UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONÓMICAS

“PROPUESTA DE IMPLEMENTACIÓN Y ADOPCIÓN DEL MODELO DE OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT), EN UNA EMPRESA ASEGURADORA, POR PARTE DE LA AUDITORÍA INTERNA, PARA LA EVALUACIÓN DE CONTROLES DE ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS.”

TESIS

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

POR

ERICK RICARDO GONZALEZ TRINIDAD

PREVIO A CONFERÍRSELE EL TÍTULO DE

CONTADOR PÚBLICO Y AUDITOR

EN EL GRADO ACADÉMICO DE

LICENCIADO

Guatemala, mayo de 2016

HONORABLE JUNTA DIRECTIVA
DE LA FACULTAD DE CIENCIAS ECONÓMICAS

Decano:	Lic. Luis Antonio Suarez Roldan
Secretario:	Lic. Carlos Roberto Cabrera Morales
Vocal Segundo:	Lic. Carlos Alberto Hernández Gálvez
Vocal Tercero:	Lic. Juan Antonio Gómez Monterroso
Vocal Cuarto:	P.C. Marlon Geovani Aquino Abdalla
Vocal Quinto:	P.C. Carlos Roberto Turcios Pérez

PROFESIONALES QUE REALIZARON LOS EXÁMENES
DE ÁREAS PRÁCTICAS BÁSICAS

Área Matemática-Estadística	Lic. Luis Enrique Valdez Ramírez
Área Contabilidad	Lic. Olivio Adolfo Cifuentes Morales
Área Auditoría	Lic. Jorge Luis Reyna Pineda

PROFESIONALES QUE REALIZARON EL EXAMEN PRIVADO DE TESIS

Presidente	Lic. Gaspar Humberto López Jiménez
Secretario	Lic. Olivio Adolfo Cifuentes Morales
Examinador	Lic. Mario Leonel Perdomo Salguero

Guatemala 10 de Agosto de 2015

Licenciado
Luis Antonio Suarez Roldan
Decano
Facultad de Ciencias Económicas
Universidad de San Carlos de Guatemala
Ciudad

Señor Decano

De conformidad con el DICTAMEN-AUDITORIA No. 067-215 se revisó el trabajo de tesis **"PROPUESTA DE IMPLEMENTACIÓN Y ADOPCIÓN DEL MODELO DE OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT), EN UNA EMPRESA ASEGURADORA, POR PARTE DE LA AUDITORÍA INTERNA, PARA LA EVALUACIÓN DE CONTROLES DE ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS"**, elaborado por el estudiante Erick Ricardo González Trinidad, previo a optar al Título de Contador Público y Auditor, en el grado académico de Licenciado.

Al considerar que el trabajo presentado cumple con los requisitos correspondientes, recomiendo su aprobación para discusión y defensa en el Examen Privado de Tesis

Atentamente,

Lic. Jorge Luis Reyna Pineda
Colegiado 7162
Asesor de Tesis

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE CIENCIAS ECONOMICAS

Edificio "S-8"

Ciudad Universitaria, Zona 12
GUATEMALA, CENTROAMERICA

DECANATO DE LA FACULTAD DE CIENCIAS ECONOMICAS. GUATEMALA, VEINTIDOS DE ENERO DE DOS MIL DIECISÉIS.

Con base en el Punto CUARTO, inciso 4.1, subinciso 4.1.1 del Acta 28-2015 de la sesión celebrada por la Junta Directiva de la Facultad el 13 de noviembre de 2015, se conoció el Acta AUDITORÍA 276-2015 de aprobación del Examen Privado de Tesis, de fecha 01 de octubre de 2015 y el trabajo de Tesis denominado: "PROPUESTA DE IMPLEMENTACIÓN Y ADOPCIÓN DEL MODELO DE OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT), EN UNA EMPRESA ASEGURADORA, POR PARTE DE LA AUDITORÍA INTERNA, PARA LA EVALUACIÓN DE CONTROLES DE ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS", que para su graduación profesional presentó el estudiante **ERICK RICARDO GONZÁLEZ TRINIDAD**, autorizándose su impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

LIC. CARLOS ROBERTO CABRERA MORALES
SECRETARIO

LIC. LUIS ANTONIO SUÁREZ ROLDÁN
DECANO

Smp.

ACTO QUE DEDICO

A Dios

Por haberme dado la oportunidad de llegar a esta instancia, y porque siempre ha sido la luz de mi vida .

A mis abuelos

Esperanza de González, Marta de Trinidad, Manuel Trinidad y Adolfo González.
Por apoyar a mis padres y a mí en todo momento.

A mis padres

Ericka Liliam Trinidad Herrera de González y Ricardo Adolfo González Melgar.
Por qué me dieron la vida y la educación necesaria para llegar a esta meta.

A mi esposa

Nancy Gabriela Juárez González de González.
Quien desde que la conocí me ha dado su apoyo y consejo incondicional.

A mi hija

Sofía Gabriela.
Por darme la oportunidad de conocer la razón por la que Dios me tiene en este mundo.

A mi familia

Por todo su apoyo y consejo en todo momento.

A mi asesor

Lic. Jorge Luis Reyna Pineda.

Por su apoyo en la realización de importante trabajo.

A la Facultad de Ciencias Económicas

Por darme la oportunidad de ser un profesional.

CONTENIDO

CAPÍTULO III

AUDITORIA INTERNA DE SISTEMAS INFORMÁTICOS

CAPÍTULO IV

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT)

CAPÍTULO V

PROPUESTA DE IMPLEMENTACIÓN Y ADOPCIÓN DEL MODELO DE OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT), EN UNA EMPRESA ASEGURADORA, POR PARTE DE LA AUDITORÍA INTERNA, PARA LA EVALUACIÓN DE CONTROLES DE ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS.

INTRODUCCIÓN

Una empresa aseguradora es una entidad financiera regulada por la Superintendencia de Bancos, el contrato de seguro por ser un servicio puede comercializarse por canales electrónicos, es decir mediante los sistemas de información, actualmente la entidad evaluada realiza transacciones tales como captura de datos en línea, emisión de pólizas de seguros en línea, pagos en línea, envío de facturas electrónicas entre otros servicios; todas estas transacciones quedan registradas en la base de datos de la organización, es por ello que la evaluación de los sistemas de información por parte de la auditoría interna ha tomado auge en respuesta a la necesidad de la administración de conocer el estado actual de la dirección de Tecnologías de Información.

La auditoría de sistemas tradicional hace uso de un experto en área de tecnologías de información, sin embargo hoy en día existen modelos de control que pueden ser adoptados por los Auditores, dichos modelos puede convertirse en herramientas de mucho beneficio al ser adoptadas por la organización.

Los Objetivos de Control de Información y Tecnología relacionada (COBIT, por sus siglas en inglés) son un modelo de control con aceptación a nivel internacional en materia de control informático y aseguramiento de información, ya que permite evaluar a la medida los controles de la gestión informática, verificando si los objetivos del área de TI son congruentes con los objetivos generales del negocio, para garantizar razonablemente a usuarios internos y externos, el suministro oportuno y confiable de la información necesaria para la toma de decisiones.

Expuesto lo anterior, el presente trabajo de tesis denominado: “PROPUESTA DE IMPLEMENTACIÓN Y ADOPCIÓN DEL MODELO DE OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS

(COBIT), EN UNA EMPRESA ASEGURADORA, POR PARTE DE LA AUDITORÍA INTERNA, PARA LA EVALUACIÓN DE CONTROLES DE ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS" tiene como objetivo aportar a los Contadores Públicos y Auditores que desarrollan su actividad como Auditores Internos en una empresa de este tipo, los lineamientos para desarrollar una auditoría de sistemas, evaluando los actuales controles del departamento de informática con base en el modelo de los Objetivos de Control de Información y Tecnología Relacionada (COBIT) en su versión 5.0, con la finalidad de tener un soporte para la opinión del auditor, en base a criterios internacionales de aceptación general que agreguen valor a las conclusiones y recomendaciones ante la administración.

El presente trabajo está desarrollado de tal manera que el lector tenga una secuencia lógica que permita adentrarse de manera adecuada al contenido del mismo.

En el primer capítulo se describen los aspectos generales de una empresa aseguradora, tales como la legislación que aplica, cuál es su modelo de negocio y los términos relacionados para el conocimiento del lector.

En el segundo capítulo se define un departamento de informática, ya que este será objeto de la evaluación en la parte práctica del modelo en cuestión.

Para el tercer capítulo y siguiendo con una secuencia de temas, se describe cual es el procedimiento de una Auditoría de sistemas en un departamento de informática, dando lugar así al cuarto capítulo, en el que se describe el modelo COBIT, como herramienta para la aplicación de la auditoría.

Por último el caso práctico, en el cual se aplican los criterios teóricos descritos en los capítulos anteriores. El dominio de COBIT aplicado es el de Adquirir e Implementar.

Posterior a la aplicación práctica se concluyó que es necesario que la empresa adopte un modelo de trabajo para la revisión del proceso seleccionado ya que los niveles de capacidad se encuentran funcionando pero pueden mejorarse y llegar a un estado óptimo.

Derivado de lo anterior se recomienda la adopción del modelo COBIT ya que con este podrán controlar y mejorar los aspectos en los que ahora tienen deficiencias, además de la capacitación en el uso de este tipo de herramientas.

CAPÍTULO I

Empresa aseguradora

1.1 Definición:

Es la empresa especializada en el contrato de seguro, cuya actividad económica consiste en producir el servicio de seguridad cubriendo determinados riesgos económicos (riesgos asegurables) a las unidades económicas de producción y consumo.

"El seguro es una operación por medio de la cual una persona (asegurado) contrata con una compañía (aseguradora) una prestación o servicio para cubrir un riesgo (suceso o evento asegurado), a cambio de un pago o retribución (prima)" (36:1).

1.2 Características:

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

- Sigue el principio de mutualidad, buscando la solidaridad entre un grupo sometido a riesgos. Esta mutualidad se organiza empresarialmente, creando un patrimonio que haga frente a los riesgos. El efecto desfavorable de estos riesgos, considerados en su conjunto, queda aminorado sustancialmente, porque, para el asegurador, los riesgos individuales se compensan: sólo unos pocos asegurados los sufren, frente a los muchos que contribuyen al pago de la cobertura. Ello permite una gestión estadística del riesgo, desde el punto de vista económico, aunque se conserve

individualmente desde el punto de vista jurídico. La actividad aseguradora es uno de los tres pilares de los mercados financieros, junto con el mercado de crédito o bancario y los mercados de valores o de instrumentos financieros.

- Su importancia estratégica, social y económica, lleva a que estén sometidas a estricta supervisión administrativa con reglas propias de funcionamiento, control e inspección.
- Las empresas de seguros por su función mediadora en el sistema financiero son unos intermediarios financieros con unas características especiales que las diferencian de las empresas de otros sectores de la economía e incluso con las restantes empresas financieras.

1.3 Naturaleza:

Su actividad es una operación para acumular riqueza, a través de las aportaciones de muchos sujetos expuestos a eventos económicos desfavorables, para destinar lo así acumulado, a los pocos a quienes se presenta la necesidad.

1.4 Objetivos generales:

Los principales objetivos de una empresa aseguradora son:

- Cumplir con una función económica propiciando el intercambio monetario y la generación de riqueza.
- Cumplir una función social al generar fuentes de empleo y contribuir al mejoramiento de la calidad de vida de sus empleados.

- Busca la obtención de un beneficio económico mediante la satisfacción de alguna necesidad de orden general o social.

- Tiene como finalidad primordial la obtención del lucro, ofreciendo a sus clientes la protección económica de sus bienes mediante un contrato de seguro.

1.5 Formas de organización:

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

1.6 Estructura organizacional:

Las funciones generales de una aseguradora son técnicas, comerciales y administrativas, donde se incluyen las funciones específicas del ramo de seguros.

1.6.1 Funciones técnicas:

Estas se refieren a las funciones específicas del seguro, dentro de las cuales existen técnicas para operarlo, las cuales son:

- Análisis de riesgo
- Distribución del riesgo
- Administración de siniestros

Para estas técnicas se llevan a cabo distintas actividades:

Actuarial: Tiene como objetivo el análisis del riesgo. La meta más importante de dicha función es la creación de nuevas tarifas de riesgos y la actualización de las existentes, así como determinar las bases técnicas en que han de fundamentarse los nuevos seguros.

Contractual: El seguro se contrata para un riesgo determinado, pero el actuario trabaja sobre promedios no sobre riesgos específicos. Es deber de las empresas de seguros vigilar que los riesgos contratados sean aquéllos para los cuales se contrató la póliza. “Para esto es importante realizar las siguientes actividades, las cuales también forman los departamentos en que la aseguradora se divide:

- Cotización: Consiste en la inspección del riesgo. Solicitar toda la información que ayude a la mejor apreciación del riesgo. Es la investigación que se lleva a cabo del bien a asegurar.

- Suscripción: Consiste en la selección del riesgo. Las personas debidamente entrenadas del departamento técnico evalúan la información anterior para determinar si se selecciona el riesgo o no. Si se selecciona el riesgo es en esta etapa donde se realiza la tarifación y condiciones necesarias.

- Emisión: Consiste en la elaboración de la póliza y sus condiciones generales y particulares que amparen las coberturas contratadas. La emisión de pólizas nuevas, renovaciones, endosos o cualquier otro documento que forme parte de la póliza debe ser cuidadosamente revisada puesto que pueden alterar los términos de la póliza.

- Reaseguramiento: Consiste en la distribución del riesgo. Como se ha descrito, el reaseguro es la contratación de respaldo para las

cantidades aseguradas. Se eligen varias reaseguradoras y se distribuye el riesgo entre ellas.

- Cobranzas: Consiste en el cobro de la póliza. En esta actividad se han realizado importantes modificaciones de cobro, como en cualquier entidad. Se puede ofrecer cobro directo, a través de corredores y agentes, por medio de tarjetas de crédito, entre otros. Aparte de esto se ha ofrecido el fraccionamiento de primas anuales. Estas facilidades muestran la importancia del pago ya que si no se realiza, se puede cancelar la póliza, depende de cada aseguradora.

- Reclamos: Consiste tramitar un ajuste de pérdidas, así como liquidación de indemnizaciones en caso de siniestro cubierto.

1.6.2 Funciones comerciales:

Esta función tiene como objetivo básico aumentar el número y volumen de contratos suscritos por la empresa de seguros. Además de la satisfacción de crecimiento de toda empresa, aumenta la masa asegurada que garantiza su desarrollo equilibrado.

Las actividades que se realizan para esta función son:

- Adquisición de nuevas pólizas.
- Aumento de las sumas aseguradas y coberturas en pólizas existentes.
- Conservación de los asegurados y sus coberturas.
- Mantenimiento de buenas relaciones con los asegurados.

1.6.3 Funciones administrativas:

Esta función afecta a casi todas las áreas de la compañía de seguros. Una función de especial trascendencia es el personal. El personal es uno de los activos más valiosos en una empresa de seguros. Es por ello que se capacita constantemente a todo el personal en diferentes áreas de importancia tales como reaseguro, calculo actuarial, prevención de lavado de dinero entre otras.

Los servicios administrativos son variados y depende de las actividades de la empresa y de su dimensión o grado de desarrollo.

Las principales áreas de actividad de los servicios administrativos son:

- Contabilidad
- Auditoría
- Procesamiento de datos

En el área financiera, una empresa de seguros debe disponer de amplios fondos cuyo manejo constituye un medio importante para obtener resultados favorables. La función financiera está muy condicionada por las leyes, para garantizar la solvencia de dichas empresas y el cumplimiento de las obligaciones.

1.7 Legislación aplicable:

Las empresas de seguros en Guatemala, están constituidas como sociedades mercantiles bajo la modalidad de sociedades anónimas, las cuales están reguladas por las disposiciones legales siguientes:

- Derecho 2-70 del Congreso de la República, Código de Comercio.
- Decreto Ley 473, Constitución y Organización de Empresas de Seguros, modificado por el Decreto 32-90 del Congreso de la República.
- Decreto 854, Ley de Inversiones y Reservas Técnicas y Matemáticas de las Compañías de Seguros.
- Decreto Ley 154-83, Cuota Anual de Sostenimiento de la Superintendencia de Bancos.
- Acuerdo Gubernativo del Ministerio de Economía No. 22-74, Reglamento de la Ley de Inversiones de Reservas Técnicas y Matemáticas de las Empresas de Seguros.
- Acuerdo Gubernativo del 14 de agosto de 1969, Reglamento del Decreto 473, Constitución y Organización de Empresas de Seguros.
- Acuerdo Gubernativo del Ministerio de Economía No. 198-93, Reglamento del Riesgo de Terremoto sobre Cobertura, Cúmulos, Reaseguro Catastrófico y Reserva Específica.
- Decreto 53-79 del Organismo Legislativo. Fija tasa máxima de interés sobre los préstamos que concedan las aseguradoras a sus asegurados con garantía de sus pólizas.
- Acuerdo Gubernativo No. 637-91, Reglamento para la promoción y el desarrollo de operaciones de fideicomiso por las empresas de seguros.
- Acuerdo Gubernativo del Ministerio de Economía No. 5-79, Reglamento para la Aprobación y Control de Tarifas de Seguros del ramo de Daños.
- Acuerdo Gubernativo del Ministerio de Economía No. 67-90. Establece el seguro para transporte especializado de productos derivados del petróleo en forma obligatoria.

- Decreto 1422, Impuesto a favor del Cuerpo Voluntario de Bomberos de Guatemala.
- Ley de Prevención del Lavado de Dinero y Otros Activos (Decreto No. 67-2001).
- Ley para prevenir y reprimir el financiamiento del terrorismo (Decreto No. 58-2005)
- Constitución Política de la República de Guatemala.
- Código de Trabajo, Decreto número 1441 y sus reformas.
- Código Tributario, Decreto número 6-91 y sus reformas.
- Ley de registro tributario unificado y control general de contribuyentes, Decreto número 25-71.
- Ley del impuesto al valor agregado, Decreto número 27-92 y sus reformas.
- Reglamento de la ley del impuesto al valor agregado, acuerdo gubernativo número 424-2006 y sus reformas.
- Ley de Timbres y de papel sellado especial para protocolos, Decreto número 37-92.
- Reglamento del impuesto de timbres fiscales y de papel sellado especial para protocolos, Acuerdo Gubernativo número 737-92.
- Ley de actualización tributaria, Decreto número 10-2012.
- Otras disposiciones específicas de los distintos ramos de seguros, contenidas en varios cuerpos legales, recopilados por la Superintendencia de Bancos en el folleto de Leyes y Disposiciones sobre seguros y fianzas.

CAPÍTULO II

EL DEPARTAMENTO DE INFORMÁTICA DE UNA EMPRESA ASEGURADORA

2.1 Definición:

El introducir equipo de cómputo en una empresa genera cambios en el manejo de la información así mismo cambios en los departamentos ligados a esas actividades, así es posible estructurar sistemas de información de manera que los equipos instalados en los diferentes departamentos se encuentren conectados para envío y recepción de datos.

Deben de asignarse a un área de organización específica, dicha área es precisamente el centro de informática. Al asignarle la responsabilidad a la función informática de una empresa a un departamento específico, es importante definir su ubicación dentro de la organización, así como su estructura interna.

La ubicación de los centros de informática dependerá de cada organización en particular.

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

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

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

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

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

2.1.1 Personal que integra el departamento de Informática:

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

- Dirección del departamento.
- Mesa de ayuda a usuarios (help desk).
- Personal especializado encargado del análisis y programación del sistema
- Personal para la administración del equipo (reparaciones, instalación de sistemas, administración de redes, etc.) y el soporte a la infraestructura tecnológica.

2.1.2 Dirección del departamento:

Cumple la función de enlace entre las necesidades informáticas de la empresa y los usuarios de los servicios computacionales, por lo tanto, la persona que funge como director de informática deberá tener sólidos

conocimientos de sistemas, equipos informáticos y de la infraestructura necesaria para su funcionamiento. Generalmente se recomienda que el encargado posea el título de Ingeniero en Sistemas o Licenciado en Administración de Sistemas.

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

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

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

- Determinar el origen de los problemas de cómputo y emprender las acciones correctivas apropiadas.

- Iniciar los reportes de problemas que se requieran y asegurar que los problemas sean resueltos a su debido tiempo.

- Obtener conocimientos detallados del sistema operativo y del software de otros sistemas.

- Responder a las interrogantes relativas a sistemas específicos.

- Controlar la instalación de software del vendedor y del sistema para mejorar su eficiencia y personalizar el sistema sobre la base de los requisitos de la organización y a la configuración de las computadoras.

- Brindar soporte técnico al procesamiento computarizado de las telecomunicaciones.

- Mantener documentación del software del vendedor, incluyendo la emisión de nuevas versiones (releases) y resolución de problemas, así como documentación de los sistemas y utilerías desarrolladas localmente.

- Comunicarse con las operaciones de sistemas para señalar patrones anormales en llamadas o comportamiento de aplicaciones.” (3:353)

2.1.4 Departamento de análisis y programación de sistemas

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

El departamento de sistemas puede dividirse en:

- Sección de análisis de sistemas:

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

- Sección de programación de sistemas:

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

- Sección de aseguramiento de calidad:

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

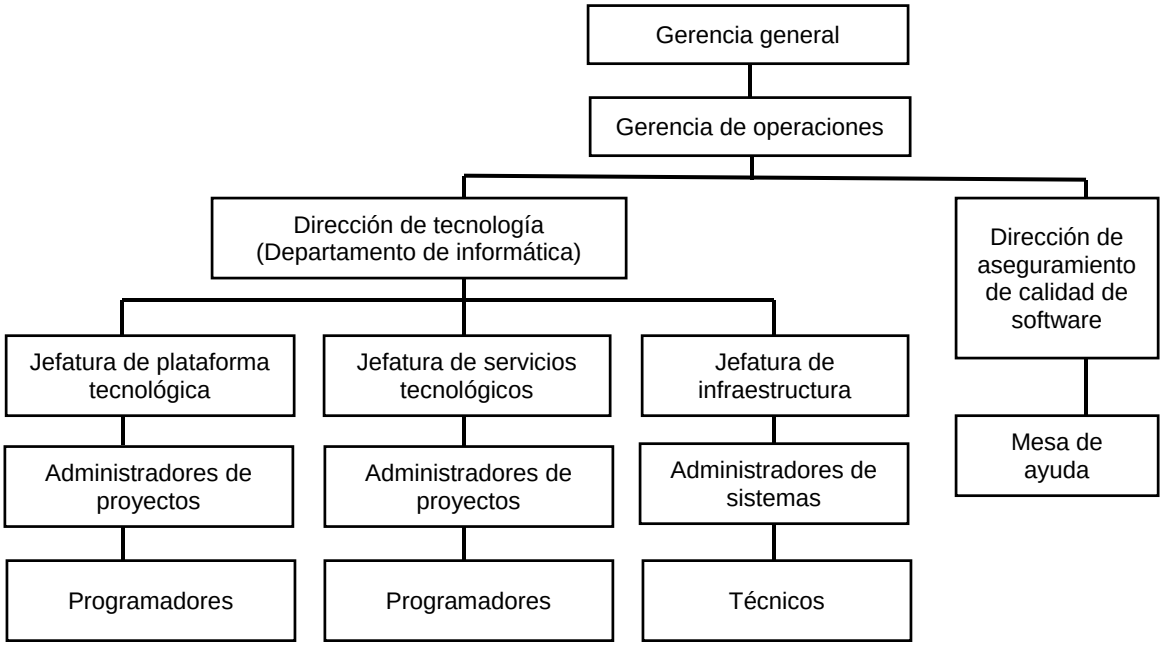
2.1.5 Departamento de soporte a la infraestructura tecnológica

Es el encargado de administrar la información resultante del proceso electrónico de datos, las copias de respaldo o back-up del sistema, realizar mantenimiento preventivo y correctivo a los equipos, el manejo de telecomunicaciones y otros relacionados. Tiene a su cargo la instalación de los sistemas de aplicación a los equipos.
Adicionalmente maneja el presupuesto anual designado para la adquisición de hardware y software, necesario para mantener el servicio y apoyar las áreas operativas y de negocios de una empresa.

Este departamento puede subdividirse en tres secciones:

- Sección de técnicos especializados en manejo de software y hardware.
- Sección de comunicaciones, que se ocupa de administrar el correo electrónico, redes, comunicaciones, internet, antivirus, etc.
- Sección de administración de la información y operaciones relacionadas con el procesamiento electrónico de datos, back-up del sistema e información, inventarios de equipos y medidas de seguridad.

ORGANIGRAMA DEL DEPARTAMENTO DE INFORMÁTICA



Fuente: Empresa el Mejor Seguro S.A.

2.2 Administración del personal del departamento de informática

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

2.3 Infraestructura necesaria para el funcionamiento del departamento de informática

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

2.3.1 El Hardware

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

2.3.2 Manuales de usuario

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

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

2.3.3 El Software

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

El software tiene algunas funciones específicas, entre ellas:

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

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

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

Existen tres tipos de software:

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

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

- **Software de usuario final:**
  “Es el que permite el desarrollo de algunas aplicaciones directamente por los usuarios finales, este software con frecuencia tiene que trabajar a

través del software de aplicación y finalmente a través del software del sistema.”(3:368)

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

- **Viabilidad**

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

- **Requerimientos**

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

- **Diseño**

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

- **Desarrollo**

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

- **Implementación**

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

- **Post Implementación**

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

2.3.4 Sistemas de comunicación

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

2.3.5 Descripción de procesos

Un departamento de informática debe contar con una apropiada documentación de sus procesos. En esta documentación deberá constar la

secuencia de las operaciones y sus procesos, su importancia, horarios de ejecución, personal responsable, posibles contingencias, etc.

2.3.6 Bases de datos

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

2.4 Políticas y procedimientos aplicables a un departamento de informática

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

2.4.1 Políticas

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

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

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

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

2.4.2 Procedimientos

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

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

2.5 Administración de la seguridad informática

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

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

2.5.1 Seguridad lógica

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

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

Existen varios elementos para fortalecer la seguridad lógica:

- Software de control de acceso

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

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

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

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

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

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

- Firewall:

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

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

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

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

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

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

- Software para prevención y detección de intrusos:
  Estos programas funcionan brindando alertas ante la realización de ataques con éxito e incluso ante ataques en progreso.

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

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

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

  Prevención, detección y reacción constituyen tres conceptos clave en todo sistema de protección que pretenda ofrecer soluciones integrales de seguridad.
  Hoy en día, prácticamente la totalidad de productos de seguridad en el mercado, se centran en la primera de esas acciones, la prevención del ataque, utilizando cortafuegos y criptografía. Aunque ningún programa de

este tipo será nunca cien por ciento infalible, lo cierto es que disminuirá la probabilidad de éxito de un ataque.

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

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

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

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

- Antivirus

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

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

2.5.2 Seguridad física

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

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

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

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

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

- Aire acondicionado
  Los equipos de computación concentrados dentro del departamento de informática generan calor que puede dañarlos, por lo que es necesario

que se cuente con equipo adecuado de aire acondicionado que evite el sobrecalentamiento, generalmente la temperatura ideal para los equipos de cómputo oscila entre 14 y 17 grados centígrados.

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

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

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

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

2.5.3 Seguridad del personal

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

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

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

2.5.4 Seguridad de la base de datos

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

2.5.5 Seguridad de los sistemas de comunicación

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

2.5.6 Seguridad en la programación de los sistemas

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

2.6 Presupuestos para adquisición y mantenimiento de tecnología de información

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

Generalmente este presupuesto se elabora para períodos anuales.

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

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

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

CAPÍTULO III

AUDITORÍA INTERNA DE SISTEMAS INFORMÁTICOS

Es una Auditoría cuyo alcance comprende la revisión y evaluación de todos los aspectos de los sistemas de procesamiento de información automatizados, incluye los procesos relacionados no automatizados y las interfaces entre ellos.

Los Auditores de sistemas de información revisan y evalúan el desarrollo, mantenimiento y operación de los componentes de los sistemas automatizados, (o los sistemas como un todo), y sus interfaces con las áreas no automatizadas de las operaciones de la organización.

Los objetivos de tales auditorías generalmente son evaluar el grado en que los sistemas o sus componentes producen información confiable y exacta y determinar si tal información está de acuerdo con los requisitos de la administración y condiciones estatutarias.

La definición de Auditoría Interna la establece en diciembre del 2000 el instituto de Auditores Internos de los Estados Unidos de América (IIA) de la siguiente forma: “La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno” (36:1)

Aunque el enfoque tradicional de auditoría interna de hasta hace algunos años, consideraba a la auditoría interna como un elemento operativo, aquel que aprobaba las transacciones, ponía el visto bueno en los asientos contable, liquidaciones, etc. El enfoque moderno pretende enfatizar su función de control, mayormente como elemento de la misma, modificando, rectificando y cambiando las funciones de

auditoría interna, de una acción de control previo, hacia una acción más positiva orientada a la evaluación de sistemas, procesos y resultados, dentro de los cuales cobra cada vez más importancia la evaluación de sistemas informáticos para el aseguramiento de información confiable y oportuna, como consecuencia del auge de la tecnología en las empresas modernas.

3.1 Auditoría interna de sistemas informáticos

La Auditoría Interna es una actividad de evaluación independiente establecida en la organización como un servicio a la misma. Es un control que funciona para examinar y evaluar lo adecuado y efectividad de otros controles.
El objetivo fundamental de la Auditoría Interna es asesorar y apoyar a los diferentes niveles de la administración en el cumplimiento efectivo de sus responsabilidades, facilitándoles análisis, apreciaciones, recomendaciones y comentarios pertinentes, relacionados con las actividades realizadas. El Auditor Interno actúa en cualquier actividad que pueda ser útil a la administración. Esto implica ir más allá de los registros contables y financieros, para comprender y analizar las operaciones revisadas.

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

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

Las anteriores definiciones destacan características importantes del trabajo que realiza la auditoría de sistemas informáticos, pero a nivel internacional se acepta de forma general el establecido por la Asociación de Auditoría y Control de Sistemas de Información (ISACA, por sus siglas en inglés), que también publicó los Objetivos de Control de Información y Tecnología Relacionada (COBIT, por sus siglas en inglés) en que se basa el presente trabajo, por lo que deberá ser el concepto a considerar y dicta de la siguiente manera: “Auditoría de Sistemas es cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos), de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.” (35:1)

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

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

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

- La falta de una clara comprensión del uso de la tecnología por parte de las unidades usuarias.

- La falta de conciencia sobre el alcance y control de la tecnología dentro de la organización.

- El permanente avance tecnológico.

- El costo representativo de equipos y aplicaciones existentes.

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

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

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

- Mayor vulnerabilidad de la organización por el avance tecnológico.

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

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

3.2 Normas y procedimientos para auditar sistemas informáticos

La Auditoría de sistemas de información es un trabajo de naturaleza especializada y las habilidades necesarias para llevar a cabo este tipo de auditorías requieren el desarrollo y la promulgación de normas específicas para la práctica profesional como las emitidas por la Asociación de Auditoría y Control de Sistemas de Información (ISACA) las cuales son aplicables para el trabajo de auditoría realizado por miembros de la asociación y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información (CISA, por sus siglas en inglés), aunque a criterio personal pueden servir de base para

cualquier auditor que cuente con las habilidades y destrezas suficientes y necesite apoyarse en una normativa específica para realizar su trabajo, debido a que el planteamiento a nivel general es similar a la normativa para la realización del trabajo de cualquier auditoría por lo que en el presente trabajo se considera la más adecuadas para una auditoría de sistemas de información.

3.3 Normas Internacionales de Auditoría

Para su desarrollo ordenado el presente tema se divide en normas ético morales y normas profesionales.

3.3.1 Normas ético morales

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

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

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

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

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

- Integridad:

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

- Objetividad:

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

- Confidencialidad:

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

- Competencia:

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

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

- Integridad:

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

- Objetividad:

    - No participar en actividades o relaciones que puedan perjudicar o que aparenten que puedan perjudicar su evaluación imparcial. Esta participación incluye aquellas actividades o relaciones que puedan estar en conflicto con los intereses de la organización.

    - No aceptar nada que pueda perjudicar o que aparente que pueda perjudicar su juicio profesional.

    - Divulgar todos los hechos materiales que conozcan y que, de no ser divulgados, pudieran distorsionar el informe de las actividades sujetas a revisión.

- Confidencialidad:

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

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

- Competencia:

  - Participar solo en aquellos servicios para los cuales tengan los suficientes conocimientos, aptitudes o experiencia.

  - Desempeñar todos los servicios de auditoría interna de acuerdo con las normas para la práctica profesional de la auditoría interna.

  - Mejorar continuamente sus aptitudes y la efectividad y calidad de sus servicios.

3.3.2 Normas profesionales

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

Las normas sobre atributos definen las características de las organizaciones y los individuos que desarrollan actividades de auditoría interna. Las normas sobre desempeño describen la naturaleza de las actividades de auditoría interna y proveen criterios de calidad con los cuales puede evaluarse el desempeño de estos servicios. Las normas sobre atributos y sobre desempeño se aplican a todos los servicios de auditoría interna en general,

mientras que las normas sobre Implantación se aplican a determinados tipos de trabajos.

El auditor interno en el medio guatemalteco deberá observar principalmente la normativa vigente para auditorías de estados financieros emitida por el Consejo de Normas de Auditoría y Atestiguamiento (IAASB, por sus siglas en inglés) de la Federación Internacional de Contadores (IFAC, por sus siglas en inglés), las cuales fueron adoptadas por el Instituto Guatemalteco de Contadores Públicos y Auditores (IGCPA) como la normativa vigente para la práctica de la profesión de auditoría en la República de Guatemala a partir de enero del 2008, las que se denominan “Normas Internacionales sobre Control de Calidad, Auditoría y Atestiguamiento y Servicios Relacionados (Normas Internacionales o Normas del IAASB), donde la evaluación del control interno, ya sea a nivel de controles administrativos o de controles de los sistemas informáticos, influyen en la extensión y alcance de las pruebas sustantivas que deben aplicarse durante la revisión por el grado de confianza que el auditor considera depositar en las cifras de los estados financieros. La norma internacional de auditoría No. 315 “Entendimiento de la entidad y su entorno y evaluación de los riesgos de representación errónea de importancia relativa” establece y proporciona guías para conocer la entidad y su entorno, incluyendo su control interno, y para evaluar los riesgos de representación errónea en un auditoría de estados financieros.

En resumen esta norma plantea los siguientes requisitos:

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

  Explica los procedimientos de auditoría que se requiere al auditor realizar para obtener el entendimiento de la entidad y su entorno, incluyendo su control interno (procedimientos de evaluación de riesgo). También

requiere la discusión entre el equipo de trabajo sobre la susceptibilidad de los estados financieros a representación errónea de importancia relativa.

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

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

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

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

  - Identificar los riesgos al considerar la entidad y su entorno, incluyendo controles relevantes, y al considerar las clases de transacciones, saldos de cuentas y revelaciones en los estados financieros.

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

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

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

- Documentación:

  Se establecen los requisitos mínimos de documentación relacionados.

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

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

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

3.4 COSO (Commitee of Sponsoring Organizations)

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

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

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

Para fines de la norma, el término “control interno” abarca los anteriores cinco componentes.

Además el término “controles” se refiere a uno o más de los componentes, o cualquiera de sus aspectos.

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

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

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

- Dependencia de sistemas o programas que procesen los datos de una manera no exacta o que procesen datos no exactos, o ambas cosas.

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

- La posibilidad de que personal de TI obtenga privilegios de acceso más allá de los necesarios para desempeñar sus deberes asignados, faltando, por lo tanto, a la segregación apropiada de funciones.

- Cambios no autorizados a datos en los archivos maestros.
- Cambios no autorizados a sistemas o programas.

- Dejar de hacer los cambios necesarios a sistemas o programas.
- Intervención manual inapropiada.
- Potencial pérdida de datos o incapacidad de acceder a los datos según se requiere.

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

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

El auditor deberá obtener un entendimiento suficiente de las actividades de control para evaluar los riesgos de representación errónea de importancia relativa al nivel de aseveración y para diseñar procedimientos adicionales de auditoría que respondan a los riesgos evaluados. Las actividades de control son las políticas y procedimientos que ayudan a asegurar que se llevan a cabo las directrices de la administración; por ejemplo, que se toman las

acciones necesarias para atender los riesgos que amenazan el logro de los objetivos de la entidad. Las actividades de control, sean dentro de sistemas de tecnología informática o manuales, tienen diversos objetivos y se aplican a diversos niveles organizacionales y funcionales. Ejemplos de actividades de control específicas incluyen las relativas a:

- Autorización
- Revisiones de desempeño
- Procesamiento de información.
- Controles físicos
- Segregación de funciones

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

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

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

Los controles de aplicación son procedimientos manuales o automatizados que típicamente operan en el ámbito del proceso del negocio. Los controles de aplicación pueden ser de naturaleza preventiva o detectiva y se diseñan para asegurar la integridad de los registros contables.

Consecuentemente, los controles de aplicación se relacionan con procedimientos que se usan para iniciar, registrar, procesar e informar transacciones u otros datos financieros. Estos controles ayudan a asegurar que las transacciones ocurrieron, que están autorizadas y que son registras y procesadas de manera completa y exacta. Los ejemplos incluyen verificaciones de emisión de cheques de datos de entrada, y verificaciones de secuencia numérica de los cheques con seguimiento manual de informes de excepción o corrección en el punto de entrada de los datos.

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

- Identifica los riesgos a lo largo del proceso de obtención de entendimiento de la entidad y su entorno, incluyendo los controles relevantes que se relacionan con los riesgos, y al considerar las clases de transacciones, saldos de cuentas y revelaciones en los estados financieros;
- Relaciona los riesgos identificados con lo que pueda estar mal al nivel de aseveraciones;
- Considera si los riesgos son de una magnitud que pudiera dar como resultado una representación errónea de importancia relativa de los estados financieros; y
- Considera la probabilidad de que los riesgos pudieran dar como resultado representación errónea de importancia relativa de los estados financieros.

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

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

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

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

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

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

- Los estándares:

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

- Las directrices

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

- Los procedimientos:

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

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

- Estatuto de Auditoría:

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

- Independencia profesional:

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

- Independencia organizacional:

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

- Ética y estándares profesionales:

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

- Competencia Profesional:

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

- Planificación:

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

- Ejecución del trabajo de auditoría:

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

- Informe:

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

- Actividades de seguimiento:

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

- Irregularidades y actos ilícitos:

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

- Gobierno de TI:

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

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

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

- Materialidad de la Auditoría:

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

- Uso del trabajo de otros expertos:

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

3.6 Metodología de la Auditoría de sistemas

Puede definirse como “una serie ordenada de acciones, tareas y procedimientos, los cuales serán utilizados conforme a un método minucioso, previamente establecido, a fin de utilizar una serie de herramientas, métodos e instrumentos necesarios en la evaluación del área de sistemas.”(34:185)

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

- Planificación:

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

- Ejecución:

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

- Informe:

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

CAPÍTULO IV

OBJETIVOS DE CONTROL PARA LA INFORMACIÓN Y TECNOLOGÍA RELACIONADA (COBIT)

4.1. Antecedentes

El desarrollo de una auditoría informática se basa en la aplicación de normas, técnicas, estándares y procedimientos que garanticen el éxito del proceso. La gran mayoría de documentación existente coincide en que las normas de auditoría son requisitos mínimos de calidad, relativos a las cualidades del auditor, a los métodos y procedimientos aplicados en la auditoría, y a los resultados. Las técnicas en cambio, son todos aquellos métodos que permiten al auditor evidenciar y fundamentar sus opiniones y conclusiones.

Actualmente Guatemala cuenta con un marco regulatorio y normativo reducido en materia informática, es por ello que se estudiarán las normas y organizaciones internacionales más relevantes en este ámbito. Las organizaciones más importantes son: Institute of Internal Auditors (IIA), e Information System Audit and Control Association (ISACA) Las organizaciones antes mencionadas, han desarrollado normas y estándares con el fin de establecer políticas y lineamientos que garanticen el proceso de auditoría.

Algunos de los estándares más conocidos son:

- COBIT: Control Objectives for Information and related Technology. Desarrollado por Information Systems Audit and Control Association (ISACA). Centra su interés en la gobernabilidad, aseguramiento, control y auditoría para Tecnologías de la Información y Comunicación (TIC).

- ITIL: Information Technology Infrastructure Library. Recoge las mejores prácticas para administrar los servicios de Tecnología de la Información (TI).

- COSO: Committee of Sponsoring Organizations. Hace recomendaciones a los administradores de TI sobre cómo evaluar, informar e implementar sistemas de control, teniendo como objetivo la efectividad y eficiencia de las operaciones, la información financiera y el cumplimiento de las regulaciones, valoración de riesgos, actividades de control, información y comunicación y la verificación.

- ISO Serie 27000: Integra un conjunto de normas sobre Sistemas de Gestión de Seguridad de la Información (SGSI), que a través de su aplicación, permite administrar la información mediante el modelo Plan – Do – Check – Act (PDCA).

- SAC: Systems Auditability and Control, ofrece una guía de estándares y controles a auditores internos sobre la forma de controlar y auditar los sistemas de información y tecnología.

A continuación una reseña de la evolución del modelo COBIT:

1992 Comienza la actualización de los objetivos de control de ISACA

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

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

2000 Se publica la 3ª Edición

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

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

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

2012 COBIT 5, Un marco de negocio para el gobierno y la gestión de las TI de la Empresa.

Bajo la metodología de COBIT 5, se solventan las necesidades actuales para la gestión y gobernabilidad de las Tecnologías de Información.

4.2. Resumen ejecutivo

La información es un recurso clave para todas las empresas y desde el momento en que la información se crea hasta que es destruida, la tecnología juega un papel importante. La tecnología de la información está avanzando cada vez más y se ha generalizado en las empresas y en entornos sociales, públicos y de negocios.

Como resultado, hoy más que nunca, las empresas y sus ejecutivos se esfuerzan en:

- Mantener información de alta calidad para soportar las decisiones del negocio.
- Generar valor al negocio con las inversiones en TI, por ejemplo, alcanzando metas estratégicas y generando beneficios al negocio a través de un uso de las TI de forma eficaz e innovadora.

- Alcanzar la excelencia operativa a través de una aplicación de la tecnología fiable y eficiente.
- Mantener los riesgos relacionados con TI en un nivel aceptable
- Optimizar el coste de los servicios y tecnologías de TI
- Cumplir con las constantemente crecientes leyes, regulaciones, acuerdos contractuales y políticas aplicables.

Durante la pasada década, el término “gobierno” ha pasado a la vanguardia del pensamiento empresarial como respuesta a algunos ejemplos que han demostrado la importancia del buen gobierno y, en el otro extremo de la balanza, a incidentes corporativos a nivel global.

Empresas de éxito han reconocido que el comité y los ejecutivos deben aceptar las TI como cualquier otra parte importante de hacer negocios. Los comités y la dirección tanto en funciones de negocio como de TI, deben colaborar y trabajar juntos, de modo que se incluya la TI en el enfoque del gobierno y la gestión. Además, cada vez se aprueba más legislación y se implementan regulaciones para cubrir esta necesidad.

COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos.

Es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

Se basa en cinco principios claves, los cuales se describen a continuación.

- **Principio 1. Satisfacer las necesidades de las partes interesadas**

  Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.

  COBIT 5 provee todos los procesos necesarios y otros catalizadores para permitir la creación de valor del negocio mediante el uso de TI. Dado que toda empresa tiene objetivos diferentes, una empresa puede personalizar COBIT 5 para adaptarlo a su propio contexto mediante la cascada de metas, traduciendo metas corporativas de alto nivel en otras metas más manejables, específicas, relacionadas con TI y mapeándolas con procesos y prácticas específicos.

- **Principio 2: Cubrir la empresa extremo-a-extremo**

  COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo:

  - Cubre todas las funciones y procesos dentro de la empresa; No se enfoca sólo en la “función de TI”, sino que trata la información y las tecnologías relacionadas como activos que deben ser tratados como cualquier otro activo por todos en la empresa.

  - Considera que los catalizadores relacionados con TI para el gobierno y la gestión deben ser a nivel de toda la empresa y de principio a fin, es decir, incluyendo a todo y todos, los que sean relevantes para el gobierno y la gestión de la información de la empresa y TI relacionadas.

- **Principio 3: Aplicar un marco de referencia único integrado**

  Hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

- **Principio 4: Hacer posible un enfoque holístico**

  Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes interactivos. COBIT 5 define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global para las TI de la empresa. Los catalizadores se definen en líneas generales como cualquier cosa que puede ayudar a conseguir las metas de la empresa. El marco de trabajo define siete categorías de catalizadores:

  – Principios, políticas y marcos de trabajo
  – Procesos
  – Estructuras organizativas
  – Cultura, ética y comportamiento
  – Información
  – Servicios, infraestructuras y aplicaciones
  – Personas, habilidades y competencias

- **Principio 5: Separar el gobierno de la gestión**

  El marco de trabajo establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos.

Distinción clave entre gobierno y gestión:

– Gobierno:

En muchas corporaciones, el gobierno global es responsabilidad del comité de dirección bajo el liderazgo del presidente. Algunas responsabilidades de gobierno específicas se pueden delegar en estructuras organizativas especiales al nivel apropiado, particularmente en las corporaciones más grandes y complejas.

– Gestión

En muchas empresas, la gestión es responsabilidad de la dirección ejecutiva bajo el liderazgo del Director general ejecutivo (CEO).

Juntos, estos cinco principios habilitan a la empresa a construir un marco de gestión de gobierno y gestión efectivo que optimiza la inversión y el uso de información y tecnología para el beneficio de las partes interesadas.

4.3. Marco de trabajo

El marco de trabajo relaciona los requerimientos de información y de gobierno TI a los objetivos de la función de servicios de TI. El modelo de procesos de COBIT permite que las actividades de TI y los recursos que los soportan sean administrados y controlados basados en los objetivos de control, alineados y monitoreados utilizando las metas y métricas establecidas por la metodología.

4.3.1. Razones para utilizarlo

El marco de referencia COBIT otorga especial importancia a los requerimientos de negocios en cuanto a efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad que deben ser satisfechos. El desarrollo de este marco de referencia ha sido limitado a objetivos de control de alto nivel en forma de necesidades de negocio dentro de un proceso de tecnología informática particular, cuyo logro es posible a través del establecimiento de controles.

La misión de COBIT es “Investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento” (COBIT 4.1 2007, p.9).

Un “Objetivo de Control”, es una definición del resultado o propósito que se desea alcanzar implementando procedimientos de control específicos dentro de una actividad de tecnología informática. COBIT identifica un conjunto de 34 objetivos de alto nivel, uno para cada uno de los procesos de tecnología informática, agrupados en cuatro dominios:

- Planeación y organización
- Adquisición e implementación
- Entrega de servicio
- Monitoreo

4.3.2. Beneficios a usuarios

Proporciona ventajas a gerentes, usuarios, e interventores. Los gerentes se benefician porque les provee un fundamento sobre el cual pueden basar las decisiones de una forma eficaz, ayuda a la definición de un plan de TI

estratégico, la definición de la arquitectura de la información, la adquisición del hardware necesario y el software para ejecutar una estrategia, la aseguración del servicio continuo, la supervisión del funcionamiento del sistema TI. Los usuarios por otro lado se benefician debido al aseguramiento proporcionado a ellos en el tratamiento de la información. Finalmente los auditores o interventores se ven beneficiados ya que permite identificar cuestiones de control de TI dentro de la infraestructura de una institución y a corroborar sus conclusiones de auditoría.

4.3.3. Orientado a procesos

Incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. Dicho modelo representa todos los procesos que normalmente se encuentran en una empresa, relacionados con las actividades de TI

Los dominios principales son:

- Gobierno

  Contiene 5 procesos de gobierno, dentro de cada proceso se definen prácticas de evaluación, orientación y supervisión.

- Gestión

  Contiene 4 dominios de acuerdo a las áreas de responsabilidad de planificar, construir, ejecutar y supervisar.

  - Alinear, planificar y organizar
  - Construir, adquirir e implementar
  - Entregar, dar servicio y soporte

- Supervisar, evaluar y valorar

Procesos del dominio construir, adquirir e implementar:

- BAI01 Gestionar los programas y proyectos: Al conjunto de proyectos se le denomina programa y un proyecto está compuesto por las actividades a realizar para obtener un objetivo, en este caso una implementación o desarrollo de un sistema informático.

- BAI02 Gestionar la definición de requisitos: Cuando se trabaja un proyecto de un sistema de información es de vital importancia escuchar y tomar nota de todas las necesidades que deberá satisfacer la herramienta, por lo que la captura de los requisitos debe realizarse de forma integral.

- BAI03 Gestionar la identificación y la construcción de soluciones: Al tener lista toda la información sobre las necesidades a satisfacer por parte de un sistema de información se debe pasar a la etapa de desarrollo de software, manteniendo bajo control los objetivos y los tiempos ya planificados, para entregar oportunamente la herramienta ofrecida.

- BAI04 Gestionar la disponibilidad y la capacidad: Una vez esté terminado el desarrollo del software, se debe pasar a la etapa de adiestramiento para usuarios finales, para que puedan posteriormente certificar que la herramienta si cumple con los requisitos planteados.

- BAI05 Gestionar la introducción de cambios organizativos: Si una necesidad de software será satisfecha por medio de un proveedor y no desarrollada en la empresa, se deberá realizar el análisis pertinente del tercero que podrá cumplir con las necesidades planteadas.

- BAI06 Gestionar los cambios: En el uso de software se cuenta con diferentes entornos de trabajo, un ambiente donde se desarrollan las aplicaciones, otro donde se realizan pruebas y el último y más importante es el ambiente de producción. Cada vez que exista un cambio o mejora de algún software que ya está en uso, debe seguirse una rigurosa revisión antes de modificar en el ambiente de producción, ya que si algo no está correcto podría causar pérdidas de información.

- BAI07 Gestionar la aceptación del cambio y de la transacción: La tarea más compleja al implementar un nuevo software es la aceptación que tendrán los usuarios finales, es por ello que este último proceso evalúa cómo se gestiona este cambio ante los usuarios.

4.3.3.1. Modelo de capacidad de los procesos

Este modelo se utiliza para medir la madurez actual o el estado en que se encuentran los procesos relacionados con las TI de la empresa, determinar la brecha entre ellos y la forma de mejorarlos.

Existen seis niveles de capacidad que se pueden alcanzar por un proceso.

0 – Proceso incompleto:

El proceso no está implementado o no alcanza su propósito. A este nivel, hay muy poca o ninguna evidencia de ningún logro sistemático del propósito del proceso.

1 – Proceso ejecutado:

El proceso implementado alcanza su propósito.

2 – Proceso gestionado:

El proceso ejecutado descrito anteriormente está ya implementado de forma gestionada (planificado, supervisado y ajustado) y los resultados de su ejecución están establecidos, controlados y mantenidos apropiadamente.

3 – Proceso establecido:

El proceso gestionado descrito anteriormente está ahora implementado usando un proceso definido que es capaz de alcanzar sus resultados de proceso.

4 – Proceso predecible:

El proceso establecido descrito anteriormente ahora se ejecuta dentro de límites definidos para alcanzar sus resultados de proceso.

5 – Proceso optimizado:

El proceso predecible descrito anteriormente es mejorado de forma continua para cumplir con las metas empresariales presentes y futuras.

4.3.3.2. Método de determinación del nivel de capacidad

El método de determinación de la capacidad por proceso en la que se encuentra la empresa es asignando un valor nominal, iniciando en incompleto (0) hasta optimizado (5).

Los resultados del modelo de capacidad son obtenidos con base a COBIT 5. El auditado deberá analizar y manifestar el nivel de alcance con cada declaración dentro de cuatro posibles respuestas que a su vez representan valores:

- No alcanzado = 0
- Parcialmente Alcanzado = 0.33
- Ampliamente Alcanzado = 0.66
- Completamente Alcanzado = 1.00

Para obtener valores sobre cada una de las respuestas a las declaraciones de COBIT, se necesita multiplicar "peso (NV)" y "respuesta (valor de cumplimiento)", a través de la siguiente formula:

$$V = P * R$$

Donde V es el valor de puntuación de la declaración de capacidad, P es el peso de cada declaración de capacidad, el cual se obtiene al sumar los valores de cada nivel y luego dividirlos dentro del peso total para cada nivel.

$$C = \Sigma(V) / \Sigma(P)$$

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

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

$$N = C / \Sigma C$$

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

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

$$Co = Nv \times N$$

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

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

$$NM = \Sigma Co$$

Donde NM es el nivel de capacidad y Co es la contribución para cada declaración del nivel de capacidad.

CAPÍTULO V

PROPUESTA DE IMPLEMENTACIÓN Y ADOPCIÓN DEL MODELO DE OBJETIVOS DE CONTROL PARA TECNOLOGÍA DE INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS (COBIT), EN UNA EMPRESA ASEGURADORA, POR PARTE DE LA AUDITORÍA INTERNA, PARA LA EVALUACIÓN DE CONTROLES DE ADQUISICIÓN Y MANTENIMIENTO DE APLICACIONES INFORMÁTICAS.

Los sistemas de información cada día toman más relevancia en la toma de decisiones de la empresa, por lo que los controles de estos, deben ser especializados y poder cubrir de una forma integral los procesos que conforman a la empresa. Para esto se desarrollara la evaluación utilizando el modelo objetivos de control para tecnología de información y tecnologías relacionadas (COBIT siglas en ingles), esta es una herramienta desarrollada por el Instituto de auditoría y control de sistemas de información (ISACA siglas en ingles).

El procedimiento para realizar la auditoria al departamento de informática de acuerdo al marco de trabajo es el siguiente:

1) Se presentarán una serie de cuestionarios a las diferentes funciones (puestos) que conformen el área de tecnología y que apliquen al dominio evaluado, son 7 procesos en total (ver página 61).

2) Cada pregunta tiene un peso, se puede identificar como “NV” en el cuestionario, este peso es una ponderación sobre el total y solo podrá estar en el rango de 0 a 5 (ver página 63). Este peso también nos sirve como agrupador de las afirmaciones o cuestionamientos, ya que posteriormente deberán sumarse.

3) Cada pregunta tiene 4 posibles respuestas siendo estas 0, 0.33, 0.66 y 1 (ver página 64). El valor de la respuesta será escogido por la persona que este llenando el cuestionario.

4) Cuando estén contestados todos los cuestionamientos, se debe de totalizar la columna de “valor de cumplimiento según respuesta”.

5) Estos totales deberán computarse por cada función (puesto). Se deben trasladar las sumas agrupadas por peso de cada grupo de preguntas, es decir las preguntas cuyo peso sea 0 se suma sus respuestas, de las que el peso sea 1 se suman entre ellas y así sucesivamente. También debe realizarse un conteo de enunciados agrupados por el mismo valor de peso. El resultado de la suma y del conteo se muestran en la siguiente imagen, siendo la columna (A) los niveles o agrupadores, la columna (B) la suma de las respuestas y/o valores de cumplimiento y la columna (C) el conteo de las respuestas y/o valores.

   La columna (D) “VALOR DE CUMPLIMIENTO” es la división de la columna B dentro de la columna C.

La columna (E) “NORMALIZACION DEL VECTOR DE CUMPLIMIENTO” es la división de la celda de la columna (D) que estemos trabajando en ese momento, dentro de la sumatoria de la columna (D).

Ejemplos:
Para la fila con nivel 0 sería: **0.00 / 2.90 = 0**
Para la fila con nivel 1 sería: **0.553 / 2.90 = 0.191**

La columna (F) “NIVEL DE CAPACIDAD” se obtiene de la multiplicación de la columna (A) por la columna (E).

El Total se obtiene de la sumatoria vertical de cada columna

El valor de prueba se obtiene de la división del Total de la columna (E) dentro de la constante 5. Se utiliza esta constante ya que 5 es el valor máximo que puede obtener cada proceso, es decir es nuestro 100%.

Ejemplo:
Para el total 3.236 de la columna (E): **3.236 / 5 = 0.671**

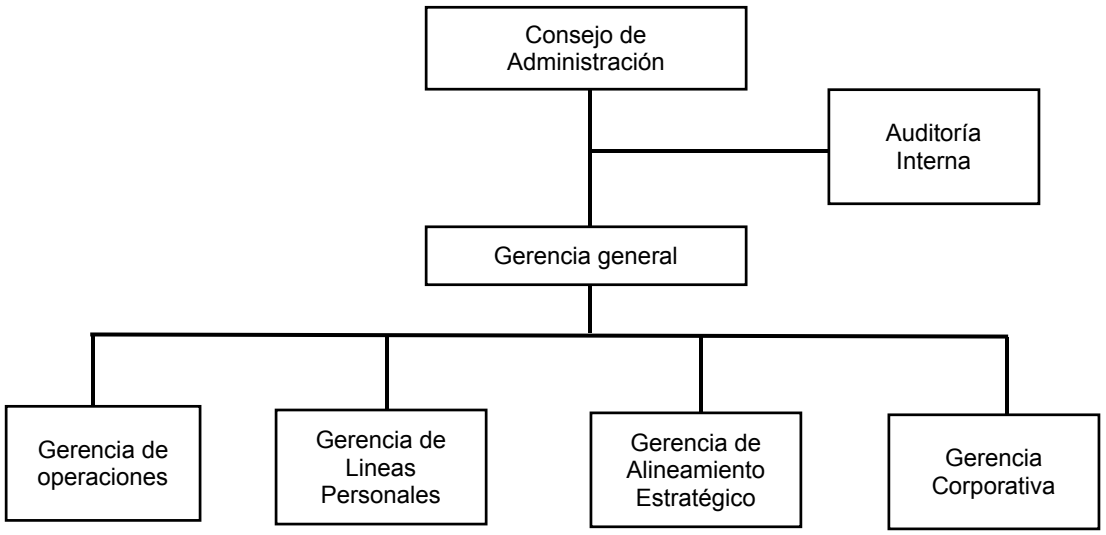
De esta forma se obtiene el nivel de cada función (puesto). Por último para obtener el nivel del proceso en general, se realiza la suma de la columna (B) de los diferentes puestos, agrupándolas como siempre por los niveles de 0 a 5 y la operación entre columnas (D), (E) y (F) es la misma.

6) Las respuestas para cada proceso cuando se indica el nivel de confianza se refiere al valor en que se encuentra de un 100%.

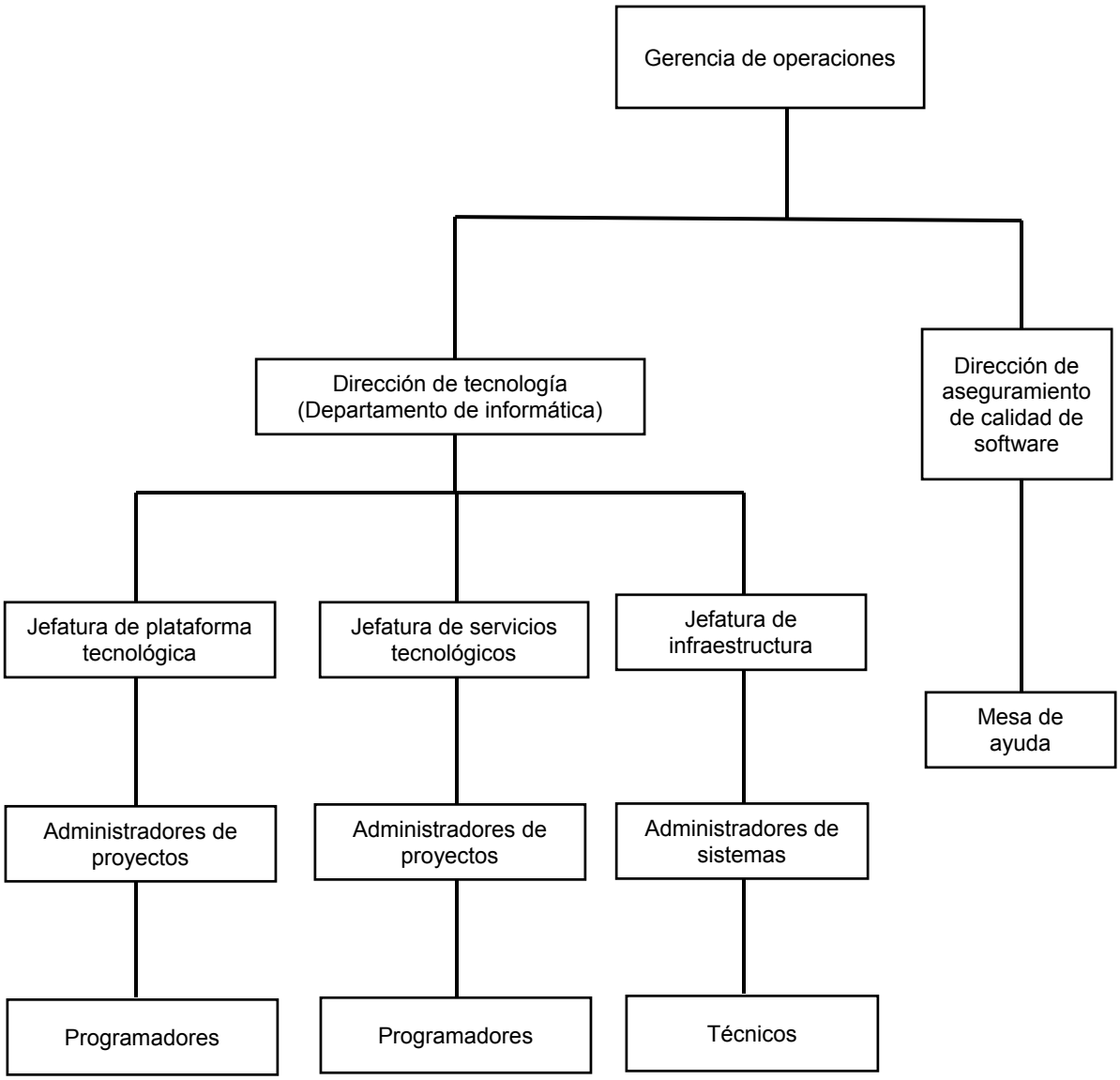
5.1 Unidad de análisis

La evaluación se realizó a la empresa El Mejor Seguro S.A. que inició sus operaciones en el año de 1960, ubicada en la zona 4 de la ciudad capital de Guatemala, siendo la empresa aseguradora más grande de Centroamérica según la Asociación Guatemalteca de Industria del Seguro (AGIS), cuenta con más de 350 mil clientes, una certificación en calidad ISO 9001 y una amplia gama de servicios electrónicos para sus intermediarios y clientes finales.

La empresa en su más alto nivel está organizada de la siguiente manera:



El departamento de informática se conforma de la siguiente manera:



5.2. Contenido del caso práctico

5.2.1. Papeles de trabajo del caso práctico

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM01 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	05/01/2015
FECHA FIN:	05/01/2015

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

Sr. Erick Gonzalez
Asistente de Auditoría
Auditoria Interna
Presente

Estimado Sr. Gonzalez

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

Los procesos a evaluar de acuerdo a la metodología se describen a continuación:

- BAI01 – Gestionar los programas y proyectos
- BAI02 – Gestionar la definición de requisitos

Papel de Trabajo	MM01 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	05/01/2015
FECHA FIN:	05/01/2015

- BAI03 – Adquirir e Implementar infraestructura tecnológica
- BAI04 – Facilitar la ejecución y el uso
- BAI05 – Gestionar la Introducción de cambios organizativos
- BAI06 – Administración de cambios
- BAI07 – Gestionar la aceptación del cambio y de la transición

El tiempo asignado para esta actividad es de 15 días, iniciando el 12 de enero del presente año.

Atentamente,

Lic. Luis Maldonado
Auditor Interno

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM02 1/1
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	05/01/2015
FECHA FIN:	05/01/2015

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

Ing. Mario Reyes
Director del departamento de informática
Presente

Respetable Ingeniero Reyes

Por este medio se le comunica que conforme a nuestro plan de trabajo, se iniciará la revisión del control interno sobre los procesos de adquisición e implementación de soluciones informáticas que se realizó en la dirección a su cargo durante el segundo semestre del año 2014. La actividad ha sido asignada al Sr. Erick Gonzalez, asistente de auditoría interna y supervisada por su servidor.

Al final de la evaluación se determinará el nivel de capacidad con que cuentan los controles actuales aplicando la metodología según COBIT, y se le estarán enviando los resultados detallando los hallazgos y recomendaciones.

Atentamente,

Lic. Luis Maldonado
Auditor Interno

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM03 1/6
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	06/01/2015
FECHA FIN:	09/01/2015

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

I. INTRODUCCIÓN

Para poder lograr que los objetivos de la dirección de tecnología estén alineados con los de la empresa, es necesario que las soluciones informáticas, desarrolladas o adquiridas, y en ambos casos implementadas e integradas al proceso de negocio, puedan ser controladas adecuadamente garantizando así la satisfacción del negocio.

II. OBJETIVO

Evaluar el nivel de capacidad de los controles informáticos en la administración de los procesos de adquisición e implementación de soluciones informáticas establecida por la dirección de informática de la empresa El Mejor Seguro S.A.

III. ALCANCE

La auditoría deberá dar una opinión soportada en el nivel de capacidad de la administración de controles informáticos para los procesos incluidos en el dominio COBIT de Adquisición e Implementación (AI), mediante las siguientes técnicas de evaluación:

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

IV. PROCEDIMIENTO

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

EVALUACION DEL CONTROL INTERNO INFORMÁTICO

Se aplicaran cuestionarios elaborados con base a las declaraciones de los niveles de capacidad de COBIT, así como también se revisará la documentación necesaria para determinar el nivel de capacidad de cada proceso.

Los procesos y actividades a evaluar son los siguientes:

Papel de Trabajo	MM03 3/6
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	06/01/2015
FECHA FIN:	09/01/2015

Procesos y actividades a evaluar:

Proceso		**Actividades**
(BAI01)	**Gestionar los programas y proyectos**	Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio.
		Reporte de análisis de riesgos.
		Estudio de factibilidad y formulación de cursos alternativos de acción.
		Requerimientos, decisión de factibilidad y aprobación.
(BAI02)	**Gestionar la definición de requisitos**	Diseño de alto nivel.
		Diseño detallado.
		Control y auditabilidad de aplicaciones.
		Seguridad y disponibilidad de aplicaciones.
		Configuración e implantación de software aplicativo adquirido.
		Actualizaciones importantes en sistemas existentes.
		Desarrollo de software aplicativo.
		Administración de los requerimientos de aplicaciones.
		Mantenimiento de software aplicativo.
(BAI03)	**Gestionar la identificación y la construcción de soluciones**	Plan de adquisición de infraestructura tecnológica.
		Protección y disponibilidad del recurso de infraestructura.
		Mantenimiento de infraestructura.
		Ambiente de prueba de factibilidad.
(BAI04)	**Gestionar la disponibilidad y la capacidad**	Plan para soluciones de operación.
		Transferencia de conocimiento a la gerencia del negocio.
		Transferencia de conocimiento a los usuarios finales.
		Transferencia de conocimiento al personal de operaciones y soporte.

Papel de Trabajo	MM03 4/6
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	06/01/2015
FECHA FIN:	09/01/2015

Proceso		Actividades
(BAI05)	**Gestionar la introducción de cambios organizativos**	Control de adquisición.
		Administración de contratos con proveedores.
		Selección de proveedores.
		Adquisición de software.
		Adquisición de recursos de desarrollo
		Adquisición de infraestructura, instalaciones y servicios relacionados.
(BAI06)	**Gestionar los cambios**	Estándares y procedimientos para cambios.
		Evaluación de impacto, priorización y autorización.
		Cambios de emergencia.
		Seguimiento y reporte del estatus de cambio.
		Cierre y documentación del cambio.
(BAI07)	**Gestionar la aceptación del cambio y de la transición**	Entrenamiento.
		Plan de prueba.
		Plan de implantación.
		Ambiente de prueba.
		Conversión de sistema y datos.
		Prueba de cambios.
		Prueba final y aceptación.
		Transferencia a producción.
		Liberación de software.
		Distribución del sistema.
		Registro y rastreo de cambios.
		Revisión posterior a la implantación

Papel de Trabajo	MM04 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

Evaluación del proceso de gestionar los programas y proyectos (BAI01)

Cuadro para tabulación de resultados de los cuestionarios aplicado s a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI01 Gestionar los programas y proyectos					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Dirección de tecnología					
(A) NIVEL DE CAPACIDAD	(B) SUMA DE VALORES DE CUMPLIMIENTO	(C) NUMERO DE DECLARACIONES	(D) VALOR DE CUMPLIMIENTO (B/C)	(E) NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	(F) NIVEL DE CAPACIDAD (A * E)
0	0.00	2	0.000	0.000	0.000
1	1.66	3	0.553	0.191	0.191
2	0.33	4	0.083	0.028	0.057
3	4.00	4	1.000	0.345	1.034
4	3.96	6	0.660	0.227	0.910
5	3.64	6	0.607	0.209	1.045
TOTAL	**13.59 * (1)**	**25.00**	**2.90**	**1.000**	**3.236**
PRUEBA					**64.71%**
					NIVEL ACTUAL
FUNCIÓN: Jefatura de servicios tecnológicos					
0	0.00	2	0.000	0.000	0.000
1	1.33	3	0.443	0.162	0.162
2	0.33	4	0.083	0.030	0.060
3	4.00	4	1.000	0.365	1.095
4	4.30	6	0.717	0.262	1.047
5	2.98	6	0.497	0.181	0.907
TOTAL	**12.94 * (2)**	**25.00**	**2.74**	**1.000**	**3.270**
PRUEBA					**65.41%**
					NIVEL ACTUAL
Función: Jefatura de plataforma tecnológica					
0	0.00	2	0.000	0.000	0.000
1	1.00	3	0.333	0.128	0.128
2	0.00	4	0.000	0.000	0.000

Papel de Trabajo	MM04 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

PROCESO: BAI01 Gestionar los programas y proyectos					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Jefatura de plataforma tecnológica					
(A) NIVEL DE CAPACIDAD	(B) SUMA DE VALORES DE CUMPLIMIENTO	(C) NUMERO DE DECLARACIONES	(D) VALOR DE CUMPLIMIENTO (B/C)	(E) NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	(F) NIVEL DE CAPACIDAD (A * E)
3	4.00	4	1.000	0.384	1.152
4	4.64	6	0.773	0.297	1.188
5	2.98	6	0.497	0.191	0.954
TOTAL	**12.62 *(3)**	**25.00**	**2.60**	**1.000**	**3.423**
PRUEBA	12.62	25.00			**68.45%**
					NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.00	2	0.000	0.000	0.000
1	3.99	3	1.330	0.161	0.161
2	0.66	4	0.165	0.020	0.040
3	12.00	4	3.000	0.364	1.092
4	12.90	6	2.150	0.261	1.043
5	9.60	6	1.600	0.194	0.970
TOTAL	**39.15 *(4)**	**25.00**	**8.25**	**1.000**	**3.306**
PRUEBA	39.15	25.00			**66.12%**
					NIVEL ACTUAL

CONCLUSIÓN:

Se determinó que en el proceso de gestionar los programas y proyectos (BAI01) se administran los controles sobre de forma “establecida”, es decir el proceso ya está formalizado, mostrando un nivel 3.306 de capacidad y un 66.12% de confiabilidad en los objetivos de control informático.

REFERENCIAS:

*(1) viene de MM04-01 1/3

*(2) viene de MM04-02 1/3

*(3) viene de MM04-03 1/3

*(4) Sumatoria de *(1) + *(2) + *(3)

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM04-01 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

PROCESO: BAI01 I Gestionar los programas y proyectos			¿Qué tanto se ha alcanzado?				
Función: Dirección del departamento			Fecha: 12/01/2015				
NV	No.	DECLARACION	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	La organización no requiere la identificación de requerimientos funcionales y operativos para el desarrollo, implementación o modificación de soluciones, como por ejemplo soluciones de sistema, de servicio, de infraestructura, de software y de datos.	X				0.00
0	2	La organización no mantiene una conciencia sobre las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	X				0.00
1	3	Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas.				X	1.00
1	4	Los grupos individuales tienden a reunirse para discutir necesidades de manera informal y los requerimientos por lo general no están documentados.		X			0.33
1	5	Las soluciones son identificadas por persona basadas en una conciencia limitada del mercado, o en respuesta a ofertas de proveedores. Hay poco o ningún análisis estructurado o investigación acerca de la tecnología disponible.		X			0.33
2	6	Hay algunos enfoques intuitivos para identificar las soluciones de TI y los mismos varían en todo el negocio.		X			0.33
2	7	Las soluciones son identificadas de manera informal sobre la base de la experiencia interna y de los conocimientos de la función de TI. El éxito de cada proyecto depende de la experiencia de unas pocas personas claves de TI.	X				0.00
2	8	La calidad de la documentación y de la toma de decisiones varía considerablemente.	X				0.00
2	9	Se emplean enfoques sin estructura para definir los requerimientos e identificar las soluciones de tecnología.	X				0.00
3	10	Se usan métodos claros y estructurados para determinar las soluciones de TI.				X	1.00
3	11	El método para la determinación de soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del usuario o del negocio, las oportunidades tecnológicas, la factibilidad económica, los análisis de riesgos y otros factores.				X	1.00

Papel de Trabajo	MM04-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	12	El proceso para la determinación de soluciones de TI se aplica a algunos proyectos basándose en factores como las decisiones hechas por el personal involucrado, la cantidad de tiempo de administración dedicado y el tamaño y la prioridad del requerimiento original del negocio.				X	1.00
3	13	Se emplea métodos estructurados para definir los requerimientos e identificar las soluciones de TI.				X	1.00
4	14	Existe una metodología establecida para la identificación y evaluación de soluciones de TI y la misma se emplea para la mayoría de proyectos.			X		0.66
4	15	La documentación de proyectos es de buena calidad y cada etapa es debidamente aprobada.			X		0.66
4	16	Los requerimientos son bien articulados y están en conformidad con estructuras predefinidas.			X		0.66
4	17	Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias.			X		0.66
4	18	La metodología es clara, definida, generalmente comprendida y medible.			X		0.66
4	19	Hay una interfaz claramente definida entre la gerencia de TI y de negocios respecto a la identificación y evaluación de soluciones de TI.			X		0.66
5	20	La metodología para la identificación y evaluación de soluciones de Ti se mejora continuamente.			X		0.66
5	21	La metodología de adquisición e implementación es lo suficientemente flexible para acomodar proyectos de pequeña y gran escala.			X		0.66
5	22	La metodología es apoyada por bases de datos de conocimientos internas y externas que contienen materiales de referencia sobre soluciones tecnológicas.		X			0.33
5	23	La metodología misma produce documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.		X			0.33
5	24	La organización puede a menudo identificar nuevas oportunidades para utilizar la tecnología para ganar ventaja competitiva, influir en el proceso de reingeniería del negocio y mejorar la eficiencia general.				X	1.00
5	25	La gerencia detecta y actúa en consecuencia si las soluciones de TI son aprobadas sin considerar tecnologías alternativas o requerimientos funcionales de negocio.			X		0.66
			TOTAL DEL NIVEL				**13.59**

Papel de Trabajo	MM04-01 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

CONCLUSIÓN:

Para la función de Dirección del departamento en el proceso BAI01 gestionar los programas y proyectos, se determinó que el valor de cumplimiento es de 13.59 puntos de 25 como máximo.

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM04-02 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

PROCESO: BAI01 Gestionar los programas y proyectos			¿Qué tanto se ha alcanzado?				
FUNCIÓN: Jefatura de servicios tecnológicos			Fecha: 12/01/2015				
NV	No.	DECLARACION	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	La organización no requiere la identificación de requerimientos funcionales y operativos para el desarrollo, implementación o modificación de soluciones, como por ejemplo soluciones de sistema, de servicio, de infraestructura, de software y de datos.	X				0.00
0	2	La organización no mantiene una conciencia sobre las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	X				0.00
1	3	Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas.				X	1.00
1	4	Los grupos individuales tienden a reunirse para discutir necesidades de manera informal y los requerimientos por lo general no están documentados.	X				0.00
1	5	Las soluciones son identificadas por persona basadas en una conciencia limitada del mercado, o en respuesta a ofertas de proveedores. Hay poco o ningún análisis estructurado o investigación acerca de la tecnología disponible.		X			0.33
2	6	Hay algunos enfoques intuitivos para identificar las soluciones de TI y los mismos varían en todo el negocio.		X			0.33
2	7	Las soluciones son identificadas de manera informal sobre la base de la experiencia interna y de los conocimientos de la función de TI. El éxito de cada proyecto depende de la experiencia de unas pocas personas claves de TI.	X				0.00
2	8	La calidad de la documentación y de la toma de decisiones varía considerablemente.	X				0.00
2	9	Se emplean enfoques sin estructura para definir los requerimientos e identificar las soluciones de tecnología.	X				0.00
3	10	Se usan métodos claros y estructurados para determinar las soluciones de TI.				X	1.00
3	11	El método para la determinación de soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del usuario o del negocio, las oportunidades tecnológicas, la factibilidad económica, los análisis de riesgos y otros factores.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM04-02 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

FUNCIÓN: Jefatura de servicios tecnológicos			**Fecha: 12/01/2015**				
NV	**No.**	**DECLARACIÓN**	**No alcanzado**	**Parcialmente**	**Ampliamente**	**Completamente**	**Valor de cumplimiento según respuesta**
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	12	El proceso para la determinación de soluciones de TI se aplica a algunos proyectos basándose en factores como las decisiones hechas por el personal involucrado, la cantidad de tiempo de administración dedicado y el tamaño y la prioridad del requerimiento original del negocio.				X	1.00
3	13	Se emplea métodos estructurados para definir los requerimientos e identificar las soluciones de TI.				X	1.00
4	14	Existe una metodología establecida para la identificación y evaluación de soluciones de TI y la misma se emplea para la mayoría de proyectos.			X		0.66
4	15	La documentación de proyectos es de buena calidad y cada etapa es debidamente aprobada.			X		0.66
4	16	Los requerimientos son bien articulados y están en conformidad con estructuras predefinidas.			X		0.66
4	17	Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias.			X		0.66
4	18	La metodología es clara, definida, generalmente comprendida y medible.				X	1.00
4	19	Hay una interfaz claramente definida entre la gerencia de TI y de negocios respecto a la identificación y evaluación de soluciones de TI.			X		0.66
5	20	La metodología para la identificación y evaluación de soluciones de Ti se mejora continuamente.			X		0.66
5	21	La metodología de adquisición e implementación es lo suficientemente flexible para acomodar proyectos de pequeña y gran escala.			X		0.66
5	22	La metodología es apoyada por bases de datos de conocimientos internas y externas que contienen materiales de referencia sobre soluciones tecnológicas.	X				0.00
5	23	La metodología misma produce documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.		X			0.33
5	24	La organización puede a menudo identificar nuevas oportunidades para utilizar la tecnología para ganar ventaja competitiva, influir en el proceso de reingeniería del negocio y mejorar la eficiencia general.				X	1.00
5	25	La gerencia detecta y actúa en consecuencia si las soluciones de TI son aprobadas sin considerar tecnologías alternativas o requerimientos funcionales de negocio.		X			0.33
			TOTAL DEL NIVEL				**12.94**

Papel de Trabajo	MM04-02 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

CONCLUSIÓN:

Para la función de jefatura de servicios tecnológicos en el proceso BAI01 gestionar los programas y proyectos, se determinó que el valor de cumplimiento es de 12.94 puntos de 25 posibles como máximo.

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM04-03 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

PROCESO: BAI01 Gestionar los programas y proyectos			¿Qué tanto se ha alcanzado?				
Función: Jefatura de plataforma tecnológica			**Fecha: 12/01/2015**				
NV	**No.**	**DECLARACION**	**No alcanzado**	**Parcialmente**	**Ampliamente**	**Completamente**	**Valor de cumplimiento según respuesta**
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
0	1	La organización no requiere la identificación de requerimientos funcionales y operativos para el desarrollo, implementación o modificación de soluciones, como por ejemplo soluciones de sistema, de servicio, de infraestructura, de software y de datos.	X				0.00
0	2	La organización no mantiene una conciencia sobre las soluciones tecnológicas disponibles que son potencialmente relevantes para su negocio.	X				0.00
1	3	Hay conciencia de la necesidad de definir requerimientos y de identificar soluciones tecnológicas.				X	1.00
1	4	Los grupos individuales tienden a reunirse para discutir necesidades de manera informal y los requerimientos por lo general no están documentados.	X				0.00
1	5	Las soluciones son identificadas por persona basadas en una conciencia limitada del mercado, o en respuesta a ofertas de proveedores. Hay poco o ningún análisis estructurado o investigación acerca de la tecnología disponible.	X				0.00
2	6	Hay algunos enfoques intuitivos para identificar las soluciones de TI y los mismos varían en todo el negocio.	X				0.00
2	7	Las soluciones son identificadas de manera informal sobre la base de la experiencia interna y de los conocimientos de la función de TI. El éxito de cada proyecto depende de la experiencia de unas pocas personas claves de TI.	X				0.00
2	8	La calidad de la documentación y de la toma de decisiones varía considerablemente.	X				0.00
2	9	Se emplean enfoques sin estructura para definir los requerimientos e identificar las soluciones de tecnología.	X				0.00
3	10	Se usan métodos claros y estructurados para determinar las soluciones de TI.				X	1.00
3	11	El método para la determinación de soluciones de TI requiere la consideración de alternativas evaluadas contra los requerimientos del usuario o del negocio, las oportunidades tecnológicas, la factibilidad económica, los análisis de riesgos y otros factores.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM04-03 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

NV	No.	DECLARACION	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	12	El proceso para la determinación de soluciones de TI se aplica a algunos proyectos basándose en factores como las decisiones hechas por el personal involucrado, la cantidad de tiempo de administración dedicado y el tamaño y la prioridad del requerimiento original del negocio.				X	1.00
3	13	Se emplea métodos estructurados para definir los requerimientos e identificar las soluciones de TI.				X	1.00
4	14	Existe una metodología establecida para la identificación y evaluación de soluciones de TI y la misma se emplea para la mayoría de proyectos.				X	1.00
4	15	La documentación de proyectos es de buena calidad y cada etapa es debidamente aprobada.			X		0.66
4	16	Los requerimientos son bien articulados y están en conformidad con estructuras predefinidas.			X		0.66
4	17	Se consideran soluciones alternativas, incluyendo un análisis de costos y ganancias.			X		0.66
4	18	La metodología es clara, definida, generalmente comprendida y medible.				X	1.00
4	19	Hay una interfaz claramente definida entre la gerencia de TI y de negocios respecto a la identificación y evaluación de soluciones de TI.			X		0.66
5	20	La metodología para la identificación y evaluación de soluciones de Ti se mejora continuamente.			X		0.66
5	21	La metodología de adquisición e implementación es lo suficientemente flexible para acomodar proyectos de pequeña y gran escala.			X		0.66
5	22	La metodología es apoyada por bases de datos de conocimientos internas y externas que contienen materiales de referencia sobre soluciones tecnológicas.	X				0.00
5	23	La metodología misma produce documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.		X			0.33
5	24	La organización puede a menudo identificar nuevas oportunidades para utilizar la tecnología para ganar ventaja competitiva, influir en el proceso de reingeniería del negocio y mejorar la eficiencia general.				X	1.00
5	25	La gerencia detecta y actúa en consecuencia si las soluciones de TI son aprobadas sin considerar tecnologías alternativas o requerimientos funcionales de negocio.		X			0.33
			TOTAL DEL NIVEL				**12.62**

Papel de Trabajo	MM04-03 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	12/01/2015
FECHA FIN:	12/01/2015

CONCLUSIÓN:

Para la función de jefatura de plataforma tecnológica en el proceso BAI01 gestionar los programas y proyectos, se determinó que el valor de cumplimiento es de 12.62 puntos de 25 como máximo.

Papel de Trabajo	MM05 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

Evaluación del proceso de gestionar la definición de requisitos (BAI02)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI02 Gestionar la definición de requisitos					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Dirección de tecnología					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE CAPACIDAD	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	NIVEL DE CAPACIDAD (A * E)
0	0.00	2	0.000	0.000	0.000
1	1.66	4	0.415	0.117	0.117
2	1.33	4	0.333	0.094	0.187
3	4.00	5	0.800	0.226	0.677
4	3.00	3	1.000	0.282	1.128
5	5.00	5	1.000	0.282	1.409
TOTAL	**14.99 *(1)**	**23.00**	**3.55**	**1.000**	**3.518**
PRUEBA					**70.36%**
					NIVEL ACTUAL
FUNCIÓN: Jefatura de servicios tecnológicos					
0	0.00	2	0.000	0.000	0.000
1	0.99	4	0.248	0.075	0.075
2	1.00	4	0.250	0.076	0.152
3	4.00	5	0.800	0.243	0.728
4	3.00	3	1.000	0.303	1.213
5	5.00	5	1.000	0.303	1.516
TOTAL	**13.99 *(2)**	**23.00**	**3.30**	**1.000**	**3.684**
PRUEBA					**73.68%**

Papel de Trabajo	MM05 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

PROCESO: BAI02 Gestionar la definición de requisitos					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Jefatura de plataforma tecnológica					
0	0.00	2	0.000	0.000	0.000
1	0.99	4	0.248	0.079	0.079
2	1.00	4	0.250	0.080	0.160
3	4.00	5	0.800	0.257	0.770
4	2.66	3	0.887	0.285	1.138
5	4.66	5	0.932	0.299	1.495
TOTAL	**13.31 *(3)**	**23.00**	**3.12**	**1.000**	**3.644**
PRUEBA					**72.87%**
					NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.00	2	0.000	0.000	0.000
1	3.64	4	0.910	0.091	0.091
2	3.33	4	0.833	0.084	0.167
3	12.00	5	2.400	0.241	0.723
4	8.66	3	2.887	0.290	1.159
5	14.66	5	2.932	0.294	1.472
TOTAL	**42.29 *(4)**	**23.00**	**9.96**	**1.000**	**3.612**
PRUEBA					**72.24%**
					NIVEL ACTUAL

CONCLUSIÓN:

Se determinó que en el proceso de gestionar los requisitos (BAI02) se administran los controles de forma "predecible", es decir que además de funcionar formalmente ya se obtienen resultados satisfactorios, mostrando un nivel 3.612 de capacidad y un 72.24% de confiabilidad en los objetivos de control.

REFERENCIAS:

*(1) viene de MM05-01 1/2

*(2) viene de MM05-02 1/2

*(3) viene de MM05-03 1/2

*(4) Sumatoria de *(1) + *(2) + *(3)

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM05-01 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

PROCESO: BAI02 Gestionar la definición de requisitos			¿Qué tanto se ha alcanzado?				
Función: Dirección del departamento			**Fecha: 13/01/2015**				
NV	**No.**	**DECLARACIÓN**	**No alcanzado**	**Parcialmente**	**Ampliamente**	**Completamente**	**Valor de cumplimiento según respuesta**
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
0	1	No existe un diseño y especificación de aplicaciones.	X				0.00
0	2	Generalmente las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales	X				0.00
1	3	Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones.				X	1.00
1	4	Los enfoques para adquisición y mantenimiento de software aplicativo varían de un proyecto a otro.			X		0.66
1	5	Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte.	X				0.00
1	6	Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño y adquisición de software aplicativo.	X				0.00
2	7	Hay procesos diferentes pero similares para adquirir y mantener aplicaciones basados en la experiencia dentro de la función y soporte TI.	X				0.00
2	8	La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y de los niveles de experiencia de la TI.				X	1.00
2	9	El mantenimiento es usualmente problemático y sufre cuando se perdieron conocimientos internos de la organización.		X			0.33
2	10	Al diseñar o adquirir el software de aplicación se presta poca o ninguna consideración a la seguridad y disponibilidad de la aplicación.	X				0.00
3	11	Hay un proceso claro, definido y generalmente comprendido para la adquisición e implementación de software de aplicación.				X	1.00
3	12	Este proceso está en concordancia con la estrategia de TI y la del negocio.				X	1.00
3	13	Se intentan aplicar coherentemente los procesos documentados en todos los proyectos y aplicaciones diferentes.				X	1.00
3	14	Las metodologías son generalmente inflexibles y difíciles de aplicar a todos los casos, de modo que los pasos son frecuentemente omitidos.	X				0.00
3	15	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM05-01 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	16	Hay una metodología formal, clara y bien atendida que incluye un proceso de diseño y especificación, criterios para la adquisición de software de aplicación, un proceso para realizar pruebas y requerimientos para la documentación.				X	1.00
4	17	Existen mecanismos de aprobación documentados y acordados para asegurar que se sigan todos los pasos y que se autoricen las excepciones.				X	1.00
4	18	Las prácticas y procedimientos evolucionaron y se adecuan a la organización, son usados por todo el personal, y se aplican a la mayoría de los requerimientos de aplicación.				X	1.00
5	19	Las prácticas de adquisición y mantenimiento de software de aplicación están alineadas con los procesos definidos.				X	1.00
5	20	El método está basado en componentes, con aplicaciones predefinidas y estandarizadas adaptadas a las necesidades del negocio. Este método se aplica a nivel de toda la organización.				X	1.00
5	21	La metodología de adquisición y mantenimiento es avanzada, posibilita una rápida implementación y permite una alta capacidad de respuesta y flexibilidad.				X	1.00
5	22	La metodología de adquisición e implementación de software de aplicación está sujeta a una mejora continua y es respaldada por bases de datos de conocimientos internas y externas que contienen materiales de referencia y buenas prácticas.				X	1.00
5	23	La metodología genera documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.				X	1.00
			TOTAL DEL NIVEL				**14.99**

CONCLUSIÓN:

Para la función de dirección del departamento en el proceso BAI02 gestionar la definición de requisitos, se determinó que el valor de cumplimiento es de 14.99 puntos de 23 como máximo.

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM05-02 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

PROCESO: BAI02 Gestionar la definición de requisitos			¿Qué tanto se ha alcanzado?				
FUNCIÓN: Jefatura de servicios tecnológicos			Fecha: 13/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No existe un diseño y especificación de aplicaciones.	X				0.00
0	2	Generalmente las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales	X				0.00
1	3	Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones.			X		0.66
1	4	Los enfoques para adquisición y mantenimiento de software aplicativo varían de un proyecto a otro.		X			0.33
1	5	Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte.	X				0.00
1	6	Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño y adquisición de software aplicativo.	X				0.00
2	7	Hay procesos diferentes pero similares para adquirir y mantener aplicaciones basados en la experiencia dentro de la función y soporte TI.	X				0.00
2	8	La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y de los niveles de experiencia de la TI.				X	1.00
2	9	El mantenimiento es usualmente problemático y sufre cuando se perdieron conocimientos internos de la organización.	X				0.00
2	10	Al diseñar o adquirir el software de aplicación se presta poca o ninguna consideración a la seguridad y disponibilidad de la aplicación.	X				0.00
3	11	Hay un proceso claro, definido y generalmente comprendido para la adquisición e implementación de software de aplicación.				X	1.00
3	12	Este proceso está en concordancia con la estrategia de TI y la del negocio.				X	1.00
3	13	Se intentan aplicar coherentemente los procesos documentados en todos los proyectos y aplicaciones diferentes.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM05-02 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	14	Las metodologías son generalmente inflexibles y difíciles de aplicar a todos los casos, de modo que los pasos son frecuentemente omitidos.	X				0.00
3	15	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1.00
4	16	Hay una metodología formal, clara y bien atendida que incluye un proceso de diseño y especificación, criterios para la adquisición de software de aplicación, un proceso para realizar pruebas y requerimientos para la documentación.				X	1.00
4	17	Existen mecanismos de aprobación documentados y acordados para asegurar que se sigan todos los pasos y que se autoricen las excepciones.				X	1.00
4	18	Las prácticas y procedimientos evolucionaron y se adecuan a la organización, son usados por todo el personal, y se aplican a la mayoría de los requerimientos de aplicación.				X	1.00
5	19	Las prácticas de adquisición y mantenimiento de software de aplicación están alineadas con los procesos definidos.				X	1.00
5	20	El método está basado en componentes, con aplicaciones predefinidas y estandarizadas adaptadas a las necesidades del negocio. Este método se aplica a nivel de toda la organización.				X	1.00
5	21	La metodología de adquisición y mantenimiento es avanzada, posibilita una rápida implementación y permite una alta capacidad de respuesta y flexibilidad.				X	1.00
5	22	La metodología de adquisición e implementación de software de aplicación está sujeta a una mejora continua y es respaldada por bases de datos de conocimientos internas y externas que contienen materiales de referencia y buenas prácticas.				X	1.00
5	23	La metodología genera documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.				X	1.00
			TOTAL DEL NIVEL				**13.99**

CONCLUSIÓN:

Para la función de jefatura de servicios tecnológicos en el proceso BAI02 gestionar la definición de requisitos, se determinó que el valor de cumplimiento es de 13.99 puntos de 23 como máximo.

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM05-03 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

PROCESO: BAI02 Gestionar la definición de requisitos			¿Qué tanto se ha alcanzado?				
Función: Jefatura de plataforma tecnológica			Fecha: 13/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No existe un diseño y especificación de aplicaciones.	X				0.00
0	2	Generalmente las aplicaciones se obtienen con base en ofertas de proveedores, en el reconocimiento de la marca o en la familiaridad del personal de TI con productos específicos, considerando poco o nada los requerimientos actuales	X				0.00
1	3	Existe conciencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicaciones.			X		0.66
1	4	Los enfoques para adquisición y mantenimiento de software aplicativo varían de un proyecto a otro.		X			0.33
1	5	Es probable que se hayan adquirido en forma independiente una variedad de soluciones individuales para requerimientos particulares del negocio, teniendo como resultado ineficiencias en el mantenimiento y soporte.	X				0.00
1	6	Se tiene poca consideración hacia la seguridad y disponibilidad de la aplicación en el diseño y adquisición de software aplicativo.	X				0.00
2	7	Hay procesos diferentes pero similares para adquirir y mantener aplicaciones basados en la experiencia dentro de la función y soporte TI.	X				0.00
2	8	La tasa de éxito de las aplicaciones depende en gran medida de las habilidades internas y de los niveles de experiencia de la TI.				X	1.00
2	9	El mantenimiento es usualmente problemático y sufre cuando se perdieron conocimientos internos de la organización.	X				0.00
2	10	Al diseñar o adquirir el software de aplicación se presta poca o ninguna consideración a la seguridad y disponibilidad de la aplicación.	X				0.00
3	11	Hay un proceso claro, definido y generalmente comprendido para la adquisición e implementación de software de aplicación.				X	1.00
3	12	Este proceso está en concordancia con la estrategia de TI y la del negocio.				X	1.00
3	13	Se intentan aplicar coherentemente los procesos documentados en todos los proyectos y aplicaciones diferentes.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM05-03 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	13/01/2015
FECHA FIN:	13/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	14	Las metodologías son generalmente inflexibles y difíciles de aplicar a todos los casos, de modo que los pasos son frecuentemente omitidos.	X				0.00
3	15	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1.00
4	16	Hay una metodología formal, clara y bien atendida que incluye un proceso de diseño y especificación, criterios para la adquisición de software de aplicación, un proceso para realizar pruebas y requerimientos para la documentación.			X		0.66
4	17	Existen mecanismos de aprobación documentados y acordados para asegurar que se sigan todos los pasos y que se autoricen las excepciones.				X	1.00
4	18	Las prácticas y procedimientos evolucionaron y se adecuan a la organización, son usados por todo el personal, y se aplican a la mayoría de los requerimientos de aplicación.				X	1.00
5	19	Las prácticas de adquisición y mantenimiento de software de aplicación están alineadas con los procesos definidos.				X	1.00
5	20	El método está basado en componentes, con aplicaciones predefinidas y estandarizadas adaptadas a las necesidades del negocio. Este método se aplica a nivel de toda la organización.			X		0.66
5	21	La metodología de adquisición y mantenimiento es avanzada, posibilita una rápida implementación y permite una alta capacidad de respuesta y flexibilidad.				X	1.00
5	22	La metodología de adquisición e implementación de software de aplicación está sujeta a una mejora continua y es respaldada por bases de datos de conocimientos internas y externas que contienen materiales de referencia y buenas prácticas.				X	1.00
5	23	La metodología genera documentación con una estructura predefinida que hace muy eficientes la producción y el mantenimiento.				X	1.00
			TOTAL DEL NIVEL				**13.31**

CONCLUSIÓN:

Para la función de jefatura de plataforma tecnológica en el proceso BAI02 gestionar la definición de requisitos, se determinó que el valor de cumplimiento es de 13.31 puntos de 23 como máximo.

Papel de Trabajo	MM06 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	14/01/2015
FECHA FIN:	14/01/2015

Evaluación del proceso de adquirir e implementar infraestructura tecnológica (BAI03).

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI03 Adquirir e implementar infraestructura tecnológica					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Dirección de tecnología					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE CAPACIDAD	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	NIVEL DE CAPACIDAD (A * E)
0	0.00	1	0.000	0.000	0.000
1	0.33	3	0.110	0.032	0.032
2	1.99	5	0.398	0.116	0.231
3	4.00	4	1.000	0.291	0.872
4	4.00	4	1.000	0.291	1.163
5	4.66	5	0.932	0.271	1.355
TOTAL	**14.98 *(1)**	**22.00**	**3.44**	**1.000**	**3.653**
PRUEBA					**73.06%**
					NIVEL ACTUAL
FUNCIÓN: Jefatura de infraestructura					
0	0.00	1	0.000	0.000	0.000
1	0.33	3	0.110	0.031	0.031
2	2.33	5	0.466	0.130	0.261
3	4.00	4	1.000	0.280	0.839
4	4.00	4	1.000	0.280	1.119
5	5.00	5	1.000	0.280	1.398
TOTAL	**15.66 *(2)**	**22.00**	**3.58**	**1.000**	**3.647**
PRUEBA					**72.94%**
					NIVEL ACTUAL

Papel de Trabajo	MM06 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	14/01/2015
FECHA FIN:	14/01/2015

PROCESO: BAI03 Adquirir e implementar infraestructura tecnológica					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
FUNCIÓN: Consolidación de resultados					
0	0.00	1	0.000	0.000	0.000
1	0.66	3	0.220	0.031	0.031
2	4.32	5	0.864	0.123	0.246
3	8.00	4	2.000	0.285	0.855
4	8.00	4	2.000	0.285	1.140
5	9.66	5	1.932	0.275	1.377
TOTAL	**30.64 *(3)**	**22.00**	**7.02**	**1.000**	**3.650**
PRUEBA	30.64	22.00			**73.00%**
					NIVEL ACTUAL

CONCLUSIÓN:

Se determinó que en el proceso de adquirir infraestructura tecnológica (BAI03) se administran los controles sobre este proceso de forma “predecible”, es decir que además de funcionar formalmente ya se obtienen resultados satisfactorios, mostrando un nivel 3.65 de capacidad y un 73% de confiabilidad en los objetivos de control.

REFERENCIAS:

*(1) viene de MM06-01 1/3

*(2) viene de MM06-02 1/2

*(3) Sumatoria de *(1) + *(2)

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM06-01 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	14/01/2015
FECHA FIN:	14/01/2015

PROCESO:BAI03 Adquirir e implementar infraestructura tecnológica			¿Qué tanto se ha alcanzado?				
Función: Dirección de tecnología			Fecha: 14/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	La arquitectura de la tecnología no es considerada un tema lo suficientemente importante como para ser tratado.	X				0.00
1	2	Se hacen cambios a la infraestructura para cada nueva aplicación sin un plan general.	X				0.00
1	3	A pesar de que hay conciencia de que la infraestructura de TI es importante, no hay un método general coherente.	X				0.00
1	4	Las actividades de mantenimiento reaccionan a las necesidades a corto plazo. El entorno de producción es el entorno de pruebas.		X			0.33
2	5	Hay coherencia entre los métodos tácticos, cuando se adquiere y se mantiene la infraestructura de TI.			X		0.66
2	6	La adquisición y el mantenimiento de la infraestructura de TI no se basan en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que deben ser apoyadas.	X				0.00
2	7	Hay una comprensión de que la infraestructura de TI es importante, y dicha comprensión es apoyada por algunas prácticas formales.				X	1.00
2	8	Se programa algún mantenimiento, pero el mismo no es programado y coordinado completamente.	X				0.00
2	9	Para algunos entornos existe un entorno de pruebas separado.		X			0.33
3	10	Existe un proceso claro, definido y generalmente entendido para adquirir y mantener la infraestructura de TI.				X	1.00
3	11	El proceso apoya las necesidades de las aplicaciones críticas del negocio y está alineado con la estrategia de TI y del negocio aunque no se aplique de forma coherente.				X	1.00
3	12	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1.00
3	13	Existen entornos separados para pruebas y producción.				X	1.00

Papel de Trabajo	MM06-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	14/01/2015
FECHA FIN:	14/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	14	El proceso de adquisición y mantenimiento para la infraestructura tecnológica se ha desarrollado hasta el punto que funciona bien para la mayoría de las situaciones, es seguido coherentemente y se concentra en la reutilización.				X	1.00
4	15	La infraestructura de TI soporta de manera adecuada las aplicaciones de negocio.				X	1.00
4	16	El proceso de adquisición y mantenimiento para la infraestructura tecnología está bien organizado y es proactivo.				X	1.00
4	17	El costo y el tiempo para alcanzar el nivel esperado de escalabilidad, flexibilidad e integración están parcialmente optimizado.				X	1.00
5	18	El proceso de adquisición y mantenimiento para la infraestructura tecnológica es proactivo y está estrechamente alineado con aplicaciones críticas del negocio y con la arquitectura de la tecnología.				X	1.00
5	19	Se siguen las mejores prácticas respecto a soluciones de tecnología y la organización está al tanto de los últimos desarrollos en plataformas y herramientas de administración.				X	1.00
5	20	Los costos son reducidos racionalizando y estandarizando los componentes de la infraestructura y usando la automatización.				X	1.00
5	21	El alto nivel de conocimientos técnicos puede identificar las mejores formas de mejorar proactivamente el desempeño, incluyendo la consideración de opciones de tercerización.				X	1.00
5	22	La infraestructura de TI es vista como el posibilitador clave para aprovechar el uso de la TI.			X		0.66
			TOTAL DEL NIVEL				**14.98**

CONCLUSIÓN:

Para la función de dirección de tecnología en el proceso BAI03 adquirir e implementar infraestructura tecnológica, se determinó que el valor de cumplimiento es de 14.98 puntos de 22 como máximo.

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM06-02 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	14/01/2015
FECHA FIN:	14/01/2015

PROCESO: BAI03 Adquirir e implementar infraestructura tecnológica			¿Qué tanto se ha alcanzado?				
FUNCIÓN: Jefatura de infraestructura			Fecha: 14/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	La arquitectura de la tecnología no es considerada un tema lo suficientemente importante como para ser tratado.	X				0.00
1	2	Se hacen cambios a la infraestructura para cada nueva aplicación sin un plan general.	X				0.00
1	3	A pesar de que hay conciencia de que la infraestructura de TI es importante, no hay un método general coherente.	X				0.00
1	4	Las actividades de mantenimiento reaccionan a las necesidades a corto plazo. El entorno de producción es el entorno de pruebas.		X			0.33
2	5	Hay coherencia entre los métodos tácticos, cuando se adquiere y se mantiene la infraestructura de TI.				X	1.00
2	6	La adquisición y el mantenimiento de la infraestructura de TI no se basan en una estrategia definida y no considera las necesidades de las aplicaciones del negocio que deben ser apoyadas.	X				0.00
2	7	Hay una comprensión de que la infraestructura de TI es importante, y dicha comprensión es apoyada por algunas prácticas formales.				X	1.00
2	8	Se programa algún mantenimiento, pero el mismo no es programado y coordinado completamente.	X				0.00
2	9	Para algunos entornos existe un entorno de pruebas separado.		X			0.33
3	10	Existe un proceso claro, definido y generalmente entendido para adquirir y mantener la infraestructura de TI.				X	1.00
3	11	El proceso apoya las necesidades de las aplicaciones críticas del negocio y está alineado con la estrategia de TI y del negocio aunque no se aplique de forma coherente.				X	1.00
3	12	Las actividades de mantenimiento son planificadas, programadas y coordinadas.				X	1.00
3	13	Existen entornos separados para pruebas y producción.				X	1.00

Papel de Trabajo	MM06-02 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	14/01/2015
FECHA FIN:	14/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	14	El proceso de adquisición y mantenimiento para la infraestructura tecnológica se ha desarrollado hasta el punto que funciona bien para la mayoría de las situaciones, es seguido coherentemente y se concentra en la reutilización.				X	1.00
4	15	La infraestructura de TI soporta de manera adecuada las aplicaciones de negocio.				X	1.00
4	16	El proceso de adquisición y mantenimiento para la infraestructura tecnología está bien organizado y es proactivo.				X	1.00
4	17	El costo y el tiempo para alcanzar el nivel esperado de escalabilidad, flexibilidad e integración están parcialmente optimizado.				X	1.00
5	18	El proceso de adquisición y mantenimiento para la infraestructura tecnológica es proactivo y está estrechamente alineado con aplicaciones críticas del negocio y con la arquitectura de la tecnología.				X	1.00
5	19	Se siguen las mejores prácticas respecto a soluciones de tecnología y la organización está al tanto de los últimos desarrollos en plataformas y herramientas de administración.				X	1.00
5	20	Los costos son reducidos racionalizando y estandarizando los componentes de la infraestructura y usando la automatización.				X	1.00
5	21	El alto nivel de conocimientos técnicos puede identificar las mejores formas de mejorar proactivamente el desempeño, incluyendo la consideración de opciones de tercerización.				X	1.00
5	22	La infraestructura de TI es vista como el posibilitador clave para aprovechar el uso de la TI.				X	1.00
			TOTAL DEL NIVEL				**15.66**

CONCLUSIÓN:

Para la función de jefatura de infraestructura en el proceso BAI03 adquirir e implementar infraestructura tecnológica, se determinó que el valor de cumplimiento es de 15.66 puntos de 22 como máximo.

Papel de Trabajo	MM07 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	15/01/2015
FECHA FIN:	15/01/2015

Evaluación del proceso facilitar la ejecución y el uso (BAI04).

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI04 Gestionar la disponibilidad y la capacidad					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Dirección de tecnología					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE CAPACIDAD	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	NIVEL DE CAPACIDAD (A * E)
0	0.99	2	0.495	0.178	0.000
1	1.65	6	0.275	0.099	0.099
2	1.33	5	0.266	0.096	0.192
3	6.28	9	0.698	0.252	0.755
4	6.28	10	0.628	0.226	0.905
5	1.65	4	0.413	0.149	0.743
TOTAL	**18.18 *(1)**	**36.00**	**2.77**	**1.000**	**2.694**
PRUEBA					**53.89%**
					NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.99	2	0.495	0.178	0.000
1	1.65	6	0.275	0.099	0.099
2	1.33	5	0.266	0.096	0.192
3	6.28	9	0.698	0.252	0.755
4	6.28	10	0.628	0.226	0.905
5	1.65	4	0.413	0.149	0.743
TOTAL	**18.18 *(2)**	**36.00**	**2.77**	**1.000**	**2.694**
PRUEBA					**53.89%**
					NIVEL ACTUAL

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM07 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	15/01/2015
FECHA FIN:	15/01/2015

CONCLUSIÓN:

Se determinó que en el proceso de gestionar la disponibilidad y la capacidad (BAI04), se administran los controles sobre este proceso de forma “establecida”, es decir ya funcional formalmente, mostrando un nivel 2.694 de capacidad y un 53.89% de confiabilidad en los objetivos de control informático.

REFERENCIAS:

*(1) viene de MM07-01 1/3

*(2) sumatoria de *(1)

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM07-01 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	15/01/2015
FECHA FIN:	15/01/2015

PROCESO: BAI04 Gestionar la disponibilidad y la capacidad			¿Qué tanto se ha alcanzado?				
Función: Dirección de tecnología			Fecha: 15/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No hay ningún proceso establecido respecto a la producción de documentación de usuario, manuales de operaciones y material de capacitación.		X			0.33
0	2	Los únicos materiales que existen son los suministrados con los productos comprados.			X		0.66
1	3	La organización está consciente de que se necesita un proceso que resuelva la documentación.			X		0.66
1	4	La documentación se produce ocasionalmente y está distribuida desigualmente entre grupos limitados.		X			0.33
1	5	Gran parte de la documentación y de los procedimientos son obsoletos.		X			0.33
1	6	Los materiales de capacitación tienden a ser esquemas que se usan una sola vez con calidad variable.		X			0.33
1	7	Prácticamente no hay integración de los procedimientos en todos los diferentes sistemas y unidades de negocio.	X				0.00
1	8	No hay colaboración por parte de las unidades de negocio en el diseño de programas de capacitación	X				0.00
2	9	Se usan enfoques similares para producir procedimientos y documentación, pero los mismos no están basados en un enfoque o marco estructurado.	X				0.00
2	10	No hay un enfoque uniforme para el desarrollo de procedimientos operativos y de usuario.	X				0.00
2	11	El material de capacitación es producido individualmente o por grupos de proyectos y su calidad depende de las personas involucradas.		X			0.33
2	12	Los procedimientos y la calidad del soporte de usuario varían de pobre a muy bueno, con muy poca coherencia e integración en toda la organización.	X				0.00
2	13	Se proveen o facilitan los programas de capacitación para el negocio y los usuarios, pero no hay un plan general para la entrega e implementación de capacitación.				X	1.00
3	14	Hay un marco claramente definido, aceptado y entendido para la documentación del usuario, los manuales de operaciones y los materiales de capacitación.				X	1.00
3	15	Los procedimientos son almacenados y mantenidos en una biblioteca formal y pueden ser accedidos por cualquiera que necesite saber.			X		0.66
3	16	Se hacen correcciones a la documentación y los procedimientos de manera reactiva.			X		0.66

Papel de Trabajo	MM07-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	15/01/2015
FECHA FIN:	15/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	17	Se cuenta con procedimientos fuera de línea y éstos pueden ser accedidos y mantenidos en caso de desastre.			X		0.66
3	18	Existe un proceso que especifica que las actualizaciones de procedimientos y materiales de capacitación son un producto explícito de un proyecto de cambio.			X		0.66
3	19	A pesar de la existencia de enfoques definidos, el contenido real varía porque no hay control para hacer cumplir las normas.			X		0.66
3	20	Los usuarios están formalmente involucrados en este proceso.			X		0.66
3	21	Se usan cada vez más herramientas automatizadas para la generación y distribución de procedimientos.			X		0.66
3	22	La capacitación de usuarios y de negocio es planificada y programada.			X		0.66
4	23	Hay un marco de trabajo definido para mantener los procedimientos y los materiales de capacitación que cuenta con el apoyo de la gerencia de TI.			X		0.66
4	24	El enfoque adoptado para mantener los procedimientos y los manuales de capacitación cubre todos los sistemas y unidades de negocio, a fin de que los procesos puedan ser vistos desde una perspectiva de negocios.			X		0.66
4	25	Los procedimientos y los materiales de capacitación están integrados para incluir interdependencias e interfaces.			X		0.66
4	26	Existen controles para asegurar que las normas se cumplen y que los procedimientos se desarrollen y se mantengan para todos los procesos.			X		0.66
4	27	La realimentación del negocio y de los usuarios acerca de la documentación y la capacitación se recopila y evalúa como parte de un proceso de mejora continua.			X		0.66
4	28	La documentación y los materiales de capacitación están por lo general a un buen nivel predecible de confiabilidad y disponibilidad.			X		0.66
4	29	Está emergiendo un proceso para documentar y administrar procedimientos de forma automática.		X			0.33
4	30	El desarrollo de procedimientos automatizados está cada vez más integrado con el desarrollo de sistemas de aplicación, facilitando la coherencia y el acceso de los usuarios.		X			0.33
4	31	La capacitación de negocios y de usuarios tiene una gran capacidad de respuesta respecto a las necesidades del negocio.				X	1.00
4	32	La gerencia de TI está desarrollando métricas para el desarrollo y la entrega de documentación, materiales de capacitación y programas de capacitación.			X		0.66

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM07-01 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	15/01/2015
FECHA FIN:	15/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
5	33	El proceso para la documentación operativa y de usuarios es mejorado continuamente a través de la adopción de nuevas herramientas o métodos.			X		0.66
5	34	Los materiales de procedimiento y capacitación son tratados como una base de conocimientos que evoluciona constantemente y es mantenida electrónicamente usando una administración de conocimientos actualizada y tecnologías de flujo de trabajo y distribución, lo cual la hace accesible y fácil de mantener.		X			0.33
5	35	El material está actualizado para reflejar cambios organizacionales, operativos y de software.		X			0.33
5	36	El desarrollo de documentación y materiales de capacitación, así como la entrega de los programas de capacitación, están totalmente integrados con el negocio y con las definiciones de procesos de negocios, apoyando así a los requerimientos a nivel de toda la organización en lugar de solo a los procedimientos orientados a TI.		X			0.33
			TOTAL DEL NIVEL				**18.18**

CONCLUSIÓN:

Para la función de dirección de tecnología en el proceso BAI04 gestionar la disponibilidad y la capacidad, se determinó que el valor de cumplimiento es de 18.18 puntos de 36 como máximo.

Papel de Trabajo	MM08 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

Evaluación del proceso gestionar la introducción de cambios organizativos (BAI05)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI05 Gestionar la introducción de cambios organizativos

COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD

Función: Dirección de tecnología

(A) NIVEL DE CAPACIDAD	(B) SUMA DE VALORES DE CUMPLIMIENTO	(C) NUMERO DE DECLARACIONES	(D) VALOR DE CUMPLIMIENTO (B/C)	(E) NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	(F) NIVEL DE CAPACIDAD (A * E)
0	0.00	2	0.000	0.000	0.000
1	0.00	4	0.000	0.000	0.000
2	3.32	6	0.553	0.156	0.311
3	6.00	6	1.000	0.281	0.844
4	7.00	7	1.000	0.281	1.126
5	6.00	6	1.000	0.281	1.407
TOTAL	**22.32 *(1)**	**31.00**	**3.55**	**1.000**	**3.689**
PRUEBA					**73.77%**
					NIVEL ACTUAL

FUNCIÓN: Jefatura de infraestructura

(A) NIVEL DE CAPACIDAD	(B) SUMA DE VALORES DE CUMPLIMIENTO	(C) NUMERO DE DECLARACIONES	(D) VALOR DE CUMPLIMIENTO (B/C)	(E) NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	(F) NIVEL DE CAPACIDAD (A * E)
0	0.00	2	0.000	0.000	0.000
1	1.32	4	0.330	0.093	0.093
2	3.98	6	0.663	0.187	0.373
3	6.00	6	1.000	0.281	0.844

Papel de Trabajo	MM08 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

PROCESO: BAI05 Gestionar la introducción de cambios organizativos

COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD

Función: Jefatura de infraestructura

(A) NIVEL DE CAPACIDAD	(B) SUMA DE VALORES DE CUMPLIMIENTO	(C) NUMERO DE DECLARACIONES	(D) VALOR DE CUMPLIMIENTO (B/C)	(E) NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	(F) NIVEL DE CAPACIDAD (A * E)
4	7.00	7	1.000	0.281	1.126
5	6.00	6	1.000	0.281	1.407
TOTAL	**24.30 *(2)**	**31.00**	**3.99**	**1.124**	**3.843**
PRUEBA					**76.87%**
					NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.00	2	0.000	0.000	0.000
1	1.32	4	0.330	0.044	0.044
2	7.30	6	1.217	0.161	0.322
3	12.00	6	2.000	0.265	0.795
4	14.00	7	2.000	0.265	1.060
5	12.00	6	2.000	0.265	1.325
TOTAL	**46.62 *(3)**	**31.00**	**7.55**	**1.000**	**3.546**
PRUEBA	46.62	31.00			**70.93%**
					NIVEL ACTUAL

CONCLUSIÓN:

Se determinó que en el proceso de gestionar la introducción de cambios organizativos (BAI05), se administran los controles sobre este proceso de forma "establecida", es decir ya funcionan formalmente, mostrando un nivel 3.546 de capacidad y un 70.93% de confiabilidad en los objetivos de control.

REFERENCIAS:

*(1) viene de MM08-01 1/3

*(2) viene de MM08-02 1/3

*(3) Sumatoria de *(1) + *(2)

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM08-01 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

PROCESO: BAI05 Gestionar la introducción de cambios organizativos			¿Qué tanto se ha alcanzado?				
Función: Dirección de tecnología			Fecha: 16/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No está definido un proceso de abastecimiento de TI.	X				0.00
0	2	La organización no reconoce la necesidad de contar con políticas y procedimientos de abastecimiento claros para asegurar que todos los recursos de TI estén disponibles de forma oportuna y costo-eficiente.	X				0.00
1	3	La organización reconoce la necesidad de contar con políticas y procedimientos documentados que vinculen la adquisición de TI con el proceso general de abastecimiento de negocio de la organización.	X				0.00
1	4	Se desarrollan y administran contratos para la adquisición de los recursos de TI por parte de los administradores de proyecto y otras personas que emplean su juicio profesional en lugar de políticas y procedimientos formales.	X				0.00
1	5	Existe una relación ad hoc entre la TI y los procesos de adquisición corporativa y de administración de contratos.	X				0.00
1	6	Los contratos de adquisición se administran al finalizar los proyectos en lugar de hacerlo de forma continua.	X				0.00
2	7	Hay conciencia en la organización acerca de la necesidad de contar con políticas y procedimientos para la adquisición de TI.				X	1.00
2	8	Las políticas y los procedimientos están parcialmente integrados con el proceso de abastecimiento general de negocios de la organización.			X		0.66
2	9	Los procesos de abastecimiento se emplean mayormente para proyectos de gran porte y visibilidad.	X				0.00
2	10	Las responsabilidades y la rendición de cuentas por el abastecimiento de TI y la administración de contratos se determinan por la experiencia individual del administrador del contrato.	X				0.00
2	11	Se reconoce la importancia de la administración y el relacionamiento con los proveedores; sin embargo los mismos se atienden basándose en iniciativas individuales.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM08-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
2	12	Los procesos de contratos se utilizan mayormente para proyectos de gran porte y visibilidad.			X		0.66
3	13	La gerencia establece políticas y procedimientos para la adquisición de TI.				X	1.00
3	14	Las políticas y los procedimientos están guiados por el proceso de abastecimiento general de negocios de la organización.				X	1.00
3	15	La adquisición de TI está mayormente integrada con los sistemas de abastecimiento generales del negocio.				X	1.00
3	16	Existen estándares de TI para la adquisición de recursos de TI.				X	1.00
3	17	Los proveedores de recursos de TI están integrados en los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.				X	1.00
3	18	La gerencia de TI comunica la necesidad de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1.00
4	19	La adquisición de TI está completamente integrada con los sistemas de abastecimiento generales del negocio.				X	1.00
4	20	Los estándares de TI para la adquisición de recursos de TI se usan para todos los abastecimientos.				X	1.00
4	21	Se toman mediciones relativas a los casos de negocio para la adquisición de TI en los contratos y en la administración del abastecimiento.				X	1.00
4	22	Se encuentra disponible una emisión de informes sobre la actividad de adquisición de TI que apoya los objetivos de negocio.				X	1.00
4	23	La gerencia generalmente es consciente de las excepciones a las políticas y procedimientos para la adquisición de TI.				X	1.00
4	24	Comienza a desarrollarse una administración estratégica de relacionamiento.				X	1.00
4	25	La gerencia de TI exige el uso del proceso de adquisición y administración de contratos para todas las adquisiciones al revisar las mediciones de desempeño.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM08-01 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
5	26	La gerencia establece recursos de adquisiciones a procesos exhaustivos para la adquisición de TI.				X	1.00
5	27	La gerencia exige el cumplimiento de las políticas y procedimientos para la adquisición de TI.				X	1.00
5	28	Se toman mediciones que son relevantes a los casos de negocio para las adquisiciones de TI en los contratos y en la administración del abastecimiento.				X	1.00
5	29	Se establecen buenas relaciones con los proveedores y socios a lo largo del tiempo y la calidad de dichas relaciones es medida y monitoreada. Las relaciones se administran estratégicamente.				X	1.00
5	30	Los estándares, políticas y procedimientos de TI para la adquisición de recursos de TI se administran estratégicamente y responden a las medidas del proceso.				X	1.00
5	31	La gerencia de TI comunica la importancia estratégica de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1.00
			TOTAL DEL NIVEL				**22.32**

CONCLUSIÓN:

Para la función de dirección de tecnología en el proceso BAI05 gestionar la introducción de cambios organizativos, se determinó que el valor de cumplimiento es de 22.32 puntos de 31 como máximo.

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM08-02 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

PROCESO: BAI05 Gestionar la introducción de cambios organizativos			¿Qué tanto se ha alcanzado?				
FUNCIÓN: Jefatura de infraestructura			Fecha: 16/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No está definido un proceso de abastecimiento de TI.	X				0.00
0	2	La organización no reconoce la necesidad de contar con políticas y procedimientos de abastecimiento claros para asegurar que todos los recursos de TI estén disponibles de forma oportuna y costo-eficiente.	X				0.00
1	3	La organización reconoce la necesidad de contar con políticas y procedimientos documentados que vinculen la adquisición de TI con el proceso general de abastecimiento de negocio de la organización.		X			0.33
1	4	Se desarrollan y administran contratos para la adquisición de los recursos de TI por parte de los administradores de proyecto y otras personas que emplean su juicio profesional en lugar de políticas y procedimientos formales.		X			0.33
1	5	Existe una relación ad hoc entre la TI y los procesos de adquisición corporativa y de administración de contratos.		X			0.33
1	6	Los contratos de adquisición se administran al finalizar los proyectos en lugar de hacerlo de forma continua.		X			0.33
2	7	Hay conciencia en la organización acerca de la necesidad de contar con políticas y procedimientos para la adquisición de TI.				X	1.00
2	8	Las políticas y los procedimientos están parcialmente integrados con el proceso de abastecimiento general de negocios de la organización.			X		0.66
2	9	Los procesos de abastecimiento se emplean mayormente para proyectos de gran porte y visibilidad.		X			0.33
2	10	Las responsabilidades y la rendición de cuentas por el abastecimiento de TI y la administración de contratos se determinan por la experiencia individual del administrador del contrato.		X			0.33
2	11	Se reconoce la importancia de la administración y el relacionamiento con los proveedores; sin embargo los mismos se atienden basándose en iniciativas individuales.				X	1.00
2	12	Los procesos de contratos se utilizan mayormente para proyectos de gran porte y visibilidad.			X		0.66

Papel de Trabajo	MM08-02 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
3	13	La gerencia establece políticas y procedimientos para la adquisición de TI.				X	1.00
3	14	Las políticas y los procedimientos están guiados por el proceso de abastecimiento general de negocios de la organización.				X	1.00
3	15	La adquisición de TI está mayormente integrada con los sistemas de abastecimiento generales del negocio.				X	1.00
3	16	Existen estándares de TI para la adquisición de recursos de TI.				X	1.00
3	17	Los proveedores de recursos de TI están integrados en los mecanismos de administración de proyectos de la organización desde una perspectiva de administración de contratos.				X	1.00
3	18	La gerencia de TI comunica la necesidad de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1.00
4	19	La adquisición de TI está completamente integrada con los sistemas de abastecimiento generales del negocio.				X	1.00
4	20	Los estándares de TI para la adquisición de recursos de TI se usan para todos los abastecimientos.				X	1.00
4	21	Se toman mediciones relativas a los casos de negocio para la adquisición de TI en los contratos y en la administración del abastecimiento.				X	1.00
4	22	Se encuentra disponible una emisión de informes sobre la actividad de adquisición de TI que apoya los objetivos de negocio.				X	1.00
4	23	La gerencia generalmente es consciente de las excepciones a las políticas y procedimientos para la adquisición de TI.				X	1.00
4	24	Comienza a desarrollarse una administración estratégica de relacionamiento.				X	1.00
4	25	La gerencia de TI exige el uso del proceso de adquisición y administración de contratos para todas las adquisiciones al revisar las mediciones de desempeño.				X	1.00
5	26	La gerencia establece recursos de adquisiciones a procesos exhaustivos para la adquisición de TI.				X	1.00

Papel de Trabajo	MM08-02 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	16/01/2015
FECHA FIN:	16/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
5	27	La gerencia exige el cumplimiento de las políticas y procedimientos para la adquisición de TI.				X	1.00
5	28	Se toman mediciones que son relevantes a los casos de negocio para las adquisiciones de TI en los contratos y en la administración del abastecimiento.				X	1.00
5	29	Se establecen buenas relaciones con los proveedores y socios a lo largo del tiempo y la calidad de dichas relaciones es medida y monitoreada. Las relaciones se administran estratégicamente.				X	1.00
5	30	Los estándares, políticas y procedimientos de TI para la adquisición de recursos de TI se administran estratégicamente y responden a las medidas del proceso.				X	1.00
5	31	La gerencia de TI comunica la importancia estratégica de una administración de adquisiciones y contratos adecuada en toda la función de TI.				X	1.00
			TOTAL DEL NIVEL				**24.30**

CONCLUSIÓN:

Para la función de Jefatura de Infraestructura en el proceso BAI05 gestionar la introducción de cambios organizativos, se determinó que el valor de cumplimiento es de 24.30 puntos de 31 como máximo.

Papel de Trabajo	MM09 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

Evaluación del proceso de administración de cambios (BAI06).

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI06 Administración de cambios					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
Función: Dirección de tecnología					
(A)	(B)	(C)	(D)	(E)	(F)
NIVEL DE CAPACIDAD	SUMA DE VALORES DE CUMPLIMIENTO	NUMERO DE DECLARACIONES	VALOR DE CUMPLIMIENTO (B/C)	NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	NIVEL DE CAPACIDAD (A * E)
0	0.00	2	0.000	0.000	0.000
1	0.00	3	0.000	0.000	0.000
2	0.00	2	0.000	0.000	0.000
3	3.00	3	1.000	0.333	1.000
4	9.00	9	1.000	0.333	1.333
5	5.00	5	1.000	0.333	1.667
TOTAL	**17.00 *(1)**	**24.00**	**3.00**	**1.000**	**4.000**
PRUEBA					**80.00%**
					NIVEL ACTUAL
Función: Jefatura de plataforma tecnológica					
0	0.00	2	0.000	0.000	0.000
1	0.00	3	0.000	0.000	0.000
2	0.00	2	0.000	0.000	0.000
3	3.00	3	1.000	0.333	1.000
4	9.00	9	1.000	0.333	1.333
5	4.66	5	0.932	0.311	1.553
TOTAL	**16.66 *(2)**	**24.00**	**2.93**	**0.977**	**3.887**

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM09 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

PROCESO: BAI06 Administración de cambios					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
PRUEBA					**77.73%**
					NIVEL ACTUAL
FUNCIÓN: Jefatura de servicios tecnológicos					
0	0.33	2	0.165	0.055	0.000
1	0.33	3	0.110	0.037	0.037
2	0.00	2	0.000	0.000	0.000
3	3.00	3	1.000	0.333	1.000
4	9.00	9	1.000	0.333	1.333
5	5.00	5	1.000	0.333	1.667
TOTAL	**17.66 *(3)**	**24.00**	**3.28**	**1.092**	**4.037**
PRUEBA					**80.73%**
					NIVEL ACTUAL
FUNCIÓN: Jefatura de infraestructura					
0	0.00	2	0.000	0.000	0.000
1	0.00	3	0.000	0.000	0.000
2	0.00	2	0.000	0.000	0.000
3	2.32	3	0.773	0.258	0.773
4	9.00	9	1.000	0.333	1.333
5	4.32	5	0.864	0.288	1.440
TOTAL	**15.64 *(4)**	**24.00**	**2.64**	**0.879**	**3.547**
PRUEBA					**70.93%**
					NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.33	2	0.165	0.014	0.000
1	0.33	3	0.110	0.009	0.009
2	0.00	2	0.000	0.000	0.000
3	11.32	3	3.773	0.319	0.956
4	36.00	9	4.000	0.338	1.351
5	18.98	5	3.796	0.320	1.602
TOTAL	**66.96 *(5)**	**24.00**	**11.84**	**1.000**	**3.918**
PRUEBA					**78.37%**
					NIVEL ACTUAL

Papel de Trabajo	MM09 3/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

CONCLUSIÓN:

Se determinó que en el proceso de administración de cambios (BAI06), se administran los controles sobre este proceso de forma "predecible", es decir además de estar funcionando formalmente ya se obtienen resultados satisfactorios, mostrando un nivel 3.918 de capacidad y un 78.37% de confiabilidad en los objetivos de control informático.

REFERENCIAS:

*(1) viene de MM09-01 1/3
*(2) viene de MM09-02 1/3
*(3) viene de MM09-03 1/2
*(4) viene de MM09-04 ½
*(5) Sumatoria de *(1) + *(2) + *(3) + *(4)

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM09-01 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

PROCESO: BAI06 Gestionar los cambios			¿Qué tanto se ha alcanzado?				
Función: Dirección de tecnología			Fecha: 19/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.	X				0.00
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.	X				0.00
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.	X				0.00
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.	X				0.00
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción, causados por una administración deficiente del cambio.	X				0.00
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.	X				0.00
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.	X				0.00
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo				X	1.00
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.				X	1.00
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM09-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.				X	1.00
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.				X	1.00
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.				X	1.00
4	14	Está establecido un proceso de aprobación para los cambios.				X	1.00
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.				X	1.00
4	16	La documentación de configuración generalmente es precisa.				X	1.00
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.				X	1.00
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.				X	1.00
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.				X	1.00
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.				X	1.00
5	21	El proceso de revisión refleja los resultados del monitoreo.				X	1.00
5	22	La información de configuración está automatizada y provee control de versiones.				X	1.00
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.				X	1.00
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.				X	1.00
			TOTAL DEL NIVEL				**17.00**

Papel de Trabajo	MM09-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

CONCLUSIÓN:

Para la función de dirección de tecnología en el proceso BAI06 gestionar los cambios, se determinó que el valor de cumplimiento es de 17.00 puntos de 24 como máximo.

Papel de Trabajo	MM09-02 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

PROCESO: BAI06 Gestionar los cambios			¿Qué tanto se ha alcanzado?				
Función: Jefatura de plataforma tecnológica			**Fecha: 19/01/2015**				
NV	**No.**	**DECLARACIÓN**	**No alcanzado**	**Parcialmente**	**Ampliamente**	**Completamente**	**Valor de cumplimiento según respuesta**
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.	X				0.00
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.	X				0.00
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.	X				0.00
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.	X				0.00
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción, causados por una administración deficiente del cambio.	X				0.00
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.	X				0.00
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.	X				0.00
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo				X	1.00
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.				X	1.00
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se está volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.				X	1.00
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM09-02 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.				X	1.00
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.				X	1.00
4	14	Está establecido un proceso de aprobación para los cambios.				X	1.00
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.				X	1.00
4	16	La documentación de configuración generalmente es precisa.				X	1.00
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.				X	1.00
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.				X	1.00
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.				X	1.00
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.				X	1.00
5	21	El proceso de revisión refleja los resultados del monitoreo.				X	1.00
5	22	La información de configuración está automatizada y provee control de versiones.				X	1.00
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.			X		0.66
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.				X	1.00
			TOTAL DEL NIVEL				**16.66**

Papel de Trabajo	MM09-02 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

CONCLUSIÓN:

Para la función de jefatura de plataforma tecnológica en el proceso BAI06 gestionar los cambios, se determinó que el valor de cumplimiento es de 16.66 puntos de 24 como máximo.

Papel de Trabajo	MM09-03 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

PROCESO: BAI06 Gestionar los cambios			¿Qué tanto se ha alcanzado?				
FUNCIÓN: Jefatura de servicios tecnológicos			Fecha: 19/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.	X				0.00
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.		X			0.33
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.		X			0.33
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.	X				0.00
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción, causados por una administración deficiente del cambio.	X				0.00
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.	X				0.00
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.	X				0.00
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo				X	1.00
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.				X	1.00
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.				X	1.00
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM09-03 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.				X	1.00
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.				X	1.00
4	14	Está establecido un proceso de aprobación para los cambios.				X	1.00
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.				X	1.00
4	16	La documentación de configuración generalmente es precisa.				X	1.00
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.				X	1.00
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.				X	1.00
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.				X	1.00
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.				X	1.00
5	21	El proceso de revisión refleja los resultados del monitoreo.				X	1.00
5	22	La información de configuración está automatizada y provee control de versiones.				X	1.00
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.				X	1.00
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.				X	1.00
			TOTAL DEL NIVEL				**17.66**

CONCLUSIÓN:

Para la función de jefatura de servicios tecnológicos en el proceso BAI06 gestionar los cambios, se determinó que el valor de cumplimiento es de 17.66 puntos de 24 como máximo.

Papel de Trabajo	MM09-04 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

PROCESO: BAI06 Gestionar los cambios			¿Qué tanto se ha alcanzado?				
FUNCIÓN: Jefatura de infraestructura			Fecha: 19/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	No hay un proceso definido de administración de cambios y se pueden hacer cambios prácticamente sin control alguno.	X				0.00
0	2	No hay conciencia de que los cambios pueden causar interrupciones tanto para la TI como para las operaciones de negocios, y ninguna conciencia de los beneficios de una buena administración de cambios.	X				0.00
1	3	Se reconoce que los cambios deben ser administrados y controlados. Las prácticas varían y es probable que ocurran cambios no autorizados.	X				0.00
1	4	Hay documentación insuficiente o inexistente de cambios, y la documentación de configuración está incompleta y no es confiable.	X				0.00
1	5	Es probable que ocurran errores junto con interrupciones en el entorno de producción, causados por una administración deficiente del cambio.	X				0.00
2	6	Está establecido un proceso informal de administración de cambios y la mayoría de los cambios siguen este método; sin embargo, el mismo no está estructurado y es rudimentario y propenso a errores.	X				0.00
2	7	La precisión de la documentación de configuración es desigual y solo tiene lugar una planificación y un estudio de impacto limitados antes de realizar un cambio.	X				0.00
3	8	Está establecido un proceso formal de administración de cambios, que incluye procedimientos de categorización, priorización, procedimientos de emergencia, autorización y administración de cambios, y su cumplimiento está emergiendo			X		0.66
3	9	Ocurren trabajos paralelos y los procesos son desviados. Es probable que ocurran errores y los cambios no autorizados ocurrirán ocasionalmente.			X		0.66
3	10	El análisis de impacto a los cambios de TI sobre las operaciones de negocio se están volviendo formales para apoyar la ejecución de los planes para nuevas aplicaciones y tecnologías.				X	1.00
4	11	El proceso de administración de cambios está bien desarrollado y es seguido de manera coherente para todos los cambios, y la gerencia tiene certeza de que apenas hay excepciones.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM09-04 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	19/01/2015
FECHA FIN:	19/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	12	El proceso es eficiente y efectivo, pero se basa considerablemente en procedimientos y controles manuales para asegurar que se logre la calidad.				X	1.00
4	13	Todos los cambios están sujetos a una planificación y estudio de impacto exhaustivos para minimizar la probabilidad de problemas posteriores a la producción.				X	1.00
4	14	Está establecido un proceso de aprobación para los cambios.				X	1.00
4	15	La documentación de administración de cambios está al día y es correcta, y los cambios son seguidos formalmente.				X	1.00
4	16	La documentación de configuración generalmente es precisa.				X	1.00
4	17	La planificación e implementación de la administración de cambios de TI se está integrando más con cambios en los procesos de negocios, para asegurar que se atienden los problemas de capacitación, cambios organizativos y continuidad de negocio.				X	1.00
4	18	Hay mayor coordinación entre la administración de cambios de TI y el rediseño de proceso de negocios.				X	1.00
4	19	Existe un proceso coherente para monitorear la calidad y el desempeño del proceso de administración de cambios.				X	1.00
5	20	El proceso de administración de cambios es revisado y actualizado regularmente para mantenerse en línea con las mejores prácticas.				X	1.00
5	21	El proceso de revisión refleja los resultados del monitoreo.				X	1.00
5	22	La información de configuración está automatizada y provee control de versiones.				X	1.00
5	23	El seguimiento de cambios es sofisticado e incluye herramientas para detectar software sin licencia o autorización.			X		0.66
5	24	La administración de cambios de TI está integrada con la administración de cambios del negocio para asegurar que la TI sea un posibilitador para aumentar la productividad y crear nuevas oportunidades de negocios para la organización.			X		0.66
			TOTAL DEL NIVEL				**15.64**

CONCLUSIÓN:

Para la función de Jefatura de Infraestructura en el proceso BAI06 gestionar los cambios, se determinó que el valor de cumplimiento es de 15.64 puntos de 24 como máximo.

Papel de Trabajo	MM10 1/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	20/01/2015
FECHA FIN:	20/01/2015

Evaluación del proceso de gestionar la aceptación del cambio y de la transición (BAI07)

Cuadro para tabulación de resultados de los cuestionarios aplicados a las funciones indicadas, agrupadas según el nivel de capacidad y el peso de la respuesta obtenida sobre cada declaración. Las columnas (D), (E) Y (F) se calculan según formula indicada. Σ (F) = Nivel de capacidad del proceso.

PROCESO: BAI07 Gestionar la aceptación del cambio y de la transición					
COMPUTO DE LOS VALORES DE CUMPLIMIENTO DEL NIVEL DE CAPACIDAD					
FUNCIÓN: Dirección de aseguramiento de calidad de software					
(A) NIVEL DE CAPACIDAD	(B) SUMA DE VALORES DE CUMPLIMIENTO	(C) NUMERO DE DECLARACIONES	(D) VALOR DE CUMPLIMIENTO (B/C)	(E) NORMALIZACION DEL VECTOR DE CUMPLIMIENTO (D/ ΣD)	(F) NIVEL DE CAPACIDAD (A * E)
0	0.00	1	0.000	0.000	0.000
1	1.00	3	0.333	0.103	0.103
2	1.00	3	0.333	0.103	0.205
3	3.00	4	0.750	0.231	0.693
4	5.32	6	0.887	0.273	1.092
5	5.66	6	0.943	0.291	1.453
TOTAL	**15.98 *(1)**	**23.00**	**3.25**	**1.000**	**3.546**
PRUEBA					**70.92%**
					NIVEL ACTUAL
FUNCIÓN: Consolidación de resultados					
0	0.00	1	0.000	0.000	0.000
1	1.00	3	0.333	0.103	0.103
2	1.00	3	0.333	0.103	0.205
3	3.00	4	0.750	0.231	0.693
4	5.32	6	0.887	0.273	1.092
5	5.66	6	0.943	0.291	1.453
TOTAL	**15.98 *(2)**	**23.00**	**3.25**	**1.000**	**3.546**
PRUEBA	15.98	23.00			**70.92%**
					NIVEL ACTUAL

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM10 2/2
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	20/01/2015
FECHA FIN:	20/01/2015

CONCLUSIÓN:

Se determinó que en el proceso de gestionar la aceptación del cambio y de la transición (BAI07), se administran los controles sobre este proceso de forma "predecible", es decir que además de funcionar formalmente ya se obtienen resultados satisfactorios, mostrando un nivel 3.546 de capacidad y un 70.92% de confiabilidad en los objetivos de control.

REFERENCIAS:

*(1) viene de MM10-01 1/3

*(2) sumatoria de *(1)

Papel de Trabajo	MM10-01 1/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	20/01/2015
FECHA FIN:	20/01/2015

PROCESO: AI7 Gestionar la aceptación del cambio y de la transición			¿Qué tanto se ha alcanzado?				
Función: Dirección de aseguramiento de calidad de software			Fecha: 20/01/2015				
NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	0	0.33	0.66	1	
0	1	Hay una total falta de procesos formales de instalación o acreditación y ni la alta gerencia o el personal de TI reconocen la necesidad de verificar que las soluciones sean adecuadas para el propósito que se pretende.	X				0.00
1	2	Hay conciencia de la necesidad de verificar y confirmar que las soluciones implementadas sirven para el propósito que se pretende.				X	1.00
1	3	Se realizan pruebas para algunos proyectos, pero la iniciativa de realizar pruebas es dejada en manos de los equipos individuales de proyecto y los enfoques emprendidos varían.	X				0.00
1	4	La acreditación y autorización formal es poco frecuente o no existe en absoluto.	X				0.00
2	5	Hay alguna coherencia entre las pruebas y los enfoques de acreditación, pero típicamente los mismos no se basan en ninguna metodología.	X				0.00
2	6	Los equipos de desarrollo individual normalmente deciden el método de prueba y hay por lo general ausencia de pruebas de integración.	X				0.00
2	7	Hay un proceso informal de aprobación.				X	1.00
3	8	Está establecida una metodología formal relativa a la instalación, migración, conversión y aceptación.				X	1.00
3	9	Los procesos de instalación y acreditación de TI están integrados en el ciclo de vida del sistema y están automatizados en cierta medida.				X	1.00
3	10	Es probable que la capacitación, prueba y transición al estado de producción así como la acreditación varíen en relación al proceso definido, basándose en decisiones puntuales.				X	1.00
3	11	La calidad de los sistemas que entran en producción es desigual, con nuevos sistemas que a menudo generan un nivel significativo de problemas posteriores a la implementación.	X				0.00
4	12	Los procedimientos son formalizados y desarrollados para que estén bien organizados y sean prácticos, con entornos de prueba y procedimientos de acreditación definidos. En la práctica, todos los grandes cambios a los sistemas siguen este método formal.				X	1.00

El Mejor Seguro. S.A.

Auditoría Interna

Papel de Trabajo	MM10-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	20/01/2015
FECHA FIN:	20/01/2015

NV	No.	DECLARACIÓN	No alcanzado	Parcialmente	Ampliamente	Completamente	Valor de cumplimiento según respuesta
		Valores de cumplimiento de cada respuesta	**0**	**0.33**	**0.66**	**1**	
4	13	La evaluación de la satisfacción de los requerimientos de usuario está estandarizada y se puede medir, produciendo métricas que pueden ser revisadas y analizadas efectivamente por la gerencia.				X	1.00
4	14	La calidad de los sistemas que entran en producción es satisfactoria para la gerencia, con niveles razonables de problemas posteriores a la implementación.				X	1.00
4	15	La automatización del proceso es ad hoc y depende del proyecto. La gerencia puede estar satisfecha con el nivel actual de eficiencia a pesar de la falta de evaluaciones posteriores a la implementación.				X	1.00
4	16	El sistema de pruebas refleja adecuadamente el entorno real.			X		0.66
4	17	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican para los proyectos de gran porte.			X		0.66
5	18	Los procesos de instalación y acreditación han sido refinados hasta el nivel de la mejor práctica, basados en los resultados del mejoramiento y refinamiento continuo.			X		0.66
5	19	Los procesos de instalación y acreditación de TI están totalmente integrados en el ciclo de vida del sistema y automatizados donde es conveniente, facilitando la capacitación, prueba y transición al estado de producción de nuevos sistemas de forma más eficiente.				X	1.00
5	20	Los entornos de prueba bien desarrollados, los registros de problemas y los procesos de resolución e fallas aseguran una transición eficiente y efectiva al entorno de producción.				X	1.00
5	21	La acreditación tiene lugar por lo general sin reprocesamiento y los problemas posteriores a la implementación están por lo general limitados a correcciones menores.				X	1.00
5	22	Las revisiones posteriores a la implementación están también estandarizadas, con lecciones aprendidas canalizadas nuevamente al proceso para asegurar una mejora continua de la calidad.				X	1.00
5	23	Las pruebas de estrés para los sistemas nuevos y las pruebas de regresión para los sistemas existentes se aplican por igual.				X	1.00
			TOTAL DEL NIVEL				**15.98**

Papel de Trabajo	MM10-01 2/3
HECHO POR:	E.R.G.T
REVISADO POR:	J.L.R.B
FECHA DE INCIO:	20/01/2015
FECHA FIN:	20/01/2015

CONCLUSIÓN:

Para la función de dirección de aseguramiento de calidad de software BAI07 Gestionar la Aceptación del Cambio y de la Transición, se determinó que el valor de cumplimiento es de 15.98 puntos de 23 como máximo.

5.2.2 Informe de la evaluación de los controles

El Mejor Seguro. S.A.

Auditoría Interna

Guatemala, 02 de febrero de 2015

Licenciado:
Mario Granai Towson
Presidente
El Mejor Seguro S.A.
Ciudad

Estimado Licenciado Granai:

De conformidad con nuestro programa de auditoría, hemos concluido con la revisión de los procesos que determinaron el nivel de capacidad de los controles informáticos aplicados en el dominio de adquisición e implementación de tecnología informática. La revisión cubrió el periodo comprendido del 1 de julio al 31 de diciembre de 2014, fue realizada por el Sr. Erick Gonzalez durante el periodo del 12 al 30 de enero de 2015.

Nuestro trabajo de auditoría fue efectuado con base en los Objetivos de Control de Información y Tecnología Relacionada (COBIT, por sus siglas en inglés) y limitado al área de la Dirección de Tecnología.

Los resultados de los 7 procesos evaluados se describen a continuación:

Hallazgo:

1. Para el proceso de gestionar los programas y proyectos, se determinó que los controles se encuentran a un 66.12% de confiabilidad de acuerdo a los objetivos de control, la calificación fue de 3.306 siendo 5 la mejor.

Causa:

Existen deficiencias en la metodología de gestión de proyectos, como la definición de tiempo y estimación de recursos.

Efecto:

El alcance de los proyectos no cumple con la expectativa requerida por el negocio.

Recomendación:

Capacitación en gestión de proyectos y uso efectivo del tiempo a los administradores del área de informática.

Hallazgo:

2. Para el proceso de gestionar la definición de requisitos, se determinó que los controles se encuentran a un 72.24% de confiabilidad de acuerdo a los objetivos de control, la calificación fue de 3.612 siendo 5 la mejor.

Causa:

Los controles evaluados se ejecutan dentro de los límites mínimos definidos para alcanzar sus resultados.

Efecto:

La toma de requisitos presenta limitaciones que afectan en la satisfacción de las necesidades reales del negocio.

Recomendación:

Definición de plantillas con la suficiente información para cumplir a cabalidad con las necesidades del negocio

Hallazgo:

3. Para el proceso de adquirir e implementar infraestructura tecnológica, se determinó que los controles están a un 73% de confiabilidad, teniendo una calificación de 3.65 siendo 5 la mejor.

Causa:

Se cuenta con los controles mínimos para la evaluación de proveedores.

Efecto:

Inadecuada adquisición de servicios o equipos informáticos.

Recomendación:

Aplicación de estándares y controles para la evaluación de proveedores y requerimientos de equipo.

Hallazgo:

4. Para el proceso de gestionar la disponibilidad y la capacidad, se determinó que los controles están a un 53.89% de confiabilidad, teniendo una calificación de 2.694 siendo 5 la mejor.

Causa:

Las aplicaciones son complejas para los usuarios ya experimentados.

Efecto:

Excesivo tiempo en capacitación por cada nueva implementación.

Recomendación:

Evaluación de la usabilidad de las aplicaciones y definición de interacción mínima por parte de los usuarios.

Hallazgo:

5. Para el proceso de gestionar la introducción de cambios organizativos, se determinó que los controles están a un 70.93% de confiabilidad, teniendo una calificación de 3.546 siendo 5 la mejor.

Causa:

Los cambios de fondo no contemplan la aprobación de todas las áreas involucradas.

Efecto:

Resistencia al cambio por parte de los usuarios finales.

Recomendación:

Involucrar a todas las áreas afectadas cada vez que se decida un cambio.

Hallazgo:

6. Para el proceso de administración de cambios, se determinó que los controles están a un 78.37% de confiabilidad, teniendo una calificación de 3.918 siendo 5 la mejor.

Causa:

Los controles evaluados se ejecutan dentro de los límites definidos para alcanzar sus resultados.

Efecto:

Despliegue de cambios en producción con un margen mínimo de pruebas integrales.

Recomendación:

Creación de política y flujo para la gestión de cambios y despliegues a producción.

Hallazgo:

7. Para el proceso de aceptación del cambio y de la transición, se determinó que los controles están a un 70.92% de confiabilidad, teniendo una calificación de 3.546 siendo 5 la mejor.

Causa:

Los controles evaluados se ejecutan dentro de los límites mínimos definidos para alcanzar sus resultados.

Efecto:

Inversión de tiempo adicional por parte del negocio para la adaptación a los cambios implementados.

Recomendación:

Definición de actividades y tiempos máximos para cada implementación, así como entregables a corto plazo.

De los procesos descritos anteriormente se puede concluir que la empresa tiene una serie de controles que si se implementan adecuadamente pueden alcanzar un nivel óptimo de control de acuerdo la norma COBIT.

Por lo que se recomienda la adopción de la herramienta para poder aprovechar al máximo los controles que ya se tienen e implementar los necesarios para corregir las deficiencias encontradas en cada proceso.

La Auditoría Interna desea expresar su agradecimiento por la cooperación recibida durante la revisión por parte del personal y funcionarios de dicho departamento.

Atentamente,

Lic. Luis Maldonado.
Auditor Interno.

CONCLUSIONES

1. La alta dependencia de tecnologías de información que tiene la empresa aseguradora, hace que la inversión en sus recursos informáticos se vuelva indispensable para poder soportar todas las transacciones electrónicas que ofrece a sus clientes, por lo que debe normarse la gestión en la implementación de software.

2. La falta de conocimiento y aplicación de metodologías de control informático aceptadas internacionalmente, por parte del departamento de Auditoría Interna en una empresa aseguradora, que permita tener un mejor gobierno de la información que necesita la administración para la toma de decisiones, incide de forma negativa en el plan de alcanzar los objetivos estratégicos empresariales, ya que no se tendrá el retorno de inversión esperado.

3. La aseguradora no cuenta con un marco de trabajo con base a los Objetivos de Control para Información y Tecnología Relacionada (COBIT 5.0) que le permita implantar un gobierno de tecnología informática que proporcione las herramientas de control y monitoreo necesarias para minimizar los riesgos sobre la información.

4. De acuerdo a la evaluación del nivel de proceso de los controles informáticos en la empresa evaluada, se determinó que el departamento de informática no cuenta con el nivel suficiente en los procesos incluidos en el dominio de construcción, adquisición e implementación de tecnología informática de los objetivos de control para información y tecnología relacionada (COBIT 5.0).

RECOMENDACIONES

1. Se deben establecer políticas de gobierno para la integridad, seguridad y disponibilidad de la información, utilizando normativa aceptada internacionalmente para los procesos relacionados con las actividades del departamento de informática.

2. La Auditoría Interna de sistemas de información debe utilizar criterios de medición basados en estándares internacionales, tal como el modelo de procesos descrito por COBIT para la evaluación del cumplimiento de controles y criterios de calidad de la información proporcionada por el departamento de informática, con el objeto minimizar los riesgos asociados a la seguridad de la información.

3. Se debe evaluar el beneficio que conlleva la implementación de la metodología COBIT en la empresa aseguradora, con la finalidad de alinear los objetivos del departamento de informática con los objetivos estratégicos de la empresa.

4. La administración debe considerar las recomendaciones sugeridas por la Auditoría Interna con base a la metodología aplicada, para poder elevar el nivel en los procesos que conciernen al dominio de construir, adquirir e implementar software, dentro de la aseguradora.

REFERENCIAS BIBLIOGRÁFICAS:

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

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

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

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

5. DECLARACIÓN SOBRE NORMAS DE AUDITORÍA No.3, (1976). Traducción Autorizada del Statement of Auditing Standards, del American Institute of Certified Public Acountants, publicada por el Instituto Mexicano de Contadores Públicos, Primera Reimpresión.

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

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

8. NORMAS INTERNACIONALES DE AUDITORÍA, (2011). Emitidas por el Comité Internacional de Práctica de Auditoría (IFAC), publicadas por el Instituto Mexicano de Contadores Públicos.

9. Derecho 2-70 del Congreso de la República, Código de Comercio.

10. Decreto Ley 473, Constitución y Organización de Empresas de Seguros, modificado por el Decreto 32-90 del Congreso de la República.

11. Decreto 854, Ley de Inversiones y Reservas Técnicas y Matemáticas de las Compañías de Seguros.

12. Decreto Ley 154-83, Cuota Anual de Sostenimiento de la Superintendencia de Bancos.

13. Acuerdo Gubernativo del Ministerio de Economía No. 22-74, Reglamento de la Ley de Inversiones de Reservas Técnicas y Matemáticas de las Empresas de Seguros.

14. Acuerdo Gubernativo del 14 de agosto de 1969, Reglamento del Decreto 473, Constitución y Organización de Empresas de Seguros.

15. Acuerdo Gubernativo del Ministerio de Economía No. 198-93, Reglamento del Riesgo de Terremoto sobre Cobertura, Cúmulos, Reaseguro Catastrófico y Reserva Específica.

16. Decreto 53-79 del Organismo Legislativo. Fija tasa máxima de interés sobre los préstamos que concedan las aseguradoras a sus asegurados con garantía de sus pólizas.

17. Acuerdo Gubernativo No. 637-91, Reglamento para la promoción y el desarrollo de operaciones de fideicomiso por las empresas de seguros.

18. Acuerdo Gubernativo del Ministerio de Economía No. 5-79, Reglamento para la Aprobación y Control de Tarifas de Seguros del ramo de Daños.

19. Acuerdo Gubernativo del Ministerio de Economía No. 67-90. Establece el seguro para transporte especializado de productos derivados del petróleo en forma obligatoria.

20. Decreto 1422, Impuesto a favor del Cuerpo Voluntario de Bomberos de Guatemala.

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

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

23. Constitución Política de la República de Guatemala.

24. Código de Trabajo, Decreto número 1441 y sus reformas.

25. Código Tributario, Decreto número 6-91 y sus reformas.

26. Ley de registro tributario unificado y control general de contribuyentes, Decreto número 25-71.

27. Ley del impuesto al valor agregado, Decreto número 27-92 y sus reformas.

28. Reglamento de la ley del impuesto al valor agregado, acuerdo gubernativo número 424-2006 y sus reformas.

29. Ley de Timbres y de papel sellado especial para protocolos, Decreto número 37-92.

30. Reglamento del impuesto de timbres fiscales y de papel sellado especial para protocolos, Acuerdo Gubernativo número 737-92.

31. Ley de actualización tributaria, Decreto número 10-2012.

WEBGRAFÍA

32. Asociación de Auditoría y Control de Sistemas Informáticos (ISACA siglas en ingles). Disponible en www.isaca.org/cobit

33. Instituto de Auditoría Interna (IIA siglas en ingles). Disponible en www.theiia.org

34. Instituto de Gobierno de Tecnología Informática (ITGI siglas en ingles). Disponible en www.itgi.org

35. Normas Generales para la Auditoría de los Sistemas de Información. Disponible en: www.isaca.org.pe/normas.htm

36. Superintendencia de bancos. Leyes aplicables a una aseguradora. Disponible en: http://infpb.sib.gob.gt/Leyes/