Estructuración del manual de programas de auditoría en tecnología de la información de ISA

Trabajo de grado para optar por el título de Ingeniero en Informática

Simón Granados Acevedo

Asesor

Camilo Ernesto Restrepo Ramírez

Ingeniero de Sistemas

Corporación Universitaria Lasallista
Facultad de Ingenierías
Ingeniería Informática
Caldas – Antioquia
2014

Resumen

Para llevar a cabo el proceso de Auditoría se requiere de una planeación en la que esté especificado que proceso del área será auditado y de qué manera se evaluará, por este motivo se creará un manual de auditorías que contiene unas guías con un paso a paso de pruebas para evaluar, revisar y verificar los principales procesos del área de TI, para esto se identifican y definen riesgos de TI y se relacionan con los controles propuestos en el modelo Cobit.

Palabras Clave: Amenaza, Riesgo, Control, Cobit, Auditoría, ISO, Prueba, Tecnologías de la información.

Abstract

To carry out the audit process it requires a planning in which it is specified what process area will be audited and how it is evaluated, for this reason will be created an audit manual that contain guides with a step by step of tests to evaluate, review and verify the major area IT processes, for this are identified and defined iT risks and associated with controls proposed in the Cobit model.

Keywords: Threat, Risk, Control, Cobit, Audit, ISO, Testing, Information technologies.

Las organizaciones tienen metas que lograr contempladas en su misión y visión, para llegar al cumplimiento de estas se tienen que enfrentar a un entorno que las obliga a buscar diariamente oportunidades de mejora en la realización de sus procesos, buscando ventajas competitivas en el mercado. Por tal motivo se propone la auditoría interna como actividad independiente y objetiva que debe estar en actualización permanente, buscando las mejores prácticas y procedimientos que ayuden a ser más eficiente la labor del auditor en la organización, permitiendo agregar valor y mejorar las operaciones de la misma.

Contenido

Lista de Ilustraciones

Lista de Tablas

Justificación

Dentro del proceso de certificación del área de auditoría de ISA se requiere iniciar un trabajo de estructuración de un manual que contenga los programas de auditoría en tecnologías de la información (Informática) que permita lograr una estandarización a nivel de objetivos y pruebas a desarrollar.

Objetivos

Objetivo General

Estructurar el programa de pruebas de auditorías con la realización de un manual en el que se proporcionen herramientas de control para la auditoria de tecnología de la información con el que se pueda evaluar la gestión de riesgos y alimentar el banco de pruebas en el sistema de información Audisoft.

Objetivos Específicos

Recopilar información de los riesgos y procesos de TI en ISA en trabajo conjunto con el área de TI.

Identificar y describir los riesgos de TI junto con las amenazas que llevarían a la materialización de tales riesgos.

Relacionar riesgos con los controles de los modelos a trabajar.

Definir guías de auditoría después de una priorización de controles.

Alimentar el banco de pruebas de auditoría de la organización en el área de TI.

Marco Teórico

Cobit:

> Objetivos de Control para Información y Tecnologías Relacionadas, ofrece una visión del negocio de extremo a extremo del gobierno empresarial de TI que refleja el papel central de la información y la tecnología en la creación de valor para las empresas. (ISACA, 2012)

Sistema de Control Interno:

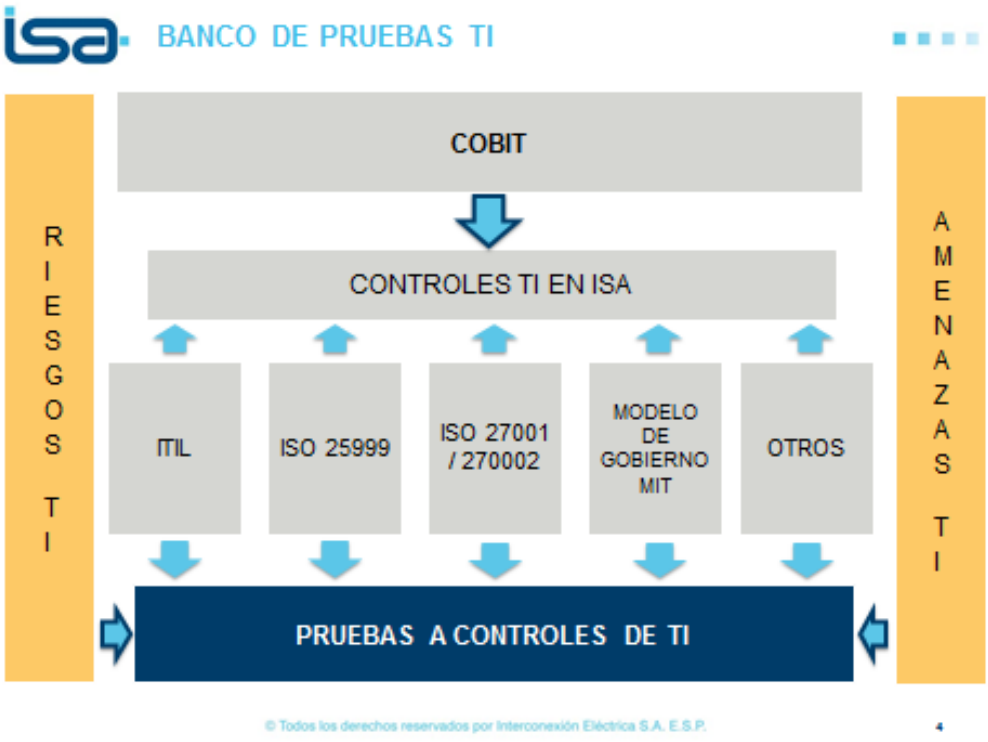
> Conjunto de elementos de una Organización (recursos, sistemas de información, procesos, cultura, normatividad, estructura, metas, etc.), que tomados integralmente apoyan a las personas en el logro de los objetivos empresariales. (Transelca, 2012)

Auditoría interna:

> Es una actividad independiente y objetiva de evaluación 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 efectividad y eficiencia de los procesos de gestión de riesgos, control interno y gobierno corporativo. (Instituto de Auditores Internos, 2004)

Metodología

Ilustración 1 Banco de pruebas de TI.



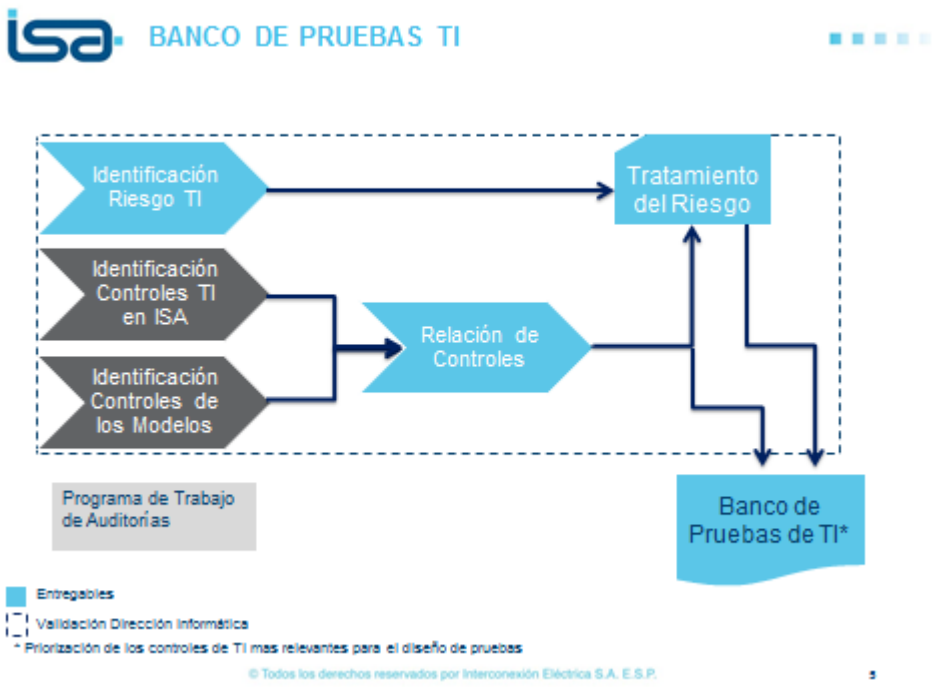
Se comienza con una lectura de revisión de los principales documentos de TI y Auditoría de la organización para establecer un marco de referencia y contexto para el trabajo de práctica, luego se hace una revisión muy profunda del modelo Cobit en su versión 5, identificando y consultando las principales diferencias o cambios que tiene respecto a la versión 4.1 para así realizar un mapeo de los procesos que se proponen en dicho modelo y de esta manera trabajar con la última versión; Cobit al igual que ISA, trabaja con el cuadro de gestión integral y sus perspectivas financiera, cliente, procesos y aprendizaje; por tal motivo el modelo es acorde con la organización.

En trabajo conjunto con la dirección de informática de la organización se revisan los riesgos ya existentes y definidos por la dirección, para realizar una identificación de amenazas que conllevarían a la materialización de dichos riesgos, igualmente se realiza una descripción de cada riesgo para que este sea de fácil entendimiento a los interesados.

El nombre de algunos riesgos es modificado para una mayor claridad de su significado y evitar confusiones en su interpretación, después de este proceso se identifica un nuevo riesgo referente a la gestión de proyectos de TI; cada riesgo de TI es asociado al riesgo corporativo en el que se vería reflejado.

Se realiza una relación de los controles propuestos en Cobit con los que cuentan el Área de TI en ISA, para que de esta manera haya concordancia en los temas y se "hable en un mismo idioma" así en un futuro las pruebas a realizar se puedan usar en todo el grupo empresarial.

Ilustración 2 Metodología de trabajo.



Luego se procede a realizar una relación entre los riesgos, los procesos y objetivos de control propuestos en Cobit 5 para identificar cuáles de estos podrían mitigar el riesgo.

De igual manera se realiza una relación entre los controles propuestos en ISO27002 y los Procesos de Cobit 5, para concluir con que control se mitiga determinado riesgo.

Revisando los controles de estos modelos se pasa a identificar algunos controles que proponen otros modelos como ITIL, BS 25999, ISO 27001 entre otros en los que se aborda a profundidad procesos que Cobit no cubre de manera completa.

Se priorizan los procesos que son más importantes para la realización de una guía de auditoría, para esto se tienen en cuenta las auditorías realizadas previamente en la organización y en cuales se evidencia la necesidad de crear un manual con guías y pruebas.

Desarrollo del Tema.

Al realizar la revisión del modelo Cobit en su versión 5 se identifica un nuevo dominio además de la modificación del nombre de los ya existentes en relación con la versión de Cobit 4.1.

Dicho dominio es el llamado Evaluar, Dirigir y Monitorear (EDM) el cual está enfocado hacia el Gobierno de TI.

Los nuevos nombres adoptados son:

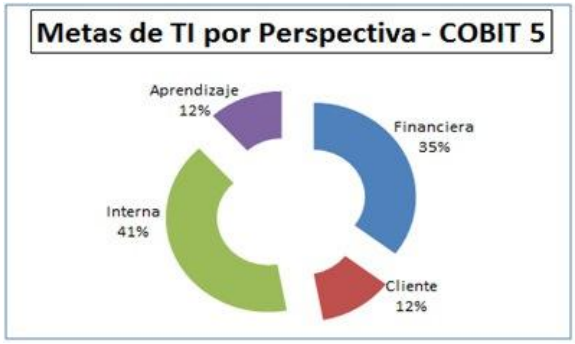
Tabla 1 Dominios Cobit.

COBIT 4.1	COBIT 5
PO-Planear y Organizar.	APO-Alinear, Planificar y Organizar.
AI-Adquirir e Implementar.	BAI-Construir, Adquirir e Implementar.
DS-Entregar y Dar Soporte.	DSS-Entregar, dar Servicio y Soporte.
ME-Monitorear y Evaluar.	MEA-Supervisar, Evaluar y Valorar.

La cantidad de procesos dela versión 4.1 a la versión 5 han pasado de ser 34 a 37.

Respecto a las metas de TI se han disminuido a 17, antes eran 28 y cada una de estas metas corresponde a una perspectiva del cuadro de gestión integral.

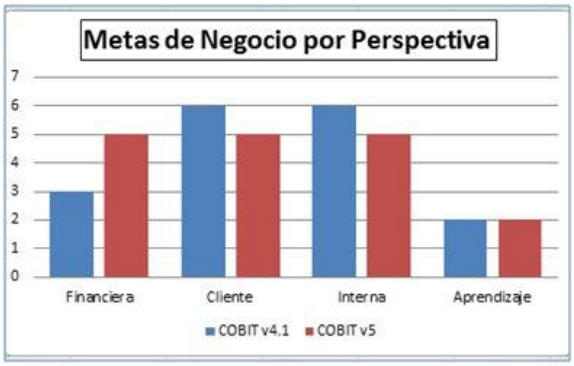
Ilustración 3 Metas de TI.



Fuente: ISACA.

Al hablar de las metas del negocio se identifica que continúan siendo 17 y se ha asignado cada una a las perspectivas del cuadro de gestión integral.

Ilustración 4 Metas de negocio.



Fuente: ISACA.

Riesgos Identificados en ISA

R1. Iniciativas del área de TI no acordes con la estrategia del negocio.

R2. Inadecuado cumplimiento del Gobierno TI.

R3. Bajo Nivel de Utilización de la TI como ventaja competitiva.

R4. Infraestructura de TI no compatible con la definida.

R5. Inadecuada relación costo-beneficio de la tecnología.

R6. Falta de Habilidades para adquirir y desarrollar las TI´s.

R7. Falta de Disponibilidad, confidencialidad e integridad de la información.

R8. Desconocimiento de los requerimientos de usuario.

R9. Deficiencia en los Servicios y/o infraestructura que intervienen en el ciclo de vida de la información.

R10. Uso indebido de la información y/o de los servicios que la suministran, procesan y/o transmiten.

R11. Inadecuada gestión de proveedores de TI.

R12. Fraude Electrónico.

R13. Ataques informáticos.

R14. Incumplimiento a los niveles de servicio de TI.

R15. Procedimientos informales.

R16. Inadecuado monitoreo de la gestión de TI.

R17. Fallas o errores en los procedimientos.

Al desarrollar la identificación de amenazas para cada uno de los riesgos se llegó a la conclusión de suprimir el riesgo 17 Ataques Informáticos, puesto que este se interpreta más como una amenaza que como un riesgo, en especial una amenaza asignada al riesgo 7 Falta de Disponibilidad, Confidencialidad e Integridad de la Información.

Se decide modificar el nombre del riesgo 6 a Falta de competencias para gestionar la TI, puesto que este se refiere más a las competencias de los recursos humanos de TI.

De igual manera se modifica el nombre del riesgo 4 agregando una palabra “Infraestructura/Soluciones de TI no compatibles con la definida”, ya que la palabra Soluciones

es utilizada en la organización para referirse a todo lo referente con TI y de esta manera ampliar el alcance del riesgo más allá de solo equipos de TI (Infraestructura).

Finalmente se identifica un riesgo nuevo el cual es llamado Inadecuada Gestión de proyectos de TI, y que fue asignado al Riesgo 13.

Identificación de amenazas, definición y actualización de riesgos de TI:

Tabla 2 Riesgo, definición y amenazas.

Riesgo TI	Definición	Amenazas
R1. Iniciativas del área de TI no acordes con la estrategia del negocio.	Se refiere a las propuestas de TI que estén fuera del contexto del grupo empresarial y que no aportan al cumplimiento de los objetivos estratégicos y de negocio que este tiene.	Déficit de personal idóneo, Rendimiento no esperado, mal uso de recursos de TI, falla en confidencialidad de la información, corrupción de datos, problemas legales.
R2. Inadecuado cumplimiento del Gobierno TI.	Se refiere al desconocimiento, incumplimiento o no aceptación por parte de la organización a lo establecido por el responsable de la TI en el grupo, lo cual puede llevar a la materialización de otros riegos en sus modelos decisional, organizacional y económico.	Compra y uso ilegal de software, Fugas o perdidas de información confidencial, Uso inadecuado o no autorizado de equipos y software, Error operacional de personal, abuso de derechos de usuario, inadecuado manejo de

		información confidencial o restringida, aplicación indebida de normas y procedimientos.
R3. Bajo Nivel de Utilización de la TI como ventaja competitiva.	Se refiere al desaprovechamiento de los recursos que proporciona TI para generar una ventaja competitiva del grupo empresarial, disminuyendo el potencial de agregación de valor de la TI.	Falta de capacitación del personal, resistencia al cambio, las soluciones informáticas no soportan suficientemente las necesidades del proceso.
R4. Infraestructura/Soluciones de TI no compatibles con la definida.	Se refiere a los inconvenientes o incompatibilidades al adquirir e incorporar productos o servicios de las Tecnologías de la Información con la arquitectura definida en la empresa. Igualmente se refiere a la falta de definiciones de la arquitectura de las TIC's que debe tener la empresa.	Falta de entendimiento de la solución informática, las compras de soluciones son descentralizadas (Falta de gobierno), la arquitectura tecnológica no está claramente definida, Incompatibilidad con SAP, errores en la operación de un equipo o software, incompatibilidad de

		periféricos con un equipo, mal uso de recursos.
R5. Inadecuada relación costo-beneficio de la tecnología.	Se refiere a las decisiones económicas en la adquisición de bienes y servicios de las TIC´s las cuales no generan un valor o beneficio mayor al de su inversión.	Decisiones tecnológicas que no contribuyen a la agregación de valor del negocio.
R6. Falta de competencias para gestionar la TI.	Se refiere a la falta de competencia y experiencia del recurso humano para planear, desarrollar, adquirir, administrar y evaluar las Tecnologías de la Información acorde a la estrategia definida para compañía.	Error operacional del personal, errores de usuario, Manipulación de datos inadvertida, Rendimiento no esperado, déficit de personal idóneo.
R7. Falta de Disponibilidad, confidencialidad e integridad de la información	Se refiere a los eventos o incidentes que se pueden presentar en toda la cadena de valor en la Gestión de Tecnologías de la Información y Comunicaciones afectando de manera directa los activos de	Ataque informático, falla de energía, acceso no autorizado, fenómeno natural, ataque terrorista, degradación en tiempo de respuesta, rendimiento no esperado, perdida de

	información (datos y elementos que permiten procesarlos, almacenarlos y protegerlos), a continuación se mencionan algunos incidentes que materializan dicho riesgo: a) Perdida de la información. b) Inexactitud o insuficiencia de información c) Daño de información. d) Robo de información. e) Perdida de acceso a la información que se requiere.	información, demoras en el restablecimiento, fallas en la restauración de la infraestructura, información y servicios, daños accidentales como fugas de agua, falta de aire acondicionado, extremos de temperaturas y humedad, campos magnéticos potentes, contaminación por polvo, daño durante mantenimientos o adecuación de infraestructura, sabotaje.
R8. Desconocimiento de los requerimientos de usuario.	Se refiere a la falta de comunicación e interacción que tiene TI con sus usuarios finales, en todas las etapas del ciclo de vida en la incorporación de las tecnologías de la información, obteniendo productos y servicios	Rendimiento no esperado, Insatisfacción del usuario, entrega de servicios equivocados, mala distribución de recursos de TI, pérdida de credibilidad.

	no deseados por el usuario final, Igualmente se refiere a la inadecuada gestión de atención de requerimientos.	
R9. Deficiencia en los Servicios y/o infraestructura que intervienen en el ciclo de vida de la información.	Se refiere a la falta de cumplimiento de los controles establecidos para incorporar, desarrollar, administrar los ambientes de desarrollo, prueba y productivo de los sistemas de información y cambios que se realicen a los datos y aplicaciones.	Comunicaciones equivocas, mal uso de recursos, uso inapropiado de los sistemas de información, abuso de derechos de usuario y administrador, incumplimiento de los controles que intervienen en el ciclo de vida de la información, error operacional, interrupción o negación del servicio.
R10. Uso indebido de la información y/o de los servicios que la suministran, procesan y/o transmiten.	Se refiere a la manipulación de la información sin la debida autorización en el registro, procesamientos y comunicación de la información.	Manipulación de datos o software, Uso no autorizado o inapropiado de medios de almacenamiento y de software, Infiltración y re-ruteo de comunicaciones,

		Robo de datos, Copia no autorizada de información, Falla para recibir información, Corrupción de datos, inexactitud e insuficiencia de la información, bajo desempeño, bloqueos e incapacidad de procesar la información.
R11. Inadecuada gestión de proveedores de TI.	Se refiere al incumplimiento de los procedimientos definidos por la compañía para las etapas precontractual, contractual y pos contractual con el proveedor. Mantener una inadecuada relación con el proveedor No realizar las gestiones pertinentes para lograr el cumplimiento adecuado de los servicios y/o productos adquiridos.	Robo de equipos o software, incumplimiento de entregas y/o pagos, software ilegal, negación del servicio, explotación de debilidades de TI, incumplimiento contractual, malas relaciones con proveedores, Manipulación de la información, falta de oportunidad del proveedor, error en la gestión

		contractual, falla en suministro de repuestos.
R12. Fraude Electrónico.	Se refiere a la falta de ética que puede llegar a ocurrir en un proceso por parte del responsable u otra persona ajena a este para manipular, sustraer información con fines de obtener beneficios económicos.	Manipulación de datos o software, Uso de software por usuarios no deseados y en forma indebida, suplantación de usuario, Infiltración de comunicaciones, uso ilegal de software, abuso de derechos del usuario, eliminación de datos, robo de información, modificaciones en los registros, asociación para delinquir.
R13. Inadecuada Gestión de proyectos de TI	Se refiere a la poca o no existente gestión de proyectos en sus etapas de planeación, ejecución, cierre y puesta en operación que puede llevar al incumplimiento de los objetivos, presupuestos y tiempos	Comunicaciones equivocas, uso inapropiado de equipos, error operacional del personal, coacción al personal, falla para recibir información, falla de

	trazados en el proyecto.	usuario, rendimiento no esperado, desalineación del proyecto con la estrategia del negocio, falta de supervisión, control y seguimiento a los planes trazados en el proyecto, inadecuada asignación de recursos, falta de gestión a los riesgos del proyecto.
R14. Incumplimiento a los niveles de servicio de TI.	Se refiere al bajo desempeño de los servicios de TI para responder a las necesidades y acuerdos establecidos con los clientes de la TI en la organización.	Tiempo de respuesta lento, falta de disponibilidad de la información, mal uso de recursos de TI, interrupción del servicio durante mantenimiento, instalación o actualización de equipos o software.
R15. Procedimientos informales.	Se refiere a la ejecución de procedimientos de TI que no se encuentran debidamente documentados y son realizados	Falta de estandarización formal de los procesos, Falta de documentación en los resultados de los procesos,

	discrecionalmente por el conocimiento de su responsable, así mismo la falta de documentación de los resultados que arroja el proceso impidiendo su trazabilidad y evidencia de su ejecución.	Aplicación discrecional de normas y procedimientos
R16. Inadecuado monitoreo de la gestión de TI.	Se refiere al bajo nivel de supervisión y medición del desarrollo de los procesos y gestión que realiza TI, la cual puede llevar a fallas y a un rendimiento bajo de sus servicios.	Debilidad o falta de monitoreo y verificación en los aspectos críticos de los procesos. Falta de seguimiento a los mejoramientos identificados, dificultad para verificar, validar y detectar fallas, Falta de medición y/o monitoreo a los servicios de la TI.
R17. Fallas o errores en los procedimientos.	Se refiere a los posibles errores y fallas que puedan ocurrir en los procesos y actividades que se desarrollan desde TI y que pueden	Falla para respaldar datos y en cambios de contraseñas, falta de disponibilidad, degradación en tiempo de

	llevar a la falta de disponibilidad del servicio o información.	respuesta, falla para recibir información, errores de usuarios y errores operacionales del personal.

Cada riesgo es relacionado con un proceso de Cobit, por lo tanto los objetivos de control que trae consigo cada proceso son asignados también al riesgo para el desarrollo de las guías.

De igual manera cada riesgo identificado en TI es relacionado a un riesgo corporativo para que se evidencie más ampliamente el alcance que posee.

Y finalmente después de un análisis con el área de riesgos de lo realizado se decide además de definición del riesgo y amenaza, identificar la consecuencia que traería a la organización la materialización del riesgo.

Para la elaboración de las guías de auditoria, se identificaron principalmente las siguientes y se han asignado a cada una los procesos de Cobit que se consideraron pertinentes:

- Guía de Gestión de Cambios:

  BAI06. Administrar cambios de TI.

  BAI07. Aceptar e incorporar cambios de TI.

- Guía de Gestión de Gobierno de TI:

  EDM01. Establecer y mantener el marco de Gobierno de TI.

  APO01. Administrar Marco de gestión TI.

  APO02. Administrar la estrategia de TI.

- Guía de Plan de Contingencia de TI:

  DSS02. Administrar requerimientos de servicio e incidentes de TI.

  DSS03. Administrar problemas de TI

  DSS04. Administrar continuidad de TI.

  DSS06. Administrar controles de procesos de TI.

- Guía de Gestión de Proveedores:

  APO10. Administrar proveedores de TI.

- Guía de Gestión de Seguridad de la Información:

  APO13. Administrar seguridad informática.

  DSS05. Administrar servicios de seguridad de TI.

  Guía de Evaluación al Sistema de Gestión de Seguridad de la Información ISO 27001.

  Guía de Evaluación de Controles de Seguridad de la Información ISO 27002.

- Guía de Gestión de Proyectos:

  BAI01. Administrar programas y proyectos de TI.

- Guía de Gestión de Soluciones de TI:

  BAI03. Identificar y construir soluciones de TI.

En el caso de la siguiente guía se tomó como referencia una guía ya existente para dicha evaluación.

- Guía de Evaluación de la Seguridad de SAP:

  1.5.1 Procedimientos de Seguridad.

  1.5.2 Estándares de Seguridad.

  1.5.3 Segregación de funciones.

1.5.4 Pruebas generales.

1.5.5 Cambio de clave a las cuentas por defecto.

1.5.6 Revisar esquema de transportes.

Igualmente para la guía de licenciamiento se toman los controles de una guía ya implementada y adicionalmente se agrega un objetivo de control de Cobit.

- Guía de Evaluación al Licenciamiento de Software:

1. Inventario de software autorizado.
2. Inventario periódico de software instalado.
3. Comparativo software instalado vs autorizado.
4. Control de licencias.
5. Gestión de software no licenciado.
6. Autorización para la instalación de software.

BAI09. Administrar activos de TI.

BAI09.05 Administrar licencias.

Para la siguiente guía se tomó cada dominio como una guía diferente en la que se evalúan todos los aspectos de cada objetivo de control de manera resumida.

- Guía de Gestión de TI:

Guía de Gestión de TI APO.

Guía de Gestión de TI BAI.

Guía de Gestión de TI DSS.

Guía de Gestión de TI MEA.

El contenido de cada guía consta de los siguientes ítems:

El nombre de la guía y un código que se forma con la letra G y el número asignado, ej. G-0001.

El objetivo donde básicamente se especifica lo que se pretende evaluar, revisar o verificar en cada guía.

El alcance que describe la profundidad de cada guía en el tema a evaluar y los principales temas que se trataran.

Los dominios de Cobit que tienen relación con la guía que de igual manera son los procesos del área de TI en los que se ubica el objetivo de la auditoría.

El o los procesos de Cobit de donde se basa el contenido de la guía.

El o los riesgos relacionados a la guía, teniendo en cuenta la relación Riesgos-Procesos realizada anteriormente.

La información necesaria, son los documentos que se recomienda solicitar para revisar o verificar y que son los mismos que se encuentran en los SIPOC (Supplier – Inputs- Process- Outputs – Customers) de los procesos de TI.

Finalmente se encuentra el control y su código, el nombre y código de la prueba y los ítems de cada prueba con el “Que hacer” al momento de aplicar la guía.

Resultados.

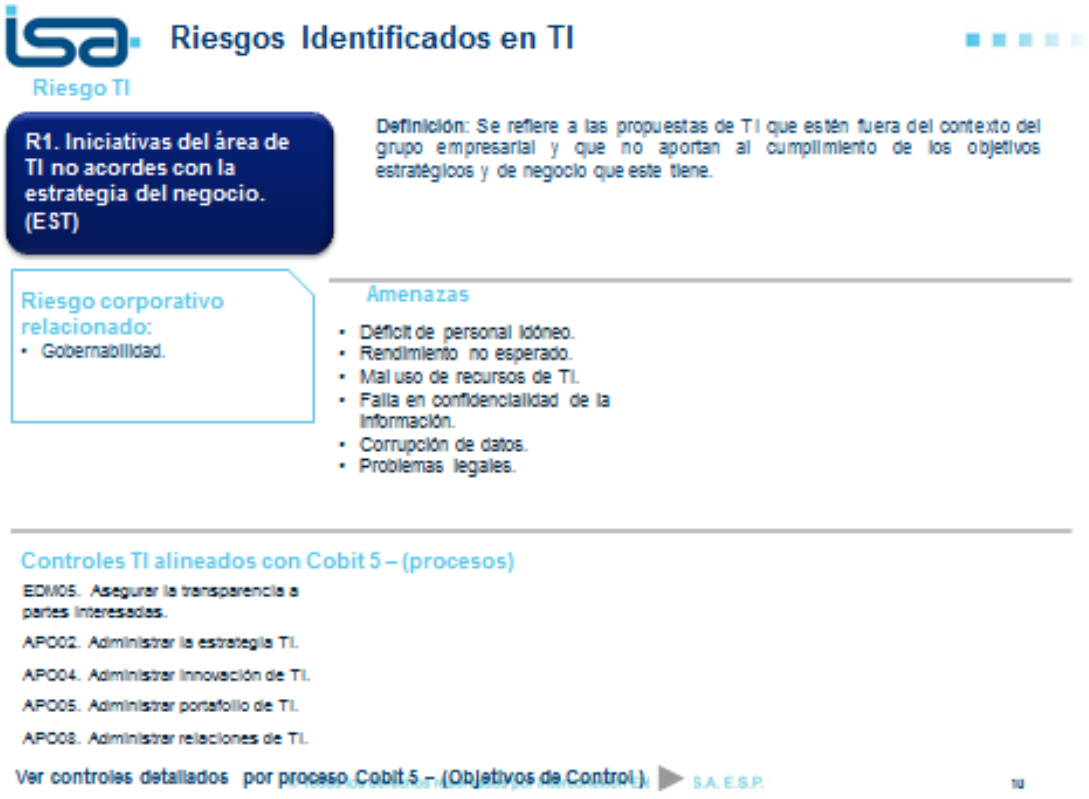
Se realiza una hoja de cálculo en Excel donde para cada uno de los 17 riesgos se encuentra una sigla identificadora, la definición del riesgo, relación con el riesgo corporativo, amenazas y consecuencias de dicho riesgo.

Ilustración 5 Definición de riesgos.

	Riesgo TI	ID Riesgo	Definición Riesgo	Amenazas	Riesgo Corporativo	Consecuencia
R2	**Inadecuado cumplimiento del Gobierno TI**	GOB	Se refiere al desconocimiento, incumplimiento o no aceptación por parte de la organización a lo establecido por el responsable de la TI en el grupo, lo cual puede llevar a la materialización de otros riegos en sus modelos decisional, organizacional y económico	Compra y uso ilegal de software, Fugas o perdidas de información confidencial, Uso inadecuado o no autorizado de equipos y software, Error operacional de personal, abuso de derechos de usuario, inadecuado manejo de información confidencial o restringida, aplicación indebida de normas y procedimientos.	Gobernabilidad (GO)	-Perdida de información relevante para el soporte o gestión del negocio por la incompatibilidad en los sistemas de información y la falta de tener una arquitectura de hardware y software homogénea para la compañía. -Sobre costos por la falta de aprovechamiento de economías de escala.
R3	**Bajo Nivel de Utilización de la TI como ventaja competitiva**	USO	Se refiere al desaprovechamiento de los recursos que proporciona TI para generar una ventaja competitiva del grupo empresarial, disminuyendo el potencial de agregación de valor de la TI.	Falta de capacitación del personal, resistencia al cambio, las soluciones informáticas no soportan suficientemente las necesidades del proceso.	Gobernabilidad (GO), Crecimiento(CR)	-Uso ineficiente del recurso humano, el cual esta desaprovechando facilidades que puedan optimizar sus tiempos. - Perdida de información catalogada como crítica por el no uso eficiente de los recursos entregados por la Gestión de TI, ej. Manejo de información en los equipos de escritorio(usuario final) de manera informal.
R4	**Infraestructura/Soluciones de TI no compatibles con la definida**	TEC	Se refiere a los inconvenientes o incompatibilidades al adquirir e incorporar productos o servicios de las Tecnologías de la Información con la arquitectura definida en la empresa. Igualmente se refiere a la falta de definiciones de la arquitectura de las TIC´s que debe tener la empresa.	Falta de entendimiento de la solución informática, las compras de soluciones son descentralizadas(Falta de gobierno), la arquitectura tecnológica no esta claramente definida, Incompatibilidad con SAP, errores en la operación de un equipo o software, incompatibilidad de periféricos con un equipo, mal uso de recursos.	Falla o falta de equipos (FE)	- Perdida de información catalogada como crítica por la incompatibilidad de los sistemas de información. -Indisponibilidad de sistemas de información catalogados como críticos para el soporte y core del negocio por causa de la degradación del funcionamiento de una arquitectura de hardware y software no homogénea. -Perdida de integridad de la información catalogada como crítica, debido a las dificultades de comunicación o compatibilidad entre los sistemas de información.
R5	**Inadecuada relación costo-beneficio de la tecnología**	COS	Se refiere a las decisiones económicas en la adquisición de bienes y servicios de las TIC´s las cuales no generan un valor o beneficio mayor al de su inversión.	Decisiones tecnológicas que no contribuyen a la agregación de valor del negocio.	Crecimiento (CR)	-Gastos mayores en la adquisición de recursos de hardware y software que no generan valor, optimizan o mejoran un proceso del negocio o en su defecto su costo es superior a los beneficios que aporta el proceso.
R6	**Falta de competencias para gestionar la TI**	RH	Se refiere a la falta de competencia y experiencia del recurso humano para planear, desarrollar, adquirir, administrar y evaluar las Tecnologías de la Información acorde a la estrategia definida para compañía.	Error operacional del personal, errores de usuario, Manipulación de datos inadvertida, Rendimiento no esperado, déficit de personal idóneo.	Capital humano(CH), Falla humana (FH)	-Faltas a la disponibilidad, integridad y confidencialidad de la información catalogada como críticas debido al mal manejo o falta de conocimiento en la administración de la TI de la organización.
R7	**Falta de Disponibilidad, confidencialidad e integridad de la información**	INF	Se refiere a los eventos o incidentes que se pueden presentar en toda la cadena de valor en la Gestión de Tecnologías de la Información y Comunicaciones afectando de manera directa los activos de información(datos y elementos que permiten procesarlos, almacenarlos y protegerlos), a continuación se mencionan algunos incidentes que materializan dicho riesgo: a)perdida de la información, b) inexactitud o insuficiencia de información, c) daño de información, d) robo de información e) perdida de acceso a la información que se requiere.	Ataque informático, falla de energía, acceso no autorizado, fenómeno natural, ataque terrorista, degradación en tiempo de respuesta, rendimiento no esperado, perdida de información, demoras en el restablecimiento, fallas en la restauración de la infraestructura, información y servicios, daños accidentales como fugas de agua, falta de aire acondicionado, extremos de temperaturas y humedad, campos magnéticos potentes, contaminación por polvo, daño durante mantenimientos o adecuación de infraestructura, sabotaje.	Reputacional (RP), Fenómenos naturales (FN), Sociopolítico (SP)	-Indisponibilidad de la información catalogada como crítica ocasionada por ataques informáticos, daños a la infraestructura, bajo desempeño de la infraestructura (equipos de red, servidores, bases de datos, Sistemas de información), errores humanos. - Perdida de reputación por la no prestación del servicio, la fuga de información de carácter confidencial que comprometa los interés de la compañía, suministro de información errónea a los diferentes públicos de interés. - Perdida de negocios relevantes para el crecimiento de la organización debido a la fuga de información de ofertas y/o convocatoria a las que se este presentando. -Perdida, daño o duplicidad de la información catalogada como crítica debido a fallas en la integridad de esta por motivos de manipulación, sistemas de información no compatibles, cambios no autorizados, entre otros.
R8	**Desconocimiento de los requerimientos de usuario**	REQ	Se refiere a la falta de comunicación e interacción que tiene TI con sus usuarios finales, en todas las etapas del ciclo de vida en la incorporación de la tecnologías de la información, obteniendo productos y servicios no deseados por el usuario final, Igualmente se refiere a la inadecuada gestión de atención de requerimientos. .	Rendimiento no esperado, Insatisfacción del usuario, entrega de servicios equivocados, mala distribución de recursos de TI, perdida de credibilidad.	Reputacional (RP), Incumplimientos contractuales (IC)	- Indisponibilidad, falta de integridad y falta de confidencialidad de la información crítica del proceso, debido al desconocimiento o falta de consideración de las características que requiere el usuario para el manejo de su información. Estos aspectos hacen que la Gestión de TI no dimensione adecuadamente sus servicios acorde a las necesidades del usuario. - Sobre costos y extra tiempos debido al reproceso en el desarrollo de las soluciones.
R9	**Deficiencia en los Servicios y/o infraestructura que intervienen en el ciclo de vida de la información**	CVI	Se refiere a la falta de cumplimiento de los controles establecidos para incorporar, desarrollar, administrar los ambientes de desarrollo, prueba y productivo de los sistemas de información y cambios que se realicen a los datos y aplicaciones .	Comunicaciones equivocas, mal uso de recursos, uso inapropiado de los sistemas de información, abuso de derechos de usuario y administrador, incumplimiento de los controles que intervienen en el ciclo de vida de la información, error operacional, interrupción o negación del servicio.	Reputacional (RP)	- Sobre costos y reprocesos en las soluciones informáticas críticas al negocio por no mantener la debida diligencia en el ciclo de vida y desarrollo de los sistemas de información. -Daños a la integridad de la información catalogada como crítica debido a la manipulación de sistemas de información y datos en los ambientes de producción.

Se entrega a la Dirección de Informática y a la Dirección de Auditoría una ficha por riesgo donde se incluyen los ítems que están en la hoja de cálculo antes mencionada.

Ilustración 6 Plantilla de riesgos.



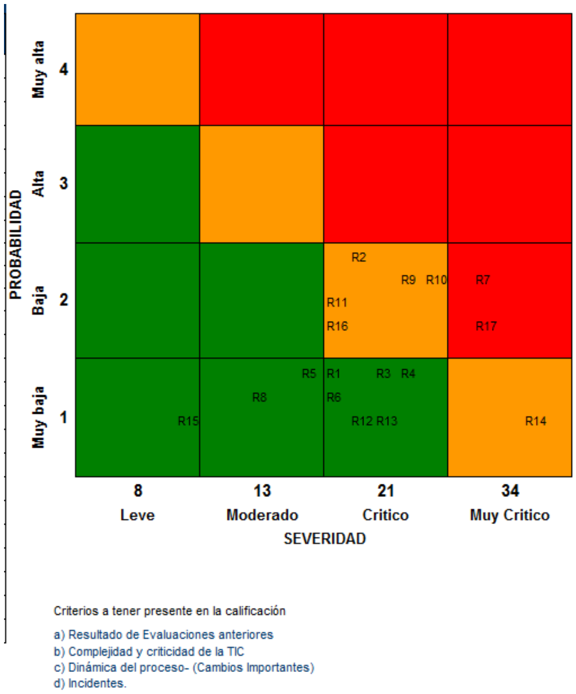
En una hoja de Excel se deja explícitamente la relación realizada entre riesgos y los 37 procesos de Cobit, por tanto con los objetivos de control propuestos en cada proceso.

Ilustración 7 Relación procesos y riesgos

Proces	Nombre Proce	Codigo Actividad	Actividad	Riesgo(s) Mitigado(s)
EDM01	Establecer y Mantener el Marco de Gobierno de TI	EDM01.01	Evaluar el sistema de gobierno	R2
		EDM01.02	Orientar el sistema de gobierno	
		EDM01.03	Supervisar el sistema de gobierno	
EDM02	Asegurar la Entrega de Beneficio	EDM02.01	Evaluar la optimización del valor	R5
		EDM02.02	Orientar la optimización del valor	
		EDM02.03	Supervisar la optimización del	
EDM03	Asegurar la Optimización del Riesgo de TI	EDM03.01	Evaluar la gestión de riesgos	R16
		EDM03.02	Orientar la gestión de riesgos	
		EDM03.03	Supervisar la gestión de riesgos	
EDM04	Asegurar la Optimización del Recurso de TI	EDM04.01	Evaluar la gestión de recursos	R5
		EDM04.02	Orientar la gestión de recursos	
		EDM04.03	Supervisar la gestión de recursos	
EDM05	Asegurar la transparencia a Partes Interesadas	EDM05.01	Evaluar los requisitos de elaboración de informes de las partes interesadas.	R1, R14, R16
		EDM05.02	Orientar la comunicación con las partes interesadas y la elaboración de informes.	
		EDM05.03	Supervisar la comunicación con las partes interesadas.	
APO01	Administrar Marco de gestión TI	APO01.01	Definir la estructura organizativa.	R2
		APO01.02	Establecer roles y responsabilidades	
		APO01.03	Mantener los elementos catalizadores del sistema de gestión.	
		APO01.04	Comunicar los objetivos y la dirección de gestión.	
		APO01.05	Optimizar la ubicación de la función de TI.	
		APO01.06	Definir la propiedad de la información (datos) y del sistema.	
		APO01.07	Gestionar la mejora continua de los procesos.	
		APO01.08	Mantener el cumplimiento con las políticas y procedimientos	

Dentro del trabajo de apoyo al área de auditoria, se realizó la actualización de la metodología de planeación de auditorías de la versión de Cobit 4.1 a 5 y las fórmulas de las hojas de Excel en donde se actualizo la matriz de riesgos con la nueva escala de valoración y con los riesgos ya definidos.

Ilustración 8 Matriz de riesgos.



Se relacionaron los riesgos de TI con las metas de TI propuestas en el framework.

Ilustración 9 Relación metas TI con riesgos.

La siguiente matriz relaciona los factores de riesgos de la TI vs las metas de la TI

	Metas de la TI - COBIT 5	R1-Iniciativas del área de TI no acordes con la estrategia del negocio	R2-Inadecuado cumplimiento del Gobierno TI	R3-Bajo Nivel de Utilización de la TI como ventaja	R4-Infraestructura/Soluciones de TI no compatibles	R5-Inadecuada relación costo-beneficio de la tecnología	R6-Falta de competencias para gestionar la TI	R7-Falta de Disponibilidad, confidencialidad e	R8-Desconocimiento de los requerimientos de usuario	R9-Deficiencia en los Servicios y/o infraestructura que intervienen en el ciclo de	R10-Uso indebido de la información y/o de los servicios que la suministran, procesan y/o transmiten.	R11-Inadecuada gestión de proveedores de TI	R12-Fraude Electrónico	R13-Inadecuada Gestión de proyectos de TI	R14-Incumplimiento a los niveles de servicio de TI	R15-Procedimientos informales	R16-Inadecuado monitoreo de la gestión de TI	R17-Fallas o errores en los procedimientos	R18	R19	R20	R21	R22	R23	R24	R25	Cantidad de Riesgos	Riesgo de Mayor Valor
	Probabilidad x Severidad	21	42	21	21	13	21	68	13	42	42	42	21	21	34	8	42	68										
Financiera	Alineamiento de TI y la estrategia de negocio.	21	42		21	13	21		13	42				21	34		42										10	42
Financiera	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas		42					68					21			8											4	68
Financiera	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	21	42												34		42										4	42
Financiera	Riesgos de negocio relacionados con las TI gestionados							68	13	42	42	42	21	21	34	8	42	68									11	68
Financiera	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	21		21		13	21							21		8											6	21
Financiera	Transparencia de los costes, beneficios y riesgos de las TI	21				13		68					21		34	8	42										7	68
Cliente	Entrega de servicios de TI de acuerdo a los requisitos del negocio	21	42		21	13		68	13	42	42	42			34	8	42	68									13	68
Cliente	Uso adecuado de aplicaciones, información y soluciones tecnológicas	21		21			21		13	42																	5	42
Interna	Agilidad de las TI	21	42	21	21	13	21					42															7	42
Interna	Seguridad de la información, infraestructuras de procesamiento y aplicaciones							68	13	42			21			8											5	68
Interna	Optimización de activos, recursos y capacidades de las TI	21	42	21	21	13	21	68		42	42				34		42	68									12	68
Interna	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	21			21				13	42					34		42										6	42
Interna	Entrega de programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	21					21	68	13	42				21		8											7	68
Interna	Disponibilidad de información útil y relevante para la toma de decisiones							68					21		34			68									4	68
Interna	Cumplimiento de las políticas internas por parte de las TI		42												34	8	42										4	42
Aprendizaj e y Crecimien	Personal del negocio y de las TI competente y motivado		42			13	21																				3	42
Aprendizaj e y Crecimien	Conocimiento, experiencia e iniciativas para la innovación de negocio	21	42	21		13	21	68	13	42							42										9	68

Finalmente la relación entre metas de TI y procesos la cual arroja como resultado las metas posiblemente vulneradas por los riesgos y los procesos (controles) de Cobit que los mitigaría.

Ilustración 10 Relación Procesos con metas TI

			Financiero						Cliente		Interno							Aprendizaje y Conocimiento		
		METAS de la TI / Procesos COBIT	Alineamiento de TI y la estrategia de negocio.	Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI	Riesgos de negocio relacionados con las TI gestionados	Realización de beneficios del portafolio de inversiones y servicios relacionados con las TI	Transparencia de los costes, beneficios y riesgos de las TI	Entrega de servicios de TI de acuerdo a los requisitos del negocio	Uso adecuado de aplicaciones, información y soluciones tecnológicas	Agilidad de las TI	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de negocio integrando aplicaciones y tecnología en procesos de negocio	a tiempo, dentro del presupuesto y satisfaciendo los requisitos y normas de calidad	Disponibilidad de información útil y relevante para la toma de decisiones	Cumplimiento de las políticas internas por parte de las TI	Personal del negocio y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio
		Por lo menos existe un riesgo con vulnerabilidad:	42	68	42	68	21	68	68	42	42	68	68	42	68	68	42	42	68
			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
Alinear, Planificar y Organizar	APO1	Gestionar el Marco de Gestión de TI	X	X							X		X				X	X	X
	APO2	Gestionar la estrategia	X						X										X
	APO3	Gestionar la Arquitectura Empresarial	X								X		X						
	APO4	Gestionar la Innovación					X			X	X		X						X
	APO5	Gestionar el Portafolio	X				X								X				
	APO6	Gestionar el Presupuesto y los costes					X	X											
	APO7	Gestionar los Recursos Humanos	X										X		X			X	X
	APO8	Gestionar las Relaciones	X						X					X					X
	APO9	Gestionar los Acuerdos de Servicio							X							X			
	APO10	Gestionar los Proveedores				X			X		X								
	APO11	Gestionar la Calidad					X		X						X				
	APO12	Gestionar el Riesgo		X		X		X				X			X				
	APO13	Gestionar la Seguridad		X		X		X				X				X			
nstruir, Adquirir e Implementar	BAI1	Gestionar los Programas y Proyectos	X			X	X								X				
	BAI2	Gestionar la Definición de Requisitos	X						X					X					
	BAI3	Gestionar la Identificación y la Construcción de Soluciones							X										
	BAI4	Gestionar la Disponibilidad y la Capacidad							X				X			X			
	BAI5	Gestionar la introducción de Cambios Organizativos								X					X				X
	BAI6	Gestionar los Cambios				X			X			X							
	BAI7	Gestionar la Aceptación del Cambio y de la Transición								X				X					

Finalmente las guías de auditoría un total de 15 guías quedan definidas con la siguiente estructura, donde se aprecia una primera parte con los ítems definidos en el desarrollo del trabajo y una segunda parte con los controles y las pruebas establecidas:

Ilustración 11 Parte 1 Guía Auditoría.

Guía de Gestión de Cambios G-001

Objetivo: Evaluar el cumplimiento del procedimiento de Gestión de Cambios de sistemas de información no SAP definidos en ISA.

Alcance:

Determinar la suficiencia en el diseño de los controles para la Gestión de Cambios en los sistemas de información para los siguientes aspectos.

-Estándares y procedimientos utilizados para la gestión de cambios.

-Mecanismos para evaluar el impacto, priorización y autorización de los cambios.

-Procedimiento para el manejo de cambios de emergencia.

-Mecanismos de seguimiento y reporte del estatus del cambio.

-Mecanismos para determinar el costo de los cambios

Dominio: Construir, adquirir e implementar.

Procesos:
BAI06. Administrar cambios de TI.
BAI07. Aceptar e incorporar cambios de TI.

Riesgos Relacionados:

R7.Falta de Disponibilidad, confidencialidad e integridad de la información.

R8.Desconocimiento de los requerimientos de usuario.

R9.Deficiencia en los Servicios y/o infraestructura que intervienen en el ciclo de vida de la información.

Información necesaria:

-Informe de gestión de cambios.

Ilustración 12 Parte 2 Guía de auditoría.

Código Control	Control	Código y nombre Prueba	Prueba
BAI06.01	Evaluar, priorizar y autorizar peticiones de cambio	P-001 Revisión de las peticiones de cambio.	a) Verifique la existencia y aplicación de un procedimiento para la gestión de solicitudes de cambio en la infraestructura, sistemas de información y aplicaciones. b) Verificar si las peticiones de cambio están categorizadas y relacionadas con los elementos que afectaría dicho cambio. c) Indagar si existe y es usada una metodología para priorizar los requerimientos de usuarios para cambios al sistema. d) Verificar que se consideran las implicaciones de seguridad, legales, contractuales y de cumplimiento normativo del cambio solicitado. e) Del listado de cambios del periodo auditado tome una muestra de los cambios a evaluar (Nota: Tener presente la clasificación que se le da a los cambios, incluya los más representativos.)
BAI06.02	Gestionar cambios de emergencia	P-002 Procedimientos en caso de cambio de emergencia.	a) Identificar la existencia de manuales, procedimientos o directrices para llevar a cabo cambios por emergencia. b) Establecer la existencia de mecanismos alternos de revisión y aseguramiento de los cambios de emergencia.
BAI06.03	Hacer seguimiento e informar de cambios de estado	P-003 Cambios de estado de cambio.	a) Indagar si se categorizan las peticiones de cambio (Rechazado, sin iniciar, en proceso y cerrado) de manera que los usuarios y personal de TI puedan realizar un seguimiento a sus requerimientos. b) Establezca que se hayan realizado los acuerdos de entendimiento entre las partes interesadas (Dueño de proceso y personal de TI).
BAI06.04	Cerrar y documentar los cambios	P-004 Cierre de cambios.	a) Verificar que se conserva la documentación del sistema antes y después del cambio y preguntar durante cuánto tiempo. b) Revisar si se actualizan los manuales de usuario y de operación para reflejar el cambio.

Conclusiones

Se puede concluir en que se ha dotado a la Auditoria Corporativa del grupo empresarial con una herramienta que facilitara el proceso de auditoría al área de tecnología de la información.

En resumen continúan siendo 17 riesgos de TI en la organización, después de haber eliminado “Ataques informáticos” por interpretarse más como una amenaza y al identificar el riesgo referente a la gestión de proyectos.

Así pues el trabajo de definición de cada riesgo, identificación de sus amenazas y consecuencias resulto siendo un gran aporte tanto al área de TI como a la de auditoría, puesto que evita interpretaciones erróneas del riesgo.

Finalmente se puede decir que la relación controles y riesgos ha resultado satisfactoria puesto que se identifica de una manera clara el que hacer para mitigar los riesgos.

Recomendaciones

El área de auditoría de sistemas es un área poco abordada en la Universidad, por tal motivo se recomienda dar un mayor énfasis en esta asignatura puesto que posee la misma importancia que tienen las demás asignaturas del pregrado de Ingeniería Informática ya que toda organización debe tener un auditor de las tecnologías de la información y más aun sabiendo que la industria se basa actualmente en dichas tecnologías para el desarrollo de sus procesos.

En la medida de lo posible se sugiere a la universidad una mayor cantidad de horas en las que se dedique un especial énfasis a los estándares, normas y modelos que dan lineamientos a las organizaciones para que el área de informática sea un área que aporta valor a la organización.

Finalmente se esperaría que el pregrado logre abordar en un futuro cercano todas las áreas en las que se puede desempeñar un ingeniero informático en el campo laboral ya que se ha identificado que se tiene una visión sesgada por parte de los estudiantes sobre el papel que desempeña un egresado del programa en la industria.

Referencias

Icontec. (2009). *Compendio Sistema de Gestión de la Seguridad de la Información (SGSI)* (Segunda Edición ed.). Bogota D.C, Colombia.

Isaca. (2007). *Manual de Preparación al Examen CISA 2007.* Illinois: Information Systems Audit and Control Association.

Isaca. (2012). *Cobit 5 Implementación.* (E. d. Madrid, Trad.) Rolling Meadows, Illinois, Estados Unidos.

Isaca. (2012). *Cobit 5 Procesos Catalizadores.* (E. d. Madrid, Trad.) Rolling Meadows, Illinois, Estados Unidos.

IT Governance Institute. (2000). *Cobit Directrices de Auditoría.* (G. A. Solís Montes, Trad.) Rolling Meadows, Illinois, Estados Unidos: Information Systems Audit and Control.

IT Governance Institute. (2005). *Cobit 4.0.* (S. Glanser Services, Trad.) Rolling Meadows, Illinois, Estados Unidos.

IT Governance Institute. (2008). *Alineando Cobit 4.1, Itil V3 e ISO/IEC 27002 en beneficio del negocio.* (F. Neira Bassp, Trad.) Rolling Meadows, Illinois, Estados Unidos.

Modiri, R. S. (2012). *An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls.* Tehran.

Rigante, F. (2011). *ISACA.* Obtenido de COBIT 5 - Cambios de la nueva versión (UPDATE - Spanish): http://www.isaca.org/Groups/Professional-English/cobit-5-use-it-effectively/Pages/ViewDiscussion.aspx?PostID=18