la administración. Las actividades de control son un componente del control interno.

- Ambiente del control[14]

Incluye las funciones de mando corporativo y de administración y las actitudes, conciencia y acciones de los encargados del gobierno corporativo y la administración concernientes al control interno de la entidad y su importancia en la entidad. El ambiente del control es un componente del control interno.

- *Controles generales de TI (Tecnología de la Información)[14]*

Políticas y procedimientos que se relacionan con muchas aplicaciones y soportan el funcionamiento efectivo de controles de aplicación, ayudando a asegurar la operación continua apropiada de los sistemas de información. Los controles

---

[13] Instituto Mexicano de Contadores Públicos. (2009). "Normas Internacionales de Auditoría y Control de Calidad." México, D.F: Editorial Caballero Gabriela, 10. ed. (pp. 27, 32 y 36)

[14] Instituto Mexicano de Contadores Públicos. (2009)." Op. Cit.

generales de TI, comúnmente, incluyen controles sobre el centro de datos y operaciones de la red; adquisición, cambio y mantenimiento de software del sistema; seguridad del acceso; y adquisición, desarrollo, y mantenimiento del sistema de aplicación.

- Amenazas[15]

Una (s) persona (s) o cosa(s) vista (s) como posible fuente de peligro o catástrofe. Ejemplos: inundación, incendio, robo de datos, sabotaje, agujeros publicados, falta de procedimientos de emergencia, divulgación de datos, implicaciones con la ley, aplicaciones mal diseñadas, gastos incontrolados, etc.

- Vulnerabilidad[16]

La situación creada, por la falta de uno o varios controles, con la que la amenaza pudiera acaecer y así afectar al entorno informático. Ejemplos: falta de control de acceso lógico, falta de control de versiones, inexistencia de un control de soportes magnéticos, falta de separación de entornos en el sistema, falta de cifrado en las telecomunicaciones, etc.

- *Procedimientos de valoración del riesgo[17]*

Los procedimientos de auditoría desempeñados para obtener un entendimiento de la entidad y su entorno, incluyendo el control interno de la entidad, para identificar y valorar los riesgos de representación errónea material, ya sea por fraude o error, en los niveles de estado financiero y de aseveración.

---

[15] Piattini Velthuis, Mario Gerardo y Del Peso, Navarro, Emilio. (2001). "Auditoría informática un enfoque práctico". México D.F.: Alfaomega Grupo Editor, 2 ed.(pp. 49, 50)

[16] Piattini Velthuis, Mario Gerardo y Del Peso, Navarro, Emilio. (2001). Op. Cit.

[17] Instituto Mexicano de Contadores Públicos. (2009). "Normas Internacionales de Auditoría y Control de Calidad." Op. Cit. (pp 44 y 49).

- *Encargados del gobierno corporativo*[18]

La(s) persona(s) u organización(es) (por ejemplo, un fiduciario corporativo) con responsabilidad de supervisar la dirección estratégica de la entidad y obligaciones relacionadas con la rendición de cuentas de la entidad. Esto incluye supervisar el proceso de información financiera. Para algunas entidades en ciertas jurisdicciones, los encargados del gobierno corporativo pueden incluir personal de la administración, por ejemplo, miembros ejecutivos de un consejo de gobierno de una entidad del sector privado o público, o un administrador-dueño.

- Tecnología de Información[19]

"Conjunto de tecnologías dedicadas al manejo de la información organizacional. Término genérico que incluye los recursos de: información, software, infraestructura y personas relacionadas".

- Ciclo de vida de desarrollo de sistemas de información (SDLC)[20]

Son las fases que se tienen en cuenta en el desarrollo o adquisición de un sistema de software. Las fases típicas incluyen el estudio de factibilidad, el estudio de los requerimientos, la definición de los requerimientos, el diseño detallado, la programación, las pruebas, la instalación, la revisión posterior a la implementación.

---

[18] Instituto Mexicano de Contadores Públicos. (2009). "Normas Internacionales de Auditoría y Control de Calidad." Op. Cit. (pp 44 y 49).

[19] Contraloría General de la República. (2007). "(N-2-2007-CO-DFOE) Normas técnicas para la gestión y el control de las Tecnologías de Información".

[20] ISACA. Manual de preparación examen CISA 2011. (p. 446)

- Metodología[21]

Según el Diccionario, Método es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra Metodología como "conjunto de métodos que se siguen en una investigación científica".

- ISACA (*Information Systems Audit and Control Association*)[22]

Es una asociación independiente, sin fines de lucro, que participa en el desarrollo, adopción y uso de conocimiento mundialmente aceptado, líder en la industria y prácticas de sistemas de información. Anteriormente conocido como la auditoría de sistemas de información y Control Association, ahora se denomina "ISACA" por sus siglas en inglés.

- IT Governance Institute (ITGI)[23]

Es una organización ligada a ISACA que se estableció en 1998 para evolucionar el pensamiento y los estándares internacionales respecto a la dirección y control de la tecnología de información de una empresa. Un gobierno de TI efectivo, ayuda a garantizar que TI soporte las metas del negocio, optimice la inversión del negocio en TI, y administre de forma adecuada los riesgos y oportunidades asociados a la TI. El IT Governance Institute ofrece investigación original, recursos electrónicos y casos de estudio para ayudar a los líderes de las empresas y a sus consejos directivos en sus responsabilidades de Gobierno de TI.

---

[21] Jennifer Dennise Maxitana Cevallos, Bertha Alice Naranjo Sánchez. Op. Cit.

[22] Tomado de la página web de ISACA. http://www.isaca.org/about-isaca/Pages/default.aspx. Capturado el 24/04/2013.

[23] IT Governance Institute. (2007). "COBIT 4.1". Versión liberada. (p. 1, 5)

- *COBIT (*Control Objective for Information and Related Technologie*s)*[24]

Es un marco de control publicado por ISACA a través de ITGI y sus Objetivos de Control para la Información y la Tecnología relacionada brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de COBIT representan el consenso de los expertos. Están enfocadas fuertemente en el control y menos en la ejecución. Estas prácticas ayudarán a optimizar las inversiones habilitadas por TI, asegurarán la entrega del servicio y brindarán una medida contra la cual juzgar cuando las cosas no vayan bien.

2.2 Adquisiciones

El diccionario de la Real Academia Española (RAE) contempla tres usos para la palabra adquisición, un vocablo que proviene del término latino adquisitĭo: la acción de conseguir una determinada cosa, la cosa en sí que se ha adquirido y la persona cuyos servicios o intervención están ampliamente valorados[25].

2.3 Adquisiciones de Tecnologías de Información

Tal como lo expone el autor Delgado Rojas, Xiomar en su libro Auditoría Informática[26] *"las adquisiciones de nuevos recursos informáticos se fundamentan en la evaluación que realiza la administración para tomar en cuenta necesidades presentes y futuras de información dentro de una empresa en particular. En otras ocasiones, se pretende proveer de la capacidad adecuada para hacer frente a la carga de trabajo en expansión que una empresa pueda tener en vista de su crecimiento en el mercado o en el desarrollo de sus operaciones".*

---

[24] Tomado de la página web de ISACA. Op.Cit.

[25] Definición de adquisiciones. http://definicion.de/adquisicion/. Capturado el 21/04/2013.

[26] Delgado Rojas Xiomar. (1997). "Auditoría Informática " (p. 139-166).

Considerando lo expuesto por este autor, es importante agregar que las adquisiciones de tecnología de información se han convertido en un proceso muy importante para todas las organizaciones, sean privadas o gubernamentales, ya que de ello depende la eficacia y eficiencia de muchos procesos dentro de las organizaciones.

Contar con información disponible, íntegra y confiable se ha vuelto un aspecto primordial para la adecuada toma de decisiones por parte del Gobierno Corporativo y para poder lograr estas metas es importante contar con tecnologías de información apropiadas, que faciliten este proceso. Para poder contar con tecnologías de información “apropiadas” el proceso de adquisición es un aspecto clave y de vital importancia, ya que debe llevarse a cabo en el menor tiempo posible, garantizando que cumpla con todos los requerimientos previamente establecidos y cuidando que no exceda el presupuesto establecido. Para poder organizar las adquisiciones de tecnologías de información es conveniente agruparlas en: adquisición de *hardware y de software*.

Adquisición de *hardware* podría entenderse como la adquisición de equipos de cómputo ya sea por renovación de equipos actuales o por nuevos requerimientos. Antes de una adquisición de *hardware*, la administración debe establecer cuáles son los requerimientos de los equipos que se necesitan y establecer sus características, los cuales deben ir alineados al cumplimiento de los objetivos tanto de TI como del Gobierno Corporativo.

Adquisición de *software* se refiere a la adquisición o desarrollo de programas o aplicaciones informáticas, los cuales deben estar basados en un estudio riguroso por parte de la administración, ya que su adquisición debe basarse en las necesidades de los usuarios, para lo cual es necesario contar con estudios de requerimientos basados en estudios de costo – beneficio.

2.4 Mejores prácticas utilizadas en las adquisiciones de TI

Las tecnologías de información se han transformado en un punto clave dentro de las organizaciones, se han convertido en la columna vertebral de los procesos corporativos, cada vez son más las empresas e instituciones que dependen de las tecnologías de información mediante el uso de transacciones en línea, Internet, redes inalámbricas, etc., haciendo de la información y de las tecnologías utilizadas para generar y respaldar dicha información sus activos más valiosos dentro de toda la organización.

Dada la creciente demanda por tecnologías de información (TI) es que algunos organismos internacionales -como ISACA-, se han dado a la tarea de estandarizar todos los procesos existentes relacionados con el uso de la TI, estableciendo las mejores prácticas existentes en el mercado, es así que *"los Objetivos de Control para la Información y la Tecnología relacionada (COBIT) brindan buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica".*[27]

Específicamente con respecto al tema de adquisiciones de tecnologías de información, COBIT, en su dominio de Adquirir e implementar (AI), indica:

"Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:

---

[27] IT Governance Institute. (2007). "COBIT 4.1". Versión liberada. (p. 5, 12-13)

• *¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?*

• *¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?*

• *¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?*

• *¿Los cambios no afectarán a las operaciones actuales del negocio?"*[24]

ISACA también ha creado guías de aseguramiento relacionadas con el tema, como estándares globales aplicables para cubrir la necesidad que tienen las organizaciones respecto al tema de las adquisiciones en tecnologías de información.

2.5 Beneficios para la DTIT en el uso de las mejores prácticas para el aseguramiento del control interno en las adquisiciones en Tecnologías de Información

Debido a la gran aceptación que ha tenido el uso de mejores prácticas, como lo es el marco de control COBIT, y a que organismos gubernamentales como la Contraloría General de la República (CGR) lo han adoptado en reglamentos de uso obligatorio como las Normas técnicas para la gestión y el control de las tecnologías de información, contar con una metodología para las adquisiciones de TI sería muy beneficioso para la Dirección de Tecnología de Información Tributaria (DTIT) de la Dirección General de Tributación del Ministerio de Hacienda ya que:

- Al aplicar una metodología de adquisiciones de TI basada en las mejores prácticas les ayudaría con la eficacia y eficiencia de los procesos de adquisiciones.
- Estarían cumpliendo con la normativa vigente por parte de la CGR.
- Generarían valor agregado al cumplir también con estándares internacionales.

- Se evitarían problemas con control interno en caso de algún estudio por parte de la Auditoría Interna o cualquier otro ente contralor.
- Mejora la seguridad y el control.
- Ayuda a reducir riesgos de TI.
- Su aplicación y seguimiento facilitarían el logro de los objetivos Institucionales.

CAPÍTULO III. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL DEL TEMA

3.1 Metodología utilizada para el control interno de las adquisiciones en TI.

Tal como se indica en el capítulo I, la DTIT se encuentra integrada por cuatro Sub Direcciones, de las cuales nos interesa rescatar dos en particular:

- La Sub Dirección de Control de Servicios de Tecnología de Información, se encarga de las adquisiciones de TI relacionadas con el *hardware* y *software.* Respecto al *software*, es importante mencionar que esta Sub Dirección se encarga de realizar todos los trámites para su adquisición cuando se realiza mediante la contratación con terceros, es decir, con empresas externas al Ministerio de Hacienda; cuando la programación va a ser realizada por personal de la DTIT, la solicitud y requerimientos son trasladados a la Sub Dirección de Ingeniería de Sistemas.
- La Sub Dirección de Ingeniería de Sistemas, es la encargada de la programación de los programas y aplicaciones requeridos por los usuarios y aprobados ya sea por el CITI (Consejo Institucional de Tecnologías de Información, el cual tiene dentro de sus funciones, la aprobación de los programas o aplicaciones de gran impacto dentro del Ministerio de Hacienda) o por el Director General de Tributación cuando se trata de programas o aplicaciones menores.

Según entrevistas realizadas al personal de la DTIT, la Sub Dirección de Control de Servicios de Tecnología de Información no cuenta con una metodología claramente establecida para el control interno de las adquisiciones en tecnologías de información, cuando las compras son requeridas, se efectúan de acuerdo con procedimientos fundamentados en la práctica, basándose en los requerimientos de los usuarios. Por su parte, la Sub Dirección de Ingeniería de Sistemas, aunque

sí cuenta con metodologías, procedimientos, políticas, relacionadas con la confección de *software* o aplicaciones, no mantienen una metodología que integre todo lo relacionado al control interno de las adquisiciones en TI relativas al desarrollo de *software* o aplicaciones, sino que existen varios documentos como procedimientos, directrices, etc. que tienen inmersos dentro de su contenido prácticas de control. Sin embargo, es importante mencionar que dicha documentación ha venido elaborándose a partir del 2010 como requisito para cumplir con disposiciones de la CGR y la documentación es mantenida por cada funcionario en forma independiente dificultando con esta práctica la ubicación de los documentos y por ende su aplicación.

3.2 Análisis del uso de la metodología actual utilizada para las adquisiciones de tecnologías de información

3.2.1 Aspectos positivos.

Si bien en la Sub Dirección de Control de Servicios de Tecnología de Información no se cuenta con una metodología para las adquisiciones de tecnologías de información claramente definida, es importante señalar que cuentan con personal experto, con años de experiencia, lo cual ha facilitado que las funciones sean realizadas de forma ágil, además, por ser una organización gubernamental, todos los documentos deben ser revisados por el área jurídica y legal correspondiente, lo cual asegura la protección de la administración en cuanto a los aspectos legales. Respecto a la Sub Dirección de Ingeniería de Sistemas, es notable que los esfuerzos por cumplir con la normativa exigida por la CGR, los ha llevado a preocuparse por elaboración de documentación que se encuentra disponible para los funcionarios cuando así lo necesiten en el desarrollo de sus funciones.

3.2.2 Aspectos negativos

Al no contar con una metodología claramente establecida para las adquisiciones en tecnología de información en la Sub Dirección de Control de Servicios de

Tecnología de Información, se genera una alta dependencia del personal que realiza estas funciones, generando con esta práctica muchos riesgos para la organización en caso de que el personal deje de laborar para esta dependencia.

La ausencia de un análisis de riesgos, incrementa la posibilidad que algún evento no previsto pueda llegar a perjudicar el desarrollo normal de las funciones dentro de la Dirección, afectando el logro de los objetivos y causando posibles perjuicios económicos para la organización.

Es importante destacar el hecho que aunque la Sub Dirección de Ingeniería de Sistemas cuente con documentación relacionada con las adquisiciones de TI, el no contar con un inventario y lugar específicos dificulta su ubicación, ocasionando con esta práctica que los funcionarios tarden mucho tiempo en encontrar el documento que se necesita.

3.3 Normativa referente a las Adquisiciones de TI que regulan la administración pública.

Dado que la DTIT pertenece al Ministerio de Hacienda que es una institución gubernamental, la normativa referente a las TI que están obligados a cumplir es:

- Ley número 8292, Ley General de Control Interno publicada en el diario oficial La Gaceta 04-09-2002, que en su artículo 16 señala:

*"Artículo 16. — **Sistemas de información**. Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, entendiendo esta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar de modo adecuado la información producida o recibida en la organización, en el desarrollo de sus actividades, con el fin de prevenir cualquier desvío en los objetivos trazados. Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las*

demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada.

En cuanto a la información y comunicación, serán deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:

a) Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requerido para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.

b) Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejo eficientes de los recursos públicos.

c) Establecer las políticas, los procedimientos y recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico."

- Normas técnicas para la gestión y el control de las tecnologías de Información. Número N-2-2007-CO-DFOE, publicadas en La Gaceta número 119 del 21/06/2007, promulgadas con resolución número R-CO-26-2007 del Despacho de la Contraloría General de la República, la cual establece: *"Artículo 1°—Aprobar el documento denominado "**Normas técnicas para la gestión y el control de las tecnologías de información**", normativa que establece los criterios básicos de control que deben observarse en la gestión de esas tecnologías y que tiene como propósito coadyuvar en su gestión, en virtud de que dichas tecnologías se han convertido en un instrumento esencial en la prestación de los servicios*

públicos, representando inversiones importantes en el presupuesto del Estado."

- Normas de Control Interno para el Sector Público. Número N-2-2009-CO-DFOE publicadas en la Gaceta número 26 del 06/02/2009, promulgadas con resolución número R-CO-9-2009 del Despacho de la Contraloría General de la República, la cual establece en su capítulo V Normas Sobre Sistemas de Información, inciso 5.9, Tecnologías de Información: *"El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información, emitida por la CGR. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información".*

3.4 Administración de riesgos realizada por la DTIT

Según entrevistas realizadas al personal clave en las adquisiciones de TI de la DTIT, esta dirección no cuenta con una metodología para la administración de riesgos referente a las adquisiciones de TI.

La administración de riesgos es aplicada únicamente en la Sub Dirección de Ingeniería de Sistemas para el desarrollo de planes de contingencias.

3.5 Análisis de la valoración de riesgo realizada por la DTIT

Antes de entrar a valorar la situación de la Dirección de Tecnología de Información Tributaria. Respecto a la valoración del riesgo, es importante hacer mención de la normativa que rige la materia:

1. De acuerdo con la Ley número 8292, Ley General de Control Interno publicada en el diario oficial La Gaceta 04-09-2002, en sus artículos 18 y 19 señala:

*"Artículo 18. — **Sistema específico de valoración del riesgo institucional**. Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo.*

La Contraloría General de la República establecerá los criterios y las directrices generales que servirán de base para el establecimiento y funcionamiento del sistema en los entes y órganos seleccionados, criterios y directrices que serán obligatorios y prevalecerán sobre los que se les opongan, sin menoscabo de la obligación del jerarca y titulares subordinados referida en el artículo 14 de esta Ley".

2. Las Normas de Control Interno para el Sector Público en su capítulo III: Normas Sobre la Valoración del Riesgo, inciso 3.1 Valoración de riesgo, indica:

"El jerarca y los titulares subordinados, según sus competencias, deben definir, implantar, verificar y perfeccionar un proceso permanente y participativo de valoración del riesgo institucional, como componente funcional del SCI. Las

autoridades indicadas deben constituirse en parte activa del proceso que al efecto se instaure."

3. La Directriz General para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) en su artículo 2, inciso 2.2, menciona:

"Se entenderá como Sistema Específico de Valoración del Riesgo Institucional al conjunto organizado de componentes de la Institución que interaccionan para la identificación, análisis, evaluación, administración, revisión, documentación y comunicación de los riesgos institucionales relevantes".

El inciso 2.3 de la misma directriz, establece*:*

"El SEVRI deberá producir información que apoye la toma de decisiones orientada a ubicar a la institución en un nivel de riesgo aceptable y así promover, de manera razonable, el logro de los objetivos institucionales".

Basado con la Normativa citada anteriormente es notoria la obligatoriedad que posee la DTIT en cuanto a la implantación del Sistema de Valoración de Riesgos, además, el tener identificados en forma clara los riesgos para las adquisiciones de TI, que es la materia que nos ocupa, facilitaría la toma de decisiones de los jerarcas de la Dirección y evitaría la materialización de algunos de estos riesgos evitando con ello las consecuencias (por lo general económicas) que podrían ocasionar.

CAPÍTULO IV. ANÁLISIS DE LA SITUACIÓN DIAGNOSTICADA

Dado que la DTIT no cuenta con la identificación clara de los posibles riesgos referentes a las adquisiciones en TI que podrían darse dentro de la Dirección, es importante para el desarrollo del presente proyecto conocer cómo debería funcionar el Sistema Específico de Valoración de Riesgos Institucional específicamente para la Dirección antes mencionada, así como los riesgos a identificar, basados en las mejores prácticas, como serían las Guías de Aseguramiento de ISACA.

4.1 Funcionamiento del Sistema Específico de Valoración de Riesgo Institucional

La Directriz General para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) en el punto 4 indica en forma clara cómo debe ser su funcionamiento, dividiéndolo en 8 incisos como se indica a continuación:

- Descripción general: la Institución deberá ejecutar actividades para identificar, analizar, evaluar, administrar, revisar, documentar y comunicar los riesgos institucionales.
- Identificación de riesgos: La Dirección de Tecnología de Información Tributaria debe identificar por área, Sub Dirección, sector o como mejor se adapte a la realidad de la Dirección, los eventos que podrían afectar el logro de los objetivos, las posibles causas, consecuencias, la ocurrencia, así como el momento y lugar en el que podrían ocurrir. También deben considerarse las medidas para la administración de riesgos con que cuenta la Dirección, relacionadas con los riesgos identificados.
- Análisis de riesgos: para los eventos identificados se debe determinar la probabilidad de que los riesgos se materialicen, la magnitud en caso de que

llegue a suceder, el nivel y los factores de riesgo, así como las medidas para la correcta administración. También es importante considerar que estos análisis pueden ser cualitativos o cuantitativos.

- Evaluación de riesgos: Los riesgos analizados deben ser priorizados por la Dirección, de acuerdo con criterios institucionales previamente establecidos, los cuales deben indicar el nivel de riesgo, grado en que la Institución puede afectar los factores del riesgo, importancia de la política, proyecto, función o actividad afectada, así como la eficacia y eficiencia de las medidas existentes para la administración de riesgo.
- Administración de riesgos: Una vez priorizados los riesgos, se deben evaluar y seleccionar las medidas para la administración de cada riesgo, tomando en consideración el costo- beneficio, cumplimiento del interés público y resguardo de la hacienda pública, viabilidad jurídica, técnica y operacional.
- Revisión de riesgos: se debe dar seguimiento a los riesgos identificados, tomando en consideración el nivel de riesgo, los factores de riesgo, grado de ejecución de las medidas para la administración de riesgos, etc.
- Documentación de riesgos: Es importante que se documente la información sobre los riesgos y las medidas para la administración de riesgos que se genera en cada actividad de la valoración de riesgos. Se debe contar con un registro de riesgos que contenga toda la información necesaria referente a cada uno de los riesgos identificados.
- Comunicación de riesgos: La Dirección debe brindar información a todos los sujetos o dependencias interesadas en relación con los riesgos institucionales.

4.2 Riesgos identificados referentes a las Adquisiciones de TI de acuerdo con el uso de las mejores prácticas

Basado en el uso de las mejores prácticas (que se explicarán en el capítulo V del presente documento) existentes en el mercado, ISACA hace referencia a que la gestión de riesgos que debe estar presente en toda organización, debe constar al menos de 5 etapas:

- Inventariar los riesgos: es conveniente que la organización realice una lluvia de ideas con todo el personal clave, para poder crear un inventario de los posibles riesgos presentes que pueden afectar el logro de los objetivos institucionales.
- Evaluación de riesgos: es importante que los riesgos identificados sean cuantificados (expresado como un porcentaje) así como el posible impacto de cada riesgo (expresado como una cantidad de dinero).
- Mitigación de los riesgos: se debe crear un plan de gestión de riesgos que describa en forma clara la estrategia que ha adoptado la organización, así como las medidas diseñadas para afrontar los riesgos identificados. Se debe tomar en consideración que cuanto más importante sea el riesgo, mayor debe ser la disponibilidad del presupuesto para contramedidas, las cuales podrían incluir actividades de prevención, detección y control o reconstrucción de daños. Cualquier riesgo puede mitigarse, evitarse, transferirse o aceptarse, en función de su gravedad, probabilidad y costo de las contramedidas y políticas de la organización.
- Descubrir riesgos: la organización debe estar atenta a identificar los riesgos cuando estos se materialicen y actuar en forma inmediata según corresponda.
- Revisar y evaluar: se debe revisar y evaluar la efectividad y los costos del proceso de gestión de riesgos adoptado por la organización.

Tomando en consideración el dominio Adquirir e Implementar del marco de control COBIT 4.1 y las guías de aseguramiento de ISACA, a continuación se presentan los riesgos identificados de acuerdo con las mejores prácticas:

Cuadro 1: Riesgos identificados basados en a las mejores prácticas, referentes a las adquisiciones de TI

AI 1 Identificar Soluciones Automatizadas	
1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio 1.2 Reporte de análisis de riesgos 1.3 Estudio de factibilidad y formulación de cursos de acción alternativos 1.4 Requerimientos, decisión de factibilidad y aprobación	• Contar una gestión de proyectos claramente definida
	• Realizar estudios de factibilidad de los proyectos por desarrollar.
	• Inspeccionar una selección de documentación de análisis de riesgo, y determinar si los riesgos de negocio y de TI son identificados, analizados, evaluados y entendidos por el negocio y TI, y si las medidas de control interno y pistas de auditoría se identifican como parte del análisis de riesgos (por ejemplo, los riesgos en la planificación de la continuidad del negocio, la planificación de recuperación de desastres, seguridad y requisitos legales).
	• Inspeccionar una selección de documentación de análisis de riesgos para determinar si la documentación del análisis de riesgo fue firmado por las partes interesadas, incluidos los representantes de la empresa y de TI.
	• Inspeccionar una selección de proyectos, auditoría u otros informes de evaluación y corroborar a través de entrevistas con el cumplimiento, auditoría, gestión de riesgos y los miembros del personal de seguridad para determinar si un equilibrio adecuado entre la detección y control de la prevención se considera en el diseño de los mecanismos de respuesta a los riesgos.
	• Evaluar los riesgos (por ejemplo, las amenazas, las vulnerabilidades potenciales de seguridad, controles internos) que no fueron identificados debido a los esfuerzos de desarrollo de sistemas sin incluir los análisis de riesgo robustos.
AI 2 Adquirir y Mantener *Software* Aplicativo	
2.1 Diseño de alto nivel	• La dependencia de conocimiento de las personas clave.
	• Ámbito desarrollo indefinido.
	• Las soluciones no cumplen con los requisitos empresariales.
	• Las soluciones no estén alineados con el plan de TI, arquitectura de la información estratégica y dirección tecnológica.
	• Altos costos de las soluciones fragmentadas.
2.2 Diseño detallado	• Procesamiento de las transacciones no válidas.
	• El aumento de los costos de rediseño del sistema.
	• Los datos de los sistemas de aplicación procesados incorrectamente.
2.3 Control y posibilidades de auditar	• Controles de compensación costosos.

las aplicaciones	• Problemas de integridad de datos.
	• Diferencias entre los controles de aplicación y las amenazas reales y los riesgos.
	• Los resultados de proceso y los registros de datos que no cumplen con los requisitos de cumplimiento.
2.4 Seguridad y disponibilidad de las aplicaciones	• Violaciones de seguridad detectados.
	• Controles de compensación costosos.
	• Las diferencias entre los controles de seguridad considerados y amenazas y los riesgos reales.
2.5 Configuración e implantación de *software* aplicativo adquirido	• Pérdida de enfoque de negocio.
	• Incapacidad para aplicar eficazmente las futuras actualizaciones
	• Reducción de la disponibilidad del sistema y la integridad de la información.
2.6 Actualizaciones importantes en sistemas existentes	• Reducción de la disponibilidad del sistema.
	• Confidencialidad, integridad y disponibilidad de los datos tratados comprometidos.
	• Falta de control de los costes de los principales acontecimientos.
2.7 Desarrollo de *software* aplicativo	• Desperdicio de los recursos
	• Pérdida de enfoque en los requerimientos del negocio.
	• Alto número de fallas.
	• Incapacidad para mantener aplicaciones de forma eficaz.
2.8 Aseguramiento de la calidad del *software*	• Calidad pobre del *software*.
	• Repetición de *software* desarrollado.
	• Pruebas que no reflejan los procesos actuales de negocio
	• Datos de prueba indebidamente usados y que comprometen la seguridad corporativa.
	• Pruebas insuficientes.
	• Incumplimiento de los requisitos de cumplimiento.
2.9 Administración de los requerimientos de aplicaciones	• Cambios no autorizados.
	• Cambios no aplicados a los sistemas deseados.
	• Brechas entre las expectativas y los requisitos.
2.10 Mantenimiento de *software* aplicativo	• Cambios no autorizados.
	• Cambios no aplicados a los sistemas deseados.
	• Brechas entre las expectativas y los requisitos.
	• Reducción de la disponibilidad del sistema.
AI 3 Adquirir y Mantener Infraestructura Tecnológica	
3.1 Plan de adquisición de infraestructura tecnológica	• No hay un modelo de adquisición.
	• Infraestructura tecnológica inconsistente.
	• La tecnología no apoya las necesidades del negocio.

	• Compromisos de la seguridad de la información.
3.2 Protección y disponibilidad del recurso de infraestructura	• Interrupciones en el procesamiento de la producción.
	• Ingresos por los controles de acceso no detectados.
	• Acceso no autorizado al *software* sensible.
	• Necesidades del negocio no apoyadas por la tecnología.
3.3 Mantenimiento de la infraestructura	• Las interrupciones en el procesamiento de la producción.
	• El acceso no autorizado al *software* sensible.
	• La tecnología no apoya las necesidades del negocio.
	• Violación de los acuerdos de licencia.
3.4 Ambiente de prueba de factibilidad	• Interrupciones de negocio.
	• Daños maliciosos.
AI 4 Facilitar la operación y el uso	
4.1 Plan para soluciones de operación	• Los cambios en mora o vencidos.
	• Las brechas entre las expectativas y la capacidad.
	• Prioridad inapropiada dado a diferentes servicios prestados.
	• Los presupuestos y los recursos insuficientes para hacer frente a las lagunas.
4.2 Transferencia de conocimiento a la gerencia del negocio	• Los cambios en mora o vencidos.
	• Las brechas entre las expectativas y la capacidad del programa.
	• Prioridad inapropiada dada a diferentes servicios prestados.
	• Los presupuestos y los recursos insuficientes para hacer frente a las lagunas.
4.3 Transferencia de conocimiento a usuarios finales	• Uso inconsistente del sistema.
	• Documentación insuficiente.
	• Aumento de la dependencia en personal clave.
	• Problemas que surgen en las operaciones diarias.
	• Que la capacitación no cumpla con los requisitos del usuario.
	• Ayudar a la sobrecarga de escritorio.
4.4 Transferencia de conocimiento al personal de operaciones y soporte	• Documentación insuficiente.
	• Aumento de la dependencia en personal clave.
	• Problemas en las operaciones diarias.
	• Que la capacitación no cumpla con los requisitos del usuario.
	• Ayudar a la sobrecarga de escritorio.
AI 5 Adquirir Recursos de TI	
5.1 Control y adquisición	• Lagunas en los requisitos de cumplimiento establecidos por los proveedores en los contratos.
	• Exposiciones comerciales y contractuales de adquisición.

	• Las soluciones automatizadas que no estén en consonancia con los planes a corto y largo plazo de la organización.
	• Insuficiente calidad del *software* en soluciones adquiridas.
	• Falta de control de costos.
5.2 Administración de contratos con proveedores	• La falta de gestión de costos.
	• Las brechas entre las expectativas de negocio y capacidades de los proveedores.
	• Costos de los servicios indefinidos.
	• Servicios no reflejan los requerimientos del negocio.
	• Falta de apoyo operacional.
5.3 Selección de proveedores	• Selección de proveedores inapropiados.
	• Apoyo insuficiente para el logro de los objetivos de la organización.
	• Las brechas entre las necesidades y capacidades de los proveedores.
5.4 Adquisición de recursos de TI	• Actualizaciones de *software* no está disponibles cuando se necesitan.
	• *Software* no puede apoyar los procesos de negocio.
	• Cambios en la solicitud no pueden ser aplicados según lo previsto.
	• Sistema propenso a problemas e incidentes, causando interrupciones en el negocio.
AI 6 Administrar Cambios	
6.1 Estándares y procedimientos para cambios	• Asignación de recursos inadecuado.
	• No hay seguimiento de cambios.
	• Control insuficiente sobre cambios de emergencias.
	• Mayor probabilidad de cambios no autorizados en los sistemas clave del negocio.
	• Incumplimiento de requisitos.
	• Cambios no autorizados.
	• Reducidas la disponibilidad del sistema.
6.2 Evaluación de impacto, priorización y autorización	• Efectos secundarios involuntarios.
	• Efectos adversos sobre la capacidad y el desempeño de la infraestructura.
	• Falta de prioridad de gestión de cambios.
6.3 Cambios de emergencias	• Incapacidad para responder con eficacia a cambios de emergencia.
	• Autorización de acceso adicional no terminado correctamente.
	• Cambios aplicados no autorizados, dando por resultado la seguridad comprometida y acceso no autorizado a información corporativa.

6.4 Seguimiento y reporte de estatus de cambio	• Insuficiente asignación de recursos.
	• Cambios no registrados y sin seguimiento.
	• Cambios no autorizados en el entorno de producción.
6.5 Cierre y documentación del cambio	• Mayor dependencia de individuos clave.
	• Documentación de configuración no reflejan la configuración actual del sistema.
	• Falta de documentación de procesos de negocio.
	• Falta de versiones de cambios de *hardware* y *software*.
AI 7 Instalar y Acreditar Soluciones y Cambios	
7.1 Entrenamiento	• Falta de detectar rápidamente problemas con sistemas o su uso.
	• Brechas en el conocimiento para realizar actividades y funciones.
	• Errores derivados de nuevos proyectos.
7.2 Plan de prueba	• Pruebas insuficientes por *scripts* de prueba automatizada.
	• Problemas de rendimiento no detectados.
	• Falta de control de costos sobre pruebas de actividades.
	• Responsabilidades y roles de pruebas sin definir.
7.3 Plan de implantación	• Asignación de recursos inadecuada para garantizar la aplicación efectiva de los cambios.
	• Las brechas de seguridad.
7,4 Ambiente de prueba	• Insuficientes pruebas utilizando automatizado scripts de prueba.
	• Problemas de rendimiento no detectados.
	• Sistema de seguridad comprometida.
7.5 Conversión de sistemas y datos	• Sistemas antiguos no disponibles cuando sea necesario.
	• Los resultados poco confiables del sistema y conversión.
	• Interrupciones de procesamiento posterior.
	• Problemas de integridad de datos.
7.6 Pruebas de cambios	• Desperdicio de recursos.
	• Degradación total de la seguridad.
	• Los cambios que afectan la disponibilidad y rendimiento del sistema.
7.7 Prueba de aceptación final	• Problemas de rendimiento no detectados.
	• Rechazos que surgen en los programas de las capacidades entregadas.
7.8 Promoción a producción	• Segregación de las violaciones a los derechos.
	• Sistemas expuestos al fraude u otros actos maliciosos.
	• Que no sea posible regresar a la versión de aplicación anterior.

7.9 Revisión posterior a la implantación	• Falta de identificar que sistemas no responden a necesidades de los usuarios finales.
	• Retorno sobre las inversiones que no cumplen con las expectativas de la gerencia.

Fuente: COBIT 4.1 y guías de aseguramiento de ISACA.

Del análisis de la situación detectada en la DTIT referente a la gestión de riesgos se desprende que contar con una adecuada valoración de los riesgos debe ser una de las prioridades de la DTIT, ya que sería más fácil determinar y adoptar las medidas de prevención adecuadas cuando existan probabilidades de que alguno de los riesgos identificados pueda llegar a materializarse.

La valoración de riesgos debe ser un proceso dinámico, que permita a la organización adoptar todas las acciones correspondientes para tener un nivel de riesgo aceptable, logrando de esta forma un aumento en la posibilidad de éxito y una disminución en la probabilidad de fallo respecto al logro de los objetivos institucionales.

CAPÍTULO V. PROPUESTA PARA MEJORAR LA SITUACIÓN

5.1 Uso de las mejores prácticas

La llegada de las tecnologías de la información ha venido a plantear un desafío para las empresas en un mercado cada vez más competitivo, día a día es notoria la dependencia de las organizaciones a los avances tecnológicos ya que esto determina en muchas ocasiones la permanencia o retiro de una organización en el mercado, la automatización de los procesos, el envío y recibo de grandes volúmenes de información para la adecuada toma de decisiones han convertido a las tecnologías de información en un tema de vital importancia en las operaciones diarias de cualquier organización y las empresas gubernamentales no escapan a esta avalancha que avanza a pasos agigantados sin contemplar diferencias entre las empresas públicas y privadas.

Las TI se han convertido en una de las principales herramientas que apoyan la gestión de las instituciones gubernamentales, mediante el envío y recibo de grandes volúmenes de datos necesarios para la toma de decisiones rápida y segura, así como para la ejecución eficaz y eficiente de las labores, y esto se evidencia en el uso de las tecnologías presentes en las empresas gubernamentales y más específicamente en la Dirección General de Tributación, cuyas tecnologías de información son responsabilidad de la Dirección de Tecnología de Información, la cual ha participado en la elaboración y soporte de muchos sistemas, entre los cuales destacan:

- S.I.I.A.T (Sistema de Información Integral de la Administración Tributaria): el S.I.I.A.T opera desde 1998. Este es un *software* adaptado, modificado prácticamente en su totalidad por funcionarios de la DTIT. En este sistema se lleva un registro de todos los contribuyentes alimentado por miles de

transacciones diarias ingresadas por los funcionarios de todo el Ministerio de Hacienda.

- EDDI (Elaboración Digital de Declaraciones de Impuestos): Diseñado en el 2003 por funcionarios de la DTIT. Es una herramienta tecnológica que le permite a los contribuyentes confeccionar los formularios de impuesto de renta, impuesto de ventas y recibo oficial de pagos, el contribuyente los puede imprimir y presentarlos en las instituciones financieras para su cancelación.
- Declar@7: Diseñado en el 2002 por funcionarios de la DTIT. Este sistema permite al informante elaborar, almacenar y generar de manera electrónica las declaraciones informativas mediante una interface amigable y sencilla. Permite capturar y almacenar el registro de los datos del informante y de los detalles, así como la generación de archivos de reporte de la declaración informativa. Para la revisión de la información anteriormente señalada, el sistema cuenta con un proceso de validación, que realiza directamente en el Sistema de Identificación al Contribuyente (SIC), que debe ser instalado en conjuntamente con el Declar@7.
- SIC (Sistema de Identificación del Contribuyente): Diseñado en el 2012 por funcionarios de la DTIT. Es un servicio web sencillo y ágil, para la consulta y verificación de datos identificativos referentes al nombre o razón social y número de cédula de las personas físicas o jurídicas que la Dirección General de Tributación (DGT), tiene registrada en su sistema de información tributaria. Dentro de él, se dispone de la información que nos facilitan el Tribunal Supremo de Elecciones, el Registro Nacional y la Dirección General de Migración y Extranjería. Los contribuyentes o responsables obligados a presentar declaraciones tributarias pueden, por medio de este sistema, verificar la identificación, la administración tributaria a la que pertenece, impuestos a los que está afecto el contribuyente o declarante, la actividad económica principal y secundaria si existe, así como la fecha de inicio respectiva.

- Tributación Digital: Diseñado en el 2007 por funcionarios de la DGT y desarrollado, inicialmente, por un proveedor externo. Es una oficina virtual, por medio de la cual el contribuyente puede realizar todos sus trámites tributarios, presentación de declaraciones, pago de impuestos, atención de dudas de forma personalizada en línea, planteamiento de consultas, acceso a su buzón y expediente electrónico, así como cumplir con otros deberes tributarios.
- Tributación Directa: Diseñado en el 2011 por funcionarios de la DTIT. Ayuda a los contribuyentes a realizar sus declaraciones autoliquidativas en línea, las deudas son enviadas por medios electrónicos directamente a algunas instituciones del Sistema Financiero Nacional para que el contribuyente los pueda cancelar de forma inmediata.
- Mi factura: Desarrollado en el 2012 tanto por funcionarios de la DTIT como por un proveedor externo, aún se encuentra en proceso. Es un sistema de facturación para profesionales liberales, es como un auto talonario de facturas digital. Los profesionales ingresarían el sitio en Internet y confeccionarían la factura en línea.

Los sistemas mencionados anteriormente son algunos de los desarrollados por la DTIT, solamente se mencionaron algunos a modo de ejemplo, para dar una comprensión de la importancia de las TI en esta Dirección, por lo que el uso de los controles y metodologías apropiadas son de vital importancia para que la ejecución de sus funciones sean efectuadas de manera eficaz y eficiente.

Además de la normativa que por ley está obligada a implementar la DTIT, y que ya se ha mencionado en capítulos anteriores del presente trabajo, es importante complementar con el uso de las mejores prácticas existente en el mercado con el fin de mejorar controles y agilizar los procesos ejecutados en dicha Dirección.

Se podría entender como mejores prácticas, el uso de métodos o procedimientos estandarizados y utilizados en el mercado, los cuales presentan procesos que

pueden ser medidos con facilidad, que ya han sido implementados por otras organizaciones con evidencia de éxito comprobable, que pueden ser implementados en cualquier organización y que además presenta mejoras y actualizaciones constantes de acuerdo con las necesidades del mercado, tal es el caso del marco de control COBIT 4.1 y la Guías de Aseguramiento de ISACA para todos los aspectos relacionados con el aseguramiento del control relacionado al tema de las tecnologías de información.

Dado el creciente auge, utilización y éxito de estas buenas prácticas diseñadas por ISACA, es que se plantea una metodología para el aseguramiento de control interno de las adquisiciones de tecnologías de información para la DTIT.

5.2 Metodología propuesta

La metodología propuesta toma en consideración el marco de control COBIT, que son Objetivos de Control para la Información y la Tecnología relacionada. COBIT brinda el uso de buenas prácticas a través de un marco de trabajo de dominios y procesos, y presenta las actividades en una estructura manejable y lógica. Las buenas prácticas de este marco de control representan el consenso de expertos en la materia, poseen un fuerte enfoque en el control, lo cual puede ayudar a la organización a optimizar las inversiones realizadas en TI, aseguran también la entrega del servicio y proporcionan un parámetro de medición contra el cual se puede comparar para determinar si las cosas no se ejecutan de acuerdo con lo establecido. COBIT proporciona información que la organización necesita para el logro de sus objetivos institucionales.

COBIT se subdivide en los siguientes dominios:

- Planear y Organizar (PO), el cual proporciona dirección para la entrega de soluciones de (AI) y la entrega de servicio (DS).
- Adquirir e Implementar (AI), proporciona las soluciones y las pasa para convertirlas en servicios.

- Entregar y Dar Soporte (DS), recibe las soluciones y las hace utilizables por los usuarios finales.
- Monitorear y Evaluar (ME), monitorear todos los procesos para asegurar que se sigue la dirección provista.

El presente proyecto se enfoca en el dominio “AI” complementado con las guías de aseguramiento establecidas por ISACA.

Según COBIT, en referencia al dominio Adquirir e implementar (AI*): “Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio. Este dominio, por lo general, cubre los siguientes cuestionamientos de la gerencia:*

• *¿Es probable que los nuevos proyectos generan soluciones que satisfagan las necesidades del negocio?*

• *¿Es probable que los nuevos proyectos sean entregados a tiempo y dentro del presupuesto?*

• *¿Trabajarán adecuadamente los nuevos sistemas una vez sean implementados?*

• *¿Los cambios no afectarán a las operaciones actuales del negocio?”*

Tomando en consideración lo descrito anteriormente, así como las normas de aseguramiento de ISACA se desarrolló la siguiente metodología, planteada a manera de preguntas para facilitar tanto su aplicación como la medición del cumplimiento.

Cuadro 2: Metodología propuesta

Metodología para ser aplicada en la adquisición de tecnologías de información					
NOMBRE DE LA ENTIDAD: Ministerio de Hacienda					
UNIDAD DE GESTIÓN: Dirección de Tecnologías de Información Tributaria					
Objetivos general					
Contar con una metodología para la adquisición de tecnologías de información basada en el dominio Adquirir e Implementar (AI) de COBIT 4.1 y en las Guías de Aseguramiento de ISACA.					
Objetivos específicos					
1) Conocer si se cuenta con la información necesaria para decidir si un proyecto debe proceder.					
2) Identificar si la organización tiene una estructura de gestión del proyecto.					
3) Conocer la gestión del proyecto.					
4) Identificar el desarrollo de aplicación del proyecto.					
5) Analizar si se transfiere el conocimiento sobre los nuevos sistemas al personal clave.					
6) Conocer si se suministran adecuadamente dentro de la organización los recursos de TI, incluyendo personas, *software*, *hardware* y servicios.					
7) Identificar si se administran correctamente los cambios relacionados con la infraestructura y los sistemas dentro de la organización.					
8) Analizar los controles existentes después de implementadas las soluciones de TI.					
Equipo:	**Nombre**		**Fecha de Revisión**		
Subdirector:	_____		_____		
Funcionario a cargo:	_____		_____		
Director del área:	_____		_____		
Por favor marcar con "1" en la casilla correspondiente a la respuesta de cada ítem: SÍ, NO o N/A.					
DESCRIPCIÓN	**AI**	**SÍ**	**NO**	**N/A**	**OBSERVACIONES**
1. Identificar soluciones automatizadas: La necesidad de una nueva aplicación o función requiere de análisis antes de la compra o desarrollo para garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y costo - beneficio y concluye con una decisión final de "desarrollar" o "comprar". Todos estos pasos permiten a las organizaciones minimizar el costo para Adquirir e Implementar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.	AI 1				
Realización del Negocio: La realización de proyectos es un compromiso entre factores importantes como costo, calidad, velocidad, confiabilidad y dependencias	AI 1				

entre factores.					
Gestión de carteras (portafolios) / programas. Un programa puede ser visto como un grupo de proyectos y tareas por realizar en un tiempo específico, que están estrechamente vinculadas a través de objetivos comunes, un presupuesto común, cronogramas y estrategias entrelazadas.	AI 1				
· ¿Los proyectos de TI de la organización identifican soluciones que satisfagan los requerimientos del usuario?	AI 1				
· ¿Cuenta la organización con una cartera de proyectos de inversión en TI?	AI 1				
· ¿Los proyectos de TI se encuentran clasificados de alguna forma? Por tamaño, importancia, tiempo.	AI 1				
· ¿Existe un proceso de pre- selección de los proyectos de inversión que van a ingresar a la cartera de proyectos? ¿Cómo se seleccionan los proyectos de inversión?	AI 1				
· ¿Existe en la organización de TI una persona que apruebe los proyectos de inversión en TI que pasan a formar parte de la cartera? ¿Quién es esa persona?	AI 1				
· ¿La organización cuenta con un dueño o patrocinador de programa?	AI 1				
· ¿La organización cuenta con un gerente de programa?	AI 1				
· ¿La organización cuenta con un equipo de programa?	AI 1				
· ¿La organización cuenta con una oficina de programa?	AI 1				
· ¿Cuenta la organización con una metodología para la gestión de programas?	AI 1				
· ¿Cuenta la organización con procesos claramente estipulados para la gestión de programas?	AI 1				
· ¿Para iniciar un programa el dueño o patrocinador del programa envía algún escrito de asignación al gerente del programa y al equipo de programa?	AI 1				
· ¿La organización cuenta con grupos de expertos para la gestión de programas?	AI 1				
· ¿La organización cuenta con una oficina para la gestión de proyectos?	AI 1				
· ¿La organización cuenta con grupos de personal por cartera (portafolio) de proyectos?	AI 1				
· ¿Cuenta la organización con alguna otra estructura específica para la gestión de programas?	AI 1				

· ¿Cuenta la organización con directrices de gestión de proyectos?	AI 1				
· ¿Cuenta la organización con planes estándares de proyectos?	AI 1				
· ¿Cuenta la oficina de gestión de proyectos, el dueño del proceso de gestión de proyectos y de gestión de programas con una estructura permanente y bien definida?	AI 1				
· ¿Cuenta la oficina de gestión de proyectos, el dueño del proceso de gestión de proyectos y de gestión de programas con personal apto y capacitado para el puesto?	AI 1				
· ¿La oficina de gestión de proyectos mejora la calidad de la gestión de proyectos y programas?	AI 1				
· ¿La oficina de gestión de proyectos ayuda a garantizar el éxito de éstos?	AI 1				
· ¿Corresponden todos los proyectos de la cartera a programas que se están llevando a cabo en un determinado momento?	AI 1				
· ¿Cuenta la cartera de proyectos con una base de datos donde se indica: dueño, cronograma, objetivos, tipo de proyectos, estatus, costo, etc.?	AI 1				
· ¿Cuenta la cartera de proyectos con la generación de informes como gráficos, matriz de riesgos y beneficios, avances, etc.?	AI 1				
Desarrollo y aprobación del caso de negocio. Una consideración importante en cualquier proyecto de TI, ya sea para el desarrollo de un nuevo sistema o para la inversión en nueva infraestructura, es el caso de negocio, el cual consiste en un documento que provee gestión con suficiente información, necesaria para permitir decidir si se soporta un proyecto propuesto, antes de que se cause inestabilidad de recursos significativos para su desarrollo. Incluye un análisis de rentabilidad ajustado al riesgo.	AI 1				
· ¿Cuenta la organización con la elaboración de casos de negocios preliminares?	AI 1				
· ¿Para elaborar el caso de negocio la organización se basa en algún estudio de factibilidad / viabilidad?	AI 1				
· ¿Está el caso de negocio debidamente detallado? Debe describir la justificación para establecer y continuar un proyecto.	AI 1				
· ¿El caso de negocio brinda las razones que justifican el proyecto? Indicar ¿por qué debe llevarse a cabo este proyecto?	AI 1				

· Si por algún motivo el caso de negocio cambia durante el curso de un proyecto de TI. ¿Éste es re-aprobado a través del proceso de planificación y aprobación?	AI 1				
Técnicas de realización de beneficios. Un gran número de beneficios de negocio son obtenidos a través de cambios habilitados por la tecnología.	AI 1				
· ¿La organización cuenta con una descripción de la gestión de beneficios o realización de beneficios?	AI 1				
· ¿En la organización se asigna una medida y un objetivo a la realización de beneficios?	AI 1				
· ¿Cuenta la organización con un régimen de medición o seguimiento de la realización de beneficios?	AI 1				
· ¿Se documentan los supuestos de realización de beneficios?	AI 1				
· ¿Se establecen las responsabilidades clave para la realización de beneficios?	AI 1				
· ¿Se validan los beneficios que se predicen en la organización?	AI 1				
· ¿Se planifica el beneficio que se va a realizar?	AI 1				
· ¿En la organización se evalúan los procesos de realización de beneficios?	AI 1				
· ¿En la realización de beneficios, la organización realiza una revisión posterior a la implementación de 6 a 18 meses, después de la implementación de los sistemas?	AI 1				
· ¿Es la realización de beneficios parte del gobierno y de la gestión de proyectos?	AI 1				
Estructura de la gestión de proyectos: Hoy, existen muchos enfoques para la gestión de proyectos. Algunos se concentran en el desarrollo de *software*, otros son más generales; algunos se concentran en una visión holística y sistémica, otros proveen un flujo de trabajo muy detallado, incluyendo plantillas para la creación de documentos.	AI 1				
Aspectos generales. Los proyectos de SI pueden ser iniciados desde cualquier parte dentro de la organización, incluyendo el Departamento de SI.	AI 1				
· ¿La gestión de proyectos dentro de la organización contiene subprocesos como la iniciación de proyectos, planificación del proyecto, coordinación del proyecto, ejecución del proyecto, control del proyecto, gestión de la discontinuidad del proyecto, cierre del proyecto, etc.?	AI 1				

Contexto y ambiente del proyecto. Un proyecto puede dividirse en un contexto de tiempo y un contexto social.	AI 1				
· ¿Se contempló la importancia que tiene el proyecto en la organización?	AI 1				
· ¿Se estableció la conexión entre la estrategia de la organización y el proyecto?	AI 1				
· ¿Se estableció la relación que existe entre el nuevo proyecto y los existentes o los otros proyectos en proceso?	AI 1				
Tipos de estructuras organizacionales de los proyectos/ Existen tres tipos principales de alineación organizacional para gestión de proyectos dentro de la organización del negocio: por influencia, pura o por matrices.	AI 1				
· ¿Cuenta la organización con una estructura organizacional de proyectos por influencia? En esta estructura el gerente de proyecto tiene una función de soporte, sin autoridad formal de gerencia.	AI 1				
· ¿Cuenta la organización con una estructura organizacional de proyectos pura? En esta estructura el gerente de proyecto tiene autoridad formal sobre las personas que forman parte en el proyecto.	AI 1				
· ¿Cuenta la organización con una estructura organizacional de proyectos por matrices? En esta estructura la autoridad gerencial es compartida entre el gerente de proyecto y los jefes de departamento.	AI 1				
· ¿En el caso de los proyectos mayores las solicitudes son presentadas al comité directivo de SI?	AI 1				
· ¿Cuenta la Dirección con un comité directivo de SI?	AI 1				
· ¿El gerente del proyecto es identificado y asignado por el comité directivo de SI?	AI 1				
· ¿Al gerente de proyecto se le entrega total control operativo sobre el proyecto y se le asignan los recursos apropiados?	AI 1				
· ¿Están establecidas las responsabilidades que cada miembro de la estructura organizacional va a tener asignadas?	AI 1				
Comunicación y cultura de proyectos/ Dependiendo del tamaño y complejidad del proyecto y de las partes afectadas, cuando se inicia el proceso de gestión del proyecto se puede lograr la comunicación mediante reuniones de uno en uno, reuniones de arranque y talleres de inicio del proyecto o una combinación de las tres.	AI 1				

· ¿Tienen dentro de la planificación del proyecto definida la forma en la que se va a realizar la comunicación con el equipo?	AI 1				
· ¿Se establecieron en agenda, reuniones de uno a uno y talleres de inicio entre los miembros del equipo del proyecto y el gerente del proyecto?	AI 1				
· ¿Se estableció en agenda, una reunión de arranque para informar al equipo sobre lo que se va a hacer en el proyecto?	AI 1				
· ¿Se definió cuál va a ser la cultura del proyecto por desarrollar? Incluye misión del proyecto, nombre, logo, reglas, eventos, etc.	AI 1				
Objetivos del proyecto/ Un proyecto necesita resultados claramente definidos que sean específicos, medibles, alcanzables, relevantes y sujetos al tiempo.	AI 1				
· ¿Cuenta la organización con algún método para definir objetivos a los proyectos?	AI 1				
· ¿Son los resultados esperados del proyecto definidos de forma específica?	AI 1				
· ¿Son medibles los resultados esperados del proyecto?	AI 1				
· ¿Son alcanzables los resultados esperados del proyecto?	AI 1				
· ¿Son relevantes los resultados esperados del proyecto?	AI 1				
· ¿Están los resultados esperados del proyecto sujetos al tiempo?	AI 1				
· ¿Se tiene definida una estructura de desglose de objetos (OBS) para el proyecto? Dicha estructura representa los componentes individuales de la solución y sus relaciones entre sí, de forma jerárquica.	AI 1				
· ¿Se diseñó una estructura de desglose de trabajo (WBS) para el proyecto, que incluya o muestre los paquetes individuales de trabajo? Este desglose sirve de base para la planificación de costos y demás recursos.	AI 1				
Roles y responsabilidades de grupos y personas. Para lograr una realización e implementación exitosa de cualquier nuevo sistema, es recomendable que la función de auditoría tenga una parte activa, cuando sea apropiado, en el desarrollo del clico de vida de la aplicación de negocio.	AI 1				
· ¿Se tiene establecido y asignado el rol de la alta gerencia, quiénes deben comprometerse con el proyecto y aprobar los recursos necesarios para realizar el proyecto?	AI 1				
· ¿Se tiene establecido y asignado el rol de gerencia de usuario? Éste debe asumir la propiedad del proyecto y darle respuesta a las siguientes preguntas:	AI 1				

¿Están las funciones requeridas disponibles en el *software*?	AI 1				
¿El *software* es confiable?	AI 1				
¿El *software* es eficiente?	AI 1				
¿Es el *software* fácil de usar?	AI 1				
¿Es fácil de migrar o adaptar los datos del sistema anterior al nuevo?	AI 1				
¿Es fácil de migrar el *software* a otro ambiente?	AI 1				
¿Es posible agregar nuevas funciones?	AI 1				
¿Satisface los requerimientos regulatorios?	AI 1				
· ¿Se tiene establecido y asignado el rol del comité directivo del proyecto?	AI 1				
· ¿El comité directivo del proyecto es el responsable de los productos, costos y cronogramas del proyecto?	AI 1				
· ¿El comité directivo del proyecto está integrado por un alto representante de cada una de la áreas de negocio que serán afectadas por el nuevo sistema?	AI 1				
· ¿Cada miembro del comité directivo del proyecto está autorizado para tomar decisiones relativas a los diseños del sistema, que afectarán a sus respectivos departamentos?	AI 1				
· ¿El gerente del proyecto es miembro del comité directivo del proyecto? El gerente del proyecto debe ser miembro del comité directivo y hasta puede tomar el rol del presidente del comité.	AI 1				
· ¿Se tiene establecido y asignado el rol de patrocinador de proyecto? El patrocinador es el que provee los fondos para el proyecto y trabaja estrechamente con el gerente del proyecto para definir factores críticos de éxito.	AI 1				
· ¿Se tiene establecido y asignado el rol de gerencia de desarrollo de sistemas? Es el que provee soporte técnico para los ambientes de *hardware* y *software,* desarrollando, instalando y operando el sistema solicitado.	AI 1				
· ¿Se tiene establecido y asignado el rol de gerente del proyecto? Es el que provee gerencia y liderazgo continuo del proyecto, asegura que las actividades del proyecto permanezcan en línea con la dirección general.	AI 1				
· ¿Se tiene establecido y asignado el rol de equipo de proyecto de desarrollo de sistemas? Realiza las tareas asignadas, se comunica efectivamente con los usuarios.	AI 1				
· ¿Se tiene establecido y asignado el rol de director de seguridad? Asegura que los controles del sistema y los procesos que lo respaldan provean un nivel efectivo de	AI 1				

protección.					
· ¿Se tiene establecido y asignado el rol de aseguramiento de la calidad o QA? Personal que revisa los resultados y productos que se deben entregar dentro de cada etapa y al final de cada etapa, y confirma el cumplimiento de los requerimientos.	AI 1				
TOTAL AI 1		**0**	**0**	**0**	
PONDERACION					
2. Adquirir y Mantener *Software* Aplicativo: Las aplicaciones deben estar disponibles con los requerimientos del negocio. Este proceso cubre el diseño de las aplicaciones, la inclusión apropiada de controles aplicativos y requerimientos de seguridad y el desarrollo y la configuración en sí de acuerdo con los estándares. Esto permite a las organizaciones apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.	AI 2				
5. Adquirir recursos de TI: Se deben suministrar recursos TI, incluyendo personas, *hardware*, *software* y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.	AI 5				
Prácticas de Gestión de Proyectos: La gestión de proyectos es la aplicación de conocimientos, destrezas, herramientas y técnicas aplicadas a una amplia gama de actividades, para lograr un objetivo establecido, como por ejemplo satisfacer los requerimientos, el presupuesto y las fechas que define el usuario para un proyecto de SI.	AI 2, AI 5				
· ¿La organización cuenta con alguna práctica de gestión de proyectos claramente establecida? Las técnicas de gestión de proyectos proveen métodos cuantitativos y cualitativos para estimar el tamaño del *software*, la programación de actividades, la asignación de recursos y medición de productividad.	AI 2, AI 5				
· ¿La práctica de gestión de proyectos utilizada toma en cuenta la interrelación de los productos, la duración y el presupuesto?	AI 2, AI 5				

Iniciación de un proyecto/ Un proyecto será iniciado por un gerente de proyecto o patrocinador recolectando la información requerida para obtener la aprobación para el proyecto que se va a crear.	AI 2, AI 5				
· ¿Se realizaron reuniones con los responsables de las áreas que se van a influir con el proyecto por realizar, para recolectar la información requerida para obtener la aprobación del proyecto?	AI 2, AI 5				
· ¿La información recolectada fue compilada en términos de referencia o de carta?	AI 2, AI 5				
· ¿En el documento se incluyó el objetivo del proyecto?	AI 2, AI 5				
· ¿En el documento se incluyeron las partes interesadas en el sistema por ser producido?	AI 2, AI 5				
· ¿Éste documento fue aprobado? Indicar quién aprobó el proyecto, debe ser aprobado por el Gerente del proyecto.	AI 2, AI 5				
Planificación del Proyecto / Los proyectos de desarrollo/adquisición o mantenimiento de *software* tienen que ser planificados y controlados.	AI 2, AI 5				
· El gerente del proyecto determinó lo siguiente:	AI 2, AI 5				
o Las tareas que necesitan realizar para producir el sistema de aplicación esperado.	AI 2, AI 5				
o La secuencia o el orden en que estas tareas necesitan ejecutarse.	AI 2, AI 5				
o La duración o ventana de tiempo para cada tarea.	AI 2, AI 5				
o La prioridad de cada tarea.	AI 2, AI 5				
o Los recursos de TI que están disponibles y que se requieren para realizar éstas tareas.	AI 2, AI 5				
o El presupuesto o cálculo del costo para cada una de estas tareas.	AI 2, AI 5				
o La fuente y medio de financiamiento.	AI 2, AI 5				
· ¿Se realizó la estimación del tamaño del *software*?	AI 2, AI 5				
· ¿Se utilizaron las líneas de código fuente para medir la estimación del tamaño del *software*?	AI 2, AI 5				
· ¿Se utilizó el análisis de punto de fusión para medir la estimación del tamaño del *software* considerando la complejidad en el desarrollo de la aplicación?	AI 2, AI 5				
· ¿Se realizó el análisis para estimar la complejidad en el desarrollo de la aplicación?	AI 2, AI 5				

· ¿Se realizó el análisis para estimar el esfuerzo que se requerirá para llevar a cabo cada tarea?	AI 2, AI 5				
· ¿Este análisis incluyó las horas hombre por tipo de personal?	AI 2, AI 5				
· ¿Este análisis incluyó las horas máquina?	AI 2, AI 5				
· ¿Este análisis incluyó otros costos externos como licenciamiento, costos de capacitación y costos de ocupación, entre otros?	AI 2, AI 5				
· ¿Se realizó el análisis para estimar los costos del *software*?	AI 2, AI 5				
· El análisis para estimar los costos del *software* incluye los siguientes componentes que son básicos en la determinación del costo:	AI 2, AI 5				
o Lenguaje de código fuente.	AI 2, AI 5				
o Limitaciones de tiempo de ejecución.	AI 2, AI 5				
o Limitada capacidad de almacenamiento principal.	AI 2, AI 5				
o Limitada capacidad de almacenamiento de datos.	AI 2, AI 5				
o Acceso a computadoras.	AI 2, AI 5				
o La máquina objetivo usada para el desarrollo.	AI 2, AI 5				
o El ambiente de seguridad.	AI 2, AI 5				
o Experiencia del personal.	AI 2, AI 5				
· ¿Se estableció la relación secuencial entre las tareas por ejecutar? Considerando fecha de inicio y fecha más tardía de terminación esperada.	AI 2, AI 5				
· ¿Se estableció la ruta crítica para cada uno de los programas de proyecto? Ruta crítica: secuencia de actividades.	AI 2, AI 5				
· ¿Cuenta la organización con gráficas de Gantt o de PERT para asistir en la programación de las actividades (tareas) que se necesiten para un proyecto? Son herramientas útiles para mostrar la secuencia de actividades de un proyecto.	AI 2, AI 5				
· ¿La organización utiliza la gestión de la caja de tiempo cómo técnica para la gestión de proyectos de desarrollo de sistemas? Define e implanta productos de *software* dentro de un intervalo de tiempo relativamente corto, fijo y con recursos predeterminados.	AI 2, AI 5				

Gestión general de proyectos. La gestión de proyectos es un conjunto de herramientas automatizadas para manejar propuestas y estimaciones de costo, así como para monitorear, predecir y reportar sobre el desempeño, con objetos de acción recomendados.	AI 2, AI 5				
· ¿Utiliza la organización alguna otra técnica para la gestión de proyectos? Indique cuál.	AI 2, AI 5				
· ¿La organización cuenta con herramientas automatizadas para manejar la documentación durante la producción, validación y el mantenimiento del programa?	AI 2, AI 5				
· ¿La organización cuenta con herramientas de automatizadas de oficinas? Las que reducen la participación del personal en funciones que se requiere para cumplir con políticas y reuniones. Por ejemplo, correo electrónico, sistemas de archivo, etc.	AI 2, AI 5				
Control de proyectos. Las actividades de control de un proyecto incluyen gestión del alcance, uso de los recursos y riesgo.	AI 2, AI 5				
· ¿Se documentan los nuevos requerimientos para un proyecto?	AI 2, AI 5				
· ¿Cuenta la organización con gestión de alcance de proyectos? La gestión de alcance de proyectos requiere una documentación cuidadosa en forma de estructura de desglose de productos.	AI 2, AI 5				
· ¿Se lleva un procedimiento de control de cambios para los proyectos?	AI 2, AI 5				
· ¿Las solicitudes de cambios a los proyectos son enviadas al gerente de proyectos?	AI 2, AI 5				
· ¿Las copias de solicitudes de cambios son archivadas en el archivo del proyecto?	AI 2, AI 5				
· ¿El gerente de proyectos es quien determina el impacto de la solicitud de cambio sobre las actividades del proyecto (alcance), el programa y el presupuesto?	AI 2, AI 5				
· ¿El consejo consultor de cambios es quien evalúa la solicitud de cambio y decide si recomienda el cambio?	AI 2, AI 5				
· ¿Cuenta la organización con una gestión del uso de recurso? Es el proceso por el cual el presupuesto del proyecto se gasta.	AI 2, AI 5				
· ¿La organización efectúa la técnica análisis de valor obtenido (EVA)? Comparar el presupuesto, gasto real y estimado a determinada fecha.	AI 2, AI 5				
· ¿Cuenta la organización con una gestión del riesgo? Posibles eventos o condiciones negativas que desestabilizan	AI 2, AI 5				

aspectos relevantes del proyecto.					
· ¿Cuenta la organización con un inventario de riesgos?	AI 2, AI 5				
· ¿La organización realiza una evaluación de riesgos?	AI 2, AI 5				
· ¿La organización realiza un plan de mitigación de riesgos?	AI 2, AI 5				
· ¿La organización realiza una identificación oportuna de la materialización de riesgos?	AI 2, AI 5				
· ¿La organización revisa y evalúa la efectividad y los costos de los procesos de gestión de riesgos?	AI 2, AI 5				
Cierre de un proyecto. Un proyecto debe tener una vida limitada, de modo que en algún momento se cierre y el sistema nuevo o modificado sea entregado a los usuarios o al personal de soporte del sistema.	AI 2, AI 5				
· ¿El patrocinador del proyecto es el que da por aceptado el sistema y el que indica que está listo para ser entregado?	AI 2, AI 5				
· ¿Una vez cerrado un proyecto se realizan entrevistas a las partes relacionadas para obtener *retroalimentación* del proceso?	AI 2, AI 5				
· ¿Se realiza una revisión posterior a la implementación del proyecto? Para medir el éxito e impacto general del proyecto sobre las unidades de negocio.	AI 2, AI 5				
Desarrollo de aplicaciones de negocios. Las compañías destinan, con frecuencia, significativos recursos de tecnología de información (personas, aplicaciones, instalaciones, tecnología, etc.) para desarrollo, adquisición y mantenimiento de sistemas de aplicación que son críticos para el funcionamiento efectivo de los procesos clave del negocio.	AI 2, AI 5				
· ¿Cuenta la organización con un proceso de desarrollo del ciclo de vida del sistema (SDLC)?	AI 2, AI 5				
· ¿Antes de la implementación de aplicaciones de negocios la organización realiza estudios de factibilidad/viabilidad de una aplicación?	AI 2, AI 5				
· ¿Después de que los programas han sido escritos se ejecutan pruebas de unidad para validar el diseño detallado?	AI 2, AI 5				
· ¿Para verificar la especificación arquitectónica del sistema se realizan pruebas del sistema?	AI 2, AI 5				

· ¿Para verificar los requerimientos del sistema se realizan pruebas de aceptación a los usuarios finales?	AI 2, AI 5				
· ¿La organización realiza proyectos de aplicación orientados a los usuarios finales?	AI 2, AI 5				
Sistemas integrados de gestión de recursos. Un número creciente de organizaciones están cambiando grupos separados de aplicaciones interrelacionadas por una solución corporativa integrada. Ejemplo: ERP ((*Enterprise Resource Planning*: Planificación de Recursos Empresariales) es un conjunto de soluciones informáticas integradas.	AI 2, AI 5				
· ¿Cuenta la organización con una implementación de soluciones integradas? Es un proyecto de adquisición de *software* muy grande.	AI 2, AI 5				
· Si la organización llevó a cabo una implementación de una solución integral. ¿se efectuó un análisis exhaustivo del impacto y del riesgo?	AI 2, AI 5				
· Si la organización llevó a cabo una implementación de una solución integral. ¿se efectuó alguna personalización del sistema?	AI 2, AI 5				
· Si la organización llevó a cabo una implementación de una solución integral. ¿la gerencia llevó a cabo los siguientes pasos?:	AI 2, AI 5				
· 1. ¿Evaluó y aprobó todos los planes?	AI 2, AI 5				
· 2. ¿Evaluó y aprobó todos los cambios en la arquitectura del sistema?	AI 2, AI 5				
· 3. ¿Evaluó y aprobó la Dirección Tecnológica?	AI 2, AI 5				
· 4. ¿Evaluó y aprobó las estrategias de migración?	AI 2, AI 5				
· 5. ¿Evaluó y aprobó los presupuestos de SI?	AI 2, AI 5				
Dirección de las etapas tradicionales de SDLC (ciclo de vida del desarrollo de sistemas). Un enfoque tradicional se compone de una serie de fases, cada una con un conjunto definido de actividades y resultados.	AI 2, AI 5				
· ¿Cuenta la organización con un proceso de desarrollo del ciclo de vida del sistema (SDLC)?	AI 2, AI 5				
· ¿Antes de la implementación de aplicaciones de negocios la organización realiza estudios de factibilidad/viabilidad de una aplicación?	AI 2, AI 5				

· Dentro del estudio de factibilidad se consideró lo siguiente:	AI 2, AI 5				
· 1. ¿Se definió un marco de tiempo para la implementación de la solución requerida?	AI 2, AI 5				
· 2. ¿Se determinó una solución óptima basada en el riesgo?	AI 2, AI 5				
· 3. ¿Se determinó si un sistema ya existente podía corregir la situación con muy poca o ninguna modificación?	AI 2, AI 5				
· 4. ¿Se determinó si el producto de algún proveedor ofrecía una solución al problema?	AI 2, AI 5				
· 5. ¿Se determinó el costo aproximado para desarrollar el sistema?	AI 2, AI 5				
· 6. ¿Se determinó si la solución encaja en la estrategia de negocio?	AI 2, AI 5				
· ¿La organización realizó un estudio del impacto? Estudio de los efectos potenciales futuros de un proyecto de desarrollo sobre proyectos y recursos actuales.	AI 2, AI 5				
· ¿Se realizó la definición de requerimientos? Identificación y especificación de los requerimientos del negocio para el sistema seleccionado a desarrollar durante el estudio de factibilidad/viabilidad.	AI 2, AI 5				
· Dentro de los requerimientos se consideró:	AI 2, AI 5				
· 1. Las descripciones de lo que deberá hacer el sistema	AI 2, AI 5				
· 2. La forma como interactúan los usuarios con el sistema	AI 2, AI 5				
· 3. Las condiciones en que el sistema operará	AI 2, AI 5				
· 4. Los criterios de información que el sistema debe satisfacer	AI 2, AI 5				
· ¿Se consultó a los usuarios sobre la especificación de sus necesidades de recursos de información, no automatizadas y automatizadas, y cómo quieren que el sistema las resuelva?	AI 2, AI 5				
· ¿Todos los grupos interesados de Gerencia y usuarios, participaron activamente en la etapa de definición de los requerimientos?	AI 2, AI 5				
· ¿Para la creación del diseño preliminar se utilizaron diagramas de Entidad - Relación (ERD)? Herramienta que facilita el diseño.	AI 2, AI 5				
· Si la decisión fue la de comprar un paquete de *software* suministrado por un proveedor. ¿el usuario participó activamente en la evaluación del paquete y en el proceso de selección?	AI 2, AI 5				
· Para la compra del *software* a un proveedor, en el estudio de factibilidad / viabilidad se consideraron las siguientes	AI 2, AI 5				

situaciones:					
· 1. ¿El *software* se necesitaba para procesos genéricos de negocio? El *software* se implementó sin adaptarlo.	AI 2, AI 5				
· 2. ¿El *software* se tuvo que adaptar a los procesos de negocio?	AI 2, AI 5				
· 3. ¿El *software* se tuvo que desarrollar por el vendedor?	AI 2, AI 5				
· Para redactar las peticiones de propuestas, o invitación a licitar. ¿se constituyó un equipo de proyecto con participación el personal de soporte técnico y de los usuarios claves?	AI 2, AI 5				
· La invitación para la licitación incluye los siguientes factores:	AI 2, AI 5				
o Producto *vs*. Requerimientos del sistema. El producto del vendedor seleccionado debería ajustarse tanto como sea posible a los requerimientos del sistema.	AI 2, AI 5				
o Referencias del cliente. Se deben verificar las referencias del vendedor, para validar los reclamos de desempeño del producto.	AI 2, AI 5				
o Factibilidad / estabilidad financiera del vendedor. El vendedor y producto debe tener buena reputación y proporcionar evidencia de estabilidad financiera.	AI 2, AI 5				
o Disponibilidad de documentación adecuada y confiable. El vendedor debe ofrecer documentación del sistema para la revisión previa a la adquisición.	AI 2, AI 5				
o Soporte del vendedor. El vendedor debería tener disponible una línea completa de productos de soporte. Ayuda 24 horas, capacitación, actualización automática, etc.	AI 2, AI 5				
o Disponibilidad del código fuente. El vendedor debería proporcionar el código fuente en un principio o tomar previsiones para poder adquirirlo en caso de que abandone el negocio. Las actualizaciones y los parches deben estar incluidos en el acuerdo de depósito de las fuentes.	AI 2, AI 5				
o Años de experiencia ofreciendo el producto. Mientras más años tenga el producto en el mercado, más confiabilidad.	AI 2, AI 5				
o Una lista de aplicaciones recientes y planificadas para el producto y las fechas. Una lista corta, puede indicar que el producto no se actualiza con frecuencia.	AI 2, AI 5				
o Número de instalaciones que usan el producto con una lista de usuarios actuales. Si el número es algo, sugiere que en	AI 2, AI 5				

apariencia el producto es bien aceptado en el mercado.					
o Prueba de aceptación del producto. La prueba es crucial par a determinar si el producto realmente satisface los requerimientos del sistema. Puede efectuarse antes del compromiso de compra.	AI 2, AI 5				
· ¿Se analizaron varias ofertas de diferentes vendedores?	AI 2, AI 5				
· ¿El equipo de proyecto fue el responsable de analizar las propuestas de los vendedores?	AI 2, AI 5				
· ¿Se utilizó un método objetivo para la valuación de proveedores? Como son metodologías de puntuación y calificación.	AI 2, AI 5				
· Se realizó un análisis para uso del *software* que contemplara los siguientes factores:	AI 2, AI 5				
o *Hardware* requerido, incluyendo memoria, espacio de disco y características del cliente o servidor.	AI 2, AI 5				
o Versiones de sistema operativo y niveles de parches admitidos.	AI 2, AI 5				
o Herramientas adicionales tales como herramientas de importación y exportación de datos.	AI 2, AI 5				
o Bases de datos respaldadas.	AI 2, AI 5				
· El contrato con el proveedor incluye como mínimo los siguientes puntos:	AI 2, AI 5				
o Descripción específica de productos y sus costos.	AI 2, AI 5				
o Fechas de compromiso para entrega de los productos.	AI 2, AI 5				
o Compromisos para la entrega de la documentación, mantenimiento, actualizaciones, notificaciones de nuevas versiones y capacitación.	AI 2, AI 5				
o Compromiso para la migración de datos.	AI 2, AI 5				
o Autorización para un acuerdo de depósito de fuentes *(escrow)*, en caso de que los productos no incluyeran el código fuente.	AI 2, AI 5				
o Descripción del soporte que se brindará durante la instalación / adaptación.	AI 2, AI 5				
o Criterios para la aceptación por el usuario.	AI 2, AI 5				
o Disposición para permitir un período razonable de pruebas de aceptación, antes de comprometerse con la compra.	AI 2, AI 5				
o Autorización para los cambios que deba hacer la organización compradora.	AI 2, AI 5				

o Acuerdo de mantenimiento.	AI 2, AI 5				
o Autorización para copiar el software, para utilizarlo en el proceso de continuidad del negocio y para fines de prueba.	AI 2, AI 5				
o Programa de pagos vinculados con las fechas de entrega.	AI 2, AI 5				
· ¿Los usuarios participaron en la parte de diseño?	AI 2, AI 5				
· En la etapa de diseño se consideraron los siguientes aspectos:	AI 2, AI 5				
· 1. ¿Se desarrollaron diagramas de flujo del sistema?	AI 2, AI 5				
· 2. ¿Se determinó el uso de técnicas de diseño estructurado? Que muestren relaciones desde el nivel superior hasta el detalle.	AI 2, AI 5				
· 3. ¿Se describieron las entradas y salidas tales como diseños de pantalla e informes?	AI 2, AI 5				
· 4. ¿Se determinaron los pasos de procesamiento y las reglas de computación en las necesidades de requerimiento funcional?	AI 2, AI 5				
· 5. ¿Se determinó el diseño de los archivos de datos o del sistema de base de datos?	AI 2, AI 5				
· 6. ¿Se prepararon las especificaciones del programa para los diversos tipos de requerimientos o de criterios de información definidos?	AI 2, AI 5				
· 7. ¿Se desarrollaron planes de prueba para los diversos niveles de prueba? Unidad (programa), subsistema (módulo), interfaz (sistema), interfaz con otros sistemas, carga e inicialización de archivos, estrés, seguridad, respaldo y recuperación.	AI 2, AI 5				
· 8. ¿Se desarrollaron planes de conversión de datos y procedimientos manuales del viejo sistema al nuevo?	AI 2, AI 5				
· ¿Se definieron los requerimientos del nivel mínimo de *software*? Punto límite en el diseño o punto en el que ocurre el establecimiento formal de la configuración del proceso de gestión de cambios del software.	AI 2, AI 5				
· ¿Cuenta el diseño detallado del *software* con la aprobación del usuario final?	AI 2, AI 5				
· ¿Cuenta la organización con procedimientos de control para la etapa de diseño?	AI 2, AI 5				
· ¿La responsabilidad de la etapa de desarrollo está en los programadores y analistas de sistemas?	AI 2, AI 5				
· En un ambiente de prueba / desarrollo, la organización ejecuta las siguientes actividades:	AI 2, AI 5				

· 1. ¿Se codifican y desarrollan programas y documentos a nivel de sistema?	AI 2, AI 5				
· 2. ¿Se depura y prueban los programas desarrollados?	AI 2, AI 5				
· 3. ¿Se desarrollan programas para convertir datos del sistema viejo y que serán usados en el nuevo?	AI 2, AI 5				
· 4. ¿Se crean procedimientos de usuario para manejar la transición al nuevo sistema?	AI 2, AI 5				
· 5. ¿Se capacitan a los usuarios seleccionados en el nuevo sistema?	AI 2, AI 5				
· 6. ¿Se asegura que las modificaciones sean documentadas y aplicadas correcta y totalmente al *software* adquirido?	AI 2, AI 5				
· ¿Se aplican estándares para la codificación de programas?	AI 2, AI 5				
· ¿Cuenta la organización con una utilidad de programación en línea? Ya sea interna o con un proveedor.	AI 2, AI 5				
· ¿El lenguaje utilizado para programación es fácil de escribir para cualquier programador?	AI 2, AI 5				
· ¿El lenguaje utilizado para programación puede ser leído por cualquier computadora?	AI 2, AI 5				
· ¿Se utilizan programas de depuración durante el desarrollo del sistema? El propósito de utilizar programas de depuración durante el desarrollo del sistema es asegurar que todas las terminaciones anormales del sistema y todos los errores de codificación del programa son detectados y corregidos antes de pasar a producción.	AI 2, AI 5				
· La organización utiliza alguna de las siguientes herramientas de depuración (programa que asistirá al programador en la tarea de afinar, reparar o depurar el programa en desarrollo).	AI 2, AI 5				
· 1. Monitoreo de ruta lógica. Reportan sobre la secuencia de eventos ejecutados por el programa.	AI 2, AI 5				
· 2. Volcado / vaciado de memoria Provee una fotografía del contenido de la memoria interna en un momento determinado.	AI 2, AI 5				
· 3. Los analizadores de salida. Ayuda a verificar si los resultados de la ejecución del programa son correctos.	AI 2, AI 5				
· ¿En la organización se emplean pruebas para verificar un programa, subsistema o una aplicación?	AI 2, AI 5				
· ¿En la organización se emplean pruebas para validar un programa, subsistema o una aplicación?	AI 2, AI 5				

· ¿En la organización se desarrolla un plan detallado de las pruebas antes de aplicarlas?	AI 2, AI 5				
· ¿Al ejecutar las pruebas se reportan los resultados?	AI 2, AI 5				
· ¿Los problemas detectados por medio de la aplicación de pruebas son corregidos?	AI 2, AI 5				
· ¿En la organización se realizan pruebas de unidad? A un programa o módulo individual.	AI 2, AI 5				
· ¿En la organización se realizan pruebas de interfaz o de integración? Pruebas de *hardware* o *software* que evalúa la conexión de dos o más componentes que pasan información de un área a otra.	AI 2, AI 5				
· ¿En la organización se realizan pruebas de sistemas? Para asegurar que los programas modificados funcionen de manera apropiada.	AI 2, AI 5				
· Dentro de las pruebas de sistemas se realizan las siguientes:	AI 2, AI 5				
· 1. Pruebas de recuperación. Capacidad del sistema para recuperarse después de una falla.	AI 2, AI 5				
· 2. Pruebas de seguridad. Asegurarse de que el nuevo sistema incluya controles.	AI 2, AI 5				
· 3. Pruebas de carga. Probar una aplicación con grandes cantidades de datos.	AI 2, AI 5				
· 4. Pruebas de volumen. Probar con un volumen incremental de registros.	AI 2, AI 5				
· 5. Pruebas de estrés. Estudiar el impacto en la aplicación, probando con un número incremental de usuarios y/o servicios.	AI 2, AI 5				
· 6. Pruebas de desempeño. Comparar el rendimiento del sistema con otros sistemas equivalentes.	AI 2, AI 5				
· ¿En la organización se realizan pruebas de aceptación final? Por parte de los usuarios.	AI 2, AI 5				
· Se realiza en la organización alguna otra prueba como las siguientes:	AI 2, AI 5				
· 1. Pruebas alfa y beta. Alfa: versión previa de un sistema de aplicaciones. Beta: prueba en la última etapa, uso en situaciones reales.	AI 2, AI 5				
· 2. Pruebas piloto. Se centra en aspectos específicos y predeterminados de un sistema.	AI 2, AI 5				
· 3. Pruebas de la caja blanca. Evalúa la efectividad de la lógica del programa de *software*.	AI 2, AI 5				
· 4. Pruebas de la caja negra. Prueba basada en la integridad.	AI 2, AI 5				
· 5. Pruebas de función / validación. Se utilizan para probar la funcionalidad del sistema.	AI 2, AI 5				

· 6. Pruebas de regresión. Volver a ejecutar una porción de un escenario de pruebas para verificar cambios o correcciones.	AI 2, AI 5				
· 7. Pruebas en paralelo. Introducir datos de prueba en dos sistemas para comparar resultados.	AI 2, AI 5				
· 8. Pruebas de socialización. Confirmar que el nuevo sistema o el modificado puede operar en su ambiente sin impactar de manera adversa los sistemas existentes.	AI 2, AI 5				
· ¿En la organización se realizan pruebas automatizadas para las aplicaciones?	AI 2, AI 5				
· ¿Durante la fase de implementación, la organización establece y prueba la operación efectiva del nuevo sistema de información?	AI 2, AI 5				
· ¿En el caso de sistemas adquiridos, el proyecto de implementación es coordinado por la gerencia de usuario con la ayuda de la gerencia de SI? El proceso total no debe ser delegado al vendedor, para evitar cambios.	AI 2, AI 5				
· ¿Antes de la implementación se verifica la estructura de soporte?	AI 2, AI 5				
· Para verificar la estructura de soporte se toma en consideración:	AI 2, AI 5				
· 1. ¿Una planeación adecuada?	AI 2, AI 5				
· 2. ¿Una metodología?	AI 2, AI 5				
· 3. ¿Una adaptación de las mejores prácticas?	AI 2, AI 5				
· ¿La transición se efectuó sin inconvenientes de la plataforma existente a la nueva plataforma sin efectos negativos para los usuarios del sistema?	AI 2, AI 5				
· ¿Cuenta la empresa con suficiente personal de soporte para operar el nuevo ambiente de sistemas y mantener el esfuerzo de nuevas contrataciones a un nivel mínimo?	AI 2, AI 5				
· ¿La capacitación al usuario final se da en el proceso de desarrollo del sistema? Los usuarios debe informarse y capacitarse desde antes de empezar con el diseño del nuevo proyecto.	AI 2, AI 5				
· ¿Cuenta la organización con un administrador de capacitación? Es lo más conveniente, ya que el personal debe capacitarse desde las primeras fases.	AI 2, AI 5				
· ¿Los sistemas de origen y destino utilizan los mismos tamaños o formatos de campo, estructuras de campo / base de datos o sistemas de codificación?	AI 2, AI 5				

· Si los sistemas de origen y destino utilizan tamaños o formatos de campo, estructuras de campo / base de datos o sistemas de codificación diferentes. ¿utiliza la organización un sistema de conversión de datos?	AI 2, AI 5				
· ¿Para el proceso de conversión de datos se realizó un análisis detallado del diseño y planificación?	AI 2, AI 5				
· ¿Cuenta la organización con un escenario (repositorio empresarial) para simular la migración de datos antes de hacer el real?	AI 2, AI 5				
· ¿Para determinar el alcance del proyecto de implementación la organización realizó un análisis del módulo para identificar los módulos funcionales afectados y las entidades de datos?	AI 2, AI 5				
· ¿Se realiza un proceso de respaldo para administrar el repositorio de la empresa?	AI 2, AI 5				
· ¿Se desarrollan especificaciones para la infraestructura del proyecto de migración?	AI 2, AI 5				
· ¿A la hora de migrar los sistemas, se utiliza un método de despliegue escalonado de aplicaciones? Es la mejor práctica para mitigar el riesgo en las aplicaciones.	AI 2, AI 5				
· ¿Cuenta la organización con un escenario de vuelta atrás o plan de contingencias en caso de ser necesario?	AI 2, AI 5				
· ¿Las reglas de conversión de datos son preparadas por el equipo de desarrollo de *software*? Esta es la mejor práctica.	AI 2, AI 5				
· ¿Los usuarios y desarrolladores realizan ciclos de pruebas hasta que los libretos de conversión son afinados?	AI 2, AI 5				
· Para realizar la conversión de los datos se toman en consideración los siguientes aspectos:	AI 2, AI 5				
· 1. Integridad de la conversión de datos. La misma cantidad de registros (en cuanto número de campos) en ambos sistemas.	AI 2, AI 5				
· 2. Integridad de los datos. Que los datos no son alterados por ningún medio.	AI 2, AI 5				
· 3. Almacenamiento y seguridad de los datos sometidos a conversión. Creación de una copia de seguridad de los datos.	AI 2, AI 5				
· 4. Consistencia de datos. Que el campo/registro requerido por la nueva aplicación debe ser consistente con el de la aplicación original.	AI 2, AI 5				
· 5. Continuidad de la nueva aplicación. La nueva aplicación debe poder continuar con los registros nuevos.	AI 2, AI 5				

· 6. ¿La última copia de los datos antes de conversión desde la antigua plataforma y la primera copia de datos después de la conversión en la nueva plataforma se mantienen en los archivos por cualquier consulta en el futuro?	AI 2, AI 5				
· Para realizar el cambio de una aplicación existente a una nueva se realiza alguna de las siguientes técnicas:	AI 2, AI 5				
· 1. Cambio en paralelo. Inicialmente ejecutar el sistema viejo, luego ejecutar tanto el viejo como el nuevo y finalmente dejar el nuevo en su totalidad.	AI 2, AI 5				
· 2. Cambio en etapas. El sistema más viejo se divide en módulos que se van cambiando al nuevo en forma gradual.	AI 2, AI 5				
· 3. Cambio abrupto. El sistema viejo es remplazado por el nuevo en una fecha y hora de corte.	AI 2, AI 5				
· ¿Cuenta la organización con alguna certificación o acreditación de los sistemas de información?	AI 2, AI 5				
· ¿Una vez implementado el sistema la organización verifica que el sistema haya sido debidamente diseñado, desarrollado y que se hayan integrado en el sistema los controles adecuados?	AI 2, AI 5				
· En la revisión posterior a la implementación se considera:	AI 2, AI 5				
· 1. Evaluar si el sistema es adecuado. Verificando si satisface el sistema los requerimientos del usuario y los objetivos de negocio. Analizando si los controles de acceso han sido definidos e implementados de manera adecuada.	AI 2, AI 5				
· 2. Evaluar las mediciones de la relación costo/efectividad o ROI proyectado	AI 2, AI 5				
· 3. Se elaboran recomendaciones que traten los aspectos inadecuados y las deficiencias del sistema	AI 2, AI 5				
· 4. Se desarrollar un plan para implementar las recomendaciones	AI 2, AI 5				
· 5. Se evalúa el proceso de desarrollo del proyecto. Verificando si se siguieron las metodologías, estándares y técnicas escogidos.	AI 2, AI 5				
· ¿El equipo de desarrollo de proyectos junto con los usuarios finales apropiados, realizan un revisión posterior del proyecto?	AI 2, AI 5				
· ¿Algún grupo independiente realiza una revisión posterior a la implementación? Como la auditoría interna o externa.	AI 2, AI 5				
· ¿Se realizan revisiones periódicas para asegurar que el sistema sigue cumpliendo con	AI 2, AI 5				

los objetivos del negocio?					
Riesgos asociados con el desarrollo de *software*. Hay muchos riesgos potenciales que pueden ocurrir cuando se diseñan y se desarrollan sistemas aplicativos.	AI 2, AI 5				
· ¿Realiza la organización un análisis del riesgo de negocio? Probabilidad de que el nuevo sistema no satisfaga las necesidades de negocio, los requerimientos y las expectativas de los usuarios.	AI 2, AI 5				
· ¿Realiza la organización un análisis del riesgo de proyecto? Riesgo de que las actividades de proyecto para diseñar y desarrollar el sistema excedan los límites de los recursos.	AI 2, AI 5				
· ¿Realiza la organización algún tipo de análisis de los riesgos de proyectos? Como son los riesgos dentro del proyecto, con los proveedores, dentro de la organización, con el ambiente exterior, con la tecnología escogida, etc.	AI 2, AI 5				
Uso de técnicas estructuradas de análisis, diseño y desarrollo. Está estrechamente asociado con el enfoque clásico y tradicional de SDLC para el desarrollo de *software*.	AI 2, AI 5				
· ¿Cuenta la organización con el empleo de alguna técnica estructurada de análisis, diseño y desarrollo de *software*? Por ejemplo con desarrollo de diagramas, diccionarios de datos, etc.	AI 2, AI 5				
· ¿Dicha técnica se encuentra bien definida y documentada?	AI 2, AI 5				
Sistemas de aplicaciones de negocio. Numerosas funciones financieras y operativas se computarizan con el fin de mejorar la eficiencia y de aumentar la confiabilidad de la información.	AI 2, AI 5				
Comercio electrónico. Es una de las implementaciones más populares del negocio electrónico.	AI 2, AI 5				
· ¿La organización realiza algún tipo de transacciones u operaciones relacionadas con el comercio electrónico? Compra o venta de productos y servicios en línea.	AI 2, AI 5				
· De las relaciones de comercio electrónico mantenidas por la organización. ¿se encuentra alguna de las siguientes?:	AI 2, AI 5				
· 1. ¿Negocio a cliente? (B to C)	AI 2, AI 5				
· 2. ¿Negocio a negocio? (B to B)	AI 2, AI 5				

· 3. ¿Negocio a empleado? (B to E)	AI 2, AI 5				
· 4. ¿Negocio a gobierno? (B to G)	AI 2, AI 5				
· 5. ¿Relaciones consumidor a gobierno? (C to G)	AI 2, AI 5				
· 6. ¿Relaciones intercambio al intercambio? (X to X)	AI 2, AI 5				
· ¿Cuenta la organización con una estructura claramente definida y documentada del comercio electrónico?	AI 2, AI 5				
· ¿Cuenta la organización con evaluaciones de los riesgos del comercio electrónico? Como son la confidencialidad, integridad, disponibilidad, autenticación y no repudio, traslado de poder a clientes, etc.	AI 2, AI 5				
· ¿Cuenta la organización con aplicaciones de comercio electrónico dado por terceros?	AI 2, AI 5				
· ¿Cuenta la organización con contratos para las aplicaciones de comercio electrónico dado por terceros?	AI 2, AI 5				
· Dentro de los controles relacionados con el comercio electrónico se consideran los siguientes aspectos:	AI 2, AI 5				
o ¿Se cuenta con una adecuada arquitectura de seguridad para *e-commerce*? Como *firewalls*, llave pública, encriptación, *passwords*, etc.	AI 2, AI 5				
o ¿Se cuenta con mecanismos de *firewall* entre la red pública y la red privada?	AI 2, AI 5				
o ¿Se cuenta con un proceso para identificar los participantes de una transacción de manera única y positiva? Por ejemplo claves encriptadas.	AI 2, AI 5				
o ¿Se cuenta con el uso de firmas digitales?	AI 2, AI 5				
- ¿La firma digital es única para la persona que la usa?	AI 2, AI 5				
- ¿La firma puede ser verificada?	AI 2, AI 5				
- ¿El mecanismo para generar y estampar la firma está bajo el control único de la persona que la usa?	AI 2, AI 5				
- ¿La firma está vinculada con los datos, de tal forma que si los datos son cambiados, la firma queda inválida?	AI 2, AI 5				
o La infraestructura para gestionar y controlar los pares de claves públicas y sus certificados incluyen:	AI 2, AI 5				
- ¿Existe una autoridad de certificación? Da fe, como proveedor confiable de pares de calves pública/privada, de la autenticidad del propietario.	AI 2, AI 5				

- ¿Existe una autoridad de registro? Entidad opcional independiente de una autoridad certificadora, pero que ayuda a esta con varias de sus funciones.	AI 2, AI 5				
- ¿Existe una lista de Certificados revocados? Instrumento para verificar la validez continua de los certificados. Por lo general es una base de datos en línea altamente controlada, a través de la cual los suscriptores y administradores pueden determinar la situación del certificado de un socio determinado.	AI 2, AI 5				
- ¿Existe una declaración de práctica de certificación? Conjunto detallado de reglas que rigen las operaciones de la autoridad de certificación.	AI 2, AI 5				
o ¿Cuenta la organización con procedimientos establecidos para controlar los cambios en la presencia de un comercio electrónico?	AI 2, AI 5				
o ¿Los registros de las aplicaciones de comercio electrónico son monitoreados por personal responsable? Registros *(logs)*, sistema operativo, mensajes, red. Registros *(logs)*, etc.	AI 2, AI 5				
o ¿Cuenta la organización con un sistema de detección de intrusos basados en la red y en el anfitrión *(host)*?	AI 2, AI 5				
o ¿Cuenta la organización con funciones en las aplicaciones de comercio electrónico para reconstruir la actividad realizada por la aplicación?	AI 2, AI 5				
o ¿Cuenta la organización con protecciones establecidas para asegurar que los datos recogidos sobre las personas no sean revelados ni utilizados para otros fines?	AI 2, AI 5				
o ¿Cuenta la organización con medios para garantizar la confidencialidad de los datos transmitidos entre clientes y proveedores?	AI 2, AI 5				
o ¿Cuenta la organización con mecanismos para proteger la presencia del comercio electrónico y sus redes privadas de virus de computadoras y para impedir que estos propaguen virus a clientes y proveedores?	AI 2, AI 5				
o ¿Cuentan con funciones dentro de la arquitectura del comercio electrónico para evitar que todos los componentes fallen y para que se reparen a sí mismos si fallaran?	AI 2, AI 5				
o ¿Se cuenta con un plan y procedimientos para continuar las actividades del comercio electrónico en el caso de una ausencia prolongada de los recursos que se	AI 2, AI 5				

requieren para el procesamiento normal?					
o ¿Cuenta la organización con prácticas y procedimientos relacionados con la seguridad, emitidos por la gerencia?	AI 2, AI 5				
o ¿La responsabilidad para la seguridad del comercio electrónico se encuentra compartida dentro de la organización?	AI 2, AI 5				
o ¿Se comunica a los clientes sobre el nivel de seguridad en la arquitectura del comercio electrónico?	AI 2, AI 5				
Intercambio electrónico de datos. El EDI es una de las primeras aplicaciones de comercio electrónico utilizada entre socios de negocio para transmitir transacciones entre organizaciones con sistemas de computador diferentes.	AI 2, AI 5				
· ¿La organización mantiene intercambio electrónico de datos con alguna otra organización o empresa?	AI 2, AI 5				
· ¿Existe contratos para los EDI mantenidos por la organización?	AI 2, AI 5				
· ¿La organización utiliza el sistema tradicional EDI? Movimiento de datos en un proceso de transmisión por lotes.	AI 2, AI 5				
· Si la organización utiliza el sistema tradicional. incluye las siguientes funciones dentro del sistema de computadoras de cada socio:	AI 2, AI 5				
o ¿Se incluye el administrador de comunicaciones? Proceso para transmitir y recibir documentos electrónicos entre los socios comerciales por medio de líneas de discado, red conmutada pública, líneas múltiples dedicadas o red de valor agregado.	AI 2, AI 5				
o ¿Se incluye la interfaz EDI? Función de interfaz que manipula y dirige los datos entre el sistema de aplicación y el operador de comunicaciones.	AI 2, AI 5				
o ¿Se incluye el sistema de aplicaciones? Son programas que procesan los datos que deben ser enviados al o recibidos del socio comercial.	AI 2, AI 5				
· ¿La organización utiliza el sistema EDI basado en la web? A través de las infraestructuras comerciales disponibles al público ofrecidas a través de internet.	AI 2, AI 5				
Riesgos y controles de EDI. Por su naturaleza híbrida, existen riesgos únicos de EDI.	AI 2, AI 5				

· ¿Utiliza la organización algún procedimiento para el control de las autorizaciones de las transacciones mantenidas por Internet?	AI 2, AI 5				
· ¿Cuenta la organización con algún plan de continuidad del negocio en caso de que se suspenda el servicio de Internet?	AI 2, AI 5				
· ¿Utiliza la organización algún procedimiento para el control de las modificaciones de datos mantenidos o manipulados por Internet?	AI 2, AI 5				
Controles en el ambiente EDI. Los riesgos de seguridad se pueden resolver al aplicar controles generales y establecer una capa adicional de procedimientos de control de aplicación sobre el proceso de EDI.	AI 2, AI 5				
· ¿Cuenta la organización con estándares para indicar el formato y el contenido de los mensajes?	AI 2, AI 5				
· ¿Existen controles para asegurar que las transmisiones estándar son correctamente convertidas para el *software* de aplicación por la aplicación de traducción?	AI 2, AI 5				
· ¿Se cuenta con controles para probar la razonabilidad de los mensajes recibidos?	AI 2, AI 5				
· ¿Se cuenta con controles para proteger contra la manipulación de datos en las transacciones activas, expedientes y archivos?	AI 2, AI 5				
· ¿Se cuenta con procedimientos para la autorización de mensajes?	AI 2, AI 5				
· ¿Existen canales de transmisión directos o dedicados entre las partes?	AI 2, AI 5				
· ¿Los datos se encuentran encriptados utilizando algoritmos?	AI 2, AI 5				
· ¿Se cuenta con firmas electrónicas para identificar origen y destino?	AI 2, AI 5				
· ¿Existen códigos de autenticación de mensajes? Para verificar que lo que se envía es lo que se recibe.	AI 2, AI 5				
· ¿Cuenta la organización con un procedimiento para el recibo de las transacciones entrantes?	AI 2, AI 5				
· El procedimiento para el recibo de las transacciones entrantes incluye los siguientes controles:	AI 2, AI 5				
o ¿Técnicas apropiadas de encriptación cuando se usan infraestructuras públicas de Internet?	AI 2, AI 5				
o ¿Chequeos de edición? Para identificar transacciones erróneas, inusuales o inválidas.	AI 2, AI 5				
o ¿Realización de verificación computarizada adicional? Para evaluar la razonabilidad de la transacción, validez, etc.	AI 2, AI 5				

o ¿Registro de cada transacción entrante a su recibo?	AI 2, AI 5				
o ¿Uso de totales de control al recibo de las transacciones? Para verificar el número y valor de la transacción.	AI 2, AI 5				
o ¿Contadores de totales por segmentos?	AI 2, AI 5				
o ¿Técnicas de control en el procesamiento de transacciones individuales? Por ejemplo, dígitos de chequeo, contadores de datos repetidos, etc.	AI 2, AI 5				
o ¿Intercambio de totales de control de transacciones enviadas y recibidas entre los socios pro intervalos predefinidos?	AI 2, AI 5				
o ¿Actualización de número de mensajes recibidos/enviados y validar el dato con los socios cada cierto tiempo?	AI 2, AI 5				
o ¿Seguridad sobre los archivos temporales? Transacciones en trámite.	AI 2, AI 5				
· ¿Cuenta la organización con un procedimiento para el recibo de las transacciones salientes?	AI 2, AI 5				
· El procedimiento para el recibo de las transacciones salientes incluye los siguientes controles:	AI 2, AI 5				
o ¿Controlan la parametrización y la modificación de los detalles de los socios?	AI 2, AI 5				
o ¿Comparan las transacciones con los perfiles de transacciones de los socios?	AI 2, AI 5				
o ¿Se hace coincidir el número de socio comercial con el archivo maestro de comerciantes? Antes de la transmisión.	AI 2, AI 5				
o ¿Se limita la autoridad de los usuarios dentro de la organización para iniciar transacciones EDI específicas?	AI 2, AI 5				
o ¿Se segregan las responsabilidades de iniciar y transmitir para las transacciones de alto riesgo?	AI 2, AI 5				
o ¿Se documenta la liberación de cada procedimiento programado así como sus cambios posteriores?	AI 2, AI 5				
o ¿Se registran todas las transacciones de pago en un archivo separado, que sea revisado para verificar si están autorizadas las transacciones, antes de su transmisión?	AI 2, AI 5				
o ¿Se segregan las funciones dentro del ciclo de transacciones, en particular cuando las transacciones sean generadas automáticamente por el sistema?	AI 2, AI 5				
o ¿Se segrega el acceso a los diferentes procesos de autorización en un ciclo de transacción?	AI 2, AI 5				

o ¿Se reportan las transacciones grandes (en valor) o inusuales para su revisión antes o después de su transmisión?	AI 2, AI 5				
o ¿Se registran las transacciones salientes en un archivo temporal seguro hasta que sean autorizadas?	AI 2, AI 5				
o ¿Se requiere autorización sin papeles? Acceso especial a campos de autorización dentro del sistema de cómputo.	AI 2, AI 5				
Correo electrónico. Puede ser la función más usada de internet en una organización.	AI 2, AI 5				
· ¿Cuenta la organización con procedimientos para la utilización del correo electrónico?	AI 2, AI 5				
· ¿Cuenta la organización con estándares para la seguridad del correo electrónico?	AI 2, AI 5				
· ¿Dentro de la seguridad, se cuenta con la firma electrónica para los correos?	AI 2, AI 5				
· ¿Cuenta la organización con contrafuegos (*firewalls*)?	AI 2, AI 5				
· ¿Cuenta la organización con enrutadores (*routers*)?	AI 2, AI 5				
· ¿Cuenta la organización con sistemas de detección de intrusos?	AI 2, AI 5				
Sistemas de punto de venta (POS) permiten la captura de datos en el momento y en el lugar que ocurren las transacciones.	AI 2, AI 5				
· ¿Cuenta la organización con sistemas de punto de venta (POS)?	AI 2, AI 5				
· Cuenta la organización con algunos de los equipos periféricos siguientes conectados a sus POS:	AI 2, AI 5				
· 1. ¿Escáneres ópticos?	AI 2, AI 5				
· 2. ¿Datáfonos?	AI 2, AI 5				
· 3. ¿Lectores de tarjetas inteligentes?	AI 2, AI 5				
· 4. ¿Otros?	AI 2, AI 5				
· ¿Se encuentran los sistemas POS en línea a una computadora central propiedad de un tercero?	AI 2, AI 5				
· ¿Se encuentra la información de los clientes almacenadas en la computadora central?	AI 2, AI 5				
· Si la información de los clientes se encuentra almacenada en el POS ¿está encriptada con métodos de encriptación fuertes?	AI 2, AI 5				
Banca electrónica. Las organizaciones bancarias vienen entregando servicios electrónicos a distancia a consumidores y	AI 2, AI 5				

negocios desde hace años.					
· ¿Posee la organización transacciones en línea con instituciones financieras?	AI 2, AI 5				
· ¿Existen contratos para las relaciones electrónicas mantenidas con instituciones financieras?	AI 2, AI 5				
· ¿Cuenta la organización con supervisión activa por parte de la dirección y la gerencia?	AI 2, AI 5				
· ¿Cuenta la organización con controles de seguridad para las transacciones de banca electrónica?	AI 2, AI 5				
· ¿Cuenta la organización con una adecuada gestión del riesgo?	AI 2, AI 5				
· La gestión de riesgos incluye los siguientes controles:	AI 2, AI 5				
· **Supervisión alta gerencia:**	AI 2, AI 5				
o ¿Se da una supervisión efectiva de las actividades de banca electrónica por parte de la alta gerencia?	AI 2, AI 5				
o ¿Existe un establecimiento de un proceso amplio de control y seguridad?	AI 2, AI 5				
o ¿Existe un proceso general de la debida diligencia de supervisión por parte de la alta gerencia de las relaciones de externalización y de otras dependencias con terceros?	AI 2, AI 5				
· **Controles de seguridad:**	AI 2, AI 5				
o ¿Se realiza una autenticación de clientes de la banca electrónica?	AI 2, AI 5				
o ¿Se da una verificación de no repudio y responsabilidad de las transacciones de banca electrónica?	AI 2, AI 5				
o ¿Existen medidas apropiadas para asegurar la separación de funciones?	AI 2, AI 5				
o ¿Existen los debidos controles de autorización dentro de los sistemas de banca electrónica, bases de datos y aplicaciones?	AI 2, AI 5				
o ¿Se verifica la integridad de datos de las transacciones, registros e información de banca electrónica?	AI 2, AI 5				
o ¿Se da un establecimiento de pistas de auditoría claras para las transacciones de banca electrónica?	AI 2, AI 5				
o ¿Existe confidencialidad de la información clave del banco?	AI 2, AI 5				
· **Gestión de riesgo legal y del riesgo de reputación:**	AI 2, AI 5				
o ¿Se cuenta con revelaciones apropiadas para los servicios de banca electrónica?	AI 2, AI 5				

o ¿Se da privacidad de la información de clientes?	AI 2, AI 5				
o ¿Existe una adecuada planeación de la capacidad, continuidad del negocio y de las contingencias para asegurar la disponibilidad de los sistemas y servicios de banca electrónica?	AI 2, AI 5				
o ¿Existe una adecuada planeación de respuesta a incidentes?	AI 2, AI 5				
Finanzas electrónicas. El comercio electrónico está permitiendo que surjan nuevos proveedores como bancos, corretajes y productos financieros, tales como préstamos, seguros, etc.	AI 2, AI 5				
· ¿Cuenta la organización con proveedores de productos financieros electrónicos?	AI 2, AI 5				
· ¿Cuenta la organización con contratos para productos financieros electrónicos mantenidos?	AI 2, AI 5				
· ¿Cuenta la organización con procedimientos de control para las transacciones realizadas con productos financieros electrónicos?	AI 2, AI 5				
Sistemas de pagos. Hay dos tipos de partes involucradas en todos los sistemas de pago, los emisores y los usuarios.	AI 2, AI 5				
· ¿Cuenta la organización con un sistema de pagos basado en el modelo de dinero electrónico?	AI 2, AI 5				
· ¿Cuenta la organización con un sistema de pagos basado en el modelo de cheques electrónicos?	AI 2, AI 5				
· ¿Cuenta la organización con un sistema de pagos basado en el modelo de transferencia electrónica?	AI 2, AI 5				
· ¿Cuenta la organización con contratos relacionados con los sistemas de pago electrónicos mantenidos?	AI 2, AI 5				
· ¿Cuenta la organización con procedimientos de control para los sistemas de pago electrónicos? Sobre todo aquellos que tienen que ver con seguridad de acceso y autorización de procesamiento.	AI 2, AI 5				
Procesamiento de imágenes. Un sistema de imágenes almacena, recupera y procesa datos gráficos como fotografías, diagramas, gráficas, etc.	AI 2, AI 5				
· ¿Cuenta la organización con un sistema de procesamiento de imágenes?	AI 2, AI 5				
· ¿Cuenta la organización con procedimientos actualizados y autorizados para el sistema de procesamiento de imágenes?	AI 2, AI 5				

· ¿Antes de la implementación del procesamiento de imágenes se contó con una planificación adecuada? Por el alto costo que un sistema de este tipo tiene.	AI 2, AI 5				
Formas alternativas de organización de proyectos de *software*. Existen métodos diferentes de organizar proyectos de *software*.	AI 2, AI 5				
· ¿La organización de proyectos de *software* cuenta con un desarrollo incremental o progresivo? Sistema construido en etapas o versiones, en lugar de ser entregado en su totalidad.	AI 2, AI 5				
· ¿El desarrollo de los proyectos de *software* se efectúa en forma iterativa? Construir el sistema en iteraciones o incrementos, haciendo mejoras después de cada incremento.	AI 2, AI 5				
· Si el desarrollo de los proyectos de *software* se efectúa en forma iterativa se considera alguna de las siguientes variantes:	AI 2, AI 5				
o Desarrollo evolutivo. La creación de prototipos.	AI 2, AI 5				
o Desarrollo en espiral. Una serie de prototipos se usa para desarrollar una solución, hasta el punto de diseño detallado, construcción y prueba.	AI 2, AI 5				
o Desarrollo ágil. El proyecto se desglosa en iteraciones de caja de tiempo, relativamente cortas.	AI 2, AI 5				
· ¿Cuenta la organización con formas alternativas de organización de proyectos de *software*? Indique cuáles.	AI 2, AI 5				
Métodos alternativos de desarrollo. Frente a la complejidad cada vez mayor de los sistemas y la necesidad de implementar nuevos sistemas en menor tiempo para lograr beneficios antes de que cambien las reglas de negocio, los profesionales del desarrollo de *software* han adoptado nuevas formas de organizar los proyectos que varían o se apartan radicalmente de los métodos tradicionales.	AI 2, AI 5				
Desarrollo de sistemas orientado a datos. El DOSD es un método para representar los requerimientos de *software* centrándose en los datos y en su estructura.	AI 2, AI 5				
· ¿Cuenta la organización con el método de desarrollo de sistemas orientado a datos?	AI 2, AI 5				
Desarrollo de sistemas orientado a objetos. El OOSD es el modelo de especificación y modelación de soluciones, donde tanto los datos como los procedimientos pueden ser agrupados en una entidad conocida como	AI 2, AI 5				

un objeto.					
· ¿Cuenta la organización con la técnica de programación de desarrollo de sistemas orientado a objetos?	AI 2, AI 5				
Desarrollo basado en componentes. Puede ser considerado como una derivación del desarrollo orientado a objetos y significa ensamblar aplicaciones de paquetes cooperativos de *software* a través de interfaces definidas.	AI 2, AI 5				
· ¿Cuenta la organización con el método de desarrollo de sistemas basado en componentes?	AI 2, AI 5				
Desarrollo de aplicaciones basadas en la web. Es un nuevo enfoque de desarrollo de *software* diseñado para lograr una integración más fácil y efectiva de módulos de código dentro y entre las empresas.	AI 2, AI 5				
· ¿Cuenta la organización con el método de desarrollo de aplicaciones basadas en la web?	AI 2, AI 5				
Reingeniería de *software*. Es el proceso de actualizar un sistema existente extrayendo y reutilizando componentes de diseño y de programas.	AI 2, AI 5				
· ¿Cuenta la organización con el proceso de actualizar sistemas utilizando reingeniería de *software*?	AI 2, AI 5				
Ingeniería inversa. Es el proceso de estudiar y analizar una aplicación de *software* o un producto para ver cómo funciona y usar esa información para desarrollar un sistema similar.	AI 2, AI 5				
· ¿Utiliza la organización el proceso de ingeniería inversa?	AI 2, AI 5				
TOTAL AI 2 Y 5		0	0	0	
PONDERACION					
3. Adquirir y Mantener Infraestructura Tecnológica: Las organizaciones deben contar con procesos para adquirir, implementar y actualizar la infraestructura tecnológica. Esto requiere de un enfoque planeado para adquirir, mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones.	AI 3				

Desarrollo de infraestructura / prácticas de adquisición. El análisis de arquitectura física, la definición de una nueva y el plan de acción necesario para moverse de una a otra es una tarea crítica para un departamento de TI.	AI 3				
Fases del proyecto de análisis de arquitectura física.	AI 3				
· ¿Cuenta la organización con fases claramente estipuladas y documentas para realizar el análisis de su arquitectura física de sistemas?	AI 3				
· ¿Antes de adquirir infraestructura nueva, se hace un proceso de revisión de los documentos más recientes sobre la arquitectura existente?	AI 3				
· ¿En la revisión de la arquitectura existente participan especialistas del departamento de tecnologías de información y comunicaciones de todas las áreas directamente impactadas?	AI 3				
· ¿En la revisión de la arquitectura existente se elabora un documento con la lista de los componentes actuales de infraestructura y las limitaciones que definen el objetivo de la arquitectura física?	AI 3				
· ¿Después de revisar la arquitectura existente, se lleva a cabo un análisis y diseño de la arquitectura física real?	AI 3				
· ¿Con el primer diseño de la arquitectura física se crea el primer (borrador) de requerimientos funcionales?	AI 3				
· ¿Mientras se redacta el borrador el requerimientos funcionales se inicia en paralelo el proceso de selección de proveedores?	AI 3				
· ¿Una vez redactado el documento de requerimientos funcionales, se realiza un taller con el personal proveniente de todas las áreas afectadas? Se deben incluir las observaciones de todos para el documento definitivo.	AI 3				
· ¿Se realiza en la organización una prueba de concepto? Para probar que el *hardware* y el *software* seleccionados pueden satisfacer todas las expectativas, incluyendo los requerimientos de seguridad.	AI 3				
· ¿Después de la prueba de concepto se obtiene como producto el prototipo para la ejecución, el documento asociado y los protocolos de prueba que describen las pruebas y sus resultados?	AI 3				
· En el prototipo se incluyen las siguientes características:	AI 3				

o El establecimiento básico del núcleo de la infraestructura de seguridad.	AI 3				
o La funcionalidad correcta de los componentes de auditoría.	AI 3				
o La implementación básica pero funcional de las medidas de seguridad que están definidas.	AI 3				
o Las transacciones seguras.	AI 3				
o La caracterización en términos de restricciones y límites de la instalación (tamaño del servidor, consumo actual del servidor, peso de los servidores, sala de servidores de seguridad física, etc.)	AI 3				
o El desempeño.	AI 3				
o La flexibilidad.	AI 3				
o El financiamiento y modelo de costos,	AI 3				
· ¿Luego de tener listo el prototipo se lleva a cabo otro taller donde se adaptan el tamaño y formato de la arquitectura del ambiente productivo? Se deben incluir las conclusiones de la prueba de concepto.	AI 3				
Planificación de implementación de infraestructura. Para asegurar la calidad de los resultados, es necesario usar un método escalonado en etapas.	AI 3				
· ¿Cuenta la organización con algún método para realizar la implementación de infraestructura?	AI 3				
· ¿Durante la etapa de adquisición se establecen los procesos de comunicación con el proyecto de análisis para obtener un panorama de la solución escogida y determinar la estructura cuantitativa de los productos?	AI 3				
· ¿Durante la etapa de adquisición se lleva a cabo también el proceso a nivel de servicio?	AI 3				
· ¿En esta etapa la organización firma los productos, contratos y acuerdos de niveles de servicio?	AI 3				
· ¿Se desarrolla en la organización un plan de entrega del producto?	AI 3				
· El plan de entrega incluye lo siguiente:	AI 3				
o Prioridades.	AI 3				
o Metas.	AI 3				
o Hechos clave.	AI 3				
o Principios.	AI 3				
o Estrategias de comunicación.	AI 3				
o Indicadores clave.	AI 3				
o Avances en las tareas clave.	AI 3				
o Responsabilidades.	AI 3				
· ¿Se desarrolla en la organización un plan de instalación producto?	AI 3				

· ¿El plan de instalación se desarrolla en cooperación con todas las partes afectadas?	AI 3				
· ¿Se desarrolla en la organización un plan de pruebas del producto instalado?	AI 3				
· El plan de pruebas incluye lo siguiente:	AI 3				
o Casos de prueba.	AI 3				
o Especificaciones de los requerimientos básicos.	AI 3				
o Definición de los procesos.	AI 3				
o Mediciones de las aplicaciones y la infraestructura.	AI 3				
Factores críticos de éxito.	AI 3				
· ¿El personal experto asiste a los talleres y participan durante todo proyecto? Con el fin de evitar demoras.	AI 3				
· ¿La documentación necesaria para llevar a cabo el trabajo está lista al inicio del proyecto?	AI 3				
· ¿Los funcionarios que toman decisiones participan en todos los pasos? Para asegurar que se tomen rápidamente todas las decisiones necesarias.	AI 3				
Adquisición de *hardware*. La selección del *hardware* de computadoras y del ambiente de *software* requiere de la preparación de las especificaciones para ser distribuida entre los proveedores y de criterios para evaluar las propuestas de los proveedores.	AI 3				
· ¿Cuenta la organización con un procedimiento formal para la adquisición de *hardware,* donde se indiquen todas las especificaciones y pasos para la adquisición?	AI 3				
· Las especificaciones para el *hardware* incluye lo siguiente:	AI 3				
o Posible uso.	AI 3				
o Tareas y requerimientos para el equipo que se necesita.	AI 3				
o Descripción del ambiente donde el equipo será utilizado.	AI 3				
o Descripciones organizacionales. Que indican si las instalaciones de computadoras están centralizadas o descentralizadas, distribuidas, externalizadas, operadas por personal o sin personal.	AI 3				
o Requerimientos de procesamiento de información, tales como:	AI 3				
- Sistemas de aplicaciones existentes principales.	AI 3				
- Sistemas de aplicaciones futuros.	AI 3				
- Requerimientos de carga de trabajo.	AI 3				
- Requerimientos de desempeño.	AI 3				
- Enfoques de procesamiento. Por ejemplo, en línea/en lote, cliente-servidor, bases de datos en tiempo real, operación	AI 3				

continua, etc.					
o Requerimientos de *hardware*, tales como:	AI 3				
- Velocidad de la unidad central de procesamiento (CPU).	AI 3				
- Requerimientos de espacio en disco.	AI 3				
- Requerimientos de memoria.	AI 3				
- Número de CPUs requeridos.	AI 3				
- Dispositivos periféricos. Por ejemplo, dispositivos secuenciales como unidades de cinta, dispositivos de acceso directo, tales como unidades de disco magnético, impresoras, unidades de disco compacto, unidades de disco de video digital, *Universal Serial Bus* (USB) periféricos y tarjetas digitales seguras (SD/MMC) necesarios o que serán excluidos (generalmente por razones de seguridad).	AI 3				
- Dispositivos de preparación / entrada de datos). Que aceptan los datos para su procesamiento.	AI 3				
- Dispositivos de entrada directa. Por ejemplo, terminales, terminales de punto de venta, cajeros automáticos.	AI 3				
- Capacidad de conexión a red. Por ejemplo, conexiones Ethernet, módems y conexiones de red digital de servicios integrados.	AI 3				
- Número de terminales o nodos que el sistema necesita respaldar.	AI 3				
o Aplicaciones de *software* de sistema, tales como:	AI 3				
- *Software* de sistema operativo. Versión actual y actualizaciones requeridas.	AI 3				
- Utilidades.	AI 3				
- Compiladores.	AI 3				
- *Software* de biblioteca de programas.	AI 3				
- *Software y* programas de administración de base de datos.	AI 3				
- *Software* de comunicaciones.	AI 3				
- *Software* de control de acceso.	AI 3				
- *Software* de creación de cronogramas de trabajo.	AI 3				
o Requerimientos de respaldo, tales como:	AI 3				
- Mantenimiento de sistemas. Para fines de prevención, detección (reporte de falla) o corrección.	AI 3				
- Capacitación para personal técnico y usuarios.	AI 3				

- Copias de respaldo. Diarias y para recuperación ante desastres.	AI 3				
o Requerimientos de adaptabilidad, tales como:	AI 3				
- Capacidad de actualización de *hardware* y *software*.	AI 3				
- Compatibilidad con las plataformas de *hardware* y *software* existentes.	AI 3				
- Migración a otras capacidades de equipos.	AI 3				
o Limitaciones, tales como:	AI 3				
- Niveles de personal.	AI 3				
- Capacidad de *hardware* existente.	AI 3				
- Fechas de entrega.	AI 3				
o Requerimientos de conversión, tales como:	AI 3				
- Tiempo de prueba para el *hardware* y *software.*	AI 3				
- Instalaciones de conversión de sistema.	AI 3				
- Cronograma de costos /precios.	AI 3				
o Al comprar o adquirir *hardware* y *software* a un proveedor en la organización, se tiene en cuenta lo siguiente:	AI 3				
- Testimonios o visitas a otros usuarios.	AI 3				
- Disposiciones de licitación competitiva.	AI 3				
- Análisis de ofertas frente a requerimientos.	AI 3				
- Comparación de ofertas mediante criterios de evaluación predefinidos.	AI 3				
- Análisis de condición financiera del proveedor.	AI 3				
- Análisis de la capacidad del proveedor de proveer mantenimiento y soporte. Incluyendo capacitación.	AI 3				
- Revisión de cronogramas de entrega frente a requerimientos.	AI 3				
- Análisis de la capacidad de actualización de *hardware* y *software.*	AI 3				
- Análisis de control y seguridad de las instalaciones.	AI 3				
- Evaluación de desempeño frente a requerimientos.	AI 3				
- Revisión y negociación de precio.	AI 3				
- Revisión de los términos del contrato. Incluyendo cláusulas de derecho a ser auditados.	AI 3				
- Elaboración de un informe formal por rescrito. Que resuma el análisis para cada una de las alternativas y la justificación para la selección basada en los beneficios y en el costo.	AI 3				

o ¿Se planifica y documenta los criterios y los datos usados para evaluar las propuestas de los proveedores?	AI 3				
o En el proceso de evaluación de los proveedores se consideran los siguientes criterios:	AI 3				
- Tiempo de procesamiento. El tiempo la mesa de ayuda o el proveedor necesita para resolver un problema desde el momento en que se inicia la sesión.	AI 3				
- Tiempo de respuesta. El tiempo que un sistema necesita para responder a una consulta específica del usuario.	AI 3				
- Tiempo de reacción del sistema. El tiempo requerido para iniciar la sesión en un sistema o conectarse a una red.	AI 3				
- *Throughput.* La cantidad de trabajo útil hecho por el sistema por unidad de tiempo. Puede medirse en instrucciones por segundo o en alguna otra unidad de rendimiento. Cuando se trata de una operación de transferencia de datos, el *throughput* mide la velocidad de transferencia de datos útiles y está expresado en kilobits por segundo (Kbps), megabits por segundo (Mbps) y gigabits por segundo (Gbps).	AI 3				
- Carga de trabajo. La capacidad para manejar el volumen requerido de trabajo, o el volumen de trabajo que el sistema del vendedor puede manejar en un marco dado de tiempo.	AI 3				
- Compatibilidad. La capacidad de una aplicación existente de ejecutar exitosamente en el sistema más nuevo suministrado por el vendedor.	AI 3				
- Capacidad. La facultad del sistema para manejar un número de solicitudes simultáneas de la red para la aplicación y el volumen de datos que puede manejar de cada uno de los usuarios.	AI 3				
- Utilización. El tiempo de disponibilidad del sistema en comparación con el tiempo de inactividad del sistema.	AI 3				
Adquisición de *software* del sistema. Cada vez el desarrollo tecnológico ha permitido mayores velocidades de cómputo o nuevas capacidades, estas han sido inmediatamente absorbidas por las exigencias puestas a los recursos de cómputo por aplicaciones más ambiciosas.	AI 3				
· ¿Cuenta la organización con un procedimiento formal para la adquisición de *software*, donde se indiquen todas las especificaciones y pasos para la adquisición?	AI 3				

· ¿La organización mantiene actualizados sus sistemas? Aplicando últimas versiones o ediciones así como las actualizaciones /parches más recientes del *software d*e los sistemas.	AI 3				
· ¿En los planes de corto y largo plazo se documenta la posición de la gerencia de SI de migrar a sistemas operativos más recientes, eficientes y altamente efectivos?	AI 3				
· ¿Cuándo se selecciona un nuevo sistema de *software* se consideran los siguientes aspectos técnicos y de negocio:	AI 3				
o Necesidades y especificaciones técnicas, funcionales y de negocio.	AI 3				
o Costo y beneficio.	AI 3				
o Obsolescencia.	AI 3				
o Compatibilidad con sistemas existentes.	AI 3				
o Seguridad.	AI 3				
o Demandas de personal existente.	AI 3				
o Requerimientos de capacitación y contratación.	AI 3				
o Necesidades futuras de crecimiento.	AI 3				
o Impacto sobre desempeño del sistema y la red.	AI 3				
o Código de fuente abierta vs. Código propietario.	AI 3				
Implementación del *software* del sistema.	AI 3				
· ¿Cuenta la organización con procedimientos claramente establecidos para la implementación de *software*?	AI 3				
· ¿La implementación del *software* del sistema incluye la identificación de característica?	AI 3				
· ¿La implementación del *software* del sistema incluye opciones de configuración?	AI 3				
· ¿La implementación del *software* del sistema incluye controles para una configuración estándar que se aplicará en toda la organización?	AI 3				
· ¿En la implementación se probó el *software* en un ambiente ajeno a la producción? Esto implica obtener algún tipo de certificación y acreditación para colocar el *software* del sistema operativo probado en producción.	AI 3				
TOTAL AI 3		0	0	0	
PONDERACION					
4. Facilitar la Operación y el Uso: El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar	AI 4				

el uso y la operación correctos de las aplicaciones y la infraestructura.					
· ¿Se desarrolla en la organización un plan para identificar y documentar todos los aspectos técnicos de las soluciones de operación? Soluciones de operación: introducción o actualización de sistemas automatizados o de infraestructura.	AI 4				
· ¿Dicho plan identifica y documenta la capacidad de operación de la solución?	AI 4				
· ¿Dicho plan identifica y documenta los niveles de servicio de la solución?	AI 4				
· ¿Se realiza una transferencia del conocimiento de la solución a la gerencia de la organización?	AI 4				
· Para garantizar la participación de la gerencia, esta se involucra en las siguientes actividades:	AI 4				
o Administración de privilegios.	AI 4				
o Segregación de tareas.	AI 4				
o Controles automatizados del negocio.	AI 4				
o Autorizaciones para respaldos /recuperaciones.	AI 4				
o Seguridad física.	AI 4				
o Archivo de la documentación fuente.	AI 4				
· ¿Se realiza una transferencia de conocimientos y habilidades a los usuarios finales para permitir que utilicen la solución con efectividad y eficiencia?	AI 4				
· ¿Cuenta la organización con un plan de entrenamiento para los usuarios finales?	AI 4				
· El plan de entrenamiento a usuarios finales incluye:	AI 4				
o Entrenamiento inicial.	AI 4				
o Entrenamiento continuo.	AI 4				
o Desarrollo de habilidades de los usuarios.	AI 4				
o Materiales de entrenamiento.	AI 4				
o Manuales de usuario.	AI 4				
o Manuales de procedimientos.	AI 4				
o Ayuda en línea.	AI 4				
o Asistencia a usuarios.	AI 4				
o Identificación del usuario clave.	AI 4				
o Evaluación.	AI 4				
· ¿Se realiza una transferencia de conocimientos y habilidades al personal de soporte técnico y de operaciones para permitir que entreguen, apoyen y mantengan la aplicación y la infraestructura asociada de	AI 4				

manera efectiva y eficiente de acuerdo con los niveles de servicio requeridos?					
· El plan de entrenamiento al personal de soporte técnico y de operaciones incluye:	AI 4				
o Entrenamiento inicial.	AI 4				
o Entrenamiento continuo.	AI 4				
o Desarrollo de habilidades.	AI 4				
o Materiales de entrenamiento.	AI 4				
o Manuales de operación.	AI 4				
o Manuales de procedimientos.	AI 4				
o Escenarios de atención al usuario.	AI 4				
TOTAL AI 4		0	0	0	
PONDERACION					
6. Administrar Cambios: Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, deben administrarse formal y controladamente. Los cambios (incluyendo procedimientos, procesos, sistema y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción.	AI 6				
Procedimientos de control de cambios al *software* del sistema.	AI 6				
· ¿Todos los resultados de pruebas después del cambio son documentados?	AI 6				
· ¿Todos los resultados de pruebas son revisados?	AI 6				
· ¿Todos los resultados de pruebas son aprobados?	AI 6				
· ¿Todos los procedimientos de control de cambios son autorizados?	AI 6				
· ¿Los cambios fueron valorados debidamente respecto al impacto sobre los sistemas en producción?	AI 6				
· ¿Respecto a los procesos de cambios, existen procedimientos apropiados de recuperación/retiro? En caso de una falla.	AI 6				
· ¿Antes de realizar algún tipo de cambio, todo el personal afectado fue debidamente informado?	AI 6				
· ¿Antes de realizar algún tipo de cambio, todo el personal afectado fue debidamente capacitado?	AI 6				

Prácticas de mantenimiento de sistemas de información: Las prácticas de mantenimiento de sistemas se refieren primordialmente al proceso de gestionar/administrar los cambios a sistemas de aplicación al mismo tiempo que se mantiene la integridad tanto del código fuente como del código ejecutable en producción.	AI 6				
Generalidades del proceso de gestión de cambios. El proceso de gestión de cambios comienza con la autorización de los cambios.	AI 6				
· ¿Cuenta la organización con proceso de cambios en los sistemas actuales?	AI 6				
· ¿Existe algún tipo de autorización para iniciar una gestión de cambios a algún sistema?	AI 6				
· ¿Cuentan con alguna metodología para dar prioridad y aprobar las solicitudes de cambios a sistemas?	AI 6				
· ¿Las solicitudes son realizadas por los usuarios finales, personal operativo, equipo de desarrollo o equipo de mantenimiento de los sistemas?	AI 6				
· ¿Las autorizaciones de cambios provienen de los niveles apropiados de usuario final y gestión de sistemas? La gestión de sistemas se refiere a grupos de control de cambio, comités de control de configuración, etc.	AI 6				
· Para los sistemas adquiridos, ¿los proveedores realizan actualizaciones de los sistemas (parches)?	AI 6				
· Para los sistemas adquiridos, ¿se revisan las actualizaciones que hacen los proveedores de los sistemas?	AI 6				
· ¿Se realizan análisis para valorar si los cambios son realmente necesarios para la organización?	AI 6				
· ¿Se realizan análisis para valorar si los cambios afectarán o no negativamente el sistema existente?	AI 6				
· ¿Existe algún formulario o medio oficial (memorándum, correo, etc.) para la solicitud de cambios?	AI 6				
· La solicitud de usuario incluye como mínimo los siguientes campos:	AI 6				
o Nombre del solicitante.	AI 6				
o Fecha de la solicitud.	AI 6				
o Fecha en que se necesita el cambio.	AI 6				
o La prioridad de la solicitud.	AI 6				
o Descripción del cambio.	AI 6				

o Efecto del cambio sobre otros sistemas o programas.	AI 6				
· ¿El formulario de cambios cuenta con un número único de control?	AI 6				
· ¿Se lleva un registro de mantenimiento de todos los cambios de programa ya sea manual o automático?	AI 6				
· ¿Todas las solicitudes de cambios y la información relacionada está mantenida por el equipo de mantenimiento del sistema como parte de la documentación permanente del sistema?	AI 6				
· La información del mantenimiento incluye:	AI 6				
o ID del programador.	AI 6				
o La hora del cambio.	AI 6				
o La fecha del cambio.	AI 6				
o El número de proyecto o de solicitud asociado al cambio.	AI 6				
o La imágenes de antes y después de las líneas de código que fueron cambiadas.	AI 6				
· Si la organización es pequeña y el operador y programador es la misma persona, ¿se cuenta con algún tipo de control para la administración de cambios? (por ejemplo un *software* automático de control de cambios, para impedir cambios no autorizados a programas).	AI 6				
· ¿Se tiene el debido cuidado para que los programadores no tengan acceso a escribir, modificar o eliminar datos en producción?	AI 6				
· Después de que el usuario ha quedado satisfecho con el cambio realizado, ¿se cuenta con aprobación de la gerencia del usuario?	AI 6				
· La evidencia que demuestra que la aprobación del usuario ha sido otorgada, ¿es archivada por el personal de mantenimiento de sistemas?	AI 6				
· ¿Todos los cambios a sistemas se encuentran debidamente documentados? Por ejemplo, con manuales, diagramas de flujo, etc.	AI 6				
· ¿Se mantienen copia de los documentos actualizados de cambios a sistemas en algún sitio fuera del lugar de trabajo? Para casos de desastres.	AI 6				
· ¿Se realizan pruebas a los cambios efectuados? Verificando que la funcionalidad, desempeño y riesgos de los sistemas actuales no se vean alterados por los cambios realizados.	AI 6				

· ¿Existe algún tipo de control para que los programas de aplicación en producción no se vean alterados por cambios no autorizados?	AI 6				
· El control de los programa de aplicación en producción incluye lo siguiente:	AI 6				
o ¿Acceso restringido a las bibliotecas del programa?	AI 6				
o ¿Se realizan revisiones de supervisión?	AI 6				
o ¿Se documentan y aprueban las solicitudes de cambio?	AI 6				
o ¿Se evalúa el impacto potencial de los cambios?	AI 6				
o ¿La solicitud de cambio está documentada en un formulario estándar?	AI 6				
o El formulario estándar de solicitud de cambios a programas de aplicación en producción incluye lo siguiente:	AI 6				
- ¿Las especificaciones de los cambios están descritas adecuadamente? Se debe incluir un análisis de costos y establecer una fecha meta.	AI 6				
- ¿El formulario de cambios está firmado por el usuario para indicar su aprobación?	AI 6				
- ¿La gestión de programas es la que revisa y aprueba el formulario de cambios?	AI 6				
- ¿Se asigna el trabajo a un analista, programador y líder del grupo en programación para sus supervisión?	AI 6				
· ¿La organización ha tenido que realizar cambios de emergencia?	AI 6				
· ¿Existen procedimientos para los cambios de emergencia en el manual de operaciones? Considerando: *ID* especiales, accesos temporales, etc.	AI 6				
· ¿Debido al poder de los privilegios que tienen los *ID* de emergencia, su uso es registrado y monitoreado/supervisado con minuciosidad?	AI 6				
· ¿La migración de programas de ambiente de pruebas al de producción es realizado por un grupo diferente a los programadores? Grupos como operaciones de computadoras, calidad o grupos de control de cambios, etc.	AI 6				
· ¿Existen restricciones de acceso para los que realizan la migración de los programas a producción?	AI 6				
· ¿En el caso de sistemas distribuidos (como puntos de ventas) existe algún control para garantizar que los cambios se efectuaron en todos los nodos?	AI 6				

Gestión de configuración. Debido a las dificultades asociadas con el control sobre las actividades de mantenimiento de programación, algunas organizaciones implementan sistemas de gestión de configuración.	AI 6				
· ¿Las solicitudes de mantenimiento son documentadas y aprobadas formalmente por un grupo de control de cambios?	AI 6				
· ¿Se ejercen controles minuciosos sobre cada etapa del proceso de mantenimiento por medio de puntos de verificación, revisiones o procedimientos de aprobación?	AI 6				
· ¿El gerente de configuración verifica los programas, documentación y datos una vez que se ha hecho algún cambio?	AI 6				
· Para implementar el proceso de gestión de configuración, ¿se desarrolla y sigue un plan de gestión de configuración y procedimientos operativos?	AI 6				
· ¿El plan de gestión de configuración y procedimientos operativos incluye todos los documentos del *software* desarrollado?	AI 6				
· ¿El plan de gestión de configuración y procedimientos operativos incluye planes de prueba?	AI 6				
· ¿El plan de gestión de configuración y procedimientos operativos incluye todos los procedimientos del sistema?	AI 6				
· Como parte de la tarea de gestión de la configuración del *software*, el encargado de mantenimiento realiza los siguientes pasos:	AI 6				
1. ¿Desarrolla el plan de gestión de configuración?	AI 6				
2. ¿Establece el nivel mínimo de código y los documentos asociados?	AI 6				
3. ¿Analiza e informa sobre los resultados del control de la configuración?	AI 6				
4. ¿Desarrolla los reportes que ofrecen información sobre el estado de configuración?	AI 6				
5. ¿Desarrolla los procedimientos de liberación?	AI 6				
6. ¿Realiza actividades de control de configuración, tales como identificación y registro de la solicitud?	AI 6				
7. ¿Actualiza la base de datos de contabilidad de estado de configuración?	AI 6				
Herramientas de desarrollo de sistemas y ayudas de productividad: Las herramientas de desarrollo de sistemas y las ayudas para la productividad incluyen generadores de código, aplicaciones de ingeniería de *software* asistida por computador (CASE) y lenguajes de cuarta generación (4GL).	AI 6				

Ingeniería de *software* asistida por computadora. La ingeniería de *software* asistida por computador (CASE) es el uso de herramientas automatizadas que ayudan en el proceso de desarrollo de *software*.	AI 6				
· ¿La organización cuenta con productos CASE? Documentar el tipo utilizado.	AI 6				
· ¿Ayudan las aplicaciones CASE al proceso de diseño de aplicaciones?	AI 6				
· ¿Existe una metodología de proyectos para CASE?	AI 6				
· ¿La integridad de los datos trasladados entre productos CASE o entre estos y procesos manuales es monitoreada, supervisada y controlada?	AI 6				
· ¿Los cambios realizados a las aplicaciones están reflejados en los datos almacenados en el producto CASE?	AI 6				
· ¿Cuenta la organización con controles para la aplicación CASE?	AI 6				
· ¿Existen controles para el repositorio (la base de datos que almacena y organiza la documentación, los modelos y otros productos de las diferentes etapas) de CASE?	AI 6				
Lenguajes de cuarta generación (4GLs).	AI 6				
· ¿Cuenta la organización con lenguaje de cuarta generación (lenguaje no procedural: la mayoría no obedecen al paradigma de ejecución continua de sentencias, utilizan un uso amplio de conceptos de programación orientado a objetos)? Indique cuál.	AI 6				
· ¿Cuenta la organización con manuales de procedimientos para los *software* que tienen lenguajes de cuarta generación?	AI 6				
· ¿Cuenta la organización con políticas de control para los *software* que tienen lenguajes de cuarta generación?	AI 6				
Proceso de mejora práctica: Los procesos de negocios requieren mejoras, las cuales se logran con ciertas prácticas y técnicas.	AI 6				
Reingeniería del proceso de negocio (BPR) y proyectos de cambios al proceso. La reingeniería de proceso de negocio es el proceso de responder a las presiones competitivas y económicas, y a las exigencias de los clientes para sobrevivir en el ambiente actual de negocio. Por lo general, esto se hace automatizando los procesos del sistema para disminuir las intervenciones y controles manuales.	AI 6				
· ¿Cuenta la organización con reingeniería de procesos de negocio (BPR)?	AI 6				
· Antes de implementar una BPR se consideraron los siguientes aspectos:	AI 6				

1. ¿Se definieron las áreas que iban a ser revisadas?	AI 6				
2. ¿Se desarrolló un plan del proyecto?	AI 6				
3. ¿Se aplicó un proceso de revisión?	AI 6				
4. ¿Se rediseñó el proceso haciéndolo más lineal y continuo?	AI 6				
5. ¿Se implementó y monitoreó el nuevo proceso?	AI 6				
6. ¿Se cuenta con un proceso continuo de mejoramiento?	AI 6				
· Para llevar realizar el BPR el equipo de proyectos realizó los siguientes procesos:	AI 6				
1. ¿Descomposición de los procesos de negocio hasta un nivel de detalle requerido para su efectiva evaluación?	AI 6				
2. ¿Se identificaron los clientes, gerentes del proceso, o propietarios de procesos responsables de principio a fin?	AI 6				
3. ¿Se documentó la información elemental del perfil del proceso?	AI 6				
· El documento con la información de perfil del proceso incluye:	AI 6				
o La duración.	AI 6				
o El disparador (lo que provoca que el proceso se ejecute).	AI 6				
o La frecuencia.	AI 6				
o El esfuerzo.	AI 6				
o La responsabilidad (propietario del proceso).	AI 6				
o La entrada y salida.	AI 6				
o Las interfaces externas.	AI 6				
o La interacción con sistemas.	AI 6				
o La información de riesgo y control.	AI 6				
o La información sobre la medición del desempeño.	AI 6				
o Las áreas problemáticas identificadas y las causas que la originan.	AI 6				
· ¿Los procesos de niveles mínimos se encuentran documentados?	AI 6				
· ¿La organización ha implementado un proceso de estudio comparativo (*benchmarking*) para mejorar sus proceso de negocio?	AI 6				
· ¿Si la organización llevó realizó un estudio comparativo el equipo de trabajo consideró los siguientes pasos:	AI 6				
1. ¿Se desarrolló un plan para identificar los procesos críticos para el estudio comparativo?	AI 6				
2. ¿Se realizó una investigación sobre los procesos de la propia organización, sobre el mercado, etc.?	AI 6				
3. ¿Se observó al socio sobre el cual se hizo el estudio comparativo?	AI 6				

4. ¿Se realizó un análisis de la información recolectada?	AI 6				
5. ¿Se adoptaron los resultados del estudio realizado?	AI 6				
6. ¿Se cuenta con un proceso continuo de mejoramiento en relación con el estudio comparativo realizado?	AI 6				
ISO 9126. La ISO 9126 es un estándar internacional para evaluar la calidad de productos de *software.*	AI 6				
· ¿La organización ha considerado dentro de su proceso de *software* las mejores prácticas de la ISO 9126?	AI 6				
· En la evaluación de la calidad de productos de *software* se evalúa:	AI 6				
1. La funcionalidad del *software* (satisface las necesidades manifestadas o implicadas)	AI 6				
2. La confiabilidad (capacidad del *software* para mantener su nivel de desempeño bajo condiciones establecidas durante un periodo de tiempo)	AI 6				
3. Utilización (es utilizado el *software* por los usuarios)	AI 6				
4. Eficiencia (relación entre el nivel de desempeño del *software* y la cantidad de recursos usados bajo condiciones establecidas).	AI 6				
5. Mantenimiento (esfuerzo que se necesita para hacer modificaciones específicas).	AI 6				
6. Portabilidad (capacidad del *softwar*e para ser transferido de un ambiente a otro).	AI 6				
Modelo de madurez de la capacidad del *software*. El modelo de madurez de la capacidad (CMM) del software, es un modelo o marco de referencia de madurez de procesos que ayuda a las organizaciones a mejorar sus procesos del ciclo de vida de *software*.	AI 6				
· ¿Cuenta la organización con CMM? Indicar el nivel.	AI 6				
Integración del modelo de madurez de capacidad (CMMI). Es un medio de combinar varios CMM en un conjunto de modelos integrados.	AI 6				
· ¿Cuenta la organización con CMMI? Indicar el nivel	AI 6				
ISO 15504. Sirve como nivel mínimo para el mejoramiento y el estudio comparativo (*benchmarking*) de los procesos y apalanca la adopción de mejores prácticas.	AI 6				
· ¿Cuenta la organización con la implementación de la ISO 15504?	AI 6				

TOTAL AI 6		0	0	0	
PONDERACION					
7. Instalar y Acreditar Soluciones y Cambios: Los nuevos sistemas necesitan estar funcionales una vez que su desarrollo se completa. Esto requiere pruebas adecuadas en un ambiente dedicado con datos de prueba relevantes, definir la transición e instrucciones de migración, planear la liberación y la transición en sí al ambiente de producción, y revisar la post-implantación. Esto garantiza que los sistemas operativos estén en línea con las expectativas convenidas y con los resultados.	AI 7				
Controles de aplicación. Los objetivos de los controles de aplicación, que pueden ser manuales o programados, son garantizar la integridad y exactitud de los registros y la validez de las entradas realizadas en ellos.	AI 7				
· ¿Cuenta la organización con controles de aplicación sobre las funciones de entrada (*input)* de datos?	AI 7				
· ¿Cuenta la organización con controles de aplicación sobre las funciones de procesamiento de datos?	AI 7				
· ¿Cuenta la organización con controles de aplicación sobre las funciones de salida (*output*) de datos?	AI 7				
· Cuenta la organización con alguno de los siguientes controles de aplicación:	AI 7				
1. Pruebas de edición.	AI 7				
2. Pruebas sobre totales.	AI 7				
3. Pruebas de reconciliación.	AI 7				
4. Pruebas de identificación.	AI 7				
5. Reporte de datos incorrectos.	AI 7				
6. Reporte de datos faltantes.	AI 7				
7. Reporte de excepciones.	AI 7				
· ¿Los controles de aplicación con que cuenta la organización ayudan a asegurar que los datos sean correctos?	AI 7				
· ¿Los controles de aplicación con que cuenta la organización ayudan a asegurar que los datos sean íntegros?	AI 7				
· ¿Los controles de aplicación con que cuenta la organización ayudan a asegurar que los datos sean válidos?	AI 7				
· ¿Los controles de aplicación con que cuenta la organización ayudan a asegurar que los datos sean verificables?	AI 7				
· ¿Los controles de aplicación con que cuenta la organización ayudan a asegurar que los datos sean consistentes?	AI 7				

Controles de entrada / origen. Los procedimientos de entrada deben asegurar que toda transacción que se vaya a procesar se reciba, procese y registre correcta y completamente. Estos controles deben asegurar que solo se introduzca información válida y autorizada, y que estas transacciones sean procesadas una vez.	AI 7				
· ¿Todas las transacciones son autorizadas y aprobadas por la gerencia antes de ser ingresadas?	AI 7				
· ¿Una vez ingresados los datos autorizados, estos permanecen inalterados o pueden ser modificados?	AI 7				
· Cuenta la organización con alguno de los siguientes tipos de autorización:	AI 7				
1. Firmas en formularios por lotes o documentos de origen.	AI 7				
2. Controles de acceso en línea.	AI 7				
3. Contraseñas (*passwords*).	AI 7				
4. Identificación de terminal o de estación de trabajo. Se usa para limitar el ingreso a terminales específicas así como también a personas específicas.	AI 7				
5. Documentos fuente (formularios numerados). Son los formularios usados para registrar los datos. Idealmente, deben ser formularios pre impresos para dar consistencia, exactitud y legibilidad.	AI 7				
· ¿Posee la organización controles de procesamiento por lote?	AI 7				
· ¿Los lotes poseen formularios para el control de preparación de los datos?	AI 7				
· ¿Los formularios están claramente identificados con el nombre de la aplicación?	AI 7				
· ¿Los formularios están claramente identificados con los códigos de transacción?	AI 7				
· Cuenta la organización con alguno de los siguientes controles de proceso por lote:	AI 7				
1. Importe monetario total. Verificación de que el valor monetario total de los elementos procesados es igual al valor monetario total de los documentos por lote.	AI 7				
2. Total de elementos. Verificación de que el número total de los elementos incluidos en cada documento del lote concuerda con el número total de los elementos procesados.	AI 7				
3. Total de documentos. Verificación de que el número total de documentos en el lote concuerda con el número total de documentos procesados.	AI 7				

4. Totales de comprobación. (*Hash* total). Verificación de que el total en un lote coincida con el total calculado por el sistema.	AI 7				
· ¿El balance entre lotes se realiza a través de reconciliación manual o automatizada?	AI 7				
· ¿La suma total del lote está combinada con procedimientos adecuados de seguimiento?	AI 7				
· ¿Existen controles para asegurar que cada transacción crea un documento de entrada?	AI 7				
· ¿Existen controles para asegurar que todos los documentos están incluidos en un lote?	AI 7				
· ¿Existen controles para asegurar que todos los lotes son remitidos para su procesamiento?	AI 7				
· ¿Existen controles para asegurar que todos los lotes son aceptados por la computadora?	AI 7				
· ¿Existen controles para asegurar que se realice la reconciliación del lote?	AI 7				
· ¿Existen controles para asegurar que se sigan los procedimientos para investigación y corrección oportuna de las diferencias?	AI 7				
· ¿Existen controles para asegurar que existan controles para el procesamiento de los elementos rechazados?	AI 7				
· Cuenta la organización con alguno de los siguientes tipos de balance de lotes:	AI 7				
1. Registro del lote. Registros que permiten la captura manual de los totales de los lotes y posterior comparación con los totales reportados por el sistema.	AI 7				
2. Cuentas de control. Se utiliza mediante el uso de un archivo inicial de edición con el cual se verifican los totales por lote. Los datos son luego procesados para el archivo maestro y se realiza una reconciliación entre los totales procesados para el archivo inicial de edición y para el archivo principal o maestro.	AI 7				
3. Reconciliaciones hechas por el computador. (*Computer Agreement)*. Una reconciliación de los totales por lote realizada por el computador se efectúa por medio del ingreso de detalles de encabezado de lote que registran los totales de lote; el sistema compara estos con los totales calculados, y acepta o rechaza el lote.	AI 7				
· ¿Se corrigen los errores que se presentan durante el proceso de conversión de datos?	AI 7				

· ¿Se realizan las correcciones a los datos por medio de un proceso normal de conversión de datos?	AI 7				
· ¿El proceso de conversión de datos es verificados?	AI 7				
· ¿El proceso de conversión de datos es autorizado?	AI 7				
· ¿El proceso de conversión de datos es reingresado al sistema como parte del procesamiento normal?	AI 7				
· Se da alguno de los siguientes tratamientos a los errores presentados en el ingreso de datos:	AI 7				
1. Se rechazan solo las transacciones que tengan errores. El resto del lote se procesa.	AI 7				
2. Se rechaza todo el lote de las transacciones. Se corrige todo el lote antes de ser procesado.	AI 7				
3. Se mantiene el lote en espera. El lote no sería rechazado, pero sería marcado y dejado en espera de corrección.	AI 7				
4. Se acepta el lote y se marcan las transacciones que contienen errores.	AI 7				
· Posee la organización alguna de las siguientes técnicas de control en el ingreso de datos:	AI 7				
1. Registro de transacciones. Lista detallada de todas las actualizaciones.	AI 7				
2. Reconciliación de los datos. Controla que todos los datos recibidos hayan sido grabados y procesados correctamente.	AI 7				
3. Documentación. Evidencia escrita de procedimientos / del usuario, de ingreso y control de datos.	AI 7				
4. Procedimiento para la corrección de errores.	AI 7				
· Los procedimientos para la corrección de errores incluyen:	AI 7				
o Registro de errores.	AI 7				
o Correcciones oportunas.	AI 7				
o Ingreso de datos corregidos.	AI 7				
o Aprobación de las correcciones.	AI 7				
o Archivo en suspenso.	AI 7				
o Archivo del error.	AI 7				
o Validación de las correcciones.	AI 7				
5. Anticipación. El usuario o grupo de control anticipa la recepción de los datos.	AI 7				
6. Registro (*log*) de transmisión. Documenta la transmisión o recepción de datos.	AI 7				
7. Cancelación de los documentos fuente. Son procedimientos para marcar los documentos fuente que ya han sido	AI 7				

ingresados.					
· En el caso de los sistemas en línea se cuenta con alguno de los siguientes controles para el ingreso de datos:	AI 7				
o Los lotes pueden generarse por la hora del día.	AI 7				
o Los lotes pueden generarse por terminal específica.	AI 7				
o Los lotes pueden generarse por individuo que ingresa los datos.	AI 7				
· ¿En el caso de los sistemas en línea, un supervisor revisa el lote en línea antes de liberarlo al sistema para su procesamiento?	AI 7				
Procedimientos y controles de procesamiento. Los procedimientos y controles de procesamiento tienen la finalidad de garantizar la confiabilidad del procesamiento mediante programas de aplicaciones.	AI 7				
· ¿Cuenta la organización con un procedimiento para asegurar que los datos que se ingresan al sistema sean validados y editados tan cerca, como sea posible, de su momento y punto de origen? Indicar el tipo de validación.	AI 7				
· En el caso de que un supervisor anule la validación y edición de los datos, ¿queda un registro automático de esa operación?	AI 7				
· ¿Posee la organización controles de procesamiento de datos?	AI 7				
· Cuenta la organización con alguna de las siguientes técnicas de control de procesamiento:	AI 7				
1. Re cálculos manuales. Para asegurar que los datos fueron procesados correctamente.	AI 7				
2. Edición. Es una instrucción o subrutina de programa que prueba que los datos ingresados y procesados por una aplicación son correctos, íntegros y válidos.	AI 7				
3. *Run - to - run totals.* La verificación de un total de ejecución en ejecución para asegurar que los datos leídos a una computadora fueron aceptados y luego aplicados al proceso de actualización.	AI 7				
4. Controles programados. Se puede utilizar software para detectar e iniciar una acción correctiva sobre los errores en los datos y en el procesamiento.	AI 7				
5. Verificación de razonabilidad de los valores calculados. Los programas de aplicación pueden verificar si las cantidades	AI 7				

calculadas son razonables.					
6. Verificación de límite sobre los valores calculados. Una verificación de edición puede proporcionar el aseguramiento mediante el uso de límites predeterminados que las sumas o cantidades calculadas hayan sido digitadas correctamente. Cualquier transacción que exceda el límite puede ser rechazada o suspendida para una investigación adicional.	AI 7				
7. Reconciliación de los totales de los archivos. Pueden realizarse a través del uso de una cuenta mantenida manualmente, un archivo de registros de control o un archivo de control independiente.	AI 7				
8. Reportes de excepción. Es generado por un programa que identifica las transacciones o los datos que parecen incorrectos.	AI 7				
· ¿Cuenta la organización con controles de archivo de datos? Detallar cuáles.	AI 7				
· Cuenta la organización con alguna de las siguientes categorías de archivo de datos :	AI 7				
1. Parámetros de control de sistema. Las entradas en estos archivos cambian los funcionamientos del sistema y pueden alterar los controles ejercidos por el sistema.	AI 7				
2. Datos vigentes. Incluyen datos, como nombres y direcciones. Los controles de entrada pueden incluir un reporte de datos cambiados que es verificado y aprobado.	AI 7				
3. Datos principales / datos de balance. Los balances y los totales resultantes de procesamiento, que son actualizados por transacciones, no deben ser susceptibles de ajustes, excepto bajo estricta aprobación y controles de revisión.	AI 7				
4. Archivos de transacción. Se controlan usando verificaciones de validación, totales de control, etc.	AI 7				
Controles de salida. Los controles de salida proveen garantía de que los datos entregados a los usuarios serán presentados, formateados y entregados en una forma consistente y segura.	AI 7				
· ¿Cuenta la organización con controles de salida de datos?	AI 7				
· ¿Incluyen los controles de salida de datos registros y almacenamiento de formularios negociables, sensibles y críticos en un lugar seguro?	AI 7				

· ¿Incluyen los controles de salida de datos generación automatizada de instrumentos negociables, formularios y firmas?	AI 7				
· ¿Incluyen los controles de salida de datos distribución de reportes de acuerdo con parámetros de distribución autorizada?	AI 7				
· ¿Incluyen los controles de salida de datos balance y conciliación de los datos procesados?	AI 7				
· ¿Incluyen los controles de salida de datos un adecuado manejo de errores de salida?	AI 7				
· ¿Incluyen los controles de salida de datos una política de retención de reporte de salida?	AI 7				
· ¿Incluyen los controles de salida de datos una adecuada verificación de recepción de reportes?	AI 7				
Aseguramiento de control de procesos. En el ambiente de una aplicación integrada, los controles están embebidos y diseñados en la aplicación que respalda los procesos. El aseguramiento de control en el proceso de negocio involucra evaluar controles al nivel del proceso y de la actividad.	AI 7				
· ¿Cuenta la organización con mapas de procesos de negocio?	AI 7				
· ¿Cuenta la organización con controles de procesos de negocio?	AI 7				
· ¿Cuenta la organización con evaluaciones de riesgos del negocio dentro del proceso?	AI 7				
· ¿Realiza la organización estudios comparativos (*benchmark*) con las mejores prácticas?	AI 7				
· ¿Cuenta la organización con roles y responsabilidades en los procesos de negocio?	AI 7				
· ¿Cuenta la organización con actividades y tareas dentro de los procesos de negocio?	AI 7				
· ¿Cuenta la organización con restricciones de datos dentro de los procesos de negocio?	AI 7				
TOTAL		0	0	0	
PONDERACION 110 preguntas					
ÚLTIMA LÍNEA					
Simbología:					
AI = Número de objetivo del dominio Adquirir e Implementar de COBIT 4.1.					
N/A = No aplica					
NOTA: La evaluación se realiza de acuerdo con la relación porcentual de las respuestas positivas en relación con el total de respuestas tanto negativas como positivas. No se incluyen las que no aplican.					

Fuente: Elaboración propia, basada en el dominio Adquirir e Implementar de COBIT 4.1, así como las guías de aseguramiento de ISACA.

Debido a la necesidad de aplicar un porcentaje de importancia por objetivo a cumplir, se le consultó al funcionario a cargo de la DTIT sobre el peso que debía tener cada objetivo en la Dirección, a lo cual consideró que los objetivos del dominio AI de COBIT, tenían un orden natural de ser y que a su criterio debían cumplirse en ese orden, teniendo más peso el objetivo 1, luego el 2 y el 5 y seguidos los 3, 4, 6 y 7. Dado lo anterior se procedió a aplicar las siguientes ponderaciones:

Cuadro 3: Porcentajes de importancia de acuerdo con cada objetivo

Objetivo del dominio Adquirir e Implementar de COBIT	Valor por orden de importancia	% de acuerdo con la relación	% obtenido en la aplicación de la metodología	% respecto a la meta propuesta	% de la diferencia no cumplida
AI 1	70	32%			
AI 2 y 5	50	23%			
AI 3	40	18%			
AI 4	30	14%			
AI 6	20	9%			
AI 7	10	5%			
TOTAL	**220**	**100%**			

El valor dado a cada objetivo en la columna que indica “Valor por orden de importancia” fue asignado dando un valor de 1 a 10 de acuerdo con lo expuesto por el funcionario a cargo de la DTIT.

Como ejemplo, para comprender la herramienta, se va a suponer que al aplicar la metodología propuesta se obtuvo los siguientes resultados:

Cuadro 4: Ejemplo 1, porcentajes de importancia de acuerdo con cada objetivo

Objetivo del dominio Adquirir e Implementar de COBIT	Valor por orden de importancia	% de acuerdo con la relación meta	% obtenido en la aplicación de la metodología	% respecto a la meta propuesta	% de la diferencia no cumplida
AI 1	10	27%	10%	3%	-24%
AI 2 y 5	8	22%	25%	5%	-16%
AI 3	7	19%	60%	11%	-8%
AI 4	6	16%	10%	2%	-15%
AI 6	4	11%	10%	1%	-10%
AI 7	2	5%	30%	2%	-4%
TOTAL	**37**	**100%**		**24%**	**-76%**

Como se puede observar, el objetivo de mayor importancia para la DTIT en estos momentos (de acuerdo al supuesto) es el 1, del cual solo un 3% se encuentra de acuerdo con las mejores prácticas, por lo que la DTIT debe tomar las medidas necesarias para tratar de mejorar el déficit que poseen en -24% cumplido.

Otro ejemplo también a considerar es suponiendo que la DTIT ha cumplido al 100% con las mejores prácticas en cuanto a las adquisiciones de TI, entonces la herramienta mostraría los siguientes resultados:

Cuadro 5: Ejemplo 2, porcentajes de importancia de acuerdo con cada objetivo

Objetivo del dominio Adquirir e Implementar de COBIT	Valor por orden de importancia	% de acuerdo con la relación meta	% obtenido en la aplicación de la metodología	% respecto a la meta propuesta	% de la diferencia no cumplida
AI 1	60	29%	100%	29%	0%
AI 2 y 5	50	24%	100%	24%	0%
AI 3	40	19%	100%	19%	0%
AI 4	30	14%	100%	14%	0%
AI 6	20	10%	100%	10%	0%
AI 7	10	5%	100%	5%	0%
TOTAL	**210**	**100%**	**600%**	**100%**	**0%**

Esta metodología va a ser suministrada a la DTIT en un archivo de Excel para facilitar su aplicación.

5.3 Aplicación de la metodología propuesta

La aplicación de la metodología propuesta anteriormente brindará a la DTIT un panorama amplio sobre la metodología, procedimientos y funciones realizados en dicha Dirección referentes a la adquisición de TI, además, dará un excelente diagnóstico tanto en el cumplimiento de las mejores prácticas como en el cumplimiento de la normativa promulgada por la CGR, ya que al comparar los objetivos de control de COBIT con las Normas Técnicas se puede observar una similitud muy identificable, tal como se muestra en el siguiente cuadro.

Cuadro 6: Normas técnicas para la gestión y control de las TI de la CGR *vs.* COBIT

Capítulo III Implementación de tecnologías de información	Objetivo de control COBIT
3.1 Consideraciones generales de la implementación de TI	AI 1 Identificar soluciones automatizadas
3.2 Implementación de *software*	AI 2 Adquirir y mantener s*oftware* a*plicativo* AI 5 Adquirir recursos de TI AI 4 Facilitar la operación y el uso AI 6 Administrar cambios
3.3 Implementación de infraestructura tecnológica	AI 3 Adquirir y mantener infraestructura tecnológica
3.4 Contratación de terceros para la implementación y mantenimiento de *software* e infraestructura	
	AI 7 Instalar y acreditar soluciones y cambios

Fuente: Elaboración propia, tomando como base las Normas técnicas para la gestión y control de las TI de la CGR y el dominio Adquirir e Implementar de COBIT 4.1.

El aplicar la metodología propuesta en el presente proyecto, brindará un increíble valor a la DTIT respecto al uso de las mejores prácticas existente en referencia a las adquisiciones en tecnologías de información.

CAPÍTULO VI.

Este capítulo tiene como finalidad mostrar el cumplimiento de los objetivos planteados, el análisis de resultados y las recomendaciones de haber desarrollado la metodología para el proceso de aseguramiento del control interno de las adquisiciones de tecnologías de información basada en COBIT 4.1 y en las guías de aseguramiento de ISACA, para la Dirección de Tecnología de Información Tributaria, de la Dirección General de Tributación del Ministerio de Hacienda.

6.1 Cumplimiento de objetivos

Respecto al objetivo general, con el desarrollo del presente proyecto fue factible diseñar la metodología para el proceso de aseguramiento del control interno de las adquisiciones de tecnologías de información basada en COBIT 4.1 y en las guías de aseguramiento de ISACA, en la Dirección de Tecnologías de Información de Tributación de la Dirección General de Tributación del Ministerio de Hacienda, no así su implementación, por las razones expuestas en la sección de limitaciones del presente trabajo.

En lo referente a los objetivos específicos, fueron cumplidos en forma parcial, ya que al no contar la DTIT con una metodología para el aseguramiento del control de las adquisiciones de TI, no fue posible analizar el impacto de los riesgos que pueden ser materializados en dicha Dirección. A pesar de esto, el estudio efectuado permitió conocer la realidad existente en dicha área referente a la necesidad de diseño y aplicación de métodos de control relacionados con el tema de adquisiciones de TI, razón por la cual se considera que la herramienta facilitada con el desarrollo del presente proyecto será de gran ayuda en el desarrollo de las funciones.

6.2 Análisis de resultados

Con el desarrollo del presente proyecto se pudo constatar el papel protagónico que poseen las TI en la producción y generación de riqueza, no solo en el ámbito privado, sino también en el público, ya que el hecho de contar con adecuadas herramientas de TI en la DGT favorece el control y cumplimiento voluntario de los deberes fiscales por parte de los contribuyentes.

Los procesos, funciones y métodos de trabajo giran en torno a las TI, razón por la cual contar con una gestión apropiada de estas es un instrumento que sirve para garantizar el logro de los objetivos institucionales.

Mantener una gestión adecuada de las TI en la DTIT garantiza que la DGT pueda cumplir con su objetivo principal: "… *contribuir con la mejora continua del sistema tributario costarricense, procurando su equilibrio y progresividad, en armonía con los derechos y garantías ciudadanas".*

En el desarrollo del presente trabajo se pudo constatar la carencia de una gestión adecuada para las adquisiciones de TI en la DTIT, ya que no se cuenta con procedimientos o metodologías claramente estipulados y del conocimiento de todos los funcionarios para las adquisiciones de *hardware* y *software.* Respecto al diseño y desarrollo de *software* dentro de la DTIT, a pesar de que sí se cuenta con documentos como metodologías, políticas o directrices, estos no se encuentran organizados en un lugar específico donde puedan ser localizados de una forma rápida y que sean del conocimiento de todos los funcionarios.

Al desarrollar esta metodología basada en las mejores prácticas, como son COBIT y las guías de aseguramiento de ISACA, se ha adquirido un conocimiento profundo sobre los procedimientos que deben realizarse para lograr el aseguramiento del control interno en las adquisiciones en tecnologías de información.

La creación de un inventario de riesgos (descrito en el apartado 4.2 del presente documento) facilita y fomenta la disposición del personal de la DTIT en el cumplimiento de la normativa de la CGR, sobre todo en lo referente al SEVRI.

El plantear la metodología propuesta en forma de cuestionario, hace que su aplicación sea más ágil y sencilla, facilitando su implementación y obteniendo un porcentaje de cumplimiento, que sirve de guía a la Administración para monitorear el avance en el logro de las mejores prácticas.

El contar con una metodología basada en las mejores prácticas facilita el cumplimiento de la normativa vigente (al estar alineadas las normas técnicas de la CGR y COBIT), además, crea un valor agregado, haciendo que los procesos sean más eficaces y eficientes, agilizando la toma de decisiones para el logro de los objetivos organizacionales.

6.3 Recomendaciones

En primera instancia es conveniente que la DTIT analice la importancia que tiene para la organización el cumplimiento de la normativa estipulada por la CGR en todo aspecto referente a las TI y en segundo lugar, la importancia que tiene para la Dirección diseñar e implementar una metodología para las adquisiciones de tecnologías de información, ya que el no contar con procedimientos claramente estipulados de acuerdo con la normativa estipulada por la CGR y con las buenas prácticas, expone a la Dirección y los funcionarios a sanciones por parte de las áreas fiscalizadoras respectivas como la CGR, la Auditoría Interna, etc., además, de poner en riesgo todo el Ministerio de Hacienda, ya que el no contar como mínimo con una identificación clara de los riesgos y sus consecuencias, puede ocasionar que cualquiera de los riesgos enumerados en el apartado 4.2 se materialicen, ocasionando graves perjuicios económicos a la Hacienda Pública, sin tomar en consideración la pérdida de imagen y la falta de credibilidad de la ciudadanía costarricense en la Administración Pública.

Considerando la importancia que tiene el uso de las TI, se recomienda a la DTIT analizar la posibilidad de implementar la metodología propuesta dados los beneficios y el gran aporte que puede traer a la DTIT en particular y al Ministerio de Hacienda en general.

En lo referente a los procesos de aseguramiento del control interno de las TI, es conveniente involucrar a las altas jerarquías, que son las que poseen el poder de decisión y en última instancia la responsabilidad de buscar los recursos necesarios para poder contar con los procesos adecuados para el logro de los objetivos.

También es importante involucrar a todo el personal, tratando de concientizar en ellos los beneficios del diseño de procedimientos de control en el desarrollo de sus funciones.

Por último, es importante que la DTIT cuente con el personal idóneo para los puestos, capacitando constantemente a los funcionarios en temas de interés relacionados con el uso de las mejores prácticas.

BIBLIOGRAFÍA

Asamblea Legislativa de la República de Costa Rica. (2009). Ley General de la Administración Pública. 22 ed. San José, Costa Rica: Editorial Investigaciones Jurídicas S.A.

Asamblea Legislativa de la República de Costa Rica. (2012). Código Contencioso Administrativo. 6 ed. San José, Costa Rica: Editorial Investigaciones Jurídicas S.A.

Autor anónimo. TI: Tecnologías de Información. (Capturado 21/04/2013). http://tecnologiahechapalabra.com/tecnologia/glosario_tecnico/articulo.asp?i=875

Asamblea Legislativa de la República de Costa Rica. (2002). "(Ley 8292) Ley General de Control Interno". San José, Costa Rica: Diario Oficial La Gaceta 04-09-2002.

Contraloría General de la República. (2007). "(N-2-2007-CO-DFOE) Normas técnicas para la gestión y el control de las Tecnologías de Información".

Contraloría General de la República. (2009). "(N-2-2009-CO-DFOE) Normas de Control Interno para el Sector Público".

Contraloría General de la República. (2005). (R-CO-64-2005) "Directrices Generales para el Establecimiento y Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)". San José, Costa Rica. Diario Oficial La Gaceta 12-07-2005.

Delgado Rojas, Xiomar. (1997). Auditoría Informática. San José, Costa Rica: Editorial Universidad Estatal a Distancia.

Echenique García, José Antonio. (2001). Auditoría en Informática. 2 ed. México D.F.: McGraw-Hill/Interamericana Editores, S.A.

Espinoza Guido, Sergio. (2009). Auditoría de aplicaciones informáticas. San José, Costa Rica: Editorial UCR.

Hidalgo Nuchera Antonio. Revista de la investigación en la gestión de la investigación de la tecnología. Gestión de la Innovación y la Tecnología. Número 23. http://www.madrimasd.org/revista/revista23/tribuna/tribuna1.asp. Capturado el 21/04/2013).

ISACA. Guías de aseguramiento. www.isaca.org.

IT Governance Institute. (2007). COBIT 4.1. Versión liberada.

Instituto Mexicano de Contadores Públicos. (2009). Normas Internacionales de Auditoría y Control de Calidad. 10. ed. México, D.F: Editorial Caballero Gabriela.

Maxitana Cevallos, Jennifer Dennise y Naranjo Sánchez, Bertha Alice. Administración de riesgos de tecnología de información de una empresa del sector informático. (Capturado el 21/04/2013) http://www.dspace.espol.edu.ec/bitstream/123456789/15896/3/Resumen%20Cicyt.-%20Administraci%C3%B3n%20de%20Riesgos%20de%20TI%20de%20una%20empresa%20del%20sector%20Inform%C3%A1tico.pdf

Morales T. Alejandro H. Medellín, Colombia. http://www.auditool.org/index.php?option=com_content&view=article&id=700:administracion-de-riesgos-conceptos-fundamentales-parte-1&catid=39:trip-deals&Itemid=56

Piattini Velthuis, Mario Gerardo y Del Peso Navarro, Emilio. (2001). Auditoría informática un enfoque práctico. 2 ed. México D.F.: Alfaomega Grupo Editor.

Redondo Gómez, Eugenio. (Actualizado por White Ward, Celia y Díaz Hernández, Cynthia). (2008), Curso Virtual Reinducción General al Ministerio de Hacienda. Costa Rica: Centro de Información y Formación Hacendaria.

Tupia Anticona, Manuel Francisco. (2010). Administración de la Seguridad de la Información. Lima, Perú: Tupia Consultores y Auditores S.A.C.