Instituto Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las organizaciones auditadas, Caso JM Auditores.

Trabajo Final de Graduación para optar por el título de Licenciatura en Administración de Tecnología de Información

Elaborado por: Adán Josué Masis Álvarez

Cartago, Junio 2017

I. Hoja de Aprobación

Instituto Tecnológico de Costa Rica

Área de Administración de Tecnologías de Información

Grado Académico: Licenciatura

Los miembros del Tribunal Examinador del Área de Administración de Tecnologías de Información reconocemos que el presente Informe Final del Proyecto de Graduación del Estudiante Adán Josué Masís Álvarez sea aceptado como requisito parcial para obtener el grado académico de Licenciatura en Administración de Tecnologías de Información.

_____
Isaac Alpízar Chacón
Profesor Asesor

_____
Nombre del Miembro Tribunal Examinado
Miembro del Tribunal Examinador

_____
Nombre del Miembro Tribunal Examinado
Miembro del Tribunal Examinador

_____
Sonia Mora Gonzales
Coordinador del Proyecto de Graduación de la Licenciatura en Administración de Tecnologías de Información

Año 2017

II. Dedicatoria

A mis padres,

Jose Masis y Mercedes Alvarez, por el apoyo brindado durante los cinco años de carrera, por las muestras de cariño, motivación, carácter y valores que me inculcaron para luchar día a día por las metas y donde hoy se está alcanzando una de ellas.

A mis hermanas,

Karen y Angie Masis, quienes a pesar de la distancia me demostraron su cariño y apoyo durante todo el tiempo.

A mi novia,

Marianela Cordero, por el apoyo brindado durante esos momentos de estrés, trasnochadas y duros momentos vividos durante todo este tiempo, donde me impulsó, me motivo y me dio palabras de aliente para siempre salir adelante para culminar con una gran etapa de mi vida.

III. Agradecimientos

Deseo manifestar mi agradecimiento a quienes hicieron posible la obtención de los objetivos del proyecto y su desarrollo.

A Dios,

Por ser mí guía, proveedor de sabiduría, paciencia, fortaleza y darme el don de la vida para lograr el desarrollo del proyecto y de mi vida profesional.

Angélica Sánchez,

Coordinadora del equipo de trabajo de la empresa donde se realizó el proyecto, por su ayuda y colaboración para el desarrollo del proyecto, además del conocimiento compartido para dicho fin.

Issac Alpizar (Profesor Asesor),

Por el aporte de su conocimiento la paciencia y atención brindada durante el periodo durante el desarrollo del proyecto.

Amigos de la Universidad,

Por el apoyo y ayuda brindada en los momentos que se necesitó y por esos momentos de distracción que sirvieron para olvidar el estrés por ciertos momentos.

¡Gracias a todos!

IV. Resumen

Establecer controles de auditoría específicos para llevar a cabo evaluaciones sobre la Gestión de Tecnología de Información en las organizaciones auditadas, implica la definición de pruebas sustantivas que respaldan y evalúen cada uno de los escenarios que se pueden presentar en las diferentes empresas.

Sin la definición de pruebas sustantivas, la evaluación de un control de auditoría se dificulta por la falta de especificaciones y lineamientos que deben realizar los auditores al momento de ejecutar una evaluación.

El presente proyecto se basa en la definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las empresas del mercado industrial, donde por medio de una rúbrica de evaluación se analizaron las metodologías: ITIL v2011, COBIT 5 y la norma ISO/IEC 20000, con el fin de determinar cuál de estas se adapta mejor a las auditorías realizadas por JM Auditores.

Como resultado del proyecto se definieron los controles de auditoría para el proceso de Gestión del Cambio y las pruebas sustantivas de cada uno de los controles establecidos por medio de COBIT 5, la cual fue seleccionada como parte del análisis realizado. Además, se realizó una actualización a la Matriz de Controles por medio de macros en Microsoft Excel de forma que permite mantener un documento central de las pruebas que han sido efectivas, inefectivas o que poseen oportunidades de mejora que reportar.

Palabras Claves: COBIT 5, Auditoría de TI, Gestión del Cambio, Controles de Auditoría, Pruebas Sustantivas, Matriz de Controles de Auditoría.

V. Abstract

Establishing specific audit controls to conduct Information Technology Management assessments in audited organizations involves defining substantive test that supports and evaluates each of the scenarios that can be presented in different companies.

Without definition substantive testing, the evaluation of audit control becomes difficult by the lack of specifications and guidelines that must be made by the auditors when performing an evaluation.

The present project is based on the definition of audit controls and substantive tests for evaluated the Change Management process on industrial market companies, where an evaluation rubric was used to analyze three methodologies: ITIL v2011, COBIT 5 and the ISO/IEC 20000 standard, in order to determine which one of these is best adapted to the audits performed by JM Auditores.

As project outcome, audit controls were defined for the Change Management process and the substantive tests of each of the controls established through COBIT 5, which was selected as part of the analysis performed. In addition, an update was made to the Control Matrix by means of macros in Microsoft Excel in order to maintain a central document of the tests that have been effective, ineffective or have improvement opportunities to report.

Keywords: COBIT 5, IT Audit, Change Management, Audit Controls, Substantive testing, Audit Controls Matrix.

VI. Contenido

VII. Contenido de Figuras

VIII. Contenido de Tablas

IX. Contenido de Gráficos

1. Introducción

Actualmente se vive en un mundo donde la tecnología es clave para la supervivencia de las organizaciones en un mercado que se encuentra en un cambio constante, donde además la forma en que se utiliza y se gestiona la tecnología es un proceso fundamental para la operación de las compañías.

Un aspecto importante en la gestión de la Tecnología de Información (TI) es mantenerse actualizado y adaptarse a las buenas prácticas dictadas por la industria y organizaciones dedicadas a la gestión de TI.

El *IT Governance Institute* establece que en múltiples ocasiones los Gerentes Operacionales (CEO) y los Gerentes de Tecnología de Información (CIO) conocían los beneficios de adaptarse a las mejores prácticas de Gestión de TI; sin embargo, no involucraban a los reguladores, quienes son los principales interesados en que las inversiones y la gestión de los componentes de TI se realicen de forma segura, así como que se encuentren protegidas y entreguen valor a la organización.

La Asociación de Control y la Auditoría de Sistemas de Información (ISACA)[1] reconoció que las firmas auditoras poseían su propia lista de auditoría para evaluar la efectividad de controles de TI, comunicándose en un lenguaje distinto a los profesionales de TI de las empresas clientes. Por tal razón, en la década de los 90 ISACA (IT Governance Institute, 2008, pág. 10) creó los Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés) como un marco de trabajo de control de TI, enfocado a la gerencia general, gerencia de TI y los auditores.

[1] Information System Audit and Control Association (ISACA)

Por este motivo la empresa, donde se llevará a cabo el Trabajo Final de Graduación, en especial el área de Administración del Riesgo ha visto la necesidad de adaptarse a un marco de trabajo que les permita comunicarse mediante un mismo idioma con sus clientes, en busca que las evaluaciones realizadas sean cada vez más efectivas, lo que origina el objetivo principal del proyecto.

Como consecuencia de lo definido anteriormente, se pretende desarrollar el presente proyecto, relacionado con la adaptación de un marco de referencia reconocido en la industria a nivel mundial. Se tomará en cuenta marcos como la Librería de Infraestructura de Tecnología de Información (ITIL, por sus siglas en Inglés), COBIT y una norma de la Organización Internacional de Normalización (ISO, por sus siglas en Inglés).

Por medio de un estudio y análisis de estas dos metodologías y la norma ISO, se determinará la mejor opción para llevar a cabo la definición de controles de auditoría para el proceso de Gestión del Cambio, por lo cual también es importante establecer los objetivos, alcance, entregables, limitaciones, restricciones y problema principal del proyecto; además, de la metodología y plan de desarrollo que se utilizará para completar el Trabajo Final de Graduación.

Para efectos del desarrollo del proyecto y para el cumplimiento de la política de confidencialidad establecida por la organización, se establece el nombre “JM Auditores” con el fin de referenciar a la organización donde se desarrollará el Trabajo Final de Graduación.

1.1 Antecedentes

1.1.1 Descripción de la organización

En este apartado se desarrolla el entendimiento de la organización donde se llevará a cabo el Trabajo Final de Graduación, para eso se define la Misión, Visión, Valores e información general de la misma.

1.1.1.1 Misión

“Proveer servicios de auditoría con el más alto nivel de calidad, buscando siempre la máxima satisfacción de nuestros clientes dentro de un marco de ética, independencia y confidencialidad.” (JM Auditores, 2016).

1.1.1.2 Visión

“Ser la mejor firma en dónde trabajar, para nuestros clientes, para nuestra gente y para nuestra comunidad.” (JM Auditores, 2016).

1.1.1.3 Sobre la organización

JM Auditores es una red global de firmas miembros independientes que brindan servicios de Asesoría, Impuestos y Auditoría específicamente en el área financiera.

JM Auditores Costa Rica fue creada en el año 1958, cuenta con más de 50 años de experiencia en el país. A partir del 2005 formó parte de JM Auditores Centroamérica, que se encuentra integrada por las firmas de JM Auditores en Costa Rica, Guatemala, Honduras, El Salvador, Nicaragua, Panamá y República Dominicana.

JM Auditores Costa Rica es una organización que centra su operación en la Auditoría Financiera para empresas como: Bancos, Cooperativas y Empresas Crediticias. Además, en compañías de industria manufacturera, prestadoras de servicios de TI y gubernamentales que se encuentren en el territorio nacional.

En la actualidad JM Auditores, cuenta con un sistema de auditoría que es utilizado por todas las firmas miembros a nivel mundial y que fue desarrollado a la medida para llevar a cabo todas las auditorías, de forma que ya se encuentran parametrizadas y configuradas cada una de las pruebas y operaciones que debe realizar el auditor.

La firma está conformada por un Director Ejecutivo y un Gerente de Operaciones, los cuales establecen las directrices empresariales de acuerdo a lo que estipula la firma a nivel global. Un nivel por debajo en la jerarquía de puestos, se encuentran siete socios empresariales, quienes son los responsables de definir las metas y los objetivos para cada uno de los departamentos que tienen a su cargo, así como de velar para que los colaboradores cumplan con lo acordado.

Cada departamento está a cargo de un Director, el cual es el encargado de descomponer las metas y los objetivos establecidos por los socios de negocios y asignarle a cada área de negocio las metas y objetivos correspondientes a las funciones específicas de los departamentos.

Los departamentos que forman parte de JM Auditores Costa Rica son nombrados en inglés de acuerdo a la estructura global de la compañía, estos departamentos son: *Adversory, Tax, Legal, Infraestructure, Audit*.

El departamento de Auditoría (*Audit*), está compuesto por el área de negocio denominado Administración de Riesgos de la información (IRM, por sus siglas en inglés). Ésta área la integran especialistas en TI, los cuales son los encargados de brindar soporte al equipo de auditoría para llevar a cabo la evaluación en sistemas de información, y de la infraestructura tecnológica que impacta directamente la situación financiera de la organización auditada, es en este departamento donde se desarrollará el proyecto.

El área de IRM se conforma por un Gerente Senior, quien es responsable principal del área de negocio, y seis especialistas en TI, que cuentan con un grado mínimo de licenciatura en carreras afines a tecnología de información.

A continuación, en la Figura 1.1 se muestra el organigrama institucional de la compañía, donde el cuadro resaltado corresponde al área donde se ejecuta el desarrollo del proyecto.

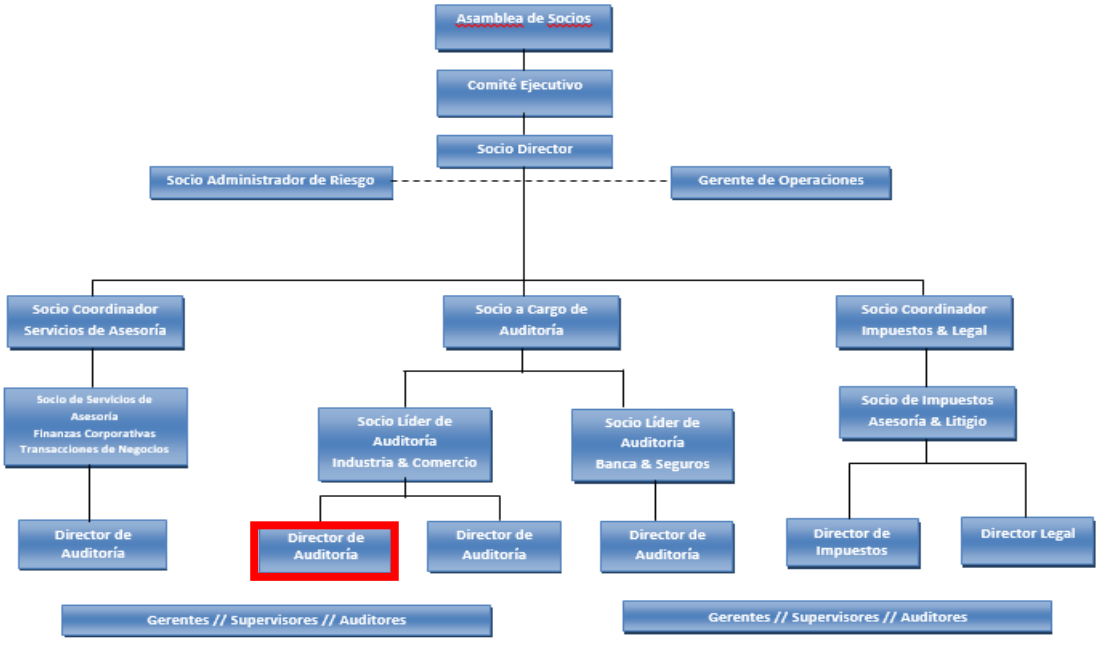

Figura 1.1. Organigrama Institucional

Fuente: Adaptado de (JM Auditores, 2016)

1.1.1.4 Propuesta de valor

La organización se basa en los siguientes valores (JM Auditores, 2016):

- Predicamos con el ejemplo.
- Trabajamos juntos.
- Respetamos a los individuos.
- Investigamos los hechos y transmitimos conocimientos.
- Nos comunicamos de forma abierta y honesta.
- Comprometidos con la sociedad.
- Por encima de todo, nos comportamos con integridad.

1.1.1.5 Equipo de trabajo

Para elaborar el Trabajo Final de Graduación, es necesario definir un equipo colaborador, el cual brindará el apoyo para el desarrollo del mismo, de forma que las habilidades y conocimientos de cada uno de los miembros del equipo faciliten el cumplimiento de los objetivos establecidos. Este equipo de trabajo está conformado por:

- **Gerente Senior del área de Administración de Riesgo:** Patrocinador del proyecto, será el encargado principal de brindar la información requerida por el estudiante, asimismo será el responsable de revisar y aprobar cada uno de los entregables del proyecto.
- **Supervisora del área de Administración de Riesgo:** Será la encargada de brindar la información operativa, además será el primer filtro de aprobación antes de ser revisado por el Gerente Senior. Por otro lado apoyará la coordinación de reuniones con el personal adecuado que se encuentra dentro de la organización, con el fin de obtener la información precisa y necesaria.

- **Especialista de TI:** Brindará apoyo en la ejecución del proyecto basándose en sus propios conocimientos, además de brindar observaciones, documentación e información relacionada con la metodología de trabajo.
- **Estudiante:** Responsable de recopilar la información descrita en las diferentes metodologías utilizadas para llevar a cabo el desarrollo del proyecto, con el fin de analizar la información de cada uno y brindar una propuesta de mejora de controles de auditoría basados en la metodología más adecuada para la revisión de los controles generales de TI de la compañía auditada.

Para comprender las funciones de los miembro del equipo de trabajo, se presenta la Tabla 1.1, donde se resume sus responsabilidades dentro de la organización y los roles que tendrán en el desarrollo del proyecto, con el fin de cumplir con el objetivo del proyecto.

Tabla 1.1. Equipo de trabajo por parte de la Organización

Posición Laboral	Responsabilidad en la empresa	Rol en el proyecto
Gerente Senior de Administración del Riesgo	• Encargado de gestionar la cartelera de clientes. • Responsable de revisar y aprobar los trabajos realizados por los especialistas de TI. • Encargado de establecer las metas y los objetivos del área. • Máximo responsable de las operaciones del área.	Patrocinador del proyecto.
Supervisor de Administración del Riesgo	• Encargado de distribuir las tareas al equipo de trabajo. • Dar seguimiento a los avances de las tareas distribuidas. • Contacto directo con el encargado del proyecto de la empresa cliente.	Supervisor del proyecto final de graduación.
Especialista de TI	• Responsables de llevar a cabo las evaluaciones en las empresas clientes. • Encargados de aplicar los controles de evaluación actualmente vigentes para las auditorías que se llevan a cabo.	Colaborar con el estudiante en el desarrollo del trabajo final de graduación.
Practicante	• Practicante en el área de Administración del Riesgo.	Desarrollador del trabajo final de graduación.

Fuente: Elaboración propia

A continuación, en la Figura 1.2 se representa la jerarquía que tendrá el equipo de trabajo, con el fin de llevar a cabo de forma eficaz y eficiente el desarrollo del Trabajo Final de Graduación.

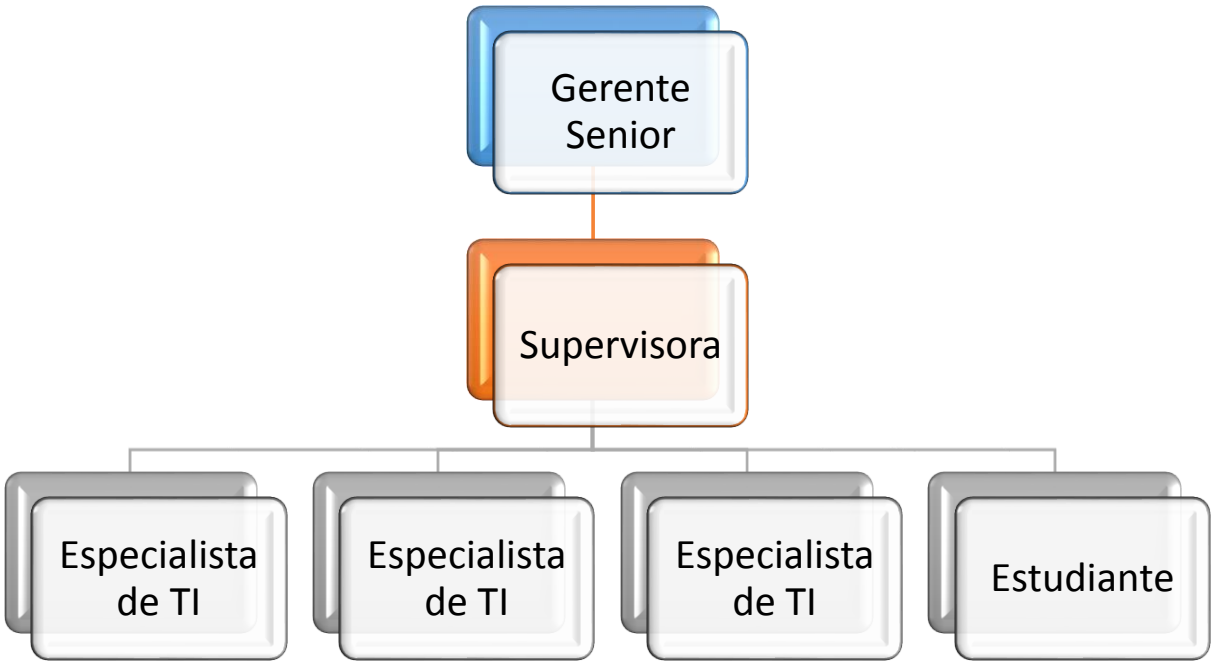

Figura 1.2. Equipo de Trabajo

Fuente: Elaboración propia

1.1.2 Trabajos similares realizados

En esta sección se describen los proyectos que se han realizado en la organización y que están relacionados con el proyecto propuesto y que servirán como insumo para el desarrollo del mismo.

Para finales del año 2015 se realizó un proyecto por la actual supervisora de IRM. A través de la experiencia de varios años en la ejecución de auditorías para el área de Administración del Riesgo, se identificó la necesidad de actualizar los controles de auditoría que se realizaban en ese momento (Sánchez, 2015).

Mediante la utilización del marco de trabajo COBIT en su versión 4.1 se inició con la actualización de la Matriz de Controles Generales de TI. Por medio de este proyecto se modificaron los controles para evaluar el área de Acceso a Programas y Datos, logrando así por medio de este proyecto reestructurar esta área de evaluación y se definieron un total de 11 controles, los cuales son los utilizados actualmente para realizar las auditorías (Sánchez, 2015).

Los controles definidos para esta área abarcan aspectos desde la documentación de políticas para el uso y la seguridad de la información hasta la forma y los mecanismos que utiliza el departamento de TI de la compañía auditada para garantizar el funcionamiento y la integridad de los sistemas financieros de la organización (Sánchez, 2015).

Por otro lado, se identificó que el área de Gestión del Cambio es un área crítica para evaluar y donde las empresas auditadas carecen de controles para llevar de forma correcta este proceso. Por tal razón se definió como una recomendación del proyecto realizar una actualización de controles de dicho apartado (Sánchez, 2015).

Otro trabajo realizado por (CEVALLOS, 2015) titulado “Plan de Continuidad de los Servicios Críticos de Red de la Empresa Actuaria Consultores CÍA. LTDA”, presenta el establecimiento de un plan de continuidad de procesos críticos para una organización, donde se tomó en cuenta estándares internacionales como COBIT, ITIL e ISO 20000. Este autor se basó en la información que brindan las tres metodologías para establecer un plan de continuidad, a partir de una comparación de cada una y se indicó la mejor opción para definir e implementar un plan de continuidad.

Tal y como se indicó, este auditor efectuó una comparación de la metodología donde definió aspectos importantes que la organización consideró al momento de solicitar el desarrollo del plan de continuidad, estos aspectos fueron además establecidos de acuerdo a la infraestructura organizacional y necesidades de la misma.

1.2 Planteamiento del problema

En esta sección se describe la problemática hallada dentro del entorno de la organización, el cual motiva el desarrollo del proyecto, así como la mención de los beneficios esperados del producto.

1.2.1 Situación problemática

El área de administración de riesgos es el responsable de llevar a cabo la evaluación de los controles generales de tecnología de información y de los sistemas de información que se encuentran involucrados en el movimiento de cuentas contables y de los reportes financieros.

Para realizar dicha evaluación la compañía posee una metodología propia de auditoría utilizada a nivel global por la firma, la cual indica las pautas y las reglas utilizadas para ejecutar las evaluaciones. Esta metodología dicta, específicamente, que el área de Administración de Riesgos debe basar sus evaluaciones en dos grandes áreas que son: Evaluación de controles de infraestructura de TI y Evaluación de controles de Aplicaciones de TI.

Para la ejecución de la evaluación de controles de aplicaciones de TI, el departamento de Auditoría Financiera como parte de la planeación de la auditoría, define los controles a evaluar en el ámbito de aplicaciones de TI de acuerdo a las necesidades y riesgos de la auditoría, y de los sistemas con los que cuenta la organización auditada.

Por otra parte, para ejecutar la evaluación de controles generales de TI la empresa cuenta con la definición de procesos de auditoría, donde se definen los controles y la documentación necesaria para desarrollar con eficacia la evaluación. Dichos procesos son:

- **Entendimiento del entorno de TI:** Se evalúa cómo se encuentra conformado el departamento de TI de la empresa auditada, cuáles son los sistemas con que cuenta la organización, cuál es la infraestructura disponible para que cada uno de los sistemas funcionen correctamente. Así como cuáles son los mecanismos que posee el departamento para garantizar una buena gestión de cada uno de los sistemas y de la infraestructura.
- **Uso de programas y datos:** En este apartado se evalúa cuáles son los usuarios que tienen acceso a los sistemas de la organización y establece si los permisos otorgados a los colaboradores para el ingreso a los sistemas son los apropiados, de acuerdo a sus operaciones diarias. Además, se evalúa si los usuarios administradores son manejados adecuadamente y si estos no realizan actividades indebidas que puedan afectar los resultados financieros.
- **Gestión de cambios:** Este apartado define los controles que se deben tomar en cuenta para determinar la gestión de cambios que posee el departamento de TI de la empresa auditada. Esto con el fin de establecer si los cambios solicitados son procesados y documentados de manera acertada, en especial si los cambios se realizan en los sistemas de información que impactan la contabilidad de la empresa auditada.

- **Creación de programas utilitarios:** Evalúa si el departamento de TI posee un desarrollo interno de los sistemas de la organización y si el ambiente de desarrollo se lleva de forma aislada al ambiente de producción. Asimismo, revisa si ejecutan pruebas adecuadas con las aprobaciones necesarias antes que un sistema entre en operación.
- **Funcionamiento computacional:** Define los controles relacionados con el funcionamiento computacional, principalmente para establecer cómo se lleva a cabo los procedimientos necesarios para mantener el funcionamiento de los servidores y los respaldos de la información financiera generada por los sistemas involucrados.

A partir de lo descrito es donde se identifica el problema que posee la organización, principalmente el departamento de Auditoría y más específico el área de Administración de Riesgos, dado que la metodología implementada y definida por la empresa carece del respaldo brindado por marcos de trabajo reconocidos a nivel mundial por las distintas industrias.

Además, los controles establecidos en la metodología para ser evaluados por los Especialistas de Administración de Riesgo, son definidos de forma superficial y algunos de ellos quedan a disposición del auditor, por ejemplo: cuáles son las pruebas que debe de realizar, con el fin de llegar al resultado esperado, esto genera que las evaluaciones efectuadas actualmente cuenten con oportunidades de mejora, que inicia en los procesos y controles de auditoría.

Por lo que es necesario establecer una Matriz de Controles Generales de TI que se encuentre alineada con el marco de referencia reconocido a nivel mundial como COBIT, ITIL e ISO, de forma que estas consideren las categorías de revisión establecidas por la organización dentro del alcance de auditoría financiera de TI.

1.2.2 Beneficios esperados del proyecto

Al identificar el problema actual, se espera que, mediante el desarrollo del proyecto, la organización cuente tanto con beneficios directos como indirectos. A continuación, se especifica cada uno de los beneficios esperados.

1.2.2.1 Beneficios Directos

Los beneficios directos, son aquellos que influyen positivamente en los resultados obtenidos para la organización tras el desarrollo del proyecto. Los identificados son:

- Confiabilidad de los controles de evaluación por parte de los especialistas de Administración de Riesgos.
- Controles de evaluación basados en las mejores prácticas (ITIL, COBIT 5, ISO) reconocidas a nivel mundial.
- Mejora en los resultados de auditoría obtenidos a partir de la evaluación.
- Mayor entendimiento en los controles evaluados por parte del departamento de TI de la empresa auditada, al estar alineado a un marco de trabajo reconocido por las organizaciones.
- Evaluaciones más completas, al contar con controles más detallados basándose en las mejores prácticas internacionales.
- Mayor satisfacción de los clientes a partir de los resultados obtenidos.
- Comunicación fluida con los encargados de la empresa auditada, dado que ambas partes conocen el lenguaje técnico.

1.2.2.2 Beneficios Indirectos

Los beneficios indirectos, son aquellos que la organización obtendrá de forma indirecta durante el desarrollo del proyecto. Los beneficios indirectos identificados son:

- Mayor atracción de clientes en el territorio nacional, al brindar auditorías más completas que aumentan la satisfacción de los mismos.
- Aumento en la calidad de las auditorías realizadas, al estar basadas en las mejores prácticas internacionales.
- Aumento en el valor agregado brindado a la empresa cliente, a partir de resultados más adecuados y precisos sobre la evaluación realizada.
- Respaldo de las mejores prácticas de la industria a nivel mundial sobre las auditorías elaboradas.

1.3 Objetivos

A continuación se define el objetivo general, el cual representa el propósito principal del desarrollo del Trabajo Final de Graduación. De igual forma, se definen los objetivos específicos que indican el cómo se alcanzará el cumplimiento de dicho objetivo y los entregables del trabajo.

1.3.1 Objetivo general

Desarrollar los controles de auditoría y las pruebas sustantivas para el proceso de Gestión del Cambio de forma que se alinee a un marco de referencia internacional, con el fin de llevar a cabo una mejor evaluación de Controles Generales de TI para las empresas industriales auditadas en el año 2017.

1.3.2 Objetivos específicos

1. Analizar tres metodologías internacionales (ITIL, COBIT, ISO 20000) basado en el proceso de Gestión del Cambio, con el propósito de recomendar la metodología más adecuada para la empresa.
2. Definir los controles generales de TI que establece la metodología seleccionada para evaluar la Gestión de Cambios.
3. Desarrollar, de forma detallada, las pruebas sustantivas para cada uno de los controles de auditoría identificados para evaluar la gestión de cambios.
4. Alinear la Matriz de Controles Generales de TI de acuerdo a los procesos identificados en la metodología seleccionada que cumplen con los procesos definidos actualmente por la organización.
5. Adaptar la matriz de controles generales de TI mediante la automatización de los controles y las pruebas sustantivas, basada en macros de Microsoft Excel, de forma que indique el resultado obtenido de la evaluación realizada.

1.4 Justificación del proyecto

En este apartado se explica la razón por la que es importante desarrollar el proyecto descrito en el presente documento.

Tal y como se estableció en el apartado 1.2.1 Situación problemática, actualmente la organización posee una metodología propia en la cual establece los controles de auditoría que se deben evaluar en cada una de las auditorías realizadas. Sin embargo, IRM cuenta con una matriz de Controles Generales de TI para realizar sus evaluaciones; no obstante, estos controles carecen de una alineación con marcos de referencia estándares y reconocidos a nivel mundial, los cuales permitirán a los auditores hablar el mismo idioma que los encargados de TI de las empresas auditadas.

El desarrollo de este proyecto, le permitirá a la empresa adaptarse a una metodología estándar aprobada por la industria a nivel mundial (ITIL V2011, COBIT 5 o ISO 20000); además, las empresas auditadas conocerán bajo que marco de trabajo serán evaluadas, de forma que se genere una credibilidad sobre la misma.

En caso que la compañía decida no desarrollar este proyecto, dejará de percibir los beneficios descritos en el apartado 1.2.2 Beneficios esperados del proyecto, los cuales se resumen en la pérdida de credibilidad e incluso podría significar la pérdida de clientes por la falta de estandarización de sus auditorías por medio de un marco de referencia reconocido a nivel mundial. Además, la compañía contará con auditorías más completas sobre el entorno de TI sobre la cual se desarrolla la contabilidad y los estados financieros de las empresas auditadas, evitando e identificando los posibles fraudes en que incurren dichas organizaciones.

Por otra parte, el desarrollo del Trabajo Final de Graduación, permite que el estudiante encargado del proyecto, aplique temas que han sido estudiados durante la carrera, entre los que se encuentran:

1. **Información Contable:** Dado a que las auditorías que se realizan, se centran en los sistemas de información involucrados en la contabilidad de las empresas auditadas. Por lo cual se pone en práctica los conocimientos adquiridos tanto en Información Contable 1 como en Información Contable 2.
2. **Gestión y Toma de Decisiones Financieras:** Las auditorías realizadas también incluye la generación de estados financieros por parte de los sistemas de información, por dicha razón lo aprendido en este curso se pondrá en práctica para establecer si la interpretación de los estados financieros y su obtención son los correctos o no.
3. **Auditoría de Tecnología de Información:** En este curso se llevó la introducción al marco de referencia de COBIT 5 y la puesta en práctica para la evaluación de sistemas de información. Por lo que lo aprendido en este curso se pondrá en práctica en un mayor grado, considerando que el trabajo se centra en el estudio del marco de trabajo de COBIT 5.

1.5 Alcance del proyecto

En esta sección se describen, de forma puntual, los aspectos que se realizaran en el proyecto en busca de los objetivos establecidos. Asimismo se incluyen los elementos no incluidos para su desarrollo.

Como se mencionó en el apartado 1.2 Planteamiento del problema, el área de Administración de Riesgos de la Información centra sus evaluaciones en:

1. Evaluación de Controles Generales de TI.
2. Evaluación de los Sistemas de Información.

Dichas evaluaciones se llevan a cabo en dos mercados distintos (banca e industria) definidos en la metodología propia de la organización. Para ambos mercados se realiza la Auditoría Financiera, pero de forma distinta. En banca, la auditoría toma en cuenta para su evaluación controles relacionados con el fraude contable y las transacciones que se realizan en estas entidades. Por su lado, las auditorías es el mercado industrial se contempla solamente la contabilidad y los estados financieros, lo que deja de lado la evaluación de fraude que se considera en la evaluación bancaria.

Como parte de la Evaluación de los Controles Generales de TI, el área de Administración de Riesgos actualmente posee una matriz denominada "Matriz de Controles Generales de TI” (MCGTI) donde se definen los controles de auditoría evaluados hoy en día, los cuales están divididos en 5 procesos que se describen a continuación:

1. **Entendimiento del entorno de Tecnologías de Información:** En este proceso se busca entender cuál es el entorno de TI con el que cuenta la organización auditada y sobre qué infraestructura y políticas se basan los sistemas de información contable. Los controles que se evalúan en esta área son:
    - Establecimiento de un Plan Estratégico de TI.
    - Existencia de un Plan de Continuidad y Plan de Capacitación.
    - Existencia de Políticas de TI y sitio de publicación de las mismas.
    - Diagrama de Red y Organigrama del Departamento de TI.
    - Listado de proyecto que se encuentra en desarrollo.
    - Listado de sistemas de información de la compañía auditada y su plataforma tecnológica.
2. **Uso de Programas y Datos:** En este proceso se evalúan los controles que buscan definir cómo se manejan los niveles de seguridad de los diferentes sistemas y de la infraestructura física de la organización. Al mismo tiempo se busca identificar los niveles de seguridad que posee el Departamento de TI. Los siguientes controles son los que se evalúan en este proceso:
    - Establecimiento de una política de seguridad que se encuentre alineada a la organización.
    - La Organización adopta una política de seguridad formal que ofrece una guía para la seguridad de la información e incluye en su alcance todos los aspectos del ambiente de TI relevantes para las aplicaciones y datos del reporte financiero (redes, seguridad de perímetro, seguridad del sistema operativo, seguridad de aplicaciones, uso aceptable de sistemas).

- La Organización ha establecido un mecanismo de autenticación para los sistemas de información incluidos en el alcance que proporcione responsabilidad individual (cuentas individuales por usuario).
- La organización ha establecido reglas para la administración de las contraseñas y su sintaxis.
- El acceso a los usuarios con mayor privilegio en las aplicaciones incluidas en el alcance, está restringido al personal a cargo de la administración del sistema.
- El acceso físico al equipo que resguarda la información de la Organización está restringido al personal adecuado.
- La organización tiene mecanismos efectivos para registrar la actividad en la seguridad e identificar violaciones potenciales, de forma que se puedan tomar medidas oportunas para reducir el riesgo de acceso no autorizado o inapropiado a los datos o aplicaciones relevantes de reporte financiero.
- Un mecanismo efectivo está implementado para asegurar que el acceso es modificado apropiadamente o revocado cuando ocurren cambios en las funciones o terminación del trabajo de un colaborador.
- La organización revisa periódicamente los usuarios activos y los derechos de acceso de usuarios para identificar y eliminar accesos inapropiados al sistema.

3. **Gestión del Cambio:** En este proceso de auditoría se evalúa que la organización auditada cuente con una gestión de cambios bien definida. Esto para que cuando se presente un cambio, primero pase por un proceso de prueba adecuado y que no afecte la operación de la empresa, con el fin de minimizar el impacto del mismo. Los controles que se llevan a cabo en esta evaluación son:
    - La Organización ha establecido un proceso de administración del cambio formal que contenga los requisitos para realizar los cambios en los sistemas y aplicaciones que tienen control sobre el reporte financiero.
    - Todas las solicitudes de cambios para los sistemas de información y aplicaciones que brinden control sobre el reporte financiero están formalmente documentadas.
    - La organización ha establecido un proceso formal de pruebas.
    - La Organización ha establecido una política que limita los cambios a producción del personal de administración de cambios.
    - Todos los cambios de emergencia se registran para facilitar la revisión detallada del cambio.
4. **Creación de Programas Utilitarios:** Mediante este proceso de auditoría busca asegurar que los programas desarrollados por el mismo Departamento de TI de la empresa auditada, cumplan con los estándares mínimos de desarrollo y que se realicen de forma segura y bajo procesos formales de desarrollo de software. Los controles evaluados en este proceso son:

- La organización ha adoptado un proceso formal para la adquisición o desarrollo de la infraestructura de TI y los sistemas de información.
- El desarrollo de sistemas significativos y proyectos de infraestructura son aprobados por TI y la alta gerencia.
- La organización efectúa suficientes pruebas y revisiones de las etapas clave en el ciclo del desarrollo de los sistemas.
- Los sistemas desarrollados o adquiridos y los proyectos de infraestructura son autorizados, probados y aprobados antes de ser puestos en producción.
- La metodología de desarrollo incluye fases de prueba y aceptación por parte de los usuarios.

5. **Funcionamiento Computacional:** Último proceso definido por la organización, el cual busca evaluar cómo la empresa auditada realiza respaldos de su información por medio de los servidores o servicios en la nube. Los controles de auditoría que se evalúan en esta área son:
    - Se ha implementado un horario de respaldo y requerimientos de retención proporcionales con el riesgo de la pérdida de datos, basándose en la criticidad del sistema y el costo de la recuperación manual.
    - Los procedimientos de respaldo y de recuperación son probados periódicamente para los sistemas incluidos dentro del alcance.

De los controles de auditoría mencionados anteriormente, es donde se establece el objetivo principal del presente Trabajo Final de Graduación, el cual busca que la MCGTI sea actualizada mediante el alineamiento de estos procesos con los estipulados en un marco de referencia que se adapte mejor a las evaluaciones de la organización, ya sea ITIL, COBIT o la norma ISO.

Por otro lado, una vez alineado cada uno de los procesos de auditoría que posee la organización con los procesos definidos en la metodología seleccionada, luego de realizar el análisis y clasificación de las mismas, se procederá a tomar el proceso de Gestión del Cambio, para el cual se definirán los controles de auditoría y las pruebas sustantivas para cada uno de los controles.

Para ejemplificar mejor el trabajo que se realizará sobre la MCGTI, a continuación se presenta la Tabla 1.2, donde se establece la tarea a realizar y los procesos de auditoría que se verán involucrados en dicha tarea.

Tabla 1.2. Alcance para cada uno de los procesos

Tarea a realizar	Procesos de auditoría en la MCGTI
Alineamiento a los procesos de COBIT 5.	Entendimiento de TI. Acceso a programas y datos. Gestión del Cambio. Desarrollo de programas. Funcionamiento computacional.
Definición de controles de auditoría y pruebas sustantivas.	Gestión del Cambio.

Fuente: Elaboración propia

Por último se define como producto tangible y final para la empresa, y como parte de este proyecto, se modificará la MCGTI, de forma que se automatizará por medio de macros en Microsoft Excel, de forma que el especialista de TI introduzca los resultados obtenidos de la evaluación realizada y la matriz le indique si el control es efectivo o no. La indicación se realiza a través de la colocación de un indicador dentro de la matriz, el cual representa el resultado final mediante un color:

- **Verde:** La prueba es efectiva, se cumple con el 100% de lo solicitado.
- **Amarillo:** Indica que el control evaluado es realizado por la organización pero su funcionamiento no es del 100%, lo que genera una oportunidad de mejora.
- **Rojo:** La prueba es inefectiva, no se cuenta con lo solicitado o fue funcionamiento no es el adecuado.

Con el fin de buscar cumplir el objetivo establecido, es necesario llevar a cabo una serie de actividades que se describen a continuación:

1. Establecer una rúbrica de medición para el análisis y calificación de las tres metodologías seleccionadas (ITIL, COBIT, ISO) con el fin de determinar la metodología que mejor se ajuste a las necesidades y operaciones de la organización.
2. Evaluar y analizar las tres metodologías (ITIL, COBIT, ISO) por medio de la rúbrica establecida en la etapa anterior, de la cual se obtendrá la metodología que mejor se adapta a las necesidades y operaciones de la Organización donde se lleva a cabo el TFG.
3. Estudiar los procesos que define la metodología seleccionada en el tema de Gestión de Cambio y que permitan definir controles de auditoría que se adapten a la evaluación Financiera que realiza la organización.

4. Analizar los controles identificados en los diferentes procesos establecidos en el marco de referencia seleccionado con el fin de determinar si el control se encuentra alineado a la auditoría realizada por la organización, y además si agregará valor para las auditorías, de forma que estas sean más detalladas.
5. Por otro lado, el análisis también debe de considerar la importancia y el impacto que tendrá la evaluación del control identificado y cómo ese control llegaría a mejorar los resultados obtenidos en la auditoría.
6. Una vez establecidos los controles de auditoría para evaluar la Gestión del Cambio, es necesario determinar las pruebas sustantivas, las cuales se encargan de establecer cómo se debe evaluar el control y la evidencia que se necesita para establecer si el control es efectivo o es inefectivo.
7. Las pruebas sustantivas definidas deben ser claras de forma que le permita al especialista de TI entender lo que debe evaluar en cada control. De mismo modo dichas pruebas sustantivas deben evaluar todos los escenarios posibles con el fin de que la evaluación sea lo más completa posible.
8. Finalmente, después de definir los controles y las pruebas sustantivas para la evaluación de la Gestión del Cambio, se han alineado como corresponde al marco de referencia seleccionado los restantes cuatro procesos de auditoría de la MCGTI. Se procede a realizar una automatización, desarrollada con macros en el programa de Microsoft Excel, donde se configurará la MCGTI para que al ingresar los resultados obtenidos por medio de la evaluación realizada, esta le indique al Especialista de TI si el control es efectivo, inefectivo o si el funcionamiento no es completamente el adecuado lo que genera una oportunidad de mejora.

A continuación se presenta la Figura 1.3, donde se presenta de forma resumida, los pasos y el trabajo a realizar para llevar a cabo el desarrollo el presente proyecto.

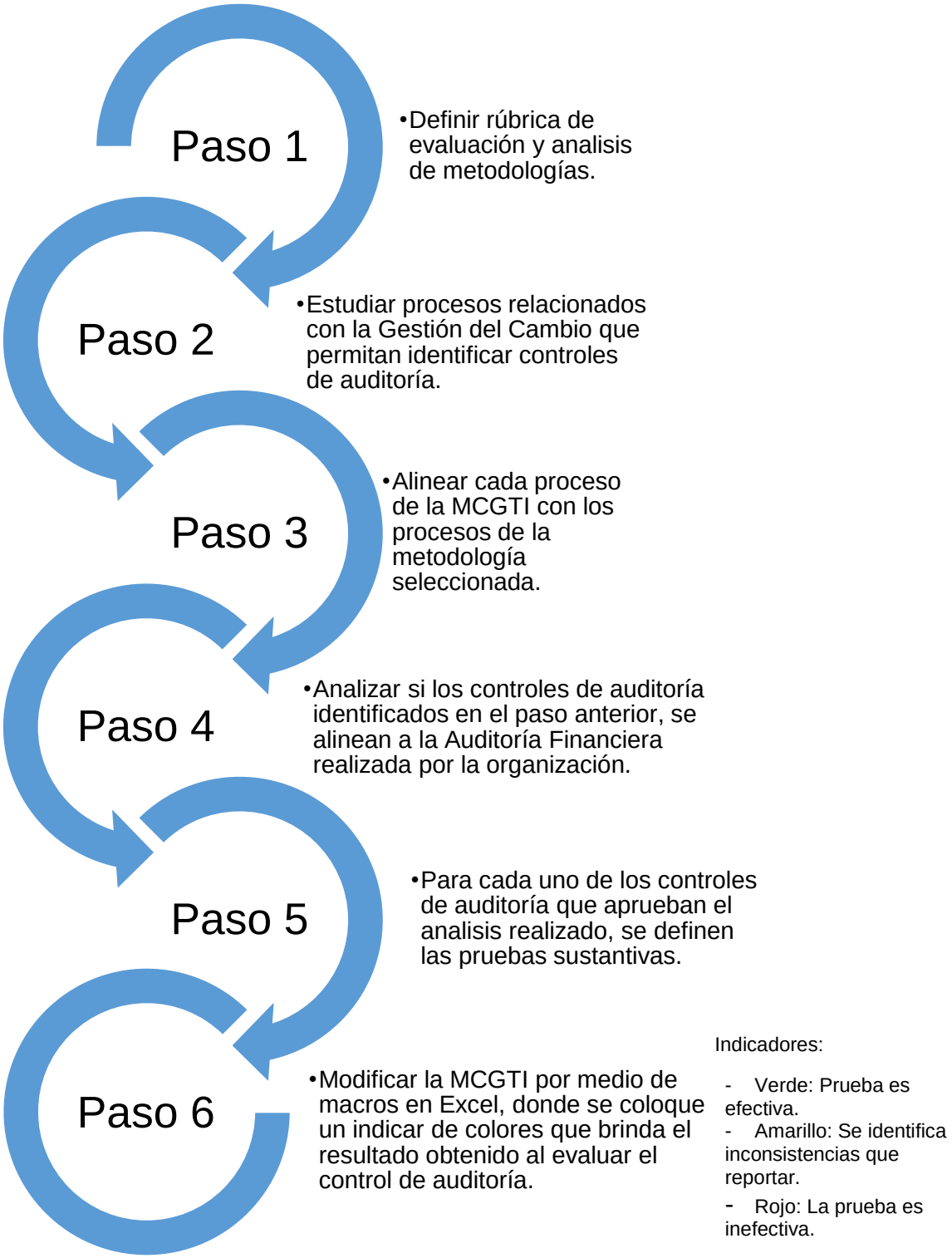

Figura 1.3. Conjunto de pasos para definir el alcance

Fuente: Elaboración propia

1.6 Entregables del proyecto

En esta sección se describen aspectos de gestión de proyecto, indicando cómo se llevará a cabo la administración del desarrollo, además de definir los entregables, donde se toma en cuenta los aspectos académicos, de gestión y productos a entregar a la organización.

1.6.1 Gestión del proyecto

La gestión de proyectos es la encargada de establecer las etapas para planificar, organizar y controlar los recursos con los que se cuenta en el proyecto con el fin de alcanzar los objetivos establecidos.

Para el presente proyecto la gestión está basada en el cumplimiento de los objetivos planteados en el apartado 1.3 Objetivos, para lo cual se establece cómo deben ser documentadas las minutas, el cronograma del proyecto con las actividades que se deben de realizar para completar con éxito el desarrollo del proyecto, además la gestión y el procedimiento para establecer cambios dentro de éste.

A continuación se describen como se llevarán a cabo cada uno de los apartados definidos en la gestión del proyecto, con el fin de buscar las metas y los objetivos establecidos.

1.6.1.1 Minutas

Para el presente proyecto se establece que para cada una de las reuniones se define una minuta escrita donde se afirman los puntos importantes. Las minutas deben ser firmadas por los participantes de la reunión y que son involucrados principales del proyecto.

El documento de la minuta debe contener los siguientes aspectos (Ver Apéndice A):

- Identificador de la minuta.
- Fecha en que se realizó la reunión.
- Objetivos de la reunión.
- Participantes de la reunión.
- Puntos importantes tratados.
- Acuerdos tomados.
- Firma de los involucrados danto fe a los acuerdos de la reunión.

1.6.1.2 Cronograma de proyecto

Para lograr el desarrollo del proyecto, es necesario establecer un cronograma que defina las actividades que se deben de llevar a cabo durante el periodo de desarrollo.

A continuación, por medio de la Tabla 1.3 se presenta el cronograma definido para el desarrollo del proyecto, este comprende las etapas metodológicas establecidas en el apartado 3 Desarrollo Metodológico del presente documento, así mismo se especifican los aspectos del informe final del trabajo el cual posee un enfoque académico. Dichas etapas se deben desarrollar durante las 16 semanas establecidas para completar el trabajo final de graduación.

Tabla 1.3. Cronograma del proyecto

Actividades/semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1. Estudio de bibliografía que respalde el desarrollo del proyecto.	X	X	X	X	X	X	X	X	X							
2. Marco Teórico	X	X	X	X	X	X	X	X								
3. Marco metodológico							X	X	X							
4. Desarrollo del proyecto						X	X	X	X	X	X	X	X	X		X
4.1. Análisis de las metodologías COBIT 5, ITIL V11, ISO 20000						X	X	X								
4.2. Alineación de la matriz de controles generales de TI a la metodología seleccionada							X	X								
4.3. Identificación de los controles de auditoría definidos en metodología seleccionada.							X	X	X							
4.4. Análisis de los controles identificados									X	X						
4.5. Definición de los controles de auditorías.										X	X					
4.6. Establecimiento de las pruebas sustantivas.										X	X	X				
4.7. Automatización la matriz de controles a evaluar.												X	X			
5. Conclusiones y recomendaciones													X	X		
6. Filólogo															X	
7. Revisión y corrección final del documento																X

Fuente: Elaboración propia

1.6.1.3 Gestión de cambios

En todo proyecto se solicitan cambios que afectan su desarrollo para lo cual se establece un procedimiento formal para gestionar los cambios que son solicitados por los involucrados del proyecto.

De acuerdo a la guía del PMBOK, define un cambio como un evento inevitable en un proyecto y que llega a impactar directamente al alcance y el desarrollo del mismo. Por tal razón es importante definir un proceso que establezca un análisis y una aprobación de los involucrados para decidir si un cambio es importante o no para el proyecto (Certificación PM, 2017).

Para llevar a cabo la aprobación de una solicitud de cambio, se define un comité de cambios que se encuentra integrado por los siguientes interesados:

- Profesor Tutor.
- Representante de la organización.
- Estudiante.

A continuación, se describe el procedimiento establecido para generar una solicitud de cambio que afectará el alcance del proyecto y cómo será el proceso de aceptación de la misma. El procedimiento establecido es el siguiente:

1. El solicitante debe completar la plantilla de solicitud de cambio (Ver Apéndice B).
2. La solicitud de cambio es evaluada por el profesor tutor del proyecto y el encargado del proyecto por parte de la organización.
3. El estudiante practicante en conjunto con el encargado del proyecto, establece si el cambio es importante para la necesidad que posee la organización y si mejorará el producto final.

4. El estudiante y el profesor tutor establecen el impacto que tendrá el cambio en el desarrollo del proyecto.
5. En caso que el cambio es de importancia para la organización y posee un impacto alto, se debe de llegar a un acuerdo entre las partes involucradas (estudiante practicante, profesor tutor, coordinador de Trabajo Final de Graduación y encargado del proyecto por parte de la organización).
6. La aprobación de la solicitud de cambio se debe de realizar por medio de la firma de cada uno de los miembros del comité de cambios.
7. Finalmente, se procede a documentar la solicitud de cambio en la bitácora de monitoreo (Ver Apéndice C), donde se documenta tanto las solicitudes aprobadas como las rechazadas.

1.6.2 Entregables de producto

En esta sección se identifican y se definen los entregables en cuanto a producto que tendrá el proyecto. A continuación se detalla cada uno de los entregables identificados.

1.6.2.1 Informe de alineación de los controles de auditoría respecto a los procesos definidos por COBIT 5

Mediante un informe escrito se especificará el proceso llevado para el análisis de las metodologías a estudiar (ITIL v11, COBIT 5, ISO 20000), así como la metodología seleccionada como producto del análisis, este mismo informe especificará el mecanismo utilizado para identificar cada uno de los procesos definidos en la metodología seleccionada, que permitan ser adaptados a los procesos de auditoría con los que se cuenta en la organización actualmente, de forma que estos se alineen la metodología.

Además, se especificarán los controles de auditoría identificados para el proceso de Gestión del Cambio tras el estudio de la metodología seleccionada, asimismo el análisis que se realizó para determinar los controles de auditoría utilizados para desarrollar las evaluaciones correspondientes.

Por último en este informe se establecerán las pruebas sustantivas para cada uno de los controles de auditoría definidos para el proceso de Gestión del Cambio.

1.6.2.2 Matriz automatizada de los Controles Generales de Tecnología de Información para el área de gestión de cambios

Este proyecto es para uso interno de la organización, para lo cual se busca identificar, analizar y definir los Controles Generales de TI para la evaluación de la Gestión del Cambio, además de alinear dicha matriz a los procesos definidos en el metodología seleccionada como producto del análisis a realizar entre ITIL v11, COBIT 5 e ISO 20000. Finalmente, se busca automatizar la Matriz por medio de una plantilla en Microsoft Excel, que le permita al auditor mayor orden y conocimiento de los controles que debe reportar ya sea con una oportunidad de mejora o con un hallazgo de auditoría. Dicha matriz es de uso interno para el auditor a la hora de realizar una evaluación.

Además se adquiere un conocimiento profesional en la definición de controles de auditoría y en la solicitud de pruebas sustantivas durante una evaluación.

1.6.2.3 Informe final del Trabajo de Graduación

El informe final cuenta con información para fines académicos donde se establecen los resultados obtenidos como producto de la investigación, desarrollo y obtención de los resultados a través de la conclusión del Trabajo Final de Graduación.

1.7 Restricciones o limitaciones del proyecto

A continuación, se describen las restricciones que afectan el proyecto durante su desarrollo. Estas restricciones contemplan factores, elementos, personas o circunstancias que afectan la realización del mismo. Los posibles factores son los siguientes:

- El apoyo que brinda la organización para el desarrollo del proyecto es únicamente por parte del área de Administración del Riesgo.
- Disponibilidad del personal involucrado para atender consultas sobre el proyecto.
- Uso de material confidencial de la organización.
- La Organización cuenta actualmente con un Sistema de Auditoría, en el cual se centran todas las pruebas y documentación realizada durante una evaluación.

1.8 Supuestos del proyecto

A continuación, se presentan los elementos que se asumen como ciertos para llevar a cabo el Trabajo Final de Graduación.

1. La información por parte de la organización es brindada al estudiante en el momento oportuno.
2. Los involucrados en el proyecto tienen interés en el desarrollo del mismo.
3. Apoyo por parte de la Gerencia General para el desarrollo del proyecto.

A partir de los objetivos, supuestos, limitaciones y demás generalidades descritas anteriormente, en el siguiente Capítulo del presente documento, se detallarán los conceptos a utilizar para el desarrollo del proyecto.

2. Marco Teórico

En el presente capítulo se establece la teoría, procedimiento y conceptos que se utilizarán en el desarrollo y constituyen la base para iniciar el proyecto.

2.1 Auditoría

Nació bajo la necesidad de identificar el fraude que realizan las organizaciones, se ha convertido en la actualidad en una herramienta que define controles sobre los procesos organizacionales que se apeguen a normas, marcos de referencia y regulaciones nacionales e internacionales que permitan establecer el buen funcionamiento en términos financieros de las empresas. La auditoría es la encargada de revisar la existencia y funcionalidad de dichos controles. A continuación, se describe su respectivo concepto.

2.1.1 Definición de Auditoría

La Real Academia Española (2017) en su diccionario define auditoría como “Revisión sistemática de una actividad o una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse.”

A partir del término anterior, se identifica que la auditoría se debe respaldar de criterios que amparen el cumplimiento de reglas establecidas por órganos reguladores o mejores prácticas del mercado, por parte de la empresa u organización auditada.

La Asociación de Auditoría y Control en Sistemas de Información (ISACA, 2015), en su glosario define auditoría de la siguiente forma: “Inspección y verificación formal para comprobar el cumplimiento a un estándar o un conjunto de lineamientos, de forma que se mantienen registros precisos o se cumplen los objetivos de eficacia y eficiencia” (pág. 8).

De acuerdo con lo anterior, la función de auditoría se basa en técnicas para obtener evidencia que justifica el cumplimiento de los lineamientos o estándares por parte del auditado. Algunas técnicas utilizadas por el auditor para obtener la evidencia son: Observación, Comparación, Indagación, Verificación, Inspección, Análisis y Rastreo.

Para que una auditoría, sea considerada como tal y logré obtener los resultados a partir de las técnicas de auditoría, esta debe ser independiente e integral en sus evaluaciones. Independiente a todas las funciones del auditado que evite el conflicto de funciones o de decisiones a tomar e integral donde comprenda todos los escenarios o elementos que son considerados dentro de la auditoría (JM Auditores, 2014).

Para una de las firmas de auditoría más importantes a nivel internacional como lo es KPMG, la auditoría se debe enfocar en tres fundamentos: Independencia, Integridad y Calidad (KPMG, 2017).

Adicionalmente, KPMG (2017) define que la auditoría debe ir más allá de una evaluación de la información financiera de una empresa, donde se consideren aspectos como: la cultura, sector de operación, competencia, entre otros elementos de la organización auditada. Además, amplia la definición al indicar que se debe enfocar la auditoría en áreas claves de riesgo, basado en las características operativas del auditado.

Por su parte, Echenique en su libro *Auditoría en Informática* establece que las compañías han mal empleado de manera inadecuada el término de auditoría, ya que esta es más que una e evaluación que busca errores, sino que es "Un examen crítico que se realiza con el objetivo de evaluar la eficacia y eficiencia de una organización y determinar acciones alternativas para la mejora de la misma" (s.f, pág. 2).

De lo anterior, es importante que la empresa auditada comprenda que la auditoría no es una acción que se basa en la búsqueda de errores como producto de las funciones que se realizan. La auditoría tampoco llega a indicar las operaciones que se realizan de mala manera, por lo contrario, la auditoría es una ayuda que se le brinda a la organización en busca de evaluar oportunidades de mejora que le permitan ajustarse a lineamientos o estándares que buscan una mejor funcionalidad en sus operaciones.

Es así como el proceso de auditoría consiste en evaluar a una empresa con el fin de establecer su situación actual de acuerdo a un objetivo específico en periodo o lugar determinado.

2.1.2 Evidencia de Auditoría

La evidencia de auditoría es la información obtenida por el auditor durante el periodo de evaluación y que respalda las opiniones, resultados y oportunidades de mejora sobre los controles auditados.

De acuerdo al glosario de términos de ISACA (2015), se define la evidencia de auditoría como "Información que es recolectada por el auditor en el curso de la auditoría, la cual es pertinente si tiene relación lógica con los resultados y conclusiones brindados al finalizar la evaluación" (pág. 40).

Por lo cual la evidencia de auditoría no es solamente la información que el auditor recolecta durante el periodo de evaluación, sino que esta debe ser analizada, evaluada y seleccionada para que permita obtener resultados que son traducidos en oportunidades de mejora. La evidencia se obtiene por medio de diferentes técnicas, el estándar 2205 de Aseguramiento y Auditoría de Sistemas de Información (ISACA, 2014) establece las técnicas más utilizadas para la obtención de la evidencia, estas técnicas son:

1. **Investigación y confirmación:** Se realizan encuestas formales por escrito y consultas orales con personal experimentado en el proceso que se evalúa.
2. **Observación:** Técnica que suele utilizarse sobre elementos físicos como instalaciones, hardware de computadora o configuración de los sistemas de información. Es importante conocer que la evidencia obtenida por este medio se limita al momento y lugar donde se realizó la observación.
3. **Inspección:** Examen de documentación y registro externo e internos. La inspección se realizan sobre activos fijos y documentación tanto física o electrónica.
4. **Procedimiento analítico:** Evaluación de datos tanto financieros como no financieros, así como la relación que se tiene entre los datos o con otra información relevante.
5. **Recalculo / Cálculo:** Técnica para validar la exactitud aritmética y matemática de documentos y registros.

6. **Análisis de rendimiento:** Rendimiento independiente de los procedimientos y/o controles que fueron ejecutados por el sistema de información.
7. **Otras técnicas:** Otras técnicas que suelen ser utilizadas por los auditores para la recolección de información son la ingeniería social o pruebas de instrucción ética.

Por otra parte la Organización Internacional para la Normalización (ISO[2]) establece el término evidencia como: “Registro, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de auditoría y que son verificables” (ISO 19011, 2011, pág. 9).

2.1.3 Criterio de Auditoría

Los criterios de auditoría son la base a partir de la cual los auditores se basan para comparar la evidencia obtenida, la norma ISO 19011 establece que un criterio de auditoría es: “Un grupo de políticas, procedimientos o requisitos usados como referencia y contra los cuales se compara la evidencia de auditoría” (2011, pág. 9).

De lo anterior, se establece que los criterios de auditoría son el medio que tiene el auditor para identificar si la evidencia obtenida durante la evaluación cumple o no con lo necesario para obtener resultado deseados o por lo contrario el incumplimiento de la evidencia daría como resultado un hallazgo de auditoría.

2.1.4 Hallazgo de Auditoría

Un hallazgo de auditoría es definido por la norma ISO 19011 como “Resultado de la evaluación de la evidencia de auditoría recopilada frente a los criterios de auditoría” (2011, pág. 9).

[2] International Organization for Standardization (ISO)

De lo anterior, los hallazgos son el resultado de la evaluación realizada a la empresa u organización auditada, los cuales son obtenidos como producto de la identificación de una inconsistencia observada desde la evidencia. La ISO 19011 amplía su definición de hallazgo de auditoría al indicar que permite convertir los hallazgos en oportunidades de mejora que se puede respaldar de las mejores prácticas del mercado (2011, pág. 9).

De acuerdo a lo establecido por la ISO 19011, se puede resumir que al momento que una evidencia no cumpla con lo establecido en un criterio de auditoría, se identifica un hallazgo de auditoría como producto de una deficiencia o debilidad identificada a la empresa u organización auditada.

2.1.5 Pruebas de auditoría

Durante el periodo de auditoría, se recauda información que es utilizada como evidencia, la cual permite desarrollar un análisis y revisión de la misma. La evidencia es obtenida por medio de las técnicas descritas anteriormente; sin embargo, para poner en práctica estas técnicas se tienen que ejecutar pruebas de auditoría, las mismas se dividen en: Pruebas de Cumplimiento y Pruebas Sustantivas, a continuación se definen cada una de ellas.

2.1.5.1 Pruebas de cumplimiento

Las pruebas de cumplimiento, le permiten al auditor verificar que la organización o el departamento auditado cuente con controles de monitoreo y que estos a la vez se encuentren funcionamiento de acuerdo a lo establecido formalmente en políticas, procedimiento o manuales organizacionales. ISACA (2015) define las pruebas de cumplimiento como “pruebas de control que se encuentran diseñadas para obtener evidencia de auditoría sobre la efectividad de los controles y su operación durante el período de auditoría” (ISACA, 2015, pág. 24).

Por otra parte, Echenique (s.f) establece que el objetivo de las pruebas de cumplimiento es determinar si los controles internos operan como fueron diseñados para operar. Asimismo agrega que el auditor como parte de sus funciones, debe determinar si los controles descritos realmente existen y si trabajan de forma confiable.

2.1.5.2 Pruebas Sustantivas

Adicionalmente, se establecen las pruebas sustantivas, las cuales son realizadas para determinar que los controles definidos se ejecutan correctamente, sin dar espacio al error. ISACA (2015) establece que las pruebas sustantivas evalúan la integridad, exactitud o existencia de actividades o transacciones durante el periodo de auditoría.

Mientras Echenique expone que el objetivo de una prueba sustantiva es obtener evidencia suficiente que permita al auditor emitir un juicio sobre el control evaluado. Asimismo, agrega que se han identificado ocho diferentes pruebas sustantivas (s.f, pág. 36):

1. Pruebas para identificar errores en el procesamiento o falta de seguridad o confidencialidad.
2. Pruebas para asegurar la calidad de los datos.
3. Pruebas para identificar la inconsistencia de los datos.
4. Pruebas para comparar con los datos o contadores físicos.
5. Confirmación de datos con fuentes externas.
6. Pruebas para confirmar la adecuada comunicación.
7. Pruebas para determinar falta de seguridad.
8. Pruebas para determinar problemas de legalidad.

Por lo anterior, se concluye que las pruebas de cumplimiento se basan en la verificación de la existencia y documentación formal de controles que permitan el monitoreo de las operaciones, mientras que las pruebas sustantivas buscan evaluar que estos controles funcionen de la forma correcta y como fueron definidos en la documentación.

2.2 Auditoría de TI

Auditoría de TI, en muchos casos conocida como Auditoría en Informática es la revisión y evaluación de los controles, sistemas y procedimientos de equipos de cómputo, utilización, eficiencia y seguridad. Además una evaluación en TI no es solamente sobre equipos de cómputo o de un sistema o procedimientos específicos, sino que también se debe evaluar los Sistemas de Información (SI) desde sus entradas, procedimientos, comunicación, controles, archivos, seguridad y obtención de la información (Echenique, s.f, pág. 19).

Por otro lado, una Auditoría de TI es una revisión con actividades independientes, al mismo tiempo que forma parte de auditorías de otras áreas organizacionales como un componente principal. En muchas organizaciones se realizan auditorías de TI con el fin de entender el grado de apoyo, conducción o la contribución de esta área al negocio y la operación del mismo (Gantz, 2014, pág. 83).

Se han definidos tipos de auditoría de acuerdo al lugar de aplicación (Interna y Externa) y área de aplicación de la misma (Financiera, Operacional, de Cumplimiento o Certificación), donde la Auditoría de TI se ha implementado. A continuación se detalla cada uno de los tipos de auditoría.

2.2.1 Por lugar de aplicación

La auditoría se puede clasificar por el lugar de aplicación, es decir, se refiere a la forma en que se realiza la evaluación y como se establece la relación laboral con la empresa auditada, por lo que se divide en Auditoría Interna donde se tiene una relación entre el auditor y la empresa; Y Auditoría Externa, en la cual el auditor no tiene relación con la empresa. Entonces conceptos se detallan a continuación.

2.2.1.1 Auditoría Interna

Una Auditoría Interna es realizada específicamente por un auditor propio de la empresa, en la cual se busca realizar un examen exhaustivo de las operaciones y sistemas involucrados dentro del alcance de la evaluación en busca de la exactitud y autenticación de los registros (Basu, 2009).

Por otro lado, este mismo autor agrega que el alcance y objetivos de una Auditoría Interna varían de acuerdo al tamaño, la estructura de la empresa auditada, así como los requerimientos brindados por la administración.

Finalmente, de acuerdo a Basu (2009) se establece que una Auditoría Interna debe contar con las características siguientes:

1. La Auditoría Interna de Sistemas es considerada como parte de un sistema de gestión de control.
2. El alcance de una auditoría interna depende de los requerimientos de la administración.
3. La natura y extensión de la evaluación depende del tamaño y tipo de negocio.
4. La Auditoría Interna es continua por naturales.
5. La existencia de una auditoría interna ayuda a la auditoría externa.

2.2.1.2 Auditoría Externa

La auditoría externa es realizada por un auditor externo, el cual es independiente a la empresa que se encuentra bajo evaluación. El ser independiente significa que es un profesional que no tiene relación con la empresa auditada, el cual le permite brindar un juicio objetivo sobre los resultados de auditoría (Basu, 2009).

Adicionalmente, define las siguientes características de una Auditoría Externa:

1. Es realizada por un auditor externo independiente.
2. Por lo general se realizan periódicamente.
3. Brindar una opinión sobre los resultados obtenidos de la evaluación.
4. Se realizan bajo un marco legal.
5. Son realizadas para mantener salvaguardar los intereses de dueños, accionistas e interesados que no tienen conocimiento del día a día de las operaciones de la empresa auditada.

De lo anterior se establecen las diferencias entre una Auditoría Interna y una Auditoría Externa. La Tabla 2.1 resume las principales diferencias establecidas por Basu (2009) en aspectos como: Naturaleza, Alcance, Propósito, Estado, Continuidad y Recomendaciones.

Tabla 2.1. Diferencia en Auditoría Externa y Auditoría Interna

Punto de Diferencia	Auditoría Externa	Auditoría Interna
Naturaleza	Se realiza para informar sobre la fiabilidad y equidad de las operaciones.	Se realiza con el objetivo de verificar el cumplimiento de las normas y procedimientos establecidos para proteger los activos de la organización.
Alcance	Estas auditorías son más completas en todos los aspectos. Su ámbito de aplicación no es restringido por la administración de la empresa auditada.	El ámbito de una auditoría interna es determinado por la administración de la empresa.
Propósito	Busca proteger los intereses de los propietarios y otras partes relacionadas con la empresa.	Busca mejorar el rendimiento, la eficiencia y la rentabilidad de la empresa.
Estado	Es una persona externa e independiente, por lo que no está obligado a cumplir las reglas y regulaciones de la empresa auditada.	El auditor interno es un colaborar de la empresa y está obligado al cumplimiento de las reglas y reglamentos de la misma.
Continuidad	Se realiza en un periodo determinado.	Por naturaleza es continua y se realiza a lo largo del año.
Recomendación	El brindar consejos o recomendaciones no es parte de las funciones de un auditor externos, este solamente informará sobre los hallazgos identificados.	El auditor interno puede asesorar a la dirección para que tome medidas correctivas contra irregularidades identificadas.

Fuente: Adaptado de (Basu, 2009)

2.2.2 Por Área de Aplicación

La auditoría de TI es un componente clave en otras auditorías como la Auditoría Financiera, Operacional, de Cumplimiento y de Certificación. (Gantz, 2014, pág. 84) La Figura 2.1 muestra como la Auditoría de TI, es un apoyo a otras auditorías realizadas en diferentes áreas de la organización.

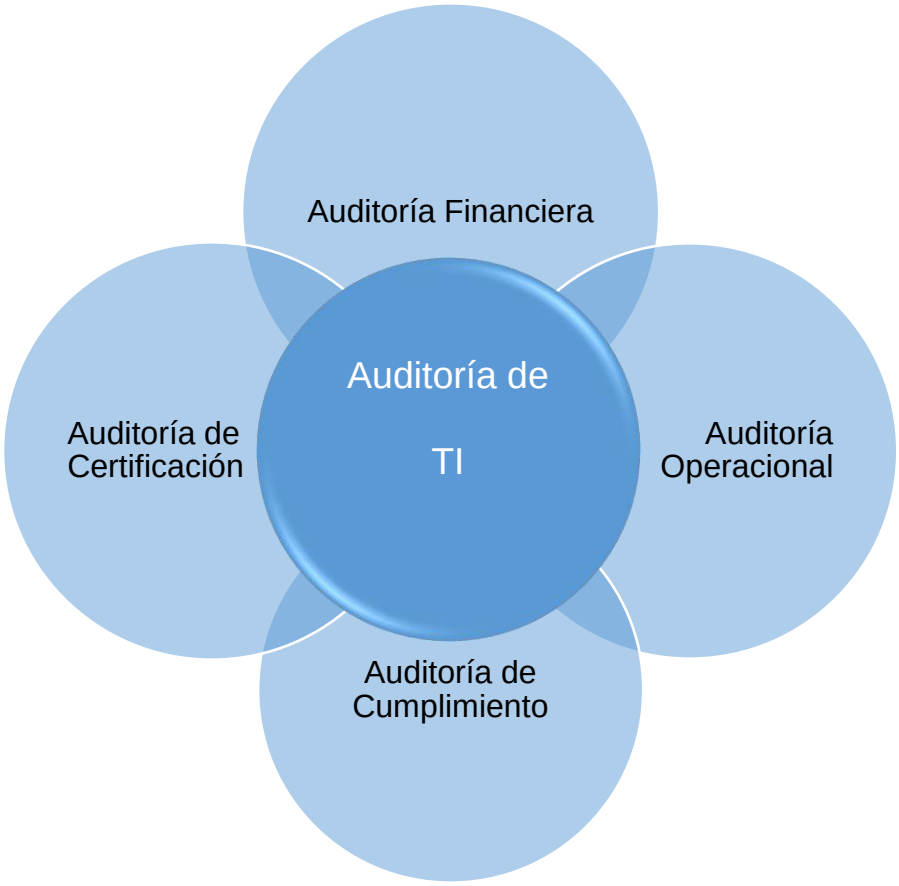

Figura 2.1. Relación de TI con otras áreas de Auditoría

Fuente: Adaptado de (Gantz, 2014, pág. 84)

2.2.2.1 Auditoría de Cumplimiento

Gantz (2014) define Auditoría de Cumplimiento como una gama de exámenes externos e internos del cumplimiento de los requisitos legales o reglamentarios de una organización, estándares de la industria, términos de licencia, compromisos contractuales u otras obligaciones formales.

Asimismo agrega que este tipo de auditorías son impulsadas por la necesidad de demostrar el cumplimiento de las disposiciones legales o reglamentarias, las cuales buscan verificar el acatamiento de las políticas, procedimientos, normas y directrices específicos para la organización (Gantz, 2014).

2.2.2.2 Auditoría de Certificación

La Auditoría de Certificación son evaluaciones formales de uno o más aspectos sobre las capacidades operaciones de una empresa. Estas evaluaciones se realizan basándose en requisitos explícitos que son asociados a normas o metodologías reconocidas (Gantz, 2014).

Por otra parte, agrega que las entidades responsables de las normas o metodologías sobre las cuales se realiza la evaluación, suelen publicar los criterios que se tomaran en cuenta para optar por la certificación.

2.2.2.3 Auditoría Operacional

Gantz (2014, pág. 87) define la Auditoría Operacional como la examinación de las prácticas de gestión, los procesos y procedimientos operativos para determinar con que eficacia o eficiencia las organizaciones cumples sus objetivos. Esta evaluación supone que la organización ha desarrollado un inventario de los procesos de negocio y el apoyo a las funciones administrativas, técnicas y se ha alineado las actividades operacionales con los objetivos a alcanzar.

Por otro lado Gantz (2014) describe que el alcance que tiene una Auditoría de TI dentro de una evaluación operacional se basa en los sistemas que soportan los procesos y la estructura organizacional que se evalúa. Por tal razón, la perspectiva de TI, desde una auditoría operacional es considerar la alineación de los sistemas, infraestructura, procesos de TI y procedimiento que soportan el cumplimiento de los objetivos organizacionales.

2.2.2.4 Auditoría Financiera

La Auditoría Financiera aborda principalmente las prácticas contables y el cumplimiento de los requisitos de información financiera, donde no solamente se basan en cómo las organización registran la información financiera, sino también en cómo las organizaciones mantienen la integridad, exactitud de dicha información (Gantz, 2014).

Aunado a lo anterior, Gantz (2014) indica que los Sistemas de Información en la Gestión Financiera ayuda a automatizar, clasificar y asegurar la información financiera, procesos contables y el registro de las transacciones. Por tal razón la Auditoría de TI en la Contabilidad Financiera se enfoca en los sistemas, software, controles de seguridad y entornos operacionales que las organizaciones establecen y mantienen para recopilar la información y presentar informes financieros.

Por otro lado, Nathaly Flores Moreno, en su tesis “Auditoría Financiera a los Estados Financieros al 31 de Diciembre de 2010 de la empresa de seguridad Omega” (pág. 106) establece que los objetivos de una Auditoría Financiera son:

1. Examinar el manejo de los recursos financieros de una unidad para establecer el grado en que sus empleados administran y utilizan los recursos y si la información financiera es oportuna, útil, adecuada y confiable.
2. Evaluar el cumplimiento de las metas y objetivos establecidos para la presentación de servicios o la producción de bienes de la empresa.
3. Verificar el cumplimiento de las disposiciones legales, reglamentarias y normativas aplicables en la ejecución de las actividades empresariales.
4. Formular recomendaciones dirigidas a mejorar el control interno y promover su eficiencia operativa.

2.3 Metodologías

A nivel mundial se han establecido diferentes metodologías o normas que dictan cómo se debe de gestionar la tecnología de información para obtener resultados acorde a la estrategia organizacional, entre las metodologías más reconocidas se encuentran ITIL[3] y COBIT[4]; mientras que la norma internacional sobre la gestión de TI la establece ISO[5].

A continuación se define en detalle cada una de las metodologías y la norma sobre la Gestión de TI.

2.3.1 ITIL v2011

La Librería de Infraestructura de Tecnologías de Información (ITIL) es una metodología para administrar TI como un servicio, su enfoque es en el usuario final en lugar de la tecnología (IT Governance Ltd, 2017).

De acuerdo a IT Governance Ltd (2017) ITIL fue desarrollada en la década de 1980 por la Agencia Central de Computadoras y Telecomunicaciones del Reino Unido (CCTA, por sus siglas en inglés), su creación se dio como un enfoque independiente de la tecnología con la capacidad de atender a las organizaciones con diferentes necesidades técnicas y de negocio. Para el año 2013 AXELOS se unió a la Oficina de Gabinete para maneja la cartera de Mejores Prácticas de Gestión, en la cual se incluye ITIL.

Esta compañía (IT Governance Ltd, 2017) ha establecido que mediante ITIL una organización se obtendría los siguientes beneficios:

[3] Information Technology Infraestructure Library (ITIL), tomado de: https://www.axelos.com/best-practice-solutions/itil
[4] Control Objectives for Information and Related Technologies (COBIT), tomado de: http://www.isaca.org/cobit/pages/default.aspx
[5] International Organization for Standardization (ISO), tomado de: https://www.iso.org/about-us.html

1. Mayor satisfacción del cliente.
2. Mayor Retención de personal.
3. Aumento del ROI en términos de TI.
4. Un enfoque más transparente de los costos y activos de TI.
5. Apoyo al cambio de negocio y la mejora continua.
6. Servicios de TI flexibles y adaptables.

2.3.1.1 Ciclo de vida de los servicios

ITIL versión 2011 define el Ciclo de Vida del Servicio por medio de cinco fases que describen los procesos que se deben desarrollar para proporcionar una estructura, estabilidad y fortaleza a la gestión del servicio (ITIL Service Strategy, 2011). La Figura 2.2 representa la interacción de las fases del ciclo de vida, las cuales son:

1. Estrategia del Servicio.
2. Diseño del Servicio.
3. Transición del Servicio.
4. Operación del Servicio.
5. Mejora Continua del Servicio.

Figura 2.2. Ciclo de Vida del Servicio

Fuente: Adaptada de (ITIL Service Strategy, 2011)

2.3.1.1.1 Estrategia del Servicio

El centro del ciclo de vida del servicio está la estrategia de servicio. El crear valor inicia desde esta fase con la compresión de los objetivos del negocio y las necesidades del cliente. Cada activo de la organización, donde un activo se entiende como personas, procesos y producto que apoyan la estrategia del negocio (ITIL Service Strategy, 2011).

Adicionalmente, ITIL en el libro de Estrategia del Servicio (2011) describe que los principios que sustentan la práctica de la administración de servicios, son útiles para desarrollar políticas, directrices y procesos de gestión de servicios a lo largo del ciclo de vida de los servicios. Entre los temas que se cubren en esta fase se incluye el desarrollo de espacios de mercado, las características de los tipos de proveedores internos y externos, los activos de servicio, la cartera de servicios y la implementación de la estrategia a lo largo del ciclo de vida. En las siguientes subsección se detallan los procesos que se definen para la Estrategia del Servicio (Bon, 2011).

2.3.1.1.1.1 Gestión de la Estrategia para Servicios de TI

Este proceso es el responsable de desarrollar y mantener las estrategias de TI desde un punto de vista comercial. Incluye una especificación del tipo de servicio prestado, de los clientes y proveedores globales de servicios, así como de los resultados generales del negocio.

2.3.1.1.1.2 Gestión del Portafolio de Servicio

Proceso que permite gestionar todas las inversiones de gestión de servicio en términos de valor para el negocio. El objetivo de la gestión del portafolio es lograr la máxima creación de valor al mismo tiempo que se gestionan los riesgos y los costos.

2.3.1.1.1.3 Gestión Financiera para Servicios de TI

Proceso que brinda la información esencial de gestión en términos financieros que se requiere para garantizar la prestación de servicios eficiente y rentable.

2.3.1.1.1.4 Gestión de la Demanda

Un aspecto esencial de la gestión de servicios es armonizar la oferta y la demanda. El objetivo de la gestión de la demanda es predecir lo más exacto posible la compra de productos y equilibrar la demanda con los recursos disponibles de la organización.

2.3.1.1.1.5 Gestión de las Relaciones del Negocio

El proceso responsable de la alineación entre los servicios y las necesidades del negocio. Ayuda a identifica y comprender las necesidades de los cliente para asegurar que el proveedor es capaz de proporcionar los servicios requeridos.

2.3.1.1.2 Diseño del Servicio

Para que un servicio ofrezca valor al negocio, debe ser diseñado de forma que se tome en cuenta los objetivos organizacionales. Esta fase es la que convierte la estrategia de servicio en un plan para entregar los objetivos del negocio (ITIL Service Strategy, 2011).

ITIL (2011) agrega que la fase de Diseños proporciona prácticas de administración de servicios que abarcan principios y métodos para convertir objetivos estratégicos en carteras y activos de servicio. Asimismo especifica que el Diseño no solamente se limita a la creación de nuevos servicios, sino que incluye cambios y mejoras necesarias para aumentar o mantener el valor de los clientes durante el ciclo de vida del servicio. Los procesos que define ITIL para el Diseño del Servicio son (Bon, 2011):

2.3.1.1.2.1 Coordinar el Diseño

Proceso encargado de coordinar el diseño que apoya a toda la fase al proporcionar un único proceso de coordinación integral para todas las actividades en la etapa de diseño del servicio.

2.3.1.1.2.2 Gestión del Catálogo de Servicio

El objetivo del catálogo de servicios es el desarrollo y mantenimiento de un inventario que incluya detalles precisos de todos los servicios, ya sean operativos, en desarrollo o retirados, asimismo debe incluirse los procesos que los soportan.

2.3.1.1.2.3 Gestión de los Niveles de Servicio

El objetivo de la gestión de los niveles de servicios es garantizar que los niveles de prestación de los servicios de TI se documenten, se acuerde y se logren tanto para los existentes como para los futuros acuerdos.

2.3.1.1.2.4 Gestión de la Disponibilidad

El objetivo de la gestión de la disponibilidad es garantizar que el nivel de disponibilidad de los servicios nuevos y modificados coincida con los niveles acordados con el cliente. Debe mantener un sistema de información que constituya la base del plan de la disponibilidad.

2.3.1.1.2.5 Gestión de la Capacidad

El objetivo de la gestión de la capacidad es asegurar que esta corresponda tanto a las necesidades actuales como las futuras de la organización.

2.3.1.1.2.6 Gestión de la Continuidad

El objetivo de este proceso es apoyar la continuidad del negocio al garantizar que las instalaciones de TI sean necesarias para restaurar el servicio dentro del tiempo acordado.

2.3.1.1.2.7 Gestión de la Seguridad

El objetivo de la gestión de seguridad de la información es garantizar que la política de seguridad de la información cumpla con la política general de seguridad de la organización y con los requisitos del gobierno corporativo.

2.3.1.1.2.8 Gestión de Proveedores

El objetivo de la gestión de proveedores es gestionar todos los proveedores y contratos con el fin de apoyar la prestación de servicio.

2.3.1.1.3 Transición del Servicio

La fase de Transición del Servicio proporciona orientación para el desarrollo y mejora de capacidades para introducir servicios nuevos y modificados en entornos compatibles, es decir, describe cómo hacer la transición de un estado a otro mientras se controla el riesgo y se apoya el conocimiento organizacional para la toma de decisiones (ITIL Service Strategy, 2011).

ITIL (2011) agrega que esta fase proporciona una orientación sobre la gestión de la complejidad relacionada con los cambios en los servicios y los procesos de gestión, en busca de evitar consecuencias indeseables que permitan la innovación. Los procesos definidos para esta fase son (Bon, 2011):

2.3.1.1.3.1 Planeación y Soporte de la Transición

Asegura la planificación y coordinación de los recursos para realizar la especificación del diseño del servicio.

2.3.1.1.3.2 Gestión del Cambio

Asegura que los cambios son desarrollados de forma controlada, además de ser evaluados, priorizados, planeado, probados, implementados y documentados.

2.3.1.1.3.3 Gestión de la Configuración y Activos de Servicio

Administra los activos de servicios y lo elementos de configuración (CI, por sus siglas en Inglés) para soportar los otros procesos de administración de servicio.

2.3.1.1.3.4 Gestión del Desarrollo y Entrega del Servicio

Prueba e implementar los servicios especificados en el diseño del servicio y asegurar que el cliente utilice el servicio de manera efectiva.

2.3.1.1.3.5 Validación y Pruebas del Servicio

La validación y prueba del servicio asegura que los servicios nuevos o modificados sean adaptados para el propósito establecido y apto para su uso, lo que genera valor para el servicio brindado.

2.3.1.1.3.6 Evaluación del Cambio

Asegura que cada punto importante del ciclo de vida de un cambio significativo se evalúe correctamente. Esta evaluación es necesaria para autorizar el paso a la siguiente etapa, por ejemplo antes de construir y probar o antes del desarrollo del mismo.

2.3.1.1.3.7 Gestión del Conocimiento

Este proceso mejora la calidad de la toma de decisiones al garantizar que la información es confiable, segura y se encuentre disponible durante todo el ciclo de vida del servicio.

2.3.1.1.4 Operación del Servicio

La Operación del Servicio brinda una orientación para lograr la efectividad en la entrega y soporte de los servicios para asegurar el valor para el cliente, usuarios y proveedor de servicios. Además proporciona orientación sobre cómo mantener la estabilidad en la operación del servicio, al permitir cambios en el diseño, escala, alcance y niveles de servicio (ITIL Service Strategy, 2011). Los procesos que se definen para esta fase son (Bon, 2011):

2.3.1.1.4.1 Gestión de Eventos

Este proceso es el encargado de recibir todos los eventos que se producen en la infraestructura de TI con el fin de supervisar el rendimiento regular esto puede ser automatizado para rastrear. Este proceso puede ser automatizado para rastrear y escalar circunstancias imprevistas.

2.3.1.1.4.2 Gestión de Incidentes

Se centra en la restauración de los fallos de los servicios lo más rápidamente posible para los clientes, de modo que éstos tengan un impacto mínimo para el negocio.

2.3.1.1.4.3 Gestión de Problemas

Este proceso toma en cuenta todas las actividades necesarias para el diagnóstico de la causa subyacente de los incidentes y para determinar una resolución a los problemas presentados.

2.3.1.1.4.4 Gestión de Activos

Este proceso es el encargado de permitir a los usuarios autorizados el acceso a un servicio mientras que prohíbe el acceso a los usuarios que no poseen el permiso correspondiente.

2.3.1.1.4.5 Solicitudes de Cumplimiento

Proceso que presenta las solicitudes de servicio de los usuarios que proporciona un canal para su solicitud, además de la información y cumplimiento de la misma.

2.3.1.1.5 Mejora Continua

Finalmente, como una fase continua por todo el ciclo de vida, la Mejora Continua de acuerdo a ITIL (2011) proporciona orientación sobre la creación y mantenimiento de valor para los clientes a través de una mejora en la estrategia, diseño, transición y operación del servicio. Esto gracias a la combinación de principios, prácticas y métodos de gestión de calidad, gestión del cambio y capacidad de mejora. Además, en la introducción del libro de Estrategia de Servicio de ITIL (2011) se establece para la fase de mejora continua un sistema de retroalimentación en bucle cerrado, basado en el ciclo *Plan-Do-Check-Act* (PDCA), el cual permite obtener retroalimentación de cualquier fase del ciclo de vida del servicio, misma que se puede utilizar para identificar oportunidades de mejora.

El ciclo PDCA (Ver Figura 2.3) es utilizada para realizar la mejora continua de los procesos, el cual de acuerdo a Garraza (2017) primeramente en la etapa de Planificar se debe los objetivos que se quiere alcanzar luego de conocer la situación de la organización para establecer un plan de mejora. Seguido a esto, en etapa de Hacer, se lleva a cabo las acciones planteada en la fase anterior, luego en la etapa Verificar, se revisan y controlan los resultados que se originaron después de aplicar las mejora y finalmente se Actúa, por medio de la documentación de lo aprendido, donde se confirma y normaliza la acción de mejora.

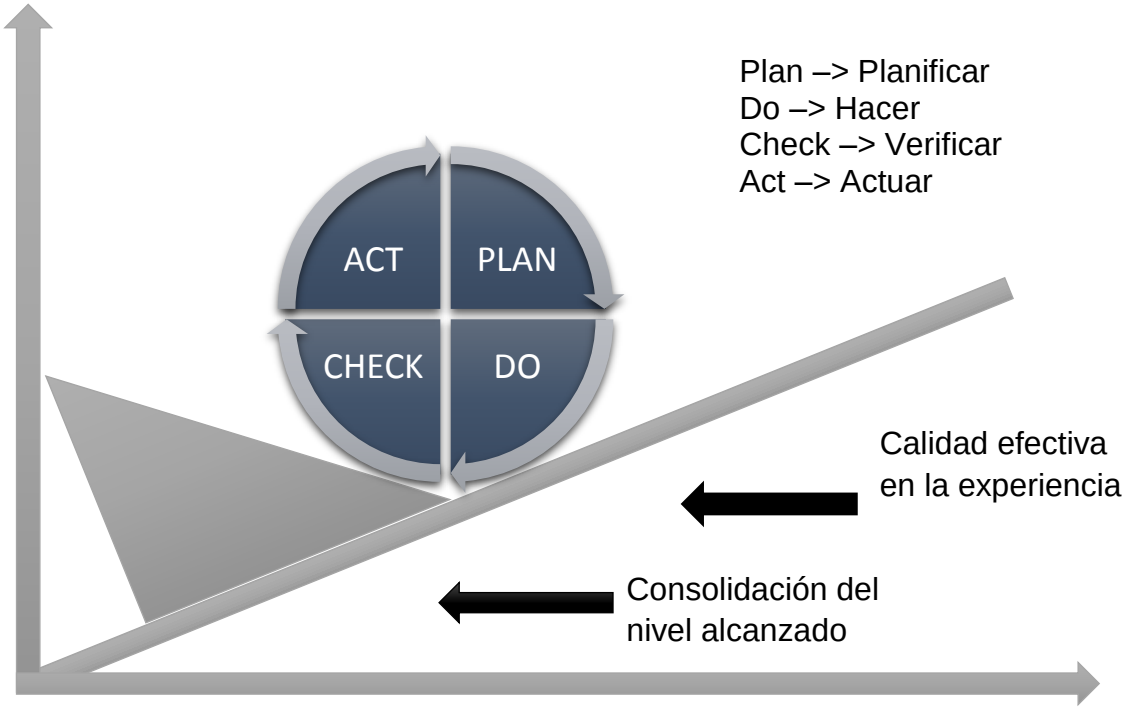

Figura 2.3. Ciclo de Plan-Do-Check-Act

Fuente: Adaptado de (ITIL Service Strategy, 2011)

De lo anterior, se resume en la Figura 2.4 los procesos que define ITIL para cada una de las fases del Ciclo de Vida de los Servicios.

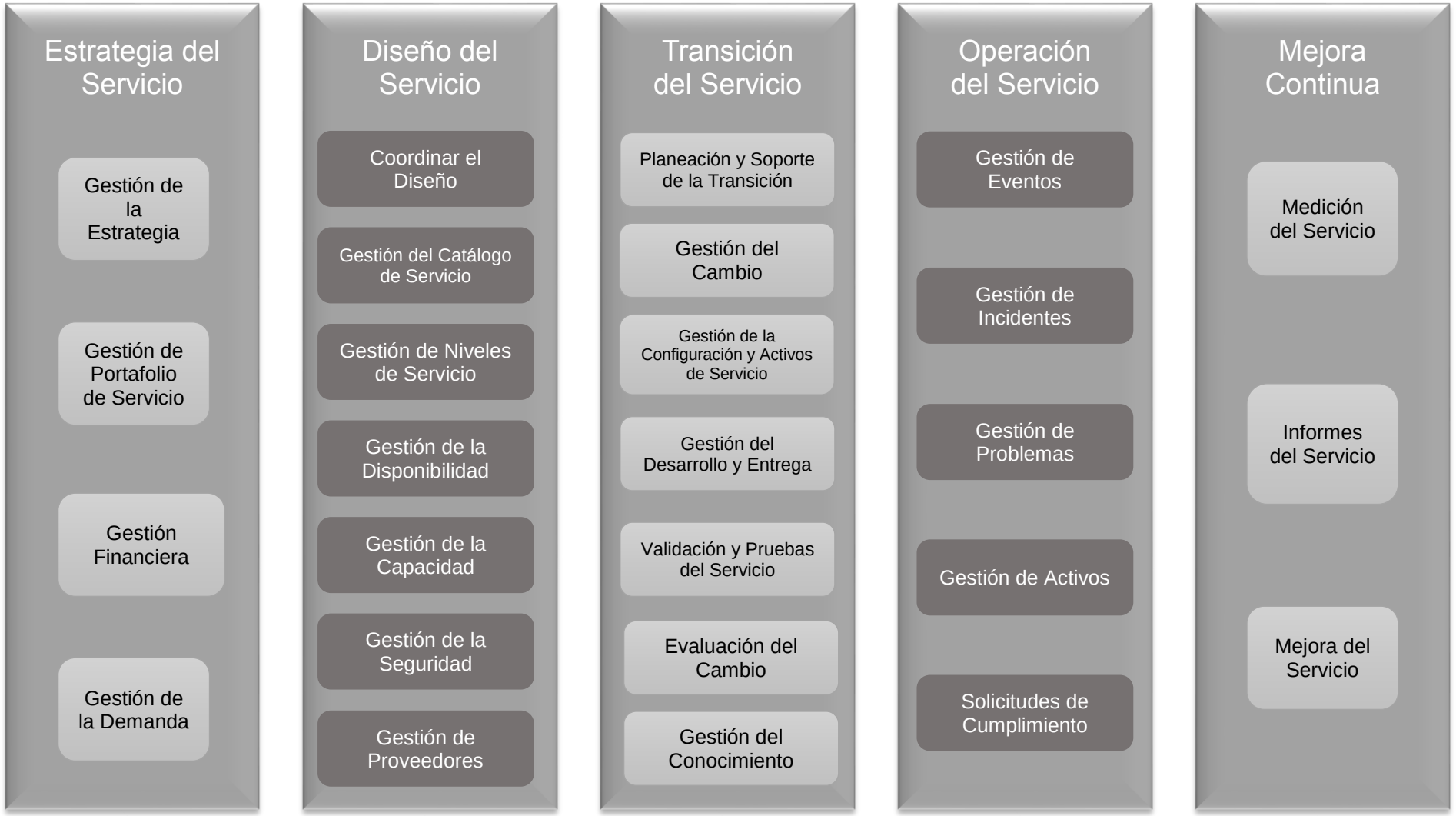

Figura 2.4. Procesos para cada fase del Ciclo de Vida

Fuente: Adaptado de (Cabinet Office, 2011)

2.3.2 COBIT 5

Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés) es un marco de referencia para el gobierno y gestión de TI que proporciona principios, prácticas, herramientas analíticas y modelos globalmente aceptados para ayudar a aumentar la confianza y el valor de los sistemas de información (ISACA, 2015).

COBIT es desarrollado por ISACA, Asociación Internacional de Miembros Profesionales en Tecnología de Información y Auditoría, con más de 100.000 miembros alrededor del mundo (De Haes & Van Grembergen, 2015).

De acuerdo a De Haes & Van Grembergen (2015) este marco se inauguró en los años 90's como un medio para llevar a cabo auditorías en entornos relacionados con TI de forma que constituía un conjunto completo de objetivos de control. Basado en lo anterior en la versión 3 se agregaron las Directrices de Gestión, que incluyó métricas, factores críticos de éxito y modelos de madurez para los procesos de TI.

Para el 2005, se lanzó la versión cuatro, la cual contiene conceptos de gestión y gobernanza, como alineación de los objetivos de negocio y de TI, además de la definición de procesos de TI, roles y responsabilidades (De Haes & Van Grembergen, 2015).

Para Abril del 2012 se publicó la última versión de COBIT, la cual contiene conceptos de Gobernanza de TI orientada a la estrategia organizacional. De acuerdo a sitio web de ISACA, COBIT 5 proporciona un marco completo que asiste a las empresas para lograr sus objetivos de gobernanza y gestión (De Haes & Van Grembergen, 2015).

2.3.2.1 Información Catalizadora

COBIT (ISACA, 2012) establece los principios básicos para agregar valor a partir de la gestión de TI. La Figura 2.5 establece los 5 principios básicos:

1. Satisfacer las necesidades de las partes interesadas.
2. Cubrir la empresa de extremo a extremos.
3. Aplicar un marco de referencia único e integrado.
4. Permitir un acercamiento holístico.
5. Separa el gobierno de la gestión.

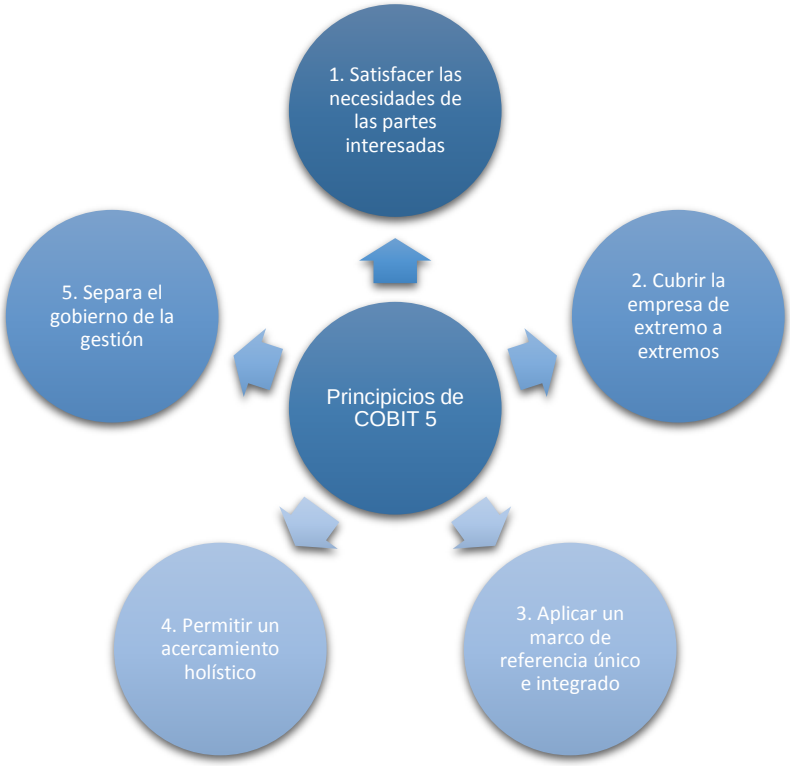

Figura 2.5. Principios Básicos

Fuente: Adaptado de (ISACA, 2012)

2.3.2.1.1 Satisfacer las necesidades de las partes interesadas

COBIT 5 establece que una empresa existe para crear valores para sus parte interesadas, que debe mantener un equilibrio entre la obtención de beneficios, la optimización del riesgo y el uso de recursos, de tal forma que los objetivos de alto nivel de una empresa se conviertan en objetivos de TI (ISACA, 2012).

2.3.2.1.2 Cubrir la empresa de extremo a extremos

Se debe cubrir todas las funciones y procesos de la empresa, donde no solo se centre en la función de TI, sino que trata la información y la tecnología como activos que deben ser manejados como cualquier otro activo de la empresa. Además, COBIT agrega que el gobierno y gestión de la información debe considerar de principio a fin todos los elementos y personas (ISACA, 2012).

2.3.2.1.3 Aplicar un marco de referencia único e integrado

Se debe establecer un estándar o buena práctica que proporcione el soporte de un subconjunto de actividades para TI (ISACA, 2012).

2.3.2.1.4 Permitir un acercamiento holístico

COBIT 5 define siete categorías de catalizadores que soportan la implementación de un completo sistema de gobierno y gestión para las TI de una empresa. Los catalizadores que se definen para alcanzar los objetivos de la empresa son:

1. Principios, políticas y marcos de trabajo.
2. Procesos.
3. Estructuras organizativas.
4. Cultura, ética y conducta.
5. Información.
6. Servicios, infraestructura y aplicaciones.
7. Persona, habilidades y competencias.

2.3.2.1.5 Separa el gobierno de la gestión

COBIT 5 implanta una clara distinción entre gobierno y gestión, los cuales abarcan diferentes tipos de actividades, requieren de diferentes estructuras de organización y sirven a propósitos diferentes (ISACA, 2012).

2.3.2.2 Modelo de referencia de Procesos de COBIT 5

Como parte de la distinción entre gobierno y gestión que establece COBIT 5 se describe lo siguiente:

1. **Proceso de Gobierno:** Los procesos de gobierno tratan de los objetivos de gobierno de las partes interesadas para entregar valor, optimizar el riesgo y los recursos. Además incluye prácticas y actividades orientadas a evaluar opciones estratégicas que proporcionen la dirección de TI, para lo cual COBIT 5 (2012) ha definido el dominio denominado “Evaluar, Orientar y Supervisar”, el cual se alimenta de las necesidades del negocio.

2. **Procesos de Gestión:** Se definen las prácticas y actividades de los procesos de gestión que cubren las áreas de responsabilidad de TI y de la empresa, de forma proporcionen cobertura de TI extremo a extremo, por tal motivo COBIT 5 (2012) ha establecido un total de cuatro dominios para la gestión de procesos, los mismo son: Planificar (APO), Construir (BAI), Ejecutar (DSS) y Supervisar (MEA). A partir de estos dominios se brinda retroalimentación de la gestión al proceso de gobierno.

En la Figura 2.6 se muestra como los cinco dominios son distribuidos entre el proceso de Gobierno y el proceso de Gestión que platea COBIT 5 (2012) para la Gobernanza de TI.

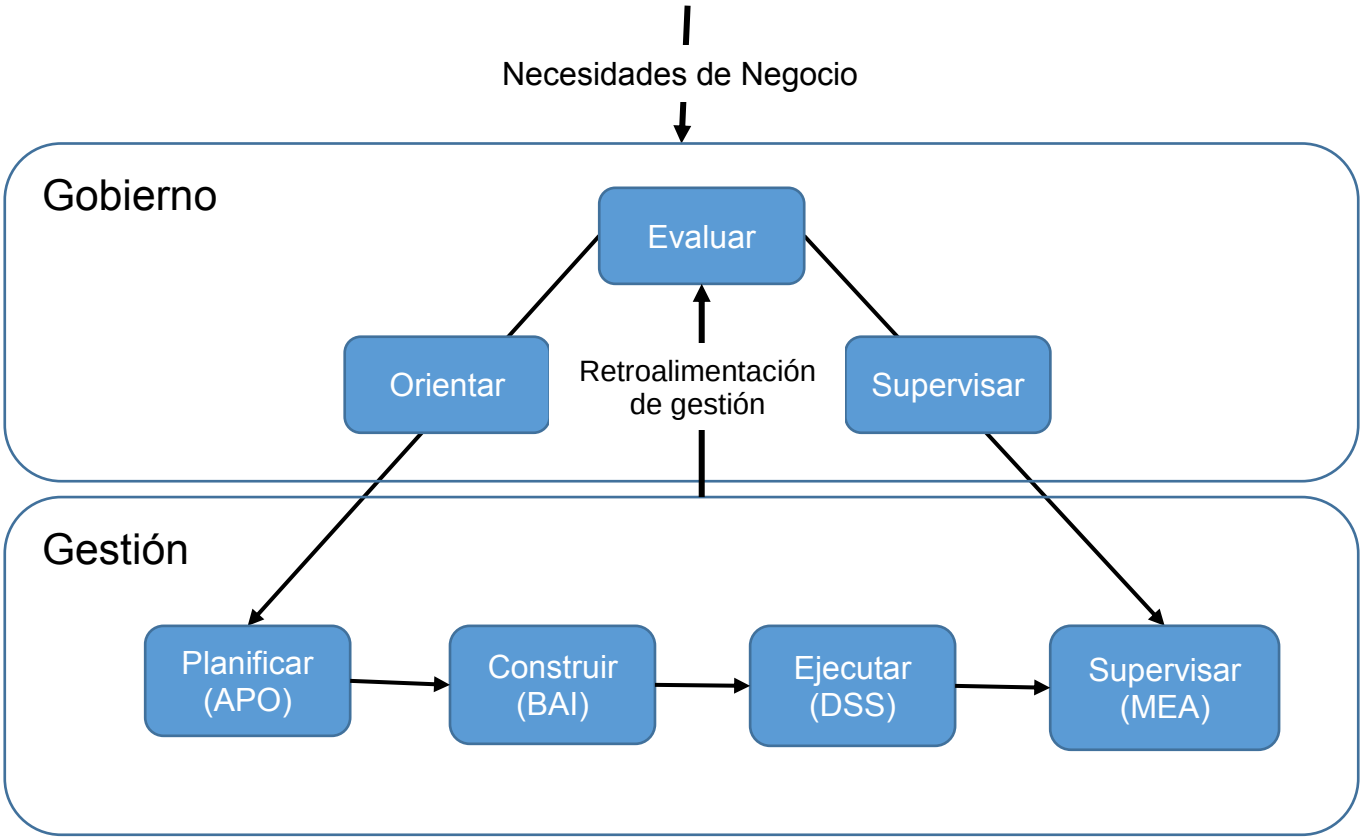

Figura 2.6. Área de Gobierno y Gestión

Fuente: Adaptado de (ISACA, 2012)

2.3.2.2.1 Procesos de COBIT 5

Bajo el modelo de procesos de COBIT 5 (2012) este establece un total de 37 procesos separados en la Gestión y Gobierno de los mismos. Estos procesos son agrupados en los cinco dominios mencionados anteriormente. Asimismo, se agrega que la incorporación de un modelo operacional y un lenguaje común a todas las partes de la empresa involucradas en actividades de TI es uno de los pasos más importantes y críticos hacían el buen gobierno de TI.

A continuación, se resumen los procesos de TI que establece COBIT 5, dicha información es tomada ISACA (2012), asimismo como las actividades que se deben ejecutar para completar cada proceso, mismos que son agrupados en los dominios descritos.

2.3.2.2.1.1 Evaluación, Orientar y Supervisar (EDM)

Este dominio forma parte del Gobierno de TI, el cual establece los objetivos de crear valor para la organización a partir de la entrega de beneficios, optimización de riego y recursos. Los procesos que los conforman son los siguientes:

2.3.2.2.1.1.1 EDM 01 Asegurar el establecimiento y mantenimiento del marco de referencia de Gobierno

Proporciona un enfoque consistente, integrado y alineado con el alcance del gobierno de la empresa, con el fin de garantizar que las decisiones relativas a TI se han adoptado en línea con la estrategia y objetivos de la empresa, lo que aprueba la supervisión de los procesos de manera efectiva y transparente, al cumplir con los requerimientos regulatorios y legales. Las actividades definidas para este proceso son:

- Evaluar el sistema de Gobierno.
- Orientar el sistema de Gobierno.
- Supervisar el sistema de Gobierno.

2.3.2.2.1.1.2 EDM 02 Asegurar la Entrega de Beneficios

Asegura un valor óptimo de las iniciativas de TI, servicios y activos disponibles al brindar un costo eficiente de los servicios y soluciones de forma confiable y precisa, además de los beneficios de las necesidades del negocio sean soportadas efectiva y eficientemente. Para este proceso se han definido las siguientes actividades:

- Evaluar la optimización del valor.
- Orientar la optimización del valor.
- Supervisar la optimización del valor.

2.3.2.2.1.1.3 EDM 03 Asegurar la Optimización del Riesgo

Asegura que los riesgos relacionados con TI no exceden ni el apetito ni la tolerancia de riesgo establecido, asimismo que el impacto de los riesgos de IT en el valor de la empresa sea identificado y se gestione, con el fin que el potencial fallo en el cumplimiento se reduce al mínimo. COBIT 5 ha definido las siguientes actividades para este proceso.

- Evaluar la gestión de riesgos.
- Orientar la gestión de riesgos.
- Supervisar la gestión de riesgos.

2.3.2.2.1.1.4 EDM 04 Asegurar la Optimización de Recursos

Busca asegurar que las necesidades de recursos de la empresa sean cubiertas de un modo óptimo, que el costo de TI sea optimizado y que con ello se incremente la probabilidad de la obtención de beneficios y la preparación para cambios futuros, para lo cual se han definidos una serie de actividades:

- Evaluar la gestión de recursos.
- Orientar la gestión de recursos.
- Supervisar la gestión de recursos.

2.3.2.2.1.1.5 EDM 05 Asegurar la Transparencia hacia las Partes Interesadas

Asegura que la comunicación con las partes interesadas sea efectiva y oportuna, de manera que se establezca una base para la elaboración de informes con el fin de aumentar el desempeño, identificar áreas susceptibles de mejora y confirmar que las estrategias y los objetivos relacionados con TI concuerdan con la estrategia corporativa, para lo cual se ha establecidos las actividades:

- Evaluar los requisitos de elaboración de informes de las partes interesadas.
- Orientar la comunicación con las partes interesadas y la elaboración de informes.
- Supervisar la comunicación con las partes interesadas.

2.3.2.2.1.2 Alinear, Planificar y Organizar (APO)

Dominio que forma parte de la Gestión de TI, el cual busca que se gestione la estrategia a partir de un marco de gestión de TI y una arquitectura empresarial que le permita gestionar la innovación, presupuesto, costos, recursos humanos, proveedores entre otros aspectos relacionados con la alineación y planificación de un proceso de TI. A continuación se detallan los procesos que conforman dicho dominio.

2.3.2.2.1.2.1 APO 01 Gestionar el Marco de Gestión de TI

Su objetivo es proporcionar un enfoque de gestión consistente que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión, estructuras, roles y responsabilidades organizacionales, basado en actividades fiables, reducibles. Para cumplir con este proceso se definieron las siguientes actividades:

- Definir la estructura organizativa.
- Establecer roles y responsabilidades.
- Mantener los elementos catalizadores del sistema de gestión.
- Comunicar los objetivos y la dirección de gestión.
- Optimizar la ubicación de la función de TI.
- Definir la propiedad de la información y del sistema.
- Gestionar la mejora continua de los procesos.

2.3.2.2.1.2.2 APO 02 Gestionar la Estrategia

Busca alinear los planes estratégicos de TI con los objetivos del negocio. Comunicar claramente los objetivos y las cuentas asociadas para que sean comprendidos por todo el personal, con la identificación de las opciones estratégicas de TI, estructurados e integrados con el plan de negocio, para lo cual las actividades definidos son:

- Comprender la dirección de la empresa.
- Evaluar el entorno, capacidades y rendimiento actual.
- Definir el objetivo de las capacidades de TI.
- Realizar un análisis de diferencias.
- Definir el plan estratégico y la hoja de ruta.
- Comunicar la estrategia y la dirección de TI.

2.3.2.2.1.2.3 APO 03 Gestionar la Arquitectura Empresarial

Representa los diferentes módulos que componen la empresa y sus interrelaciones, así como los principios de su diseño y evaluación en el tiempo, lo que permite una entrega, sensible y eficiente de los objetivos operativos y estratégicos. Para cumplir con lo anterior se debe llevar a cabo lo siguiente:

- Desarrollar la visión de la arquitectura de empresa.
- Definir la arquitectura de referencia.
- Seleccionar las oportunidades y las soluciones.
- Definir la implantación de la arquitectura.
- Proveer los servicios de arquitectura empresarial.

2.3.2.2.1.2.4 APO 04 Gestionar la Innovación

Buscar la ventaja competitiva, mediante la innovación empresarial que se realiza con eficiencia y eficacia operativa, para mejorar los desarrollos tecnológicos para la explotación de la información de forma que se ejecuten las siguientes actividades:

- Crear un entorno favorable para la innovación.
- Mantener un entendimiento del entorno de la empresa.
- Supervisar y explorar el entorno tecnológico.
- Evaluar el potencial de las tecnologías emergentes y las ideas innovadoras.
- Recomendar iniciativas apropiadas adicionales.
- Supervisar la implementación y el uso de la innovación.

2.3.2.2.1.2.5 APO 05 Gestionar el Portafolio

Optimiza el rendimiento del portafolio global en respuesta al rendimiento de programas y servicios, asimismo como de los cambios de prioridades y de la demanda corporativa. La gestión del portafolio se desarrolla por medio de las siguientes actividades:

- Establecer la mezcla del objetivo de inversión.
- Determinar la disponibilidad y las fuentes de fondos.
- Evaluar y seleccionar los programas a financiar.
- Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.
- Mantener los portafolios.
- Gestionar la consecución de beneficios.

2.3.2.2.1.2.6 APO 06 Gestionar el presupuesto y los costos

Fomenta la colaboración de TI con las partes interesadas de la empresa, con el fin de catalizar el uso eficaz y eficiente de los recursos relacionados con TI para brindar transparencia el costo y valor del negocio. Además permite a la empresa tomar decisiones informadas con respecto a la utilización de soluciones y servicios de TI. Lo anterior mediante el desarrollo de las actividades siguientes:

- Gestionar las finanzas y la contabilidad.
- Priorizar la asignación de recursos.
- Crear y mantener prepuestos.
- Modelar y asignar costos.
- Gestionar costos.

2.3.2.2.1.2.7 APO 07 Gestionar los Recursos Humanos

Establece como objetivo optimizar las capacidades de recursos humanos para cumplir los objetivos de la empresa, para lo cual se debe ejecutar lo siguiente:

- Mantener la dotación de personal suficiente y adecuada.
- Identificar personal clave de TI.
- Mantener las habilidades y competencias del personal.
- Evaluar el desempeño laboral de los empleados.
- Planificar y realizar un seguimiento del uso de recursos humanos de TI y del negocio.
- Gestionar le personal contratado.

2.3.2.2.1.2.8 APO 08 Gestionar las relaciones

Gestiona las relaciones entre el negocio y TI de modo formal, enfocándose en el objetivo común de obtener resultados empresariales exitosos apoyados de los objetivos estratégicos. Las actividades establecidas para este proceso son:

- Entender las expectativas del negocio.
- Identificar oportunidades, riesgos y limitaciones de TI para mejorar el negocio.
- Gestionar las relaciones con el negocio.
- Coordinar y comunicar.
- Proveer datos de entrada para la mejora continua de los servicios.

2.3.2.2.1.2.9 APO 09 Gestionar los acuerdo de servicio

Alinea los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, que incluyen la identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios de TI, niveles de servicio e indicadores de rendimiento. Las actividades a llevar a cabo para este proceso son:

- Identificar servicios de TI.
- Catalogar servicios basados en TI.
- Definir y preparar acuerdos de servicio.
- Supervisar e informar de los niveles de servicio.
- Revisar acuerdos de servicio y contratos.

2.3.2.2.1.2.10 APO 10 Gestionar proveedores

Administra todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, que incluye la selección de los proveedores, la gestión de las relaciones, gestión de contratos, revisión y supervisión del desempeño, para un cumplimiento de los mismos. En busca de una gestión eficiente de los proveedores se debe realizar lo siguiente:

- Identificar y evaluar las relaciones y contratos de proveedores.
- Seleccionar proveedores.
- Gestionar contratos y relaciones con proveedores.
- Gestionar el riesgo en el suministro.
- Supervisar el cumplimiento y el rendimiento del proveedor.

2.3.2.2.1.2.11 APO 11 Gestionar la Calidad

Define y comunica los requisitos de calidad en todos los procesos, procedimiento y resultados relacionados con la organización, que incluye controles, vigilancia constante y el uso de prácticas y estándares de mejora continua. Las actividades definidos para llevar a cabo la gestión de la calidad son:

- Establecer un sistema de gestión de la calidad.
- Definir y gestionar los estándares, procesos y prácticas de calidad.
- Enfocar la gestión de la calidad en los clientes.
- Supervisar, controlar y revisar la calidad.
- Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.
- Mantener una mejora continua.

2.3.2.2.1.2.12 APO 12 Gestionar el Riesgo

Identifica, evalúa y reduce los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Lo anterior se lleva a cabo por medio de las actividades siguientes:

- Recopilar datos.
- Analizar datos.
- Mantener un perfil de riesgo.
- Expresar el riesgo.
- Definir un portafolio de acciones para la gestión de riesgos.
- Responder al riesgo.

2.3.2.2.1.2.13 APO 13 Gestionar la Seguridad

Definir, opera y supervisa un sistema para la gestión de la seguridad de la información por medio de una serie de actividades, las cuales son:

- Establecer y mantener un Sistema de Gestión de Seguridad de la Información (SGSI).
- Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
- Supervisar y revisar el SGSI.

2.3.2.2.1.3 Construir, Adquirir e Implementar (BAI)

Dominio que corresponde a la Gestión de TI y que permite la definición de procesos desde la recolección de requerimientos, hasta la gestión de disponibilidad y capacidad del mismo. Además de mantener la configurar, conocimiento y gestionar los cambios que se deben de realizar durante la operación. Los procesos que se han definido para este dominio de describen a continuación.

2.3.2.2.1.3.1 BAI 01 Gestionar programas y proyecto

Gestionar todos los programas y proyecto del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa, de forma que inicia, planifica, controla, ejecuta programas, proyecto y a la hora de realizar el cierre revisa la post-implementación. Para lo anterior, se han definido las actividades siguientes:

- Mantener un enfoque estándar para la gestión de programas y proyecto.
- Iniciar un programa.
- Gestionar el compromiso de las partes interesadas.
- Desarrollar y mantener el plan de programa.
- Lanzar y ejecutar el programa.
- Supervisar, controlar e informar de los resultados del programa.
- Lanzar e iniciar proyectos dentro de un programa.
- Planificar proyectos.
- Gestionar la calidad de los programas y proyectos.
- Gestionar el riesgo de los programas y proyectos.
- Supervisar y controlar proyecto.
- Gestionar los recursos y los paquetes de trabajo del proyecto.
- Cerrar un proyecto o iteración.
- Cerrar un programa.

2.3.2.2.1.3.2 BAI 02 Gestionar la definición de requisitos

Identifica soluciones y analiza requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocio, aplicaciones, información/datos, infraestructura y servicios, para lo cual se establecen las actividades siguientes:

- Definir y mantener los requerimientos técnicos y funcionales del negocio.
- Realizar un estudio de viabilidad y proponer soluciones alternativas.
- Gestionar los riesgos de los requerimientos.
- Obtener la aprobación de los requerimientos y soluciones.

2.3.2.2.1.3.3 BAI 03 Gestionar la identificación y construcción de soluciones

Establece y mantiene soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Asimismo, gestiona la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios. Todo lo anterior mediante la ejecución de las actividades:

- Diseñar soluciones de alto nivel.
- Diseñar los componentes detallados de la solución.
- Desarrollar los componentes de la solución.
- Obtener los componentes de la solución.
- Construir la solución.
- Realizar controles de calidad.
- Preparar pruebas de la solución.
- Ejecutar pruebas de la solución.
- Gestionar cambios a los requerimientos.
- Mantener soluciones.
- Definir los servicios TI y mantener el catálogo de servicios.

2.3.2.2.1.3.4 BAI 04 Gestionar la disponibilidad y la capacidad

Brinda un equilibrio de las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costos. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados. Lo anterior por medio de lo siguiente:

- Evaluar la disponibilidad, rendimiento y capacidad actual y crear una línea de referencia.
- Evaluar el impacto en el negocio.
- Planificar requisitos de servicios nuevos o modificados.
- Supervisar y revisar la disponibilidad y la capacidad.
- Investigar y abordar cuestiones de disponibilidad, rendimiento y capacidad.

2.3.2.2.1.3.5 BAI 05 Gestionar la introducción del cambio organizacional

Maximiza la probabilidad de la implementación exitosa en toda la empresa del cambio organizacional de forma rápida y con un riesgo reducido, de forma que se cubre por completo el ciclo de vida del cambio, con todas las partes interesadas y TI. Lo anterior se logra mediante las actividades siguientes:

- Establecer el deseo de cambiar.
- Formar un equipo de implementación efectivo.
- Comunicar la visión deseada.
- Facultar a los que juegan algún papel e identificar ganancias en el corto plazo.
- Facilitar la operación y el uso.
- Integrar nuevos enfoques.
- Mantener los cambios.

2.3.2.2.1.3.6 BAI 06 Gestionar los cambios

Gestiona todos los cambios de una forma controlada, al incluir cambios estándares, de mantenimientos y de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte cierre y documentación. Las actividades establecidas para este proceso son:

- Evaluar, priorizar y autorizar peticiones de cambio.
- Gestionar cambios de emergencia.
- Hacer seguimiento e informar de cambios de estados.
- Cerrar y documentar los cambios.

2.3.2.2.1.3.7 BAI 07 Gestionar la aceptación del cambio y la transición

Ofrece una aceptación formal para hacer operativas nuevas soluciones, que incluye la planificación de la implementación, la conversión de los datos, además, envuelve las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de los procesos de negocio o servicio de TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación. Todo mediante la siguiente una serie de actividades:

- Establecer un plan de implementación.
- Planificar la conversión de procesos de negocio, sistemas y datos.
- Planificar pruebas de aceptación.
- Establecer un entorno de pruebas.
- Ejecutar pruebas de aceptación.
- Pasar a producción y gestionar los lanzamientos.
- Proporcionar soporte en producción desde el primer momento.
- Ejecutar una revisión post-implementación.

2.3.2.2.1.3.8 BAI 08 Gestionar el conocimiento

Mantiene disponible el conocimiento relevante, valido y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones, de forma que se planifique la identificación, recopilación, organización, mantenimiento, uso y retirada del conocimiento. Para lo cual se deben llevar a cabo las siguientes actividades:

- Cultivar y facilitar una cultura de intercambio de conocimiento.
- Identificar y clasificar las fuentes de información.
- Organizar y contextualizar la información, transformándola en conocimiento.
- Utilizar y compartir el conocimiento.
- Evaluar y retirar la información.

2.3.2.2.1.3.9 BAI 09 Gestionar los activos

Gestiona los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un costo óptimo, que se mantendrán en funcionamiento, justificados y protegidos físicamente. Además administra las licencias de software para asegurar que se adquiere el número óptimo y que se despliegan en relación con el uso necesario para el negocio, asimismo que el software instalado cumple con los acuerdos de licencia. Para cumplir con lo anterior se deben de ejecutar las siguientes actividades:

- Identificar y registrar activos actuales.
- Gestionar activos críticos.
- Gestionar el ciclo de vida de los activos.
- Optimizar el costo de los activos.
- Administrar licencias de software.

2.3.2.2.1.3.10 BAI 10 Gestionar la configuración

Define y mantiene las definiciones de las relaciones entre los principales recursos y capacidades necesarias para la prestación de los servicios proporcionados por TI, que incluyen la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación de la información y la actualización del repositorio de configuración. Las actividades definidas para cumplir con lo anterior son:

- Establecer y mantener un modelo de configuración.
- Establecer y mantener un repositorio de configuración, mediante una base de referencia.
- Mantener y controlar los elementos de configuración.
- Generar informes de estado y configuración.
- Verificar y revisar la integridad del repositorio de configuración.

2.3.2.2.1.4Entrega, Servicio y Soporte (DSS)

Dominio que pertenece a la Gestión de TI, el cual busca brindar soporte a los servicios definidos en el dominio anterior, esto por medio de la gestión de operaciones, problemas, continuidad y servicio de seguridad. Los procesos definidos se detallan a continuación.

2.3.2.2.1.4.1 DSS 01 Gestionar operaciones

Coordina y ejecuta las actividades y los procedimientos operativos requerimientos para entregar servicios de TI tanto internos como externos, que incluyen la ejecución de procedimientos operativos estándares predefinidos y las actividades de monitorización requeridas. Las actividades definidas para este proceso son:

- Ejecutar procedimientos operativos.
- Gestionar servicios externos de TI.
- Supervisar la infraestructura de TI.
- Gestionar el entorno.
- Gestionar las instalaciones.

2.3.2.2.1.4.2 DSS 02 Gestionar peticiones e incidentes de servicio

Provee una respuesta oportuna y efectiva de las peticiones de usuarios y la resolución de todo tipo de incidentes. Recupera el servicio normal; registra y completa las peticiones de usuarios, al registrar, investigar, diagnosticar, escalar y resolver incidentes. Lo anterior se desarrolla por medio de actividades que se enlistan a continuación:

- Definir esquemas de clasificación de incidentes y peticiones de servicio.
- Registrar, clasificar y priorizar peticiones e incidentes.
- Verificar, aprobar y resolver peticiones de servicio.
- Investigar, diagnosticar y localizar incidentes.
- Resolver y recuperarse de incidentes.
- Cerrar peticiones de servicio e incidentes.
- Seguir el estado y emitir informes.

2.3.2.2.1.4.3 DSS 03 Gestionar problemas

Identifica y clasifica problemas a partir de las causa raíz identificada con el fin de proporcionar una resolución a tiempo para prevenir incidentes recurrentes. Por lo cual proporciona recomendaciones de mejora por medio de las actividades descritas para este proceso, estas son:

- Identificar y clasificar problemas.
- Investigar y diagnosticar problemas.
- Levantar errores conocidos.
- Revolver y cerrar problemas.
- Realizar una gestión de problemas proactiva.

2.3.2.2.1.4.4 DSS 04 Gestionar la continuidad

Establece y mantiene un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio sobre la operación continua de los procesos críticos para el negocio y los servicios de TI requeridos, con el fin de mantener la disponibilidad de la información a un nivel aceptable para la empresa. Las actividades definidas se describen a continuación.

- Definir la política de continuidad del negocio, objetivos y alcance.
- Mantener una estrategia de continuidad.
- Desarrollar e implementar una respuesta a la continuidad del negocio.
- Ejecutar, probar y revisar el plan de continuidad.
- Revisar, mantener y mejorar el plan de continuidad.
- Proporcionar formación en el plan de continuidad.
- Gestionar acuerdo de respaldo.
- Ejecutar revisiones post-reanudación.

2.3.2.2.1.4.5 DSS 05 Gestionar servicios de seguridad

Busca proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la misma. Lo anterior se lleva a cabo por medio de las actividades que se detallan enseguida.

- Proteger contra software malicioso (malware).
- Gestionar la seguridad de la red y las conexiones.
- Gestionar la seguridad de los puestos de usuario final.
- Gestionar la identidad del usuario y el acceso lógico.
- Gestionar el acceso físico a los activos de TI.
- Gestionar documentos sensibles y dispositivos de salida.
- Supervisar la infraestructura para detectar eventos relacionados con la seguridad.

2.3.2.2.1.4.6 DSS 06 Gestionar controles de procesos de negocio

Define y mantiene controles apropiados del negocio para asegurar que la información relacionada con la organización satisface todos los requerimientos relevantes para el control. Además identifica los requisitos de la información para gestionar y operar los controles adecuados, de forma que se asegura que la información y su procesamiento satisfacen estos requerimientos. Para desarrollar lo anterior es necesario cumplir con las actividades siguientes:

- Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.
- Controlar el procesamiento de la información.
- Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización.
- Gestionar errores y excepciones.
- Asegurar la trazabilidad de los eventos y responsabilidad de información.
- Asegurar los activos de información.

2.3.2.2.1.5 Supervisar, Evaluar y Valorar (MEA)

Ultimó dominio que pertenece a la Gestión de TI, el cual tiene como propósito supervisar, evaluar y valorar, tal y como lo indica su nombre, los procesos, rendimiento y conformidad de las actividades y gestiones realizadas en los dominios anteriores. Para lo cual se han definido un total de tres procesos que se detallan a continuación.

2.3.2.2.1.5.1 MEA 01 Supervisa, evaluar y valorar el rendimiento y la conformidad

Recolecta, valida y evalúa métricas y objetivos de negocio, de TI y de procesos con el fin de supervisar que trabajen acorde al rendimiento acordado, conforme a los objetivos y métricas para proporcionar informes de forma sistemática y planificada. Para cumplir con lo anterior, se definieron las actividades siguientes:

- Establecer un enfoque de la supervisión.
- Establecer los objetivos de cumplimiento y rendimiento.
- Recopilar y procesar los datos de cumplimiento y rendimiento.
- Analizar e informar sobre el rendimiento.
- Asegurar la implantación de medidas correctivas.

2.3.2.2.1.5.2 MEA 02 Supervisar, evaluar y valorar el sistema de control interno

Supervisa y evalúa de forma continua el entorno de control, al incluir tanto autoevaluación con revisiones externas e independientes con el fin de facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Las actividades establecidas para este proceso son:

- Supervisar el control interno.
- Revisar la efectiva de los controles sobre los procesos de negocio.
- Realizar autoevaluaciones de control.
- Identificar y comunicar las deficiencias de control.
- Garantizar que los proveedores de aseguramiento son independientes y están cualificados.
- Planificar iniciativas de aseguramiento.
- Estudiar las iniciativas de aseguramiento.
- Ejecutar las iniciativas de aseguramiento.

2.3.2.2.1.5.3 MEA 03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos

Evalúa el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de la tecnologías de información, con el fin de garantizar que lo identificado, cumpla con los requisitos y que TI se encuentre alineado al cumplimiento de la empresa en general. Las actividades definidas para este proceso son:

- Identificar requisitos externos de cumplimiento.
- Optimizar la respuesta a requisitos externos.
- Confirmar el cumplimiento de requisitos externos.
- Obtener garantía de cumplimiento de requisitos externos.

Con el fin de resumir la conformación de los dominios de COBIT 5, así como los procesos que integran cada uno de estos, la Figura 2.7 muestra de forma gráfica la clasificación de los procesos y la relación que tiene uno con otro.

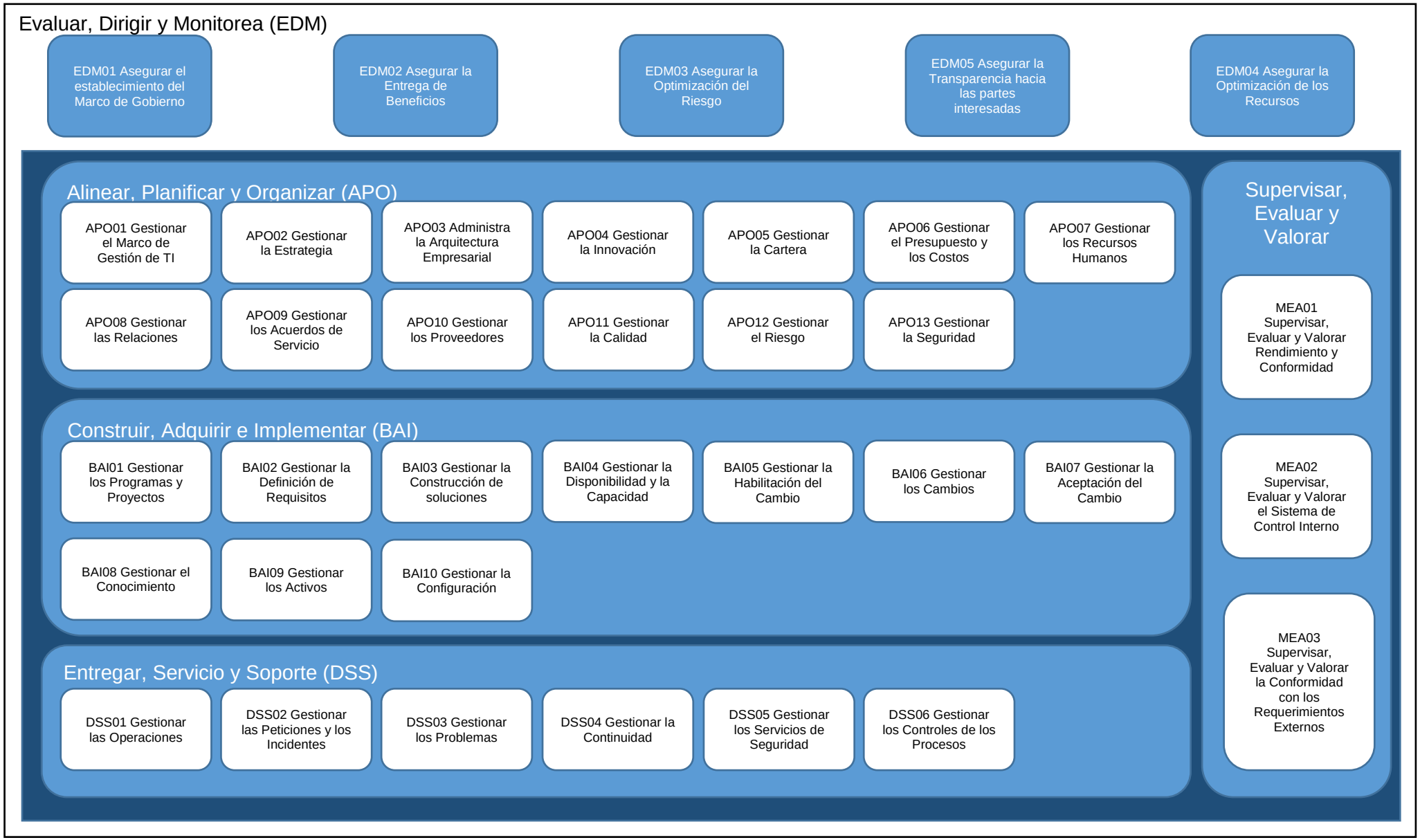

Figura 2.7. Dominios y procesos de COBIT 5

Fuente: Adaptado de (COBIT 5 Enabling Processes, 2012)

2.3.3 ISO/IEC 20000

La dinámica industrial de tecnologías de la información y las comunicaciones (TIC), presenta la necesidad de desarrollar, en paralelo al avance tecnológico, metodologías de trabajo que ofrezcan soluciones de gestión a los retos planteados, es por esto que la Organización Internacional de Normalización (ISO, por sus siglas en Inglés) y la Comisión Electrotécnica Internacional (IEC, por sus siglas en Inglés) propiciaron la elaboración de normas que consolidan las prácticas establecidas relacionadas con la gestión de TI, específicamente la elaboración de la Norma ISO/IEC 20000 publicada en junio del 2007 (ISO/IEC, 2007).

La Norma ISO/IEC 20000 (2007, pág. 16) define los procesos y las actividades esenciales para que las áreas de TI puedan prestar un servicio eficiente y alineado con las necesidades de la empresa u organización. Esta norma es construida sobre la base del modelo ITIL.

Por otro lado, se establece que esta Norma no es de índole técnico, ni tecnológico, sino que describe los principales flujos de actividades cuyo fin es lograr una entrega efectiva y de calidad. Además de definir un sistema reconocido y probado de gestión que permite a los proveedores de TI planificar, gestionar, entregar, monitorear, informar, revisar y mejorar los servicios (ISO/IEC, 2007).

2.3.3.1 Estructura de la Norma ISO/IEC 20000

La industria ya ha iniciado el camino para la definición de las actividades más relevantes, aquellas que se tienen que definir y optimizar para que las organizaciones de TI mejoren su funcionamiento. Algunas de los procesos esenciales que establece ISO/IEC 20000 (2007) ayudan a:

- Resolver de forma rápida los incidentes ocurridos en el servicio.
- Mejorar paulatinamente las tareas ocultas en la tecnología que soportan los servicios.
- Conocer con precisión la configuración de los servicios y sus componentes.
- Realizar cambios de una forma segura y eficiente.
- Entender con claridad las necesidades del cliente.
- Identificar y controlar los costos para optimizar la eficiencia de la organización.
- Controlar el desempeño de los suministros contratados.

A partir de lo anterior, ISO/IEC 20000 (2007) establecen un modelo de estructura mostrado en la Figura 2.8 que inicia con los sistemas de gestión de TI y en la planificación e implementación de la gestión del servicio. Seguidamente se basa en la definición del proceso agrupados en: Planificación e implementación de servicios nuevos o modificados; provisión del servicio, resolución, control y entrega de los procesos.

Asimismo, la Figura 2.8 hacia el interior muestra las actividades implementación de un sistema de gestión que establece la ISO/IEC 20000 con 14 procesos, mismos que se describen con mayor detalle a continuación a partir de la información obtenida de la norma (ISO/IEC, 2007).

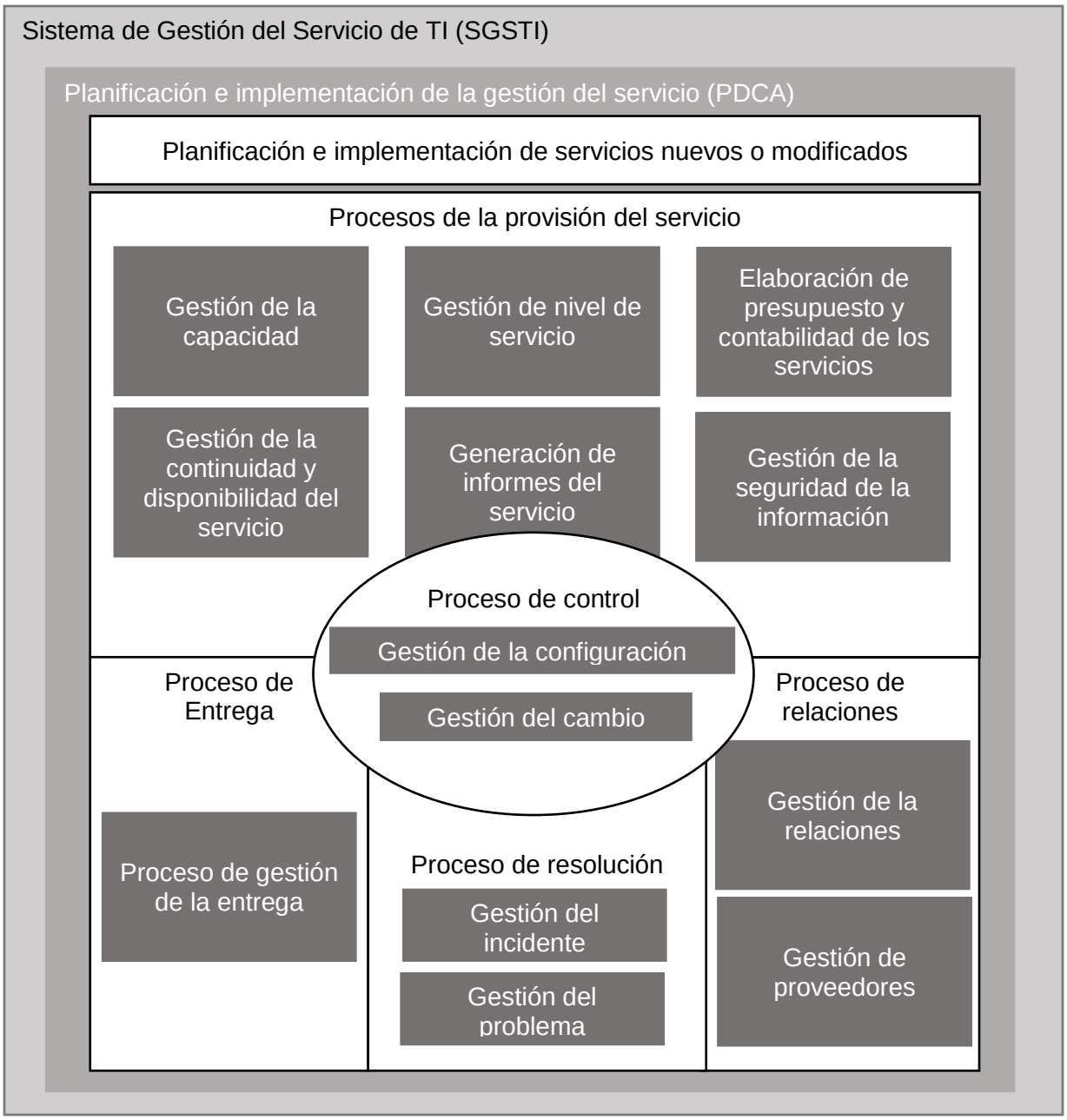

Figura 2.8. Estructura de procesos Norma ISO/IEC 20000

Fuente: Tomada de (ISO/IEC, 2007)

2.3.3.1.1 Sistema de gestión de TI (SGSTI)

Su objetivo es proveer una gestión de TI que incluya políticas y un marco de trabajo para hacer posible una efectiva gestión e implementación de todos los servicios de TI. Para conseguir la transformación de la actividad de TI, ISO/IEC 20000 (2007) establece que la gestión de TI se organice y regule alineada con el modelo de gestión del resto de la empresa.

2.3.3.1.2 Planificación e implementación de la gestión del servicio (PDCA)

En esta etapa del modelo ISO/IEC 20000 (2007) define el proceso de implementación de la norma, es decir, la propia gestión del servicio de TI, que toma en cuenta el ciclo de mejora continua, basado en el modelo PDCA internacional, que se describe brevemente como:

1. **P - Planificar:** Establece los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos de los clientes y las políticas de la organización.
2. **D - Hacer:** Implantación de los procesos.
3. **C - Verificar:** Realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, objetivos y requisitos para el producto e informar sobre los resultados.
4. **A - Actuar:** Tomar acciones para mejorar continuamente el desempeño de los procesos. Sirve de entrada a planificar.

2.3.3.1.3 Planificación e implementación de servicios nuevos o modificados

Describe el proceso de creación de un servicio nuevo o de realizar modificaciones a los servicios existentes, para que se puedan gestionar y entregar con los costos, calidad y plazo acordados con los clientes.

2.3.3.1.4 Proceso de provisión de servicios

Regula las actividades necesarias para que los servicios cumplan los cometidos pactados con el negocio. Toman relevancia frente a la necesidad de prestar servicios de TI de calidad, alineados a los objetivos del negocio, que cubran las necesidades actuales y que deben ser capaces de evolucionar rápidamente para cubrir las necesidades futuras. ISO/IEC 20000 (2007) define 6 procesos para la provisión del servicio.

2.3.3.1.4.1 Gestión del nivel de servicios

Proceso que se encarga de mantener y mejorar la calidad de los servicios de TI mediante una gestión eficiente de los acuerdo de nivel de servicio firmados con los clientes. Aporta los siguientes beneficios:

- Implementa un ciclo completo de creación y entrega de los servicio.
- Los servicios se crean de una forma eficiente.
- Los servicios se crean en los plazos acordados.
- Los servicios se crean con la participación de todas las áreas de la organización de TI. Gobierno, arquitectura, desarrollo.
- La organización de TI y sus clientes tienen una expectativa clara y formal del servicio solicitado.

2.3.3.1.4.2 Generación de informes del servicio

Proceso que centraliza la generación de todos los informes de TI para que sean homogéneos, útiles y entendibles por los destinatarios. Aporta los siguientes beneficios:

- Al centralizar en un proceso la generación de informes, obtiene una visión homogénea sobre TI.
- Se cubren todas las necesidades de informar y comunicar.
- La información es fiable.
- Centraliza todos los indicadores y mediciones de TI.
- Aumenta la productividad en la generación de informes.
- Hay un responsable que vela por la generación de informes en plazo, forma y calidad.

2.3.3.1.4.3 Gestión de la continuidad y disponibilidad del servicio

Proceso responsable de ofrecer unos niveles de disponibilidad adecuados a las necesidades de los clientes y unos niveles de funcionamiento acordados tras una contingencia. Este proceso brinda los siguientes aportes a la gestión de TI:

- Un plan de disponibilidad orientado a mejorar la disponibilidad general.
- Toma de conciencia sobre los servicios críticos para el negocio.
- Garantizar que se puedan satisfacer las necesidades de disponibilidad actuales y futuras.
- Conseguir reducir la frecuencia y la duración de los incidentes que quebranten la disponibilidad.

2.3.3.1.4.4 Elaboración de presupuesto y contabilidad de los servicios de TI

Proceso centrado en la gestión económica de los servicios de TI, que realizar una administración cuidadosa, responsable y eficiente de los costos. Entre los beneficios que brinda, se encuentran:

- Define las directrices para la gestión económica de TI.
- Integración con el área financiera de la empresa.
- Aumento del rigor en la definición y gestión de los presupuestos.
- Conocimiento exacto de los costos totales de propiedad a los largo de la vida de los servicios.
- Identifica ineficiencias existentes en relación a los costos.
- Permite un uso más eficiente de los recursos y los servicios de TI, al moderar la demanda de los clientes.

2.3.3.1.4.5 Gestión de la capacidad

Proceso que vela por que los servicios tengan en todo momento la capacidad necesaria y trabajen con un rendimiento óptimo, lo que brinda a la gestión de TI los siguientes aportes:

- Conocimiento de la evolución de actividades del negocio en su relación con la utilización de las TI.
- Gestión adecuada de la capacidad existente, que evita carencias y excesos.
- Un rendimiento optimizado.
- Garantía de que los servicios cumplen con la capacidad requerida en cada momento.
- Ahorro de costos, al tener los recursos ajustados a las necesidades.

- Minimiza las incidencias por falta de capacidad.

2.3.3.1.4.6 Gestión de seguridad de la información

Proceso responsable de gestionar la seguridad de la información al equilibrar las medidas con los costos que supone implementar. Entre los beneficios que se obtendría, se encuentran:

- Reduce el riesgo de virus, troyanos, gusanos, etc.
- Mejora custodia de los activos de información de la empresa.
- Aumenta la fiabilidad de los servicios, al reducir la probabilidad de incidentes de seguridad.
- Desarrolla métodos más eficientes en la resolución de incidentes de seguridad.
- Una gestión integral que proporcione una visión conjunta del impacto de la seguridad en el negocio.

2.3.3.1.5 Procesos de relaciones

Especifica las actividades de TI con su mundo exterior. Se centra en dos apartados claves: por un lado la relación entre el proveedor del servicio y el cliente; por otro lado la gestión de los proveedores, con el fin de garantizar la provisión sin interrupciones de los servicios de TI.

2.3.3.1.5.1 Gestión de relaciones

Proceso que regula las relaciones entre el departamento de TI y las áreas de los clientes. Entre los beneficios que se pueden alcanzar, se encuentran:

- El objetivo de TI es la satisfacción del cliente.
- Saca a TI de su mundo tecnológico.
- Fuerza a TI a trabajar para lo que necesita el negocio.
- Las relaciones con las áreas cliente se gestionan con mayor profesionalismo.
- Los servicios prestados se revisan de forma regular con los clientes de TI.
- Se formalizan los reclamos.
- Se impulsan acciones de mejora de los servicios.

2.3.3.1.5.2 Gestión de proveedores

Proceso que gestiona todo el aprovisionamiento y la prestación de los productos y servicios que TI necesita. Abarca las áreas de desarrollo de software, producción, entre otras. Los beneficios ligados a este proceso son:

- Asegurar la ejecución de la estrategia de *sourcing* relacionado con la contratación externa.
- Implementa una sistemática relación y gestión de proveedores para que realice de forma homogénea en todas las unidades de negocio.
- Implementa las mejores prácticas del mercado en la gestión de los suministradores.
- Alinea los servicios contratados con las necesidades de TI.

2.3.3.1.6 Proceso de resolución

Se centra en la resolución de incidentes nuevos o reincidentes ocurridos sobre los servicios, que dificultan o impiden que estos cumplan su cometido. Por un lado, se trata de restaurar el servicio para cumplir con los niveles de servicio acordados, y por otro lado se intenta minimizar los efectos negativos de las interrupciones de los servicios.

2.3.3.1.6.1 Gestión de Incidentes

Proceso que se ocupa del tratamiento de los sucesos que provocan la degradación o pérdida del funcionamiento normal de un servicio, con el objetivo fundamental de recuperar el servicio para el cliente lo más rápido posible. Los beneficios asociados a este proceso son:

- Prioriza la atención de incidentes de acuerdo con los compromisos de servicios.
- Reduce el impacto de los incidentes, al realizar la restauración cuanto antes del servicio.
- Gestiona el conocimiento en relación a la resolución de incidentes.
- Mejora la eficiencia en el tratamiento de los incidentes y peticiones de los usuarios.
- Colabora en la identificación proactiva de mejoras en los servicios y en los procedimientos.

2.3.3.1.6.2 Gestión de problemas

La misión del proceso es evitar que se produzcan incidentes repetitivos o nuevos. Para lo cual se identifican y subsanan los defectos en los componentes de los servicios. Este proceso le brinda a la gestión de TI los aportes siguientes:

- Reduce el número de incidentes.
- Asegura la resolución de defectos graves que afectan al servicio.
- Propone proyectos de mejora para resolver los defectos.
- Identifica la causa raíz de las incidencias y evita su repetición.
- Propone proyectos de mejora para resolver los defectos.
- Encuentra soluciones provisionales y permanentes.
- Realiza el seguimiento de la resolución de los problemas identificados.

2.3.3.1.7 Proceso de control

Asegura a los gestores la calidad de la información sobre los servicios, así como, que todo cambio se realiza de forma controlada. Contempla dos apartados claves: Primeramente, el control de todos los componentes del servicio y la infraestructura, al mantener la información precisa sobre la configuración de dichos componentes. Y en segundo lugar asegura que todos los cambios que se produzcan sobre dichos componentes sean valorados, aprobados, implementados y revisados.

2.3.3.1.7.1 Gestión de la configuración

Proceso responsable de gestionar y mantener actualizada toda la información común que necesitan las áreas de TI. Los aportes que brinda este proceso son:

- Información precisa y actualizada sobre los componentes de TI.
- Visión de todos los elementos que componen un servicio y las relaciones entre ellos.
- Fiabilidad en las actualizaciones al disponer de información precisa.
- Eficiencia en el trabajo al tener accesible la información común que se necesita.
- Compartir la información común entre todos los procesos.
- Control de todos los elementos de software instalado.

2.3.3.1.7.2 Gestión del cambio

Proceso responsable del control y tratamiento de los cambios en los servicios y en la infraestructura de TI, en busca de asegurar que todos los cambios son registrados, evaluados, aprobados, implementados y revisados de una manera controlada. Dentro de los aportes que brinda este proceso a la gestión de TI, se encuentran:

- Mayor fiabilidad de los servicios al minimizar el impacto sobre la calidad del servicio por los cambios.
- Asegurar el empleo de métodos para manejar eficaz y eficientemente un alto volumen de cambios.
- Implantar una gestión integral que proporcione una visión conjunta del impacto de los cambios en el negocio.
- Realizar cambios en los servicios de manera ordena y estructurada, que permite coordinar las actividades a realizar.
- Garantizar que todos los cambios son registrados adecuadamente.

2.3.3.1.8 Proceso de entrega

Se centra en definir las actividades a realizar durante la etapa de tránsito de los cambios, desde la etapa de desarrollo hasta su paso a producción. Asimismo asegura que todos los componentes necesarios para la puesta en producción real de un servicio están correctamente definidos y probados.

2.3.3.1.8.1 Gestión de la entrega

Proceso que organiza y controla los pasos al entorno de producción de los cambios aprobados, con el fin de entregar, distribuir y realizar el seguimiento de uno o más cambios en el entorno de producción real. Los beneficios asociados a este proceso son:

- Ordenar el trabajo continuo de implementar los cambios.
- Planificar la actualización de todas las entregas a implementar.
- Integrar los desarrollos en el entorno producto.
- Información actualizada sobre lo instalado en producción.
- Colabora en el control de las versiones del software instalado.
- Calidad en las actualizaciones al disponer de información precisa.
- Control del almacén de componentes de hardware.

2.4 Gestión del Cambio

Como se mencionó en el apartado 2.3 Metodologías, se realizó una descripción resumida de Gestión del Cambio de cada una de las metodologías involucradas en el proyecto; no obstante, en el este apartado se brindará un mayor detalle de la definición de Gestión del Cambio de acuerdo a ITIL v2011, COBIT 5 e ISO/IEC 20000.

2.4.1 ITIL v2011

ITIL (ITIL Service Transition , 2011) define un cambio como es la adición, modificación o eliminación de todo lo que podría tener efecto en los servicios de TI. Agrega que el ámbito debe incluir cambios en todas las arquitecturas, procesos, herramientas, métricas y documentación, así como cambios en los servicios de TI y otros elementos de configuración.

Asimismo, se define en la fase de Transición de ITIL (2011) que todos los cambios deben ser registrados y gestionados de forma controlada. El alcance de la Gestión de Cambios abarca cambios en todos los elementos de configuración a lo lardo de todo el ciclo de vida del servicio, ya sean activos físico como servidores o redes, activos virtuales como servidores virtuales o almacenamiento virtual u otro tipo de activo como acuerdos o contratos. También cubre todos los cambios en cualquier de los cinco aspectos del diseño del servicio.

Los objetivos que establece ITIL (2011) al implementar la Gestión del Cambio en una organización son:

1. Responder a los requerimientos cambiantes del negocio del cliente mientras maximiza el valor y reduce los incidentes, la interrupción y el re trabajo.
2. Responde a las solicitudes de cambio de negocio y TI donde se alineen a los servicios con las necesidades del negocio.
3. Asegurar que los cambios sean registrados, evaluados, que los cambios autorizados son priorizados, planificados, probados, implementados, documentados y revisados de manera controlada.
4. Optimiza el riesgo global del negocio.

Por medio de una Solicitud de Cambio se insta a realizar un cambio en los servicios de TI, ITIL (ITIL Service Transition , 2011) define una Solicitud de Cambio como una comunicación formal que busca la alteración de uno o más elementos de configuración. Por otro lado agrega que se existen diferentes tipos de cambios que requieren diferentes tipos de solicitudes. Se puntualizan tres tipos de cambio:

1. **Cambio Estándar:** Es un cambio pre autorizado, considerado de bajo riesgo debido a que sigue un procesamiento o una instrucción de trabajo ya conocida.
2. **Cambio de emergencia:** Un cambio que debe implementarse lo antes posible.
3. **Cambio normal:** Cualquier cambio de servicio que no es cambio estándar o un cambio de emergencia.

Muy a menudo los términos “Cambios”, “Registro del Cambios” y “Solicitud del Cambio (RFC[6])” son utilizados de forma errónea de acuerdo a ITIL (2011), por lo cual define cada uno de estos términos de la siguiente forma:

1. **Cambios:** Es la adición, modificación o eliminación de cualquier cosa que afecte un los servicios de TI, que incluye las arquitecturas, procesos, herramientas, métricas y documentación.
2. **Solicitud de Cambio (RFC):** Es una propuesta formal para un cambio que debe hacerse, el cual incluye detalles del cambio propuesto. Con frecuencia se utiliza como un registro de cambio.
3. **Registro del Cambio:** Es un documento que contiene los detalles del cambio, en el cual se describe todo el ciclo de vida de un solo cambio. Se debe crear un registro del cambio para cada solicitud que se reciba, incluso para los cambios que son rechazados.

Finalmente ITIL (2011) define un proceso con las actividades que se deben realizar para Gestionar los Cambios en una organización. La Figura 2.9 muestra el proceso definido, asimismo como las actividades y la relación de cada uno. Las actividades definidas son:

1. Crear y registrar una Solicitud de Cambio (RFC).
2. Revisar la Solicitud de Cambio (RFC).
    - Realizar un filtro del cambio, ya sea por cambio incompletos.

[6] Request For Change (RFC) tomado de: (ITIL Service Transition , 2011)

3. Evaluar el cambio.
    - Se establecen niveles apropiados de autorización del cambio.
    - Establecer las áreas relevantes de interés para los cambios.
    - Evaluar la justificación del negocio, impacto, costo, beneficios, riesgos y rendimiento previsto del cambio.
4. Autorizar el cambio.
    - Obtener la autorización o el rechazo del cambio.
    - Comunicar la decisión a todas las partes interesadas.
5. Planificar las actualizaciones.
6. Coordinar la implementación del cambio.
7. Revisar y cerrar el cambio.
    - Agrupar la documentación del cambio.
    - Revisar la documentación.
    - Asegurar que los detalles de las lecciones aprendidas han sido incluidas como parte de la gestión del conocimiento.
    - Cerrar el documento de cambio cuando se hayan completado todas las acciones.

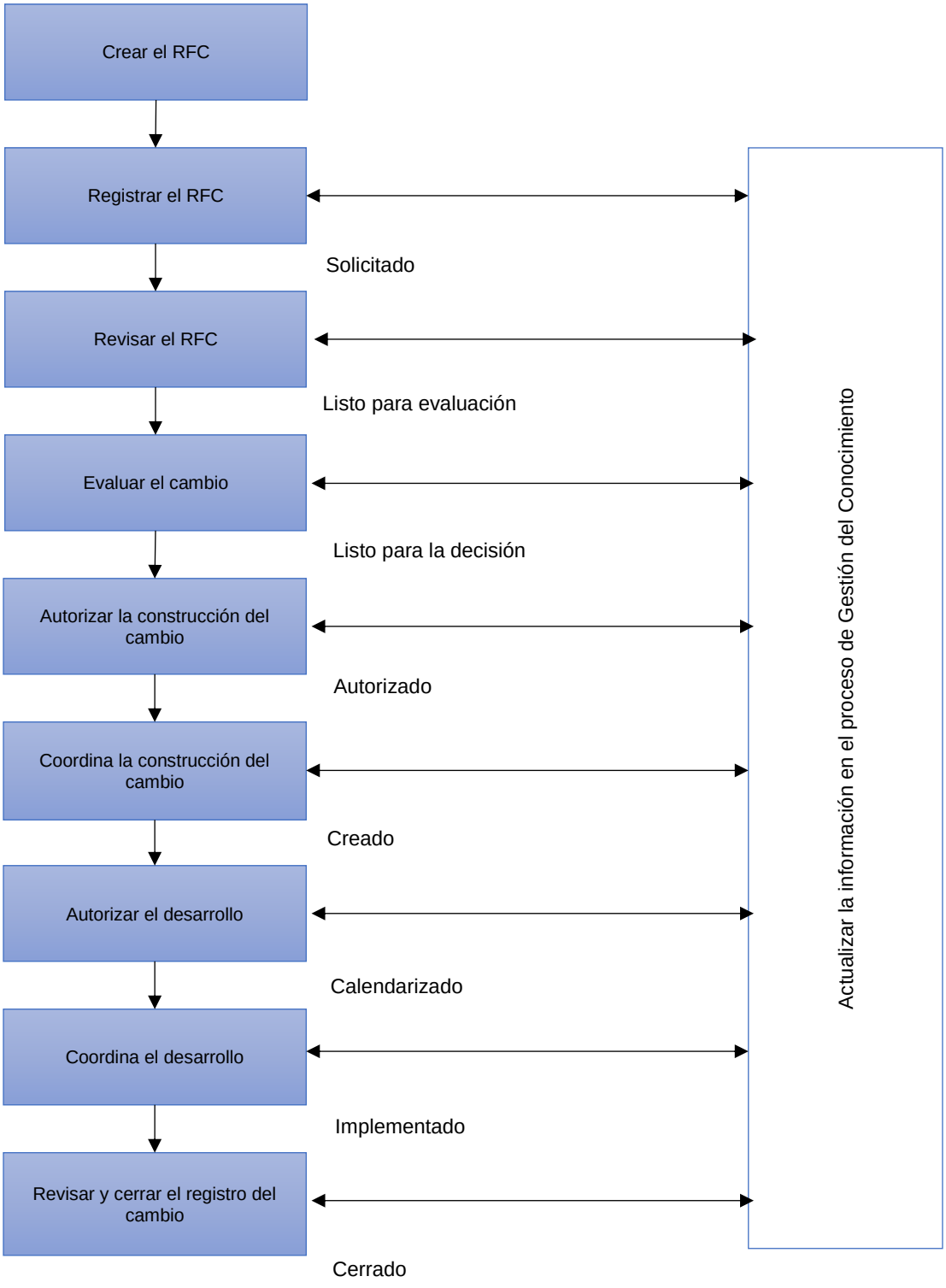

Figura 2.9. Proceso de Gestión del Cambio

Fuente: Adaptado de (ITIL Service Transition , 2011)

2.4.2 COBIT 5

COBIT 5 (2012) define el proceso de Gestión del Cambio, como el encargado de gestionar todos los cambios de una forma controlado, que incluye los cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto encierra normas y procedimientos de cambio, análisis de impacto, priorización, autorización seguimiento, reporte, cierre y documentación.

COBIT en su documentación es menos específico que otras metodologías, este se limita a definir las actividades necesarias para llevar a cabo la Gestión de un Cambio en los procesos de TI, estas se detallan a continuación de acuerdo a lo establecido en COBIT 5, proceso BAI[7] 06 Gestión del Cambio (ISACA, 2012).

1. Utilizar solicitudes de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones.
2. Realizar una categorización de las solicitudes de cambio que se relacionen con los elementos de configuración afectados.
3. Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio.
4. Planificar y evaluar todas las peticiones de una manera estructurada.
5. Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI.

[7] Built, Acquire and Implement (BAI) tomado de: (ISACA, 2012)

6. Planificar y programar todos los cambios aprobados.
7. Asegurar que se tenga un procedimiento documentado para declarar, evaluar, aprobar de forma preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
8. Supervisar todos los cambios de emergencia y realizar revisiones post-implantación que involucren a todas las partes interesadas.
9. Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del estado de los cambios, de forma que sirvan como evidencia de auditoría.

2.4.3 ISO/IEC 20000

La norma ISO/IEC 20000 (2007) establece que la gestión del cambio es el proceso con la responsabilidad sobre el control y tratamiento de los cambios en cualquier elemento que forme parte de los servicios de TI, lo que minimiza el riesgo y vela por la eficiencia. El trabajo de este proceso es asegurar que los cambios:

1. Son necesarios y están justificados.
2. Se llevan a cabo sin perjuicio de la calidad del servicio de TI.
3. Están convenientemente registrados, clasificados y documentados.
4. Cumplen los plazos acordados.
5. Han sido cuidadosamente probados en un entorno de prueba.
6. Pueden deshacerse mediante planes de marcha atrás del cambio.

Por otro lado, se define que los tres principios de la gestión del cambio son la fiabilidad, agilidad y eficiencia (Ver Figura 2.10). Fiabilidad para evitar errores y fallos, agilidad para ser capaz de cambiar los servicios para responder al "*time to market*" y eficiencia para realizar el proceso con los costos mínimos.

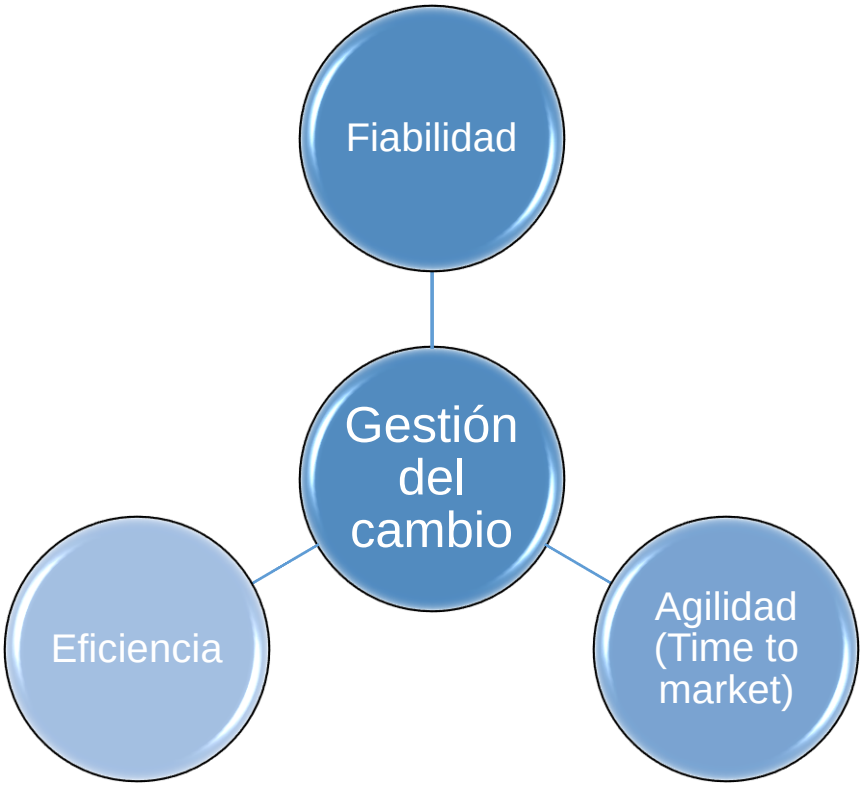

Figura 2.10. Principios que rigen la gestión de cambio

Fuente: Adaptado de (ISO/IEC, 2007)

Un cambio es la acción específica y prevista que alterará o tendrá un efecto sobre los servicios o la infraestructura de TI, es decir, es cualquier adición, eliminación modificación o movimiento de uno o más Elementos de Configuración. Los cambios se clasifican en función de una serie de criterios (ISO/IEC, 2007):

1. Alcance, complejidad o impacto.
    - Cambio Grande.
    - Cambio Significativo.
    - Cambio Menor.
2. Forma en que se ejecuta el cambio.
    - Cambio Normal.
    - Cambio Estándar.
    - Cambio pre autorizado.
    - Cambio urgente o de emergencia.

ISO/IEC 20000 (2007) al igual que ITIL v2011 establecen un ciclo de vida del cambio, el cual tiene la misión de establecer orden y control por medio de etapas y aprobaciones que se deben de seguir. La Figura 2.11 muestra cada una de estas etapas que se mencionan a continuación.

1. Registrar, evaluar y aceptar o rechazar las solicitudes de cambio.
2. Aprobar la construcción del cambio, por medio del comité de cambios (CAB)[8].
3. Coordinar la construcción e implementación del cambio.
4. Aprobar la implantación del cambio.
5. Controlar la etapa implantación que comprende la integración, pruebas y despliegue del cambio.
6. Aprobar el paso a producción del cambio.
7. Evaluar los resultados del cambio mediante la revisión post-implementación.
8. Gestionar la mejora del proceso.

[8] Change Advisory Board (CAB)

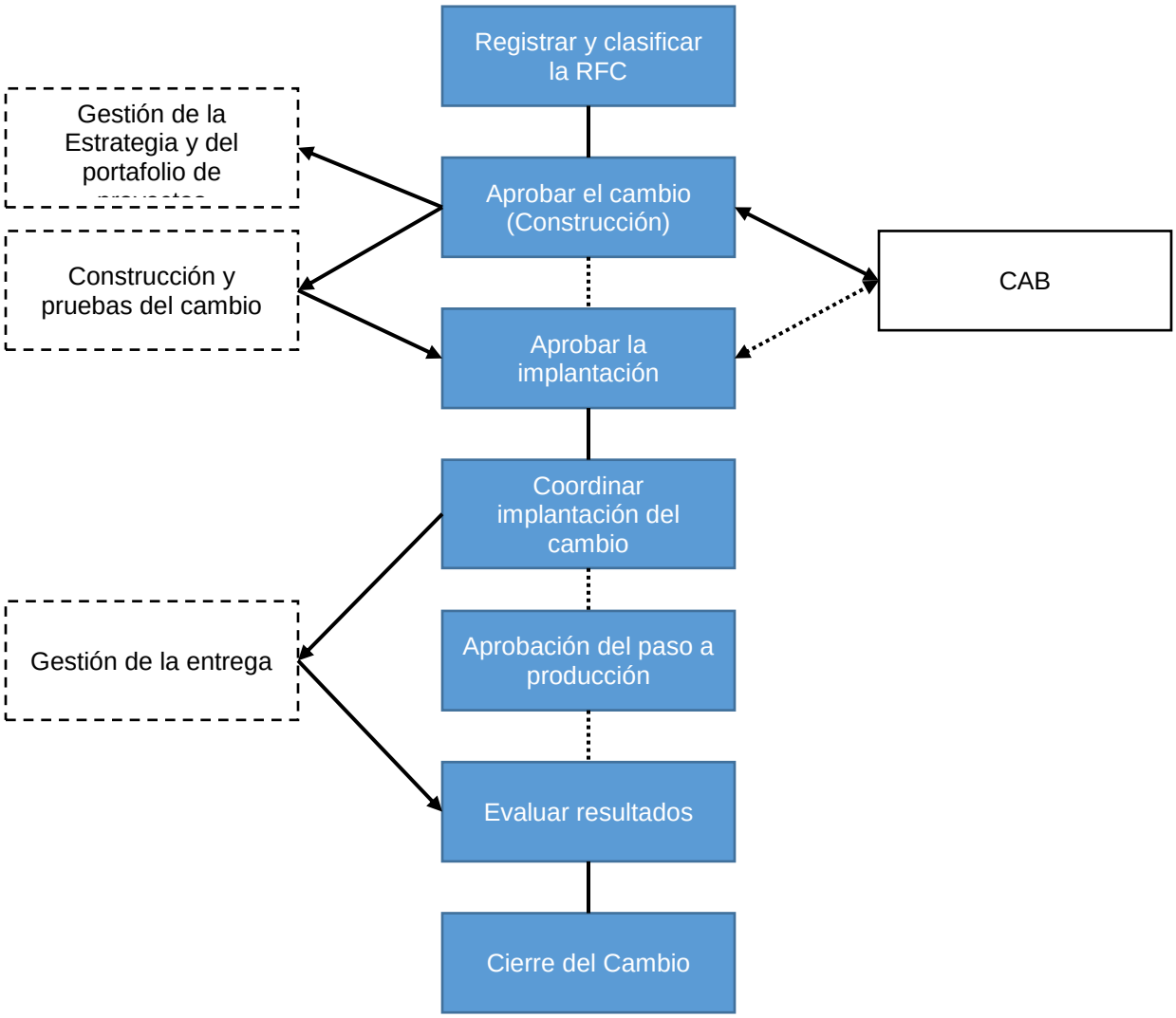

Figura 2.11. Ciclo de vida del Cambio

Fuente: Adaptado de (ISO/IEC, 2007)

2.5 Matriz de Controles Generales de TI (MCGTI)

De acuerdo con la Metodología propia de JM Auditores (2014) establece una herramienta para que los auditores realicen las evaluaciones en los diferentes clientes de la organización. Misma herramienta es denominada “Matriz de Controles Generales de TI” en ella de detalla un total de cinco procesos de revisión dividido en controles de auditoría y las pruebas sustantivas vinculadas a los controles.

A continuación se describen los procesos de revisión, asimismo los controles que componen cada proceso.

2.5.1 Entendimiento de TI

Se establece en la Metodología propia de JM Auditores (2014) que el entendimiento de TI, o refiérase también al entendimiento del entorno busca identificar y evaluar los riesgos relacionados con el ambiente tecnológico de la organización auditada. Entre los controles que se evalúan en este proceso se encuentran:

1. Existencia de un Plan Estratégico de Tecnología de Información.
2. Verificación de un inventario de los sistemas y plataforma tecnológica con los que cuenta la organización.
3. Verificación de los proyecto en vigencia donde el Departamento de TI se encuentran vinculado.
4. Examinación del Organigrama del Departamento de TI.
5. Examinación del diagrama de red.
6. Existencia de un Plan de Continuidad de los servicios que brinda TI al negocio.

7. Existencia de un Plan de Capacitación para el personal del Departamento de TI.
8. Políticas relacionadas con TI y el acceso al sitio donde se encuentran publicadas para su conocimiento.

2.5.2 Acceso a programas y datos (APD)

Este proceso busca establecer controles para reducir el riesgo de acceso no autorizado o indebido a los sistemas de información relevantes y prevenir que algún colaborador de la empresa cometa y/o oculte un error o irregularidad. Asimismo este proceso no solo busca la evaluación del acceso lógico a la información, sino que también se centra en el acceso físico a las instalaciones de la organización (JM Auditores, 2014). Los controles que se han definido para este proceso son:

1. Establecimiento de una función de seguridad de la información alineada a la Organización.
2. Implantación de una política de seguridad formal que incluya en su alcance todos los aspectos del ambiente de TI de la Organización.
3. Establecimiento de mecanismos de autenticación para los sistemas de información.
4. En caso que el mecanismo de autenticación a las aplicaciones de TI son las contraseñas, se verifican las reglas de administración de las mismas.
5. Los usuarios con mayor privilegio para las aplicaciones dentro del alcance, se encuentran limitados al personal encargado de la administración del sistema.

6. Identificación de operaciones consideradas críticas por parte de la Organización, mismas se encuentran limitadas al personal correspondiente.
7. Restricción del acceso físico al equipo que resguarda la información de la Organización.
8. Establecimiento de mecanismo de monitoreo para identificar violaciones potenciales a la seguridad de la información y de la Organización como tal.
9. La Organización cuenta con un mecanismo para modificar los accesos cuando ocurren cambios de funciones o terminación del trabajo por parte de un colaborador.
10. Implantación de un mecanismo para revisar periódicamente los accesos que se le han otorgado a cada uno de los colaboradores de la Organización.
11. Establecimiento de un mecanismo para determinar cambios en la segregación de funciones.

2.5.3 Gestión del Cambio (PC)

Este proceso busca establecer controles sobre los cambios realizados a los programas o aplicaciones dentro del alcance de la auditoría, con el fin de determinar que los cambios son autorizados, probados, debidamente implementados y documentados (JM Auditores, 2014). Para lo cual se han definido los siguientes controles:

1. Se ha establecido un proceso formal para la administración de cambios en los sistemas y aplicaciones de la Organización.
2. Todas las solicitudes de cambios a los sistemas y aplicaciones dentro del alcance de la auditoría se encuentran documentadas.

3. Se mantiene un proceso formal para realizar las pruebas una vez desarrollado el cambio solicitado.
4. Los cambios directos en el ambiente de producción se encuentran limitados por medio de una política formal.
5. Los cambios de emergencia se encuentran formalmente documentados para su revisión posterior.

2.5.4 Desarrollo de programas utilitarios (PD)

El desarrollo de programas utilitarios busca determinar en primer lugar si la organización cuenta con un departamento de desarrollo de aplicaciones y/o un proceso de adquisición de tecnología. En segundo lugar busca que tanto el desarrollo como la adquisición cuenten con una autorización, aprobación, implementación adecuada y documentación (JM Auditores, 2014). Los controles que se han definido para este proceso son:

1. Se ha establecido un proceso formal para la adquisición o desarrollo de la infraestructura de TI.
2. El desarrollo de sistemas significativos y proyectos de infraestructura son aprobados por TI y la alta gerencia de la Organización.
3. Ser realizan pruebas y revisiones a lo largo del ciclo de desarrollo de los sistemas.
4. Los sistemas desarrollados o las adquisiciones de tecnología son autorizados, probados y aprobados antes de ser puesto en producción.
5. La metodología de desarrollo toma en cuenta la aceptación del usuario mediante la ejecución de pruebas.

2.5.5 Operación Computacional (CO)

La operación computación establece controles para verificar que el procesamiento de los sistemas y aplicaciones han sido debidamente autorizados y desarrollados, además que las desviaciones presentadas por los mismos han sido identificadas y corregidas (JM Auditores, 2014). Para lo cual se han establecidos los controles siguientes:

1. La Organización ha establecido un horario para realizar los respaldos de la información y de los sistemas dentro del alcance de auditoría, asimismo se ha establecido un periodo de retención de los datos que proporcione con el riesgo de pérdida de los mismos.
2. Se tienen establecidos procedimientos de respaldo y de recuperación de la información, además que estos procedimientos sean probados periódicamente para los sistemas dentro del alcance de auditoría.

2.6 Rúbrica de Evaluación

Para el presente proyecto, se establece una evaluación entre dos metodologías (ITIL v2011, COBIT 5) y una norma internacional (ISO/IEC 20000), para identificar cual es metodología o norma que se apega más a las operaciones diarias de JM Auditores y a partir de ahí establecer la solución al problema presente. Por lo anterior es necesario establecer una rúbrica de evaluación como mecanismo de selección de la metodología o norma para llevar a cabo el desarrollo del proyecto, para lo cual es importante primeramente conocer que es una rúbrica, cuál es su propósito, ventajas y como se construye la misma, cada uno de estos aspectos se describe a continuación.

2.6.1 Rúbrica

De acuerdo a Susan Brookhart (2013) una rúbrica es un conjunto coherente de criterios que incluye descripciones de los niveles de calidad de desempeños de dicho criterios. De igual forma, agrega que el sentido de las rúbricas es que son descriptivas y no evaluativas, si bien se pueden utilizar para evaluar, su principio de funcionalidad es que coincida con el rendimiento de la descripción.

Por su parte Mira Costa, Irvine Valley (2014) establecen que las rúbrica son el tipo más flexible de una evaluación directa y que son utilizadas para puntual cualquier producto o medida de rendimiento. Por otro lado agrega que al momento de utilizar una rúbrica para una evaluación, se debe definir un sistema de puntuación detallado que delimite los criterios utilizados.

De lo anterior, se establece que una rúbrica es un medio para realizar evaluación a partir de un conjunto de criterios y métricas, tal y como lo establece Brookhart (2013), que indica que el propósito principal de las rúbricas es evaluar el funcionamiento de los aspectos seleccionados.

2.6.2 Ventajas de una rúbrica de evaluación

A continuación se detallan algunas de las ventajas que definen Brookhart (2013) y Costa, Valley (2014) sobre el uso de una rúbrica.

- Define expectativas claras sobre los evaluados.
- Permite comprende mejor las puntuaciones.
- Se pueden utilizar para anotar muchos tipos de asignaciones.
- Los productos o comportamiento complejos puede ser examinados eficientemente.

2.6.3 Como se construye una rúbrica

Costa y Valley (2014) definen una serie de pasos que se deben seguir para construir una rúbrica, estos pasos son:

1. Identifique lo que desea evaluar.
2. Identifique las características de lo evaluado.
3. Describa el mejor trabajo que podría esperar. Esto describe la categoría superior.
4. Describa el peor trabajo aceptable o inaceptable por medio de estas características. Esto describe la categoría más baja aceptable.
5. Desarrolle descripciones de trabajo de nivel intermedio y asignarlos a categorías intermedias. Una opción es desarrollar una escala de va de uno a cinco (Por ejemplo: Inaceptable, marginal, competente, muy competente, pendiente).
6. Para evaluar los resultados, se recomienda una escala de 4 o 5 puntos, de forma que se diseñe una asignación acordada y conforme a los criterios de evaluación para cada punto o nivel de la rúbrica.
7. En algunos casos se identifican criterios implícitos que no se indican en la escala de puntuación, estos criterios implícitos puede ayudar al instructor a refinar la escala de puntuación.

2.6.4 Grafico del Río

De acuerdo a Parcell & Collison (2009), el Diagrama de Río[9] es una herramienta diseñada para visualizar los resultados de la autoevaluación y los datos de múltiples fuentes. Específicamente permite representar de forma visual rúbricas de múltiples fuentes que contienen cada una su propia matriz de información.

Este es un gráfico sencillo que toma el nivel máximo y mínimo para cada medición, muestra el rango de puntuaciones a través del grupo entero de información (Parcell & Collison, 2009).

El sitio web de Better Evaluación (s.f) establece que la construcción de un Diagrama de Río, se lleva a cabo al tomar las puntuaciones máximas y mínimas de las evaluaciones individuales, dicha área es coloreada de color azul, para simular un río, mientras que el resto del grafico se colorea de color verde, para simular los bordes y zonas verdes que rodea un río.

Una vez definidos los conceptos que serán la base del desarrollo del proyecto, se establece la metodología de trabajo para alcanzar los objetivos establecidos, la cual será documentada en el siguiente capítulo.

[9] The River Diagram

3. Desarrollo Metodológico

En el presente capítulo se describe el marco metodológico donde se define el tipo de investigación, tipos de instrumentos de recolección de datos, técnicas de investigación, herramientas utilizadas y etapas realizadas de la metodología de desarrollo en busca de cumplir con el objetivo general definido.

3.1 Tipo de Investigación

Para el presente trabajo, se utilizó un modelo de investigación cualitativo el cual de acuerdo a Hernández (2014) se enfoca en comprender los fenómenos explorándolos desde la perspectiva de los participantes en un ambiente natural y en relación con su contexto. La Figura 3.1 muestra el proceso cualitativo que propone este autor, el cual se centra en un marco de referencia como literatura existente, misma que interactúa a lo largo del desarrollo del proyecto.

Hernández (2014) agrega que un modelo cualitativo posee las siguientes características:

- El investigador plantea un problema, pero no sigue un proceso definido claramente.
- En la mayoría de los estudios cualitativos no se pruebas hipótesis, sino que se genera durante el proceso y se perfecciona conforme se recaban más datos, es decir es el resultado del estudio.
- El enfoque se basa en métodos de recolección de datos.
- Se utilizan técnicas para recolectar datos como la observación no estructurada, entrevistas abiertas, revisión de documentos, entre otras.

- Las indagaciones cualitativas no pretenden generalizar de manera probabilística los resultados a poblaciones más amplias ni obtener necesariamente muestra representativas.

Por lo anterior, se define que el proyecto se centra en una investigación cualitativa, la cual tendrá como fuente principal y central una metodología o norma internacional que será utilizada en cada una de las fases y etapas de desarrollo del proyecto. Asimismo, no se asienta en datos número o en comprobar una hipótesis, por lo contrario, busca la mejora de procesos y de las operaciones que realiza actualmente la organización.

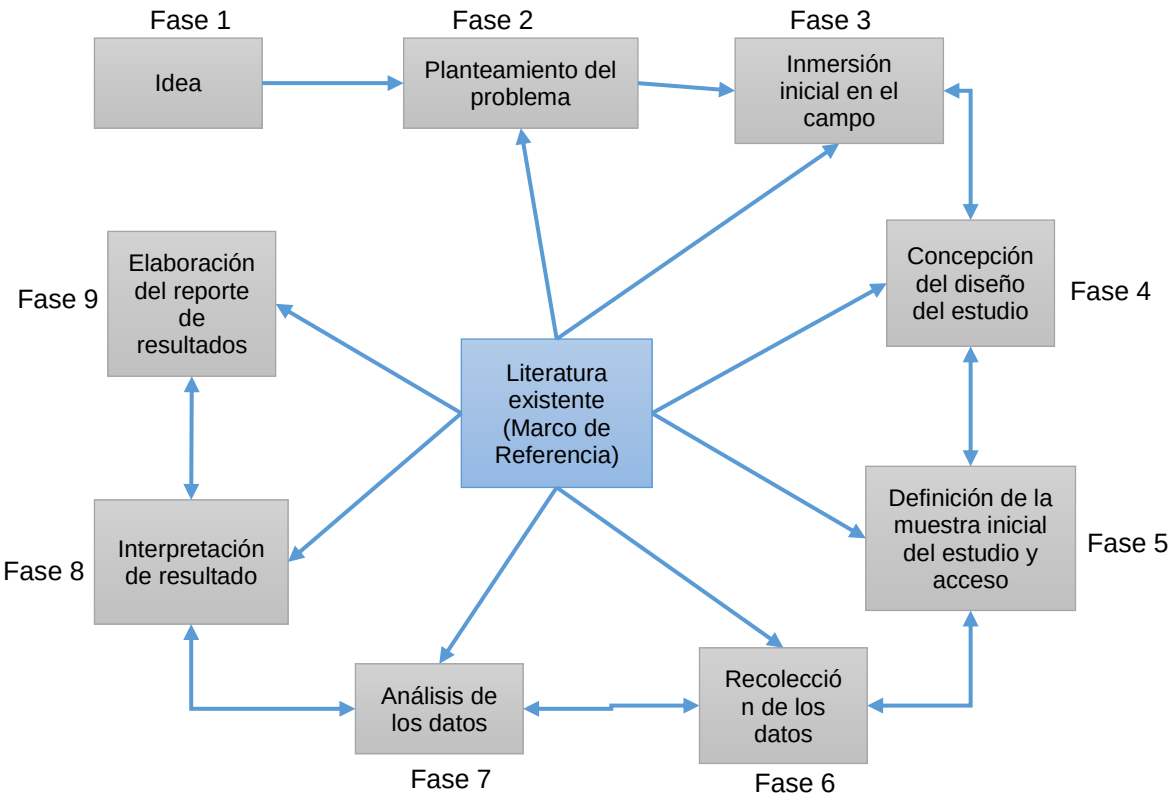

Figura 3.1. Proceso cualitativo genérico

Fuente: Adaptado de (Hernández, 2014)

3.2 Diseño de investigación

Una vez establecida la problemática del proyecto, se puede determinar el diseño de la investigación (Hernández, 2014), para el presente proyecto se basa en un diseño de Investigación-acción, cuya finalidad es comprender y resolver problemáticas específicas de una colectividad vinculada a un ambiente, con frecuencia se aplica la teoría y mejores prácticas de acuerdo con el planteamiento (Hernández, 2014). Asimismo, se agrega que la Investigación-acción se basa en una problemática donde se necesita resolver y que pretende buscar un cambio.

Este mismo autor hace referencia a Álvarez-Gayou (2003), el cual establece que la Investigación-acción se basa en tres perspectivas:

1. **Visión técnico-científica:** Consiste en un conjunto de decisiones en espiral, las cuales se basan en ciclos repetidos de análisis para conceptualizar y redefinir el problema una y otra vez. La Investigación-acción se integra con fases secuenciales de acción: planificación, identificación de hechos, análisis, implementación y evaluación.
2. **Visión deliberativa:** Se enfoca principalmente en la interpretación humana, la comunicación interactiva, la deliberación, la negociación y la descripción detallada.
3. **Visión emancipadora:** Su objetivo va más allá de revolver problemas o desarrollar mejoras a un proceso, pretende que los participantes generen un profundo cambio social por medio de la investigación.

Por su parte, Hernández (2014) establece que el diseño de Investigación-acción se basa en tres fases esenciales:

- **Observación:** Construcción de un bosquejo del problema y la recolección de la información.
- **Pensamiento:** Analizar e interpretar la información recolectada.
- **Actuar:** Resolver el problema e implementar mejora a partir de la solución identificada.

3.3 Metodología de Trabajo

A partir de lo anterior, se ha establecido la metodología para el desarrollo del proyecto, la cual tiene como finalidad establecer los pasos necesarios para alcanzar los objetivos establecidos, dichos pasos se especifican a continuación.

- Definir rúbrica, evaluar las metodologías (ITIL v2011, COBIT 5) y la norma (ISO/IEC 20000), y realizar análisis de los resultados.
- Estudiar procesos relacionados con la Gestión del Cambio en la metodología que sea seleccionada como producto del análisis inicial, de forma que estos permitan identificar controles de auditoría.
- Alinear cada proceso de la MCGTI con los procesos de la metodología seleccionada.
- Identificar los controles de auditoría para el proceso de Gestión del Cambio.
- Analizar los controles identificados.
- Definir los controles de auditorías para el proceso de Gestión del Cambio.
- Establecer las pruebas sustantivas.
- Automatizar la Matriz de Controles Generales de TI.

A continuación, en la Figura 3.2 se detalla las fases metodológicas mencionadas anteriormente, mismas que se detallarán en la subsección siguientes.

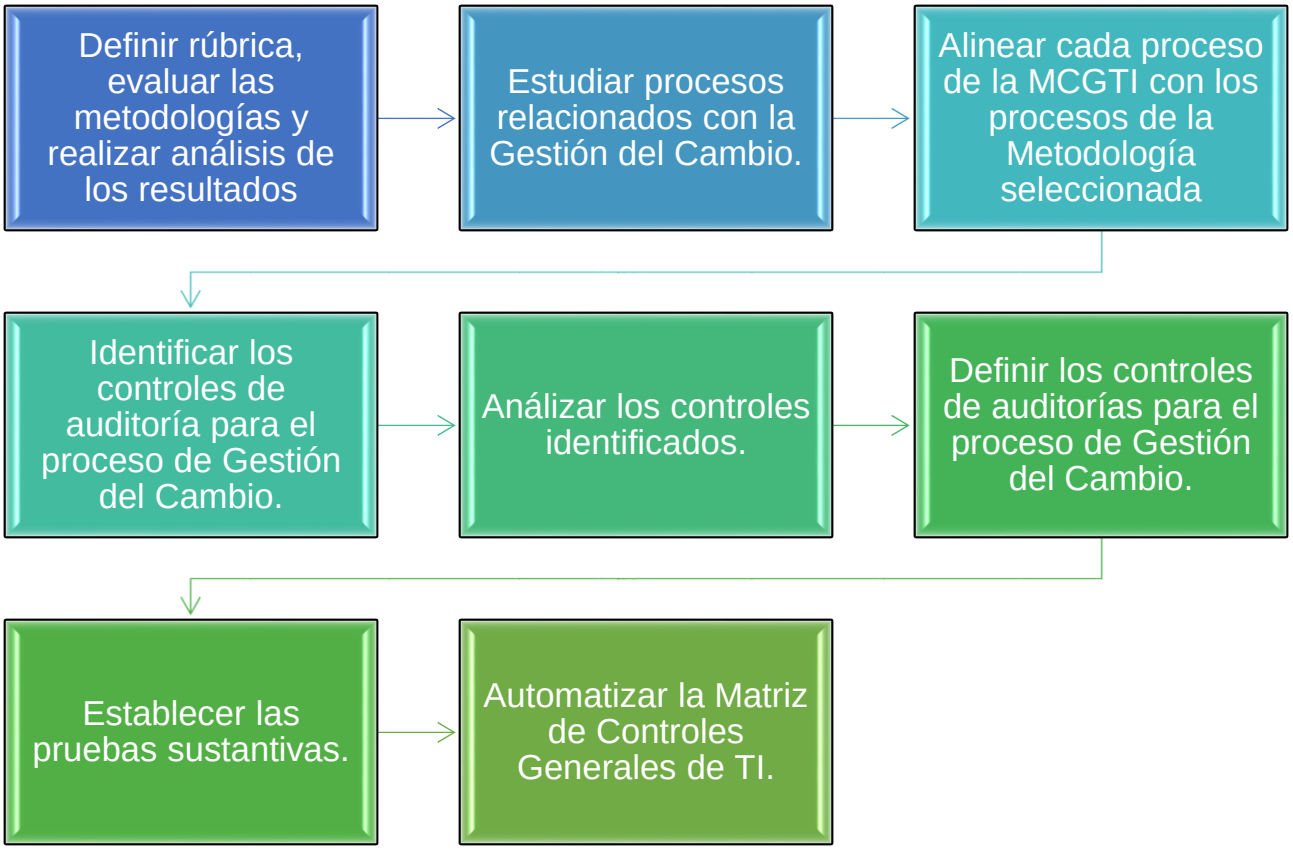

Figura 3.2. Fases de la Metodología de Trabajo

Fuente: Elaboración propia

3.3.1 Definir rúbrica, evaluar las metodologías y realizar análisis de los resultados

Para cumplir con esta etapa de la metodología se deben seguir las actividades siguientes:

1. Establecer criterios de evaluación y comparación para cada una de las metodologías seleccionadas para el estudio.
2. Brindar un peso (valor) a cada uno de los criterios establecidos, de forma que la suma de los pesos esa igual al 100%.
3. Realizar la evaluación de cada una de las metodologías (ITIL, COBIT, ISO) y la norma de forma que se complete la rúbrica definida.
4. Analizar los resultados obtenidos de la rúbrica de evaluación por medio del diagrama del Río.

3.3.2 Estudiar procesos relacionados con la Gestión del Cambio en la metodología seleccionada

Para completar la segunda etapa de la metodología de desarrollo, se debe llevar a cabo la actividad siguiente:

1. Identificar en la metodología seleccionada los procesos que se encuentran vinculados a la Gestión del Cambio.
2. Estudiar a profundidad los procesos que fueron identificados como parte de la Gestión del Cambio.

3.3.3 Alinear cada proceso de la MCGTI con los procesos de la metodología seleccionada

Para la conclusión de esta etapa de la metodología, las actividades que se debe realizar son:

1. Alinear cada uno de los procesos de la MCGTI a la metodología seleccionada y justificar por qué se realiza la asociación de cada uno.

3.3.4 Identificar los controles de auditoría para el proceso de Gestión del Cambio

Para cumplir con esta etapa de la metodología se deben llevar a cabo la siguiente actividad:

1. Identificar los controles de auditoría que establece la metodología seleccionada en los procesos que se vinculan en la Gestión del Cambio, estos procesos se deben adaptar al tipo de auditoría que realiza la organización, al mismo tiempo que se encuentren dentro del alcance de las mismas.

3.3.5 Analizar los controles de auditoría identificados

La siguiente actividad se debe llevar a cabo para completar esta etapa de la metodología de desarrollo.

1. Analizar si el control identificado se adapta a las auditorías que se realizan en la organización y si es importante ejecutar dicho control para determinar el buen manejo de la tecnología en la empresa auditada.

3.3.6 Definir los controles de auditorías para el proceso de Gestión del Cambio

La siguiente actividad se debe efectuar para completar esta etapa de la metodología de desarrollo.

1. Definir los controles de auditoría que han cumplido con el análisis de la etapa anterior, de forma que se adapte al tipo de auditoría que realiza la organización, asimismo que le brinde un valor agregado a dichas evaluaciones.

3.3.7 Establecer las pruebas sustantivas

Para completar esta etapa de la metodología se debe completa la actividad siguiente:

1. Establecer las pruebas sustantivas para cada uno de los controles de auditoría definidos en la etapa anterior, dichas pruebas deben evaluar todos los escenarios posibles del control de forma que la evaluación sea completa y se obtenga un resultado adecuado a lo que posee la organización auditada.

3.3.8 Automatizar la Matriz de Controles Generales de TI

Para realizar con éxito esta etapa de la metodología de desarrollo, se deben realizar las siguientes tareas:

1. Desarrollar la Matriz de Controles Generales de TI que abarcan los 5 procesos descritos anteriormente. Dentro de la matriz se establecen los controles definidos para cada proceso y las pruebas sustantivas definidas para cada uno de estos.

2. Automatizar la MCGTI por medio de macros en Microsoft Excel, en la cual se establecen los resultados obtenidos después de realizar la evaluación, la matriz será la encargada de establecer si la prueba es efectiva o no, a partir de la información obtenida.

3.4 Fuentes de Información

La información para el desarrollo del proyecto se debe obtener desde diferentes fuentes y sujetos, mismos que se detallan a continuación.

3.4.1 Fuentes

Las fuentes de información son el lugar donde el investigar encuentra los datos requeridos que pueda convertirse en información útil. Dichos datos representan los fundamentos requeridos para llegar al conocimiento y deben ser suficientes para sustentar y defender el trabajo (Eyssautier de la Mora, 2006).

A continuación, se presentan las diferentes fuentes utilizadas para la investigación.

3.4.1.1 Fuentes primarias

Establecen el objetivo de la investigación bibliográfica o revisión de la literatura y proporcionan datos de primera mano (Hernández, 2014, pág. 61). Las fuentes primarias utilizadas para el desarrollo del proyecto fueron consultadas por medio de los sitios web oficiales de las Organizaciones que brindar las metodologías en estudio, así como consultas a la plataforma de Google y al sitio electrónico de la Biblioteca José Figueres Ferrer.

La Tabla 3.1 muestra las fuentes primarias utilizadas y el sitio donde fue consultado para su obtención, si es el caso se indica las palabras claves utilizadas para su búsqueda.

Tabla 3.1. Fuente de información primaria

Fuente	Sitio consultado
ISO/IEC 20000	Sitio web oficial de Organización Internacional para la Normalización (ISO).
ITIL Service Strategy	Sitio web oficial de Axelos, organización encargada del Marco de Referencia de ITIL.
ITIL Service Transition	Sitio web oficial de Axelos, organización encargada del Marco de Referencia de ITIL.
COBIT 5	Sitio web oficial de Asociación de Auditoría y Control de Sistemas de Información (ISACA), organización encargada del Marco de COBIT.
Metodología propia	Documentación Interna de JM Auditores.
Fundamentals of Auditing	Plataforma de Google Books por medio de la palabra clave “Auditoría”.
Metodología de la Información	Documentación brindada y recomendada por los profesores asesores y la coordinación del TFG.
Auditoría en Informática	Plataforma electrónica de la Biblioteca José Figueres Ferres del Instituto Tecnológico de Costa Rica, por medio de la palabra clave “Auditoría en Informática”.

Fuente: Elaboración propia

3.4.1.2 Fuentes secundarias

Son compilaciones, resúmenes sobre un área particular, principalmente de documentos de fuentes primarias (Hernández, 2014, pág. 67). La Tabla 3.2 muestra las fuentes secundarias utilizadas para el desarrollo del proyecto y los sitios consultados para su obtención, en algunos casos se indican las palabras clases utilizadas en la consulta.

Tabla 3.2. Fuente de información secundaria

Fuente	Sitio Consultado
Auditoría financiera a los estados financieros.	Búsqueda en la plataforma de Google por medio de la palabra clave “Auditoría Financiera”.
PDCA	Búsqueda en la plataforma de Google por medio de la palabra clave “Ciclo PDCA”.
ITIL 2011 Edition – Apocket Guide	Documentación brindada por el profesor de la carrera, como parte de la bibliografía del curso de Administración de Servicios de Tecnología de Información.
How to Create and Use Rubrics for Formative Assessment and Grading	Búsqueda en la plataforma de Google por medio de la palabra clave “Rubric”.

Fuente: Elaboración propia

3.4.1.3 Otras fuentes.

Otras fuentes consultadas para el desarrollo del proyecto y de donde se obtuvo información fueron los sitios web de organizaciones reconocidas internacionalmente y que se enfocan en la gestión de TI y en la auditoría de financiera, asimismo se visitó un sitio web para el estudio del diagrama del río para la representación de los resultados obtenidos de la rúbrica de evaluación. Los sitios consultados son:

- *IT Governance.*
- KPMG.
- Asociación de Auditoría y Control de Sistemas de Información (ISACA).
- *Better Evaluation.*

3.5 Técnicas de Recopilación de Información

La recolección de datos busca obtener los datos, de personas, situaciones o procesos en profundad, para lo cual es necesario utilizar técnicas de recolección de información. Para el presente proyecto se han ligado a cada uno de los objetivos específicos, de forma que se seleccionaron las herramientas más adecuadas para satisfacer su cumplimiento. Las técnicas de recopilación de información utilizadas son las siguientes:

- **Encuesta** – Según Sampieri (2014) las encuestas son consideradas en algunos casos como diseño o método. Asimismo, llama a las encuestas como cuestionarios, el cual consiste en un conjunto de preguntas respecto a una o más variables a medir. Los tipos de preguntas que se pueden establecen en una encuesta (cuestionario) son:
    - **Preguntas cerradas:** Obtienen categorías u opciones de respuesta que han sido previamente delimitadas.
    - **Preguntas abiertas:** No delimitan de antemano las alternativas de respuesta. En teoría, es infinito y puede variar de población en población.

- **Observación** – De acuerdo a Sampieri (2014) una observación desde una investigación cualitativa implica adelantarnos profundamente en detalles, sucesos, eventos e interacciones. Este autor agrega que los propósitos esenciales de la observación son:
    - Explorar y describir ambientes, comunidades, subculturas, por medio de su análisis y los actores que los generan.
    - Comprender procesos, vinculación entre personas y sus situaciones, experiencias o circunstancias, los eventos que suceden al paso del tiempo.
    - Identificar problemas en la organización.
- **Revisión Documental** – Consiste en la obtención y análisis de documentos productivos en el curso de la vida cotidiana. Esta es una técnica no obstructiva, rica en bosquejar los valores y creencias de los participantes en el campo (Scribano, 2007, pág. 26). Por su parte Latorre (2007) agrega que la revisión documental facilita la elaboración del marco conceptual o teoría donde se quiere situar el tema en estudio.

Para cada una de las técnicas de recopilación de información utilizada, se realizó un análisis de forma que se asoció cada técnica con los objetivos específicos establecidos, con el fin de satisfacer su cumplimiento. La Tabla 3.3 establece los objetivos específicos y cada uno de las técnicas utilizadas.

Tabla 3.3. Técnicas de Recopilación de Información

Objetivo Específico	Técnica
Realizar un análisis de dos metodologías internacionales (ITIL v2011, COBIT 5) y una norma (ISO/IEC 20000) basado en el proceso de Gestión del Cambio, con el propósito de recomendar la metodología más adecuada para la empresa.	• Revisión documental de las metodologías seleccionadas para el análisis.
Definir los controles generales de TI que establece la metodología seleccionada para evaluar la Gestión de Cambios.	• Revisión documental de la metodología seleccionada luego del análisis correspondiente. • Encuesta al equipo de trabajo.
Desarrollar de forma detallada las pruebas sustantivas para cada uno de los controles de auditoría identificados para evaluar la gestión de cambios.	• Observación de las pruebas utilizadas actualmente. • Encuesta al equipo de trabajo.
Alinear la Matriz de Controles Generales de TI de acuerdo a los procesos identificados en la metodología seleccionada que cumplen con los procesos definidos actualmente por la organización.	• Revisión documental de la metodología seleccionada luego del análisis correspondiente.
Modificar la matriz de controles generales de TI mediante la automatización de los controles y las pruebas sustantivas, basada en macros de Microsoft Excel, de forma que indique el resultado obtenido de la evaluación realizada.	• Para este objetivo no aplica la recolección de datos, debido a que su cumplimiento se realiza basado en la información obtenida de los objetivos anteriores.

Fuente: Elaboración propia

3.6 Instrumentos de investigación

Los instrumentos de investigación son aquellos que son utilizados en conjunto con las técnicas de obtención de información para obtener los datos necesarios para el desarrollo del proyecto. A continuación, en la Tabla 3.4 se definen los objetivos específicos ligados con los instrumentos de investigación utilizados.

Tabla 3.4. Instrumentos de Investigación

Objetivo Específico	Instrumento
Realizar un análisis de dos metodologías internacionales (ITIL v2011, COBIT 5) y una norma (ISO/IEC 20000) basado en el proceso de Gestión del Cambio, con el propósito de recomendar la metodología más adecuada para la empresa.	• Rúbrica de Evaluación de Metodologías (Ver Apéndice D). • Diagrama del Rio (The River Diagram).
Definir los controles generales de TI que establece la metodología seleccionada para evaluar la Gestión de Cambios.	• Encuesta con el equipo de trabajo por parte de la Organización (Ver Apéndice E).
Desarrollar de forma detallada las pruebas sustantivas para cada uno de los controles de auditoría identificados para evaluar la gestión de cambios.	• Encuesta con el equipo de trabajo por parte de la Organización (Ver Apéndice F).
Alinear la Matriz de Controles Generales de TI de acuerdo a los procesos identificados en la metodología seleccionada que cumplen con los procesos definidos actualmente por la organización.	• No aplica un instrumento de investigación. Se realiza basado en la técnica de recolección de información.

Objetivo Específico	Instrumento
Modificar la matriz de controles generales de TI mediante la automatización de los controles y las pruebas sustantivas, basada en macros de Microsoft Excel, de forma que indique el resultado obtenido de la evaluación realizada.	• No aplica un instrumento de investigación, debido a que es un objetivo de implementación y se realiza con base a lo obtenido en los demás objetivos.

Fuente: Elaboración Propia

3.7 Procedimiento y Análisis de Datos

Con la información obtenida de las técnicas de recolección de la información que se aplicaron y que se especificaron en el apartado 3.5 Técnicas de Recopilación de Información, se realizó un análisis que permitió ordenar la información de acuerdo con los objetivos planteados. En la Tabla 3.5 se define el análisis y procedimientos de los datos para cada uno de los objetivos.

Tabla 3.5. Procedimiento y Análisis de los Datos

Objetivos	Técnicas	Análisis y Procesamiento de Datos
Realizar un análisis de dos metodologías internacionales (ITIL v2011, COBIT 5) y una norma (ISO/IEC 20000) basado en el proceso de Gestión del Cambio, con el propósito de recomendar la metodología más adecuada para la empresa.	• Rúbrica de Evaluación de Metodologías (Ver Apéndice D). • Diagrama del Río (*The River Diagram*).	Para analizar la información obtenida de la rúbrica de evaluación, se hará uso del Diagrama del Río, el cual permitirá observar los resultados de la evaluación.

Objetivos	Técnicas	Análisis y Procesamiento de Datos
Definir los controles generales de TI que establece la metodología seleccionada para evaluar la Gestión de Cambios.	• Revisión documental de la metodología seleccionada del análisis. Encuesta con el equipo de trabajo por parte de la Organización (Ver Apéndice E).	Tras obtener un resultado de la rúbrica, sobre la metodología a utilizar, se hará uso del estudio de la misma para determinar los procesos relacionados con la Gestión del Cambio.
Desarrollar de forma detallada las pruebas sustantivas para cada uno de los controles de auditoría identificados para evaluar la gestión de cambios.	• Observación de las pruebas utilizadas actualmente. • Encuesta con el equipo de trabajo por parte de la Organización (Ver Apéndice F).	Por medio de la observación se determinarán los controles de auditoría que se utilizan actualmente en la Organización. Para luego con ayuda de la metodología seleccionada y de una entrevista con el equipo de trabajo por parte de la Organización, se determinarán las nuevas pruebas sustantivas.
Alinear la Matriz de Controles Generales de TI de acuerdo a los procesos identificados en la metodología seleccionada que cumplen con los procesos definidos actualmente por la organización.	• Revisión documental de la metodología seleccionada luego del análisis correspondiente.	De acuerdo al resultado de evaluación de las metodologías, se toma la seleccionada y se realizará un estudio de la misma para establecer cual proceso de metodología se adecua a las áreas de evaluación que realiza la organización.

Objetivos	Técnicas	Análisis y Procesamiento de Datos
Modificar la matriz de controles generales de TI mediante la automatización de los controles y las pruebas sustantivas, basada en macros de Microsoft Excel, de forma que indique el resultado obtenido de la evaluación realizada.	• Para este objetivo no aplica la recolección de datos, debido a que su cumplimiento se realiza basado en la información obtenida de los objetivos anteriores.	Una vez alineados los procesos y definidos los controles de auditoría y las pruebas sustantivas para la evaluación de Gestión del Cambio, se realizará la automatización de la MCGTI por medio de macros en Microsoft Excel.

Fuente: Elaboración propia

Basado en los pasos descritos para la metodología de trabajo, asimismo como de las técnicas de obtención de información y de los instrumentos de investigación detallados anteriormente, se desarrollará el siguiente capítulo del proyecto, en el cual se analizarán los resultados y la documentación obtenida.

4. Análisis de Resultados

En este capítulo se realiza el análisis de los resultados obtenidos a partir de la aplicación de las técnicas de recolección de información y los instrumentos de investigación que se describieron en el capítulo anterior.

4.1 Análisis de Datos

Para llevar a cabo el análisis de datos, se estableció una herramienta de investigación o técnica de recolección de información para cada uno de los objetivos del proyecto, mismos que serán asociados con cada una de las etapas de la metodología de trabajo. A continuación se describe el análisis de la información adquirida.

4.1.1 Definir rúbrica, evaluar las metodologías y realizar análisis de los resultados

Como primera fase de la metodología de trabajo, se estableció la definición de una rúbrica para evaluar y analizar dos metodologías (COBIT 5 e ITIL v2011) y la norma ISO/IEC 20000. A continuación se establece cada paso realizado para completar esta fase de la metodología.

4.1.1.1 Definición de la Rúbrica

Para llevar a cabo la evaluación de las metodologías se definió la rúbrica de evaluación de metodología, la cual se realizó de acuerdo a las operaciones que realiza la Organización y el criterio del estudiante a partir del conocimiento de las metodologías obtenido como parte de su formación académica, dicha rúbrica se dividió en tres categorías principales, conformadas por criterios de evaluación (Ver Apéndice D).

En la Tabla 4.1 se establecen las categorías y los criterios de evaluación definidos son:

Tabla 4.1. Categorías y Criterios de la Rúbrica de Evaluación

Categoría	Criterio
Información General	Permite Certificación.
	Valor de capacitación para el personal.
	Tiempo de capacitación para el personal.
	Cantidad de procesos definidos para la gestión de TI.
	Descripción del proceso de Gestión del Cambio.
	La metodología toma en cuenta los demás procesos que evalúa la organización.
Evaluación de Gestión del Cambio	Registro de solicitudes de cambio.
	Aprobación de las solicitudes de Cambio.
	Mantiene un proceso de pruebas para los cambios.
	Aprobación del cambio por parte del usuario solicitante.
	Registro de los cambios puestos en producción.
Valor agregado en su aplicación	Mejora la administración de los activos.
	Administración del Riesgo en los diferentes procesos.
	Gestiona la Madurez de los procesos.
	Alineamiento de los procesos de TI con la estrategia organizacional.
	Maximiza la calidad y eficiencia de los procesos de TI.

Fuente: Elaboración Propia

4.1.1.2 Evaluación de las metodologías

Una vez creada la Rúbrica de Evaluación, se procedió con una evaluación de cada una de las metodologías (ITIL v2011 y COBIT 5) y la norma (ISO/IEC 20000) de forma separada. Para realizar la evaluación se realizó un análisis y revisión documental de cada metodología para determinar el valor de cada uno de los criterios que se evalúan. Las evaluaciones realizadas se encuentran en Apéndice G, Apéndice H y Apéndice I.

4.1.1.3 Análisis de Resultados

A continuación se indica el análisis realizado por medio del Diagrama del Río, donde se presentan tres gráficos, uno para cada categoría de la rúbrica de evaluación de metodologías. En dichos diagramas se indica la metodología que obtuvo el puntaje más alto y el puntaje más bajo cada uno de los criterios evaluados. El análisis se realizó bajo el conocimiento tanto técnico como administrativo que obtuvo el estudiante a lo largo de la carrera académica.

Gráfico 4.1. Muestra la primera categoría que corresponde a “Información General”, donde se consideraron aspectos como: Valor de capacitación del personal, cantidad de procesos definidos, descripción del proceso de Gestión del Cambio y Ajuste con los procesos actuales de la Organización.

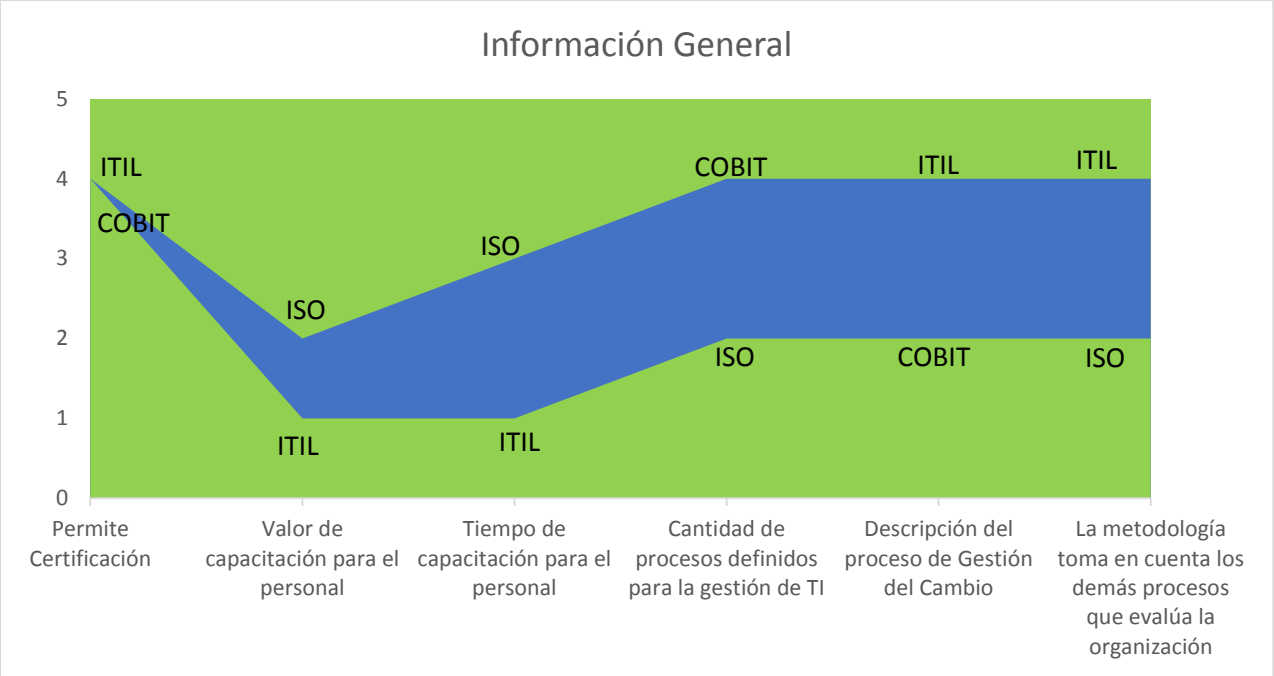

Gráfico 4.1. Información General

Fuente: Elaboración Propia

Como se puede observar en el Gráfico 4.1 en cuanto al criterio de certificaciones existe una similitud entre las Metodologías ITIL v2011 y COBIT 5, las cuales brindan la opción de certificarse en más de 4 niveles, donde ambas metodologías inician por la parte de Fundamentos. Por otro lado, al comparar el valor y tiempo de capacitación del personal la norma ISO/IEC 20000 se ve mejor calificada que ITIL debido a que el valor y el costo es menor lo que le da mayor accesibilidad a la empresa.

Al analizar el siguiente criterio, se puede observar como COBIT 5 obtuvo un mayor puntaje que las otras metodologías bajo estudio, esto debido a que COBIT define un total de 37 procesos, mientras que la norma ISO/IEC 20000 solamente define un total de 13 procesos e ITIL establece 26 procesos. Asimismo se evaluó la definición del proceso de Gestión del Cambio que establece cada metodología donde se puede observar que ITIL mantiene una ventaja sobre COBIT debido a que la primera mantiene una definición más detalla de cada una de las actividades que se deben realizar una buena gestión en los cambios de los aplicativos y sistemas de la organización.

Por su parte, COBIT solamente indica, de forma general, qué se debe hacer para gestionar los cambios. Una vez hecho esto, se comparó sobre la definición de los procesos que evalúa actualmente JM Auditores y lo que define la metodología en estudio, donde se puede observar que ITIL v2011 describe los cinco procesos que evalúa la Organización, mientras que la ISO/IEC 20000 solamente contempla dos de los cinco procesos.

Gráfico 4.2. Establece la evaluación correspondiente a la segunda categoría de la rúbrica, la cual corresponde a “Criterios de Evaluación de la Gestión del Cambio” que realiza actualmente JM Auditores, esto con el fin de determinar cuál metodología se apega más a sus operaciones.

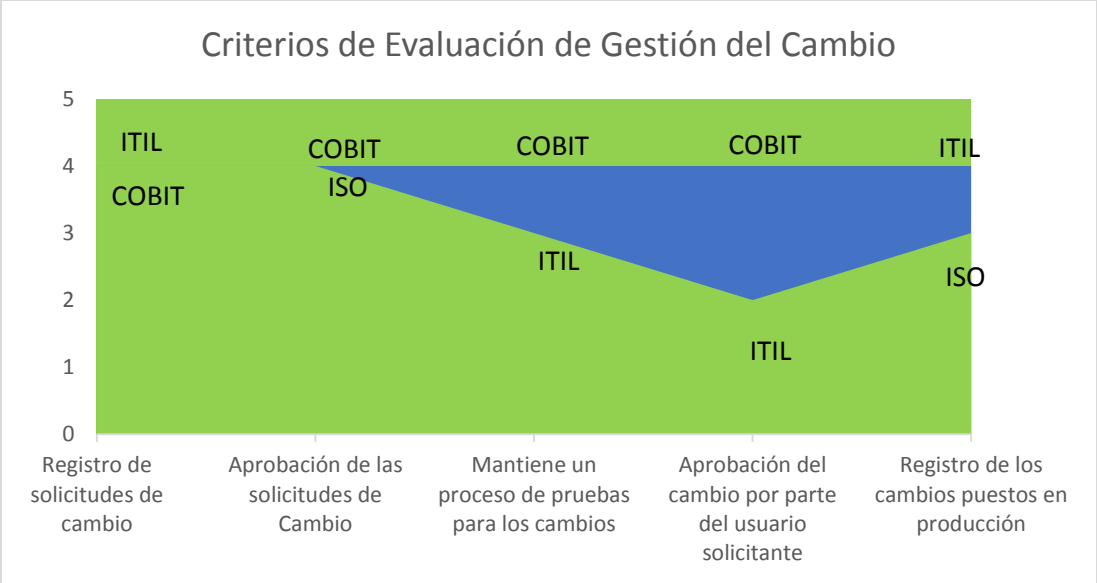

Gráfico 4.2. Criterios de Evaluación de Gestión del Cambio

Fuente: Elaboración propia

Como se puede observar en el Gráfico 4.2, en el primer criterio no existe diferencia entre ITIL v2011 y COBIT 5 respecto al registro de solicitudes de cambio, ya que ambos consideran que se deben registrar todas las solicitudes de cambio, misma situación al evaluar la aprobación de las solicitudes de cambio. Al analizar el siguiente criterio, se identificó que existe una similitud entre COBIT 5 e ISO/IEC 20000 donde tanto la metodología como la norma establecen que se debe llevar una aprobación de la solicitud de cambio para proceder con el desarrollo del mismo.

En lo que respecta a la definición de un proceso para realizar pruebas a los cambios COBIT 5 supera a ITIL en este aspecto, debido a que ITIL no profundiza en dicho proceso, por tal razón existe una mayor discrepancia entre ambas metodologías al evaluar el criterio de “Aprobación del cambio por parte del usuario”. Finalmente, en el registro de los cambios puestos en producción se ve una diferencia entre ITIL v2011 e ISO/IEC 20000, el cual este último no define a profundidad dicho aspecto.

Gráfico 4.3. Corresponde a la última categoría de evaluación, la cual es “Valor agregado en su aplicación”, lo que se busca en esta categoría es evaluar la metodología o la norma a partir del valor agregado que brindar su aplicación en las diferentes organizaciones.

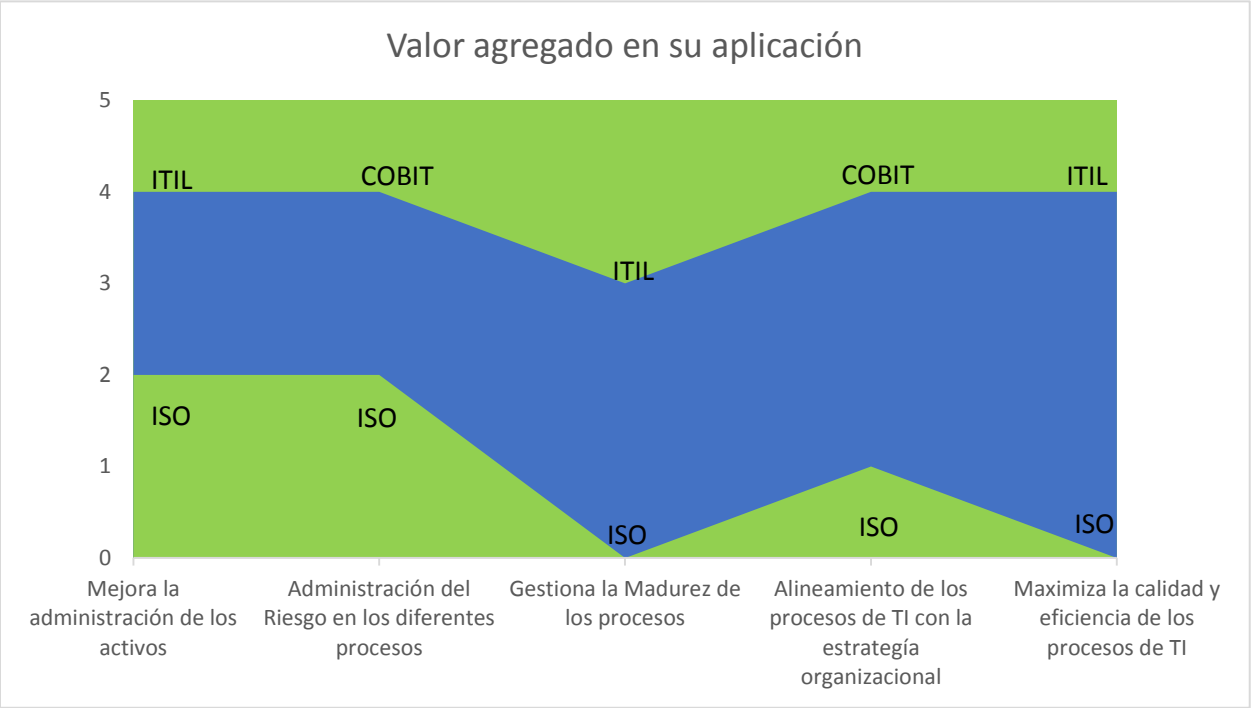

Gráfico 4.3. Valor agregado en su aplicación

Fuente: Elaboración propia

Como se puede observar en el Gráfico 4.3 existe una mayor diferencia entre COBIT 5 e ITIL v2011 respecto a la norma ISO/IEC 20000 en todos los criterios. Al momento de evaluar la Gestión de la Madurez de los procesos, hay una mayor brecha entre ITIL v2011 e ISO/IEC 20000, donde el segundo no describe como alcanzar la madurez en los procesos que se brindan a los usuarios. Misma situación pasa en el criterio de “Maximizar la calidad y eficiencia de los procesos de TI”, donde la norma ISO/IEC 20000 no indica como maximizar la calidad y hacer las efectivos los procesos, por su parte ITIIL v2011 si es más enfático en este aspecto.

4.1.1.4 Selección de la metodología de desarrollo

El objetivo principal de la rúbrica de evaluación de las metodologías y la norma seleccionada, es elegir aquella que mejor se adapta a las operaciones y auditorías que realiza JM Auditores a sus clientes, con el fin de obtener dicha metodología como la base del desarrollo del proyecto.

El Gráfico 4.4 establece los puntajes numéricos obtenidos de la evaluación, en la cual se puede observar que en la primera categoría, “Información General”, tanto ITIL v2011 como ISO/IEC 20000 obtuvieron un 70.83% lo que representa 17 puntos de los 24 totales que se asignan en esta categoría, mientras que COBIT obtuvo un 66.67%. Por su parte la segunda categoría, “Criterios de Evaluación de la Gestión del Cambio”, la norma ISO/IEC 20000 obtuvo el mayor puntaje con un 90% de los puntos de dicha categoría, mientras que ITIL v2011 85% y COBIT 5 un 100%, lo que indica que COBIT se apega a las operaciones actuales de la Organización, en relación a la Gestión del Cambio. La última categoría de la rúbrica, “Valor Agregado a su Aplicación” muestra como hay una gran diferencia entre ITIL v2011 con un 85% y COBIT 5 con un 80% contra el 25% de ISO/IEC 20000, lo que indica que la aplicación en la norma no genera valor a las empresa y por lo contrario ITIL y COBIT brindan mayor aporte a la Gestión de TI.

A partir de lo anterior y al sumar el puntaje obtenido de cada una de las categorías de la rúbrica, se obtiene que ITIL alcanzó un 83% del total de puntaje, mientras que COBIT 5 consiguió un 86% y ISO/IEC 20000 logró 62.5%, lo que indica que COBIT 5 es la metodología que mejor se adapta a las evaluaciones que realiza JM Auditores.

Desde los resultados obtenidos de la rúbrica de evaluación, los cuales fueron presentados a la Organización (Ver Apéndice J), la misma tomó la decisión de seleccionar a COBIT 5 para el desarrollo del proyecto, esto debido a futuras evaluaciones giran alrededor de evaluaciones basadas en esta metodología, lo que al mismo tiempo se tiene planificado que el personal se capacite y se certifique en el manejo de la metodología.

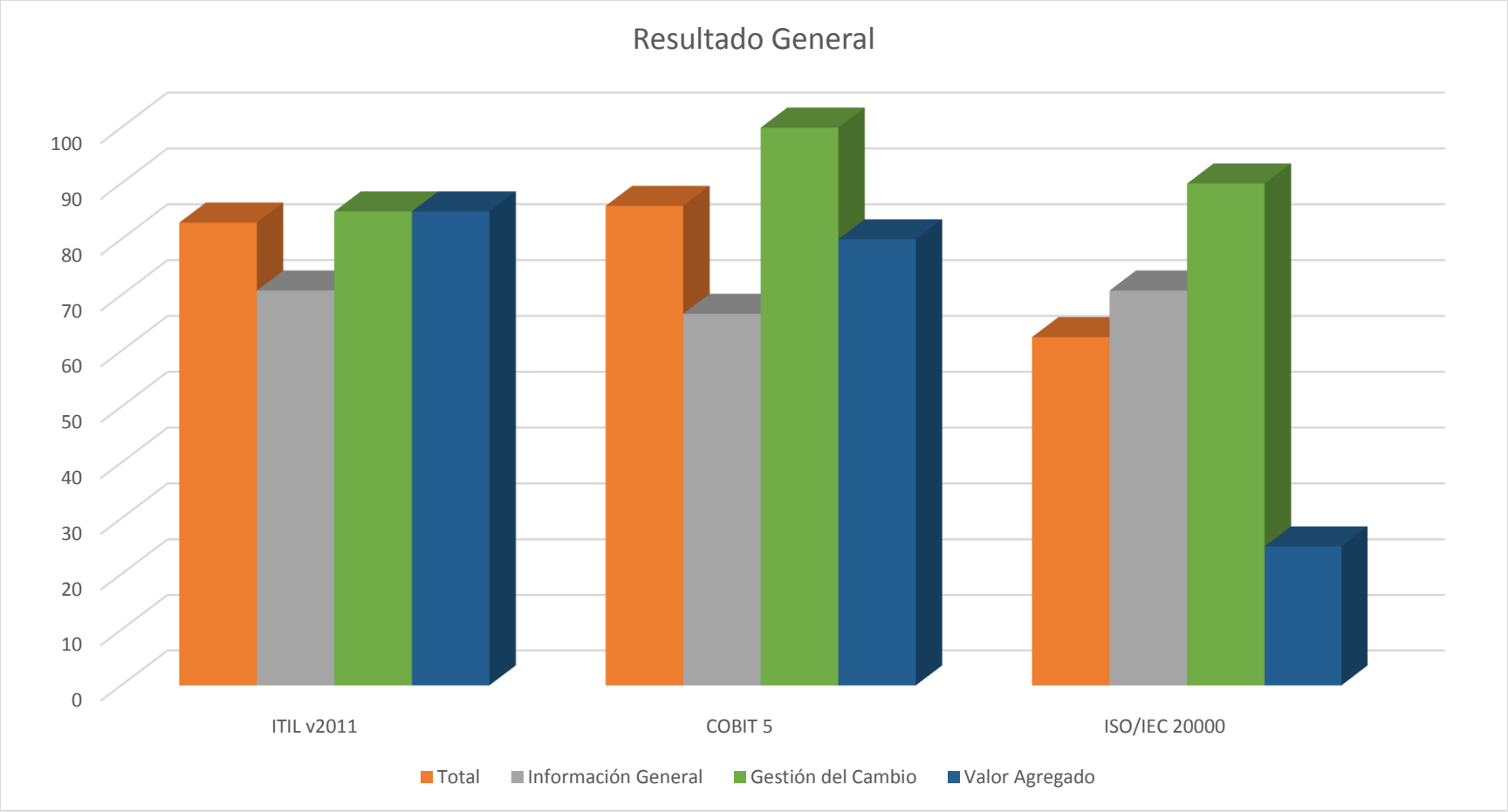

Gráfico 4.4. Resultado General de la Evaluación

Fuente: Elaboración propia

4.1.2 Estudiar procesos relacionados con la Gestión del Cambio en la metodología seleccionada

Como se indicó en la sección anterior, la Organización decidió seleccionar a COBIT 5 como metodología para el establecimiento de los controles de auditoría, este resultado obtenido de la rúbrica de evaluación, donde COBIT reflejó ser la metodología que mejor se adapta a la evaluación que realiza actualmente la organización respecto a la Gestión del Cambio. Por lo cual se procedió a realizar un estudio de la misma para determinar los procesos que se ven relacionados con la Gestión del Cambio, la Tabla 4.2 muestra los procesos identificados y por qué se relacionan con la Gestión del Cambio.

Tabla 4.2. Procesos relacionados con la Gestión del Cambio

Código de COBIT	Proceso	Justificación de su relación
APO01	Gestión del Marco de la Administración de TI.	Establece la creación de políticas para conducir las expectativas de control de TI en temas claves, en las que se vinculan los cambios a los componentes tecnológicos. Asimismo, define que se tiene que velar por el cumplimiento de las políticas y que las mismas deben ser comunicadas a todo el personal de la Organización.
APO02	Gestión de la Estrategia.	Precisa que se debe identificar y evaluar las amenazas por las actuales y las nuevas tecnologías adquiridas, lo que indica que a la hora de realizar un cambio, se debe evaluar si es necesario la adquisición de nueva tecnología o si la existente puede convertirse en una amenaza a partir del cambio.

Código de COBIT	Proceso	Justificación de su relación
APO08	Gestión de las Relaciones.	Define que se debe coordinar y comunicar todo cambio o proceso de transición a los interesados, para que se conozca el estatus, afectaciones y/o mejoras que se brindan a los servicios de TI.
APO11	Gestión de la Calidad.	Indica que se deben integrar las prácticas de gestión de la calidad en el desarrollo de todas las soluciones, asimismo que se deben de tomar en cuenta a los involucrados de un problema o un cambio para que se determinen la causa raíz, impacto y resultados a partir de una mejora.
APO13	Gestión de la Seguridad.	Establece que se debe obtener la autorización de la dirección para realizar cambio a nivel del Sistema de Seguridad; sin embargo, apegándolo a las operaciones de JM Auditores se establece que todo cambio a un componente de TI debe ser autorizado.
BAI02	Gestión de la Definición de Requisitos.	Define que todos los requisitos, y orientándolo a la Gestión de Cambio, todo requerimiento debe ser validado por las partes interesadas, lo incluye la definición de criterios de aceptación de la solución a brindar.
BAI03	Gestión de la Construcción de Soluciones.	Detalla que se deben registrar las peticiones de cambio. Además, detalla que se debe mantener registro de todas las revisiones, resultados o excepciones obtenidas de las pruebas o actividades realizadas al respecto y lo más importante establece que se debe implementar un ambiente de pruebas lo más cercano al ambiente de producción para simular actividades reales de las soluciones desarrolladas.

Código de COBIT	Proceso	Justificación de su relación
BAI05	Gestión de la Habilitación del Cambio.	Precisa que se debe tomar en cuenta el personal que se verá afectado por la implementación de un cambio, asimismo cual será la actitud del mismo para adoptar la nueva solución, por lo que se tiene que evaluar el alcance y el cambio de lo solicitado.
BAI06	Gestión del Cambio.	Proceso principal de estudio, el cual establece el ciclo de vida del cambio, documentación y la especificación de los cambios de emergencia que también se deben considerar.
BAI07	Gestión de la Aceptación del Cambio.	Establece el post de la creación de la solución del cambio, el cual indica que se debe contar un plan de pruebas que considere los criterios de aceptación de los interesados y los criterios de calidad.
BAI10	Gestión de la Configuración.	Detalla la revisión de los cambios propuestos, los cuales van a afectar elementos de configuración, con el fin de garantizar integridad en los elementos, también define que al momento de realizar un cambio, este debe ser comunicado para mantener los elementos de configuración actualizados. Por ultimo establece que el enlazar los cambios con la configuración permite determinar cambios realizados sin una autorización.

Fuente: Elaboración Propia

4.1.3 Alinear cada proceso de la MCGTI con los procesos de la metodología seleccionada

Una vez estudiada la metodología seleccionada, así como identificado los procesos relacionados con la Gestión del Cambio se procedió a alinear la MCGTI con la metodología (COBIT 5), para lo cual se utilizó la revisión documental y el conocimiento financiero y técnico que posee el estudiante para determinar si los procesos que establece la metodología se adaptan al proceso y forma de evaluar de la Organización. A continuación, se presenta la Tabla 4.3 que indica cada proceso de la MCGTI, el proceso asociado de la metodología y lo indicado por la misma, que implica la relación.

Tabla 4.3. Alineación de la MCGTI con la Metodología

Proceso de la MCGTI	Proceso de COBIT 5	Porque se asocian
Entendimiento de TI	APO 01 Gestión del Marco de Administración de TI.	Este proceso indica que se deben llevar las operaciones de TI alineadas a las necesidades del negocio, para lo cual es necesario declarar roles, responsabilidades, así como definir políticas que regulen las expectativas de TI.
	APO 02 Gestión de la Estrategia.	Este proceso define la dirección que se brindará al Departamento de TI, la cual debe estar de igual forma alineada a la dirección del negocio, esto se consigue por medio de la definición del Plan Estratégico de TI y la hoja de ruta, los cuales comprenden los proyectos a realizar por el departamento.
Acceso a Programas y Datos	APO 07 Gestión de Recursos Humanos.	Debido a que el proceso establece que se debe identificar el personal clave dentro del departamento de TI, encargado de realizar las funciones criticas del negocio.
	DSS 01 Gestión de Operaciones.	Este proceso hace énfasis en la gestión de las instalaciones lo que se vincula con el acceso físico a las mismas, principalmente a los espacios donde se encuentra el almacenamiento de la información. El proceso establece que se debe asegurar las instalaciones donde se encuentran los componentes de TI más críticos y con alta disponibilidad para no afecta la operativa del negocio.
	DSS 05 Gestión de los Servicios de Seguridad.	Debido a que establece que se deben gestionar los accesos tanto físicos como lógicos del personal a la información sensible del negocio. Este proceso es vinculante con el DSS 01 respecto a la seguridad de la información.

Proceso de la MCGTI	Proceso de COBIT 5	Porque se asocian
Gestión del Cambio	BAI 05 Gestionar la Habilitación del Cambio.	Este proceso, evalúa el alcance e impacto del cambio solicitado, de forma que permita habilitar y comunicar las afectaciones y mejoras que se van a realizar a todo el personal involucrado.
	BAI 06 Gestión del Cambio.	Establece el procedimiento para llevar a cabo un cambio solicitado, desde la priorización, análisis de impacto, autorización y documentación de los cambios.
	BAI 07 Gestión de la Aceptación del Cambio.	Este proceso es el encargado de colocar en producción los cambios desarrollados, para lo cual define que se deben realizar pruebas que cumplan con los criterios de aceptación, además, de comunicar y coordinar la implementación del cambio.
Desarrollo de programas utilitarios	APD 05 Gestión del Portafolio de Servicio.	Este proceso es el encargado de priorizar las inversiones de acuerdo a los objetivos los objetivos estratégicos del negocio.
	BAI 01 Gestión de los Programas y Proyecto.	Detalla como priorizar los programas de desarrollo y los proyectos de inversión, de acuerdo al portafolio de servicios. Así mismo establece un ciclo de vida o un procedimiento de cómo llevar a cabo un proyecto, ya sea de adquisición o de desarrollo.
	BAI 03 Gestión de la Construcción de Soluciones.	Es el proceso encargado de establecer una metodología de desarrollo de soluciones computacionales, el cual indica que se debe iniciar por el diseño de la solución y concluir con la implementación de la solución.

Proceso de la MCGTI	Proceso de COBIT 5	Porque se asocian
Operación Computacional	DSS 01 Gestión de Operaciones.	Define que se deben programar, realizar y registrar copias de respaldo de la información de acuerdo a las políticas y procedimientos establecidos por el negocio.
	DSS 04 Gestión de la Continuidad.	Detalla que se deben de hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo a la planificación del negocio. Estas copias deben considerar la frecuencia, tipos de copias, tipo de soporte, entre otros aspectos. Además, describe que las copias se deben mantener legibles y archivadas por un tiempo establecido.

Fuente: Elaboración propia

4.1.4 Identificación de los controles de auditoría para el proceso de Gestión del Cambio

Luego de determinar los procesos que se relacionan con la Gestión del Cambio en el apartado 4.1.2 Estudiar procesos relacionados con la Gestión del Cambio en la metodología seleccionada, se procedió a identificar las actividades que define COBIT 5, donde se obtuvo un total de 52 actividades, las cuales se identificaron entre los 37 procesos establecidos por la metodología. Más adelante del documento, precisamente en el apartado 4.1.5 Análisis de los controles de auditoría identificados, se indica el análisis realizado para traducir las 52 actividades de COBIT en controles de auditoría. A continuación se enlistan las actividades identificadas en COBIT 5:

- Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
- Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativos o de negocio.
- Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.
- Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.

- Garantizar que la información comunicada engloba las políticas y procedimientos, los roles y las responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado para cada respectiva audiencia dentro de la empresa.
- Identificar las amenazas por el rechazo a las actuales y nuevas tecnologías adquiridas.
- Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
- Llevar a cabo análisis de satisfacción de clientes y proveedores. Asegurar que se actúa sobre las cuestiones detectadas y que se reportan los resultados y estados.
- Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.
- Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.
- Identificar ejemplos recurrentes de los defectos de calidad, determinar su causa raíz, evaluar su impacto y resultado y acordar acciones de mejora con todos los miembros de los proyectos y los servicios.
- Validar todos los requerimientos mediante aproximaciones tales como revisión por iguales, validación del modelo o prototipo operativo.

- Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para las partes interesadas, patrocinadores de negocio y personal de la implementación técnica, reconociendo que los requerimientos pueden cambiar y llegar a ser más detallados según se implementen.
- Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información (debido por ejemplo a falta de involucración de los usuarios, expectativas irreales, desarrolladores añadiendo funcionalidad innecesaria).
- Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
- Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.
- Mantener un registro con todas las revisiones, resultados, excepciones y correcciones.
- Crear un entorno de pruebas que soporte el alcance completo de la solución y refleje, lo más fielmente posible, las condiciones del mundo real.
- Crear procedimientos de prueba alineados con el plan y las prácticas y que permitan la evaluación de la operativa de la solución en condiciones reales.

- Asegurar que los procedimientos de prueba evalúan la adecuación de los controles, basado en estándares de toda la empresa que definan roles, responsabilidades y criterios de prueba y sean aprobado por las partes interesadas del proyecto y por el patrocinador/dueño del proceso de negocio.
- Realizar las pruebas de las soluciones y sus componentes en concordancia con el plan de pruebas. Incluir probadores independientes del equipo de la solución, con representación de los dueños de los procesos y usuarios finales del negocio. Asegurar que las pruebas son realizadas solo en los entornos de desarrollo y pruebas.
- Identificar, registrar y clasificar (por ejemplo, fallos menores, significativos, críticos) los errores durante las pruebas
- Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.
- Evaluar el impacto de todas las peticiones de cambio de la solución en el desarrollo de la solución.
- Hacer seguimiento de los requerimientos, facilitando a las partes interesadas la supervisión, revisión y aprobación de los cambios. Asegurar que los resultados de los procesos de cambio están completamente entendidos y están de acuerdo todos las partes interesadas y el patrocinador/propietario del proceso de negocio.

- Evaluar el alcance y el impacto del cambio divisado, las diferentes partes interesadas que se verán afectadas, la naturaleza del impacto y la involucración necesaria por cada grupo de partes interesadas y la disposición y habilidad actual para adoptar el cambio.
- Planificar las necesidades de formación del personal para desarrollar las habilidades y actitudes adecuadas para que se sientan facultados.
- Identificar y gestionar líderes que continúen resistiéndose a la necesidad de cambio.
- Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio.
- Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.
- Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
- Planificar y programar todos los cambios aprobados.
- Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.

- Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
- Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.
- Definir qué constituye un cambio de emergencia.
- Categorizar las peticiones de cambio en el proceso de seguimiento.
- Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.
- Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio como parte integral del cambio.
- Confirmar que todos los planes de implantación son aprobados por las partes interesadas tanto de ámbito técnico como de negocio, y revisados por auditoría interna, si es apropiado.

- Desarrollar y documentar el plan de pruebas, de forma que esté alineado con el programa y plan de calidad del proyecto y estándares relevantes de la organización. Comunicar y consultar con los propietarios de procesos de negocio y grupos de interés de TI adecuados.
- Confirmar que todos los planes de prueba son aprobadas por las partes interesadas.
- Crear una base de datos de pruebas que sea representativa del entorno de producción.
- Asegurar que el entorno de pruebas es representativo del escenario futuro de operaciones y de negocio, incluyendo procedimientos y roles de los proceso de negocio, carga de trabajo probable, sistemas operativos, aplicaciones software necesarias, sistemas de gestión de bases de datos, redes e infraestructura de comunicaciones utilizadas en el entorno de producción.
- Aprobar la aceptación mediante una firma formal de los propietarios de los procesos de negocio, terceras partes (según sea necesario) y grupos de interés de TI antes del paso a producción.
- Asegurar que las pruebas y los resultados preliminares están de acuerdo con los criterios de éxito definidos en el plan de pruebas.
- Actualizar inmediatamente la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.
- Crear, revisar y formalizar acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.

- Asegurar que todas las bibliotecas de medios son actualizadas inmediatamente con la versión del componente de la solución que está siendo transferido al entorno de producción.
- Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.
- Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.
- Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.
- Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.

4.1.5 Análisis de los controles de auditoría identificados

Tras haber identificado las actividades descritas por COBIT 5 relacionadas con la Gestión del Cambio, se procedió a realizar el análisis de cada uno, para lo cual se subdividieron en varios pasos que se detallan a continuación.

4.1.5.1 Clasificación de las actividades

En conjunto con la Supervisora del Departamento (Ver Apéndice K) se realizó la clasificación de las actividades identificadas, las cuales se analizaron para establecer si aplican para un control de auditoría o si son complementarios a otros y pueden ser catalogados como pruebas sustantivas. La Tabla 4.4 muestra la clasificación realizada.

Tabla 4.4. Clasificación de Actividades de COBIT 5

Actividad para Control	Actividad para Prueba Sustantiva
Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.	Evaluar y actualizar las políticas, como mínimo una vez al año, para ajustarlas a los cambiantes entornos operativos o de negocio.
	Implantar y aplicar las políticas de TI a todo el personal relevante, de forma que estén incorporadas y sean parte integral de las operaciones empresariales.
	Asegurarse de que los procedimientos estén en funcionamiento para realizar un seguimiento del cumplimiento con las políticas y definir las consecuencias de la no conformidad.
	Garantizar que la información comunicada engloba las políticas y procedimientos, los roles y las responsabilidades, etc. Comunicar la información con el nivel de detalle adecuado para cada respectiva audiencia dentro de la empresa.
	Hacer seguimiento de los requerimientos, facilitando a las partes interesadas la supervisión, revisión y aprobación de los cambios. Asegurar que los resultados de los procesos de cambio están completamente entendidos y están de acuerdo todos las partes interesadas y el patrocinador/propietario del proceso de negocio.

Actividad para Control	Actividad para Prueba Sustantiva
Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.	Evaluar el impacto de todas las peticiones de cambio de la solución en el desarrollo de la solución.
	Evaluar el alcance y el impacto del cambio divisado, las diferentes partes interesadas que se verán afectadas, la naturaleza del impacto y la involucración necesaria por cada grupo de partes interesadas y la disposición y habilidad actual para adoptar el cambio.
	Identificar y gestionar líderes que continúen resistiéndose a la necesidad de cambio.
	Identificar las amenazas por el rechazo a las actuales y nuevas tecnologías adquiridas.
	Categorizar las peticiones de cambio en el proceso de seguimiento.
	Revisar los cambios propuestos a los elementos de configuración respecto a la base de referencia para garantizar su integridad y precisión.

Actividad para Control	Actividad para Prueba Sustantiva
Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados, obtenidos, priorizados y registrados de un modo comprensible para las partes interesadas, patrocinadores de negocio y personal de la implementación técnica, reconociendo que los requerimientos pueden cambiar y llegar a ser más detallados según se implementen.	Validar todos los requerimientos mediante aproximaciones tales como revisión por iguales, validación del modelo o prototipo operativo.
	Involucrar a las partes interesadas para crear una lista potencial de requerimientos técnicos, funcionales, de calidad y riesgos relativos al procesamiento de la información (debido por ejemplo a falta de involucración de los usuarios, expectativas irreales, desarrolladores añadiendo funcionalidad innecesaria).
	Crear un entorno de pruebas que soporte el alcance completo de la solución y refleje, lo más fielmente posible, las condiciones del mundo real.
	Crear procedimientos de prueba alineados con el plan y las prácticas y que permitan la evaluación de la operativa de la solución en condiciones reales. Asegurar que los procedimientos de prueba evalúan la adecuación de los controles, basado en estándares de toda la empresa que definan roles, responsabilidades y criterios de prueba y sean aprobado por las partes interesadas del proyecto y por el patrocinador/dueño del proceso de negocio.
	Identificar, registrar y clasificar (por ejemplo, fallos menores, significativos, críticos) los errores durante las pruebas.

Actividad para Control	Actividad para Prueba Sustantiva
Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.	
Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.	
Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.	Incluir los cambios en la documentación (ej. procedimientos de negocio y operativos de TI, documentación de continuidad de negocio y recuperación frente a desastres, información de configuración, documentación de la aplicación, pantallas de ayuda y material de formación) en el procedimiento de gestión del cambio como parte integral del cambio.
Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.	

Actividad para Control	Actividad para Prueba Sustantiva
Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.	Mantener un registro con todas las revisiones, resultados, excepciones y correcciones.
	Desarrollar y documentar el plan de pruebas, de forma que esté alineado con el programa y plan de calidad del proyecto y estándares relevantes de la organización. Comunicar y consultar con los propietarios de procesos de negocio y grupos de interés de TI adecuados.
	Asegurar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio.
Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.	Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo a su prioridad.
	Actualizar inmediatamente la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.
	Asegurar que todas las bibliotecas de medios son actualizadas inmediatamente con la versión del componente de la solución que está siendo transferido al entorno de producción.
	Planificar las necesidades de formación del personal para desarrollar las habilidades y actitudes adecuadas para que se sientan facultados.
	Actualizar los detalles de configuración con los cambios aprobados a los elementos de configuración.

Actividad para Control	Actividad para Prueba Sustantiva
Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.	Llevar a cabo análisis de satisfacción de clientes y proveedores. Asegurar que se actúa sobre las cuestiones detectadas y que se reportan los resultados y estados.
Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.	Confirmar que todos los planes de prueba son aprobadas por las partes interesadas.
Planificar y programar todos los cambios aprobados.	

Actividad para Control	Actividad para Prueba Sustantiva
Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se ha aplicado el cambio.
	Definir qué constituye un cambio de emergencia.
Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.	

Actividad para Control	Actividad para Prueba Sustantiva
Crear una base de datos de pruebas que sea representativa del entorno de producción.	Asegurar que el entorno de pruebas es representativo del escenario futuro de operaciones y de negocio, incluyendo procedimientos y roles de los proceso de negocio, carga de trabajo probable, sistemas operativos, aplicaciones software necesarias, sistemas de gestión de bases de datos, redes e infraestructura de comunicaciones utilizadas en el entorno de producción.
	Asegurar que las pruebas y los resultados preliminares están de acuerdo con los criterios de éxito definidos en el plan de pruebas.
Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.	Crear, revisar y formalizar acuerdos sobre los cambios en las líneas de referencia de configuración cuando sea necesario.

Fuente: Elaboración Propia

Es importante destacar que hasta este punto solamente se realizó una clasificación de las actividades de COBIT 5 para determinar cuáles actividades ayudarán para establecer los controles de auditoría y cuales ayudan para las pruebas sustantivas. Como se pudo observar en la Tabla 4.4 algunas actividades fueron identificadas para establecer un Control de Auditoría pero no cuentan con actividades que faciliten el establecimiento de pruebas sustantivas, lo que brinda mayor importancia a la fase siete de la metodología de trabajo, misma que se detalla en el apartado 4.1.7 Establecimiento de las pruebas sustantivas.

4.1.5.2 Especificación de controles de auditoría

Para obtener la definición de los controles, es importante respaldarse de las actividades que establece COBIT 5 en sus procesos, los cuales fueron descritos anteriormente. A partir de dichas actividades se establece la Tabla 4.5, en la cual se definen en una primera instancia los controles de auditoría que se adaptan a las actividades de COBIT 5 de acuerdo al criterio del estudiante y por el conocimiento adquirido durante su formación académica.

Tabla 4.5. Primera definición de los controles de auditoría

Controles de Auditoría	
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos, restricciones.
2	La Organización ha establecido un procedimiento para analizar las Solicitudes de Cambio presentadas por los colaboradores, dicho análisis incluye evaluar el alcance e impacto en componentes de TI como en el personal de la empresa.
3	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.
4	El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos.
5	Los desarrollos a la Solución del Cambio presentado, se realizan basado en un plan de calidad que toma en cuenta las expectativas de los interesados.
6	Se realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo, se confirman los criterios de aceptación.
7	Todas las Solicitudes de Cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la Gestión de TI, se encuentran formalmente documentados.
8	Los accesos otorgados para el desarrollo de la solución son revocados al momento del cierre de la solicitud de cambio.
9	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.
10	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.

Controles de Auditoría	
11	Todas las Solicitudes de Cambios son aprobadas por los niveles correspondientes de aprobación.
12	Las Solicitudes de Cambio aprobadas son planificadas y programadas.
13	La Organización cuenta con un procedimiento formal para declarar, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia.
14	Se han establecido bitácoras de seguimiento de las solicitudes de cambios presentadas.
15	Las pruebas se realizan bajo un ambiente similar a las condiciones del ambiente de producción.
16	Todo cambio de configuración en los sistemas o aplicativos son administrados y aprobados por la Gestión de Cambio.

Fuente: Elaboración propia

A partir de lo anterior, se realizó una encuesta (Ver Apéndice E) al equipo de trabajo del área de Administración de Riesgo de la Información, mismo que está conformado por un total de cuatro personas, población total que es posible utilizar en la encuesta, misma que es aplicada debido a que son los encargados de realizar las evaluaciones de TI como apoyo a la auditoría financiera y brindan un criterio de experto, a partir del conocimiento y experiencia propia de cada uno. Dicha encuesta busca determinar si los controles de auditoría establecidos en la Tabla 4.5 se apegan a las actividades de COBIT 5 y a las evaluaciones que se realiza JM Auditores.

A continuación se presentan una recopilación de los resultados obtenidos de las encuestas aplicadas, las cuales se pueden observar en el Apéndice L.

Pregunta 1: De la Tabla 1 y Tabla 2 (De la encuesta) indique cuales procesos se ajustan adecuadamente a la actividad que establece COBIT y las evaluaciones que se realizan en la firma. ¿Justifique su respuesta para aquello controles que no se ajustan?

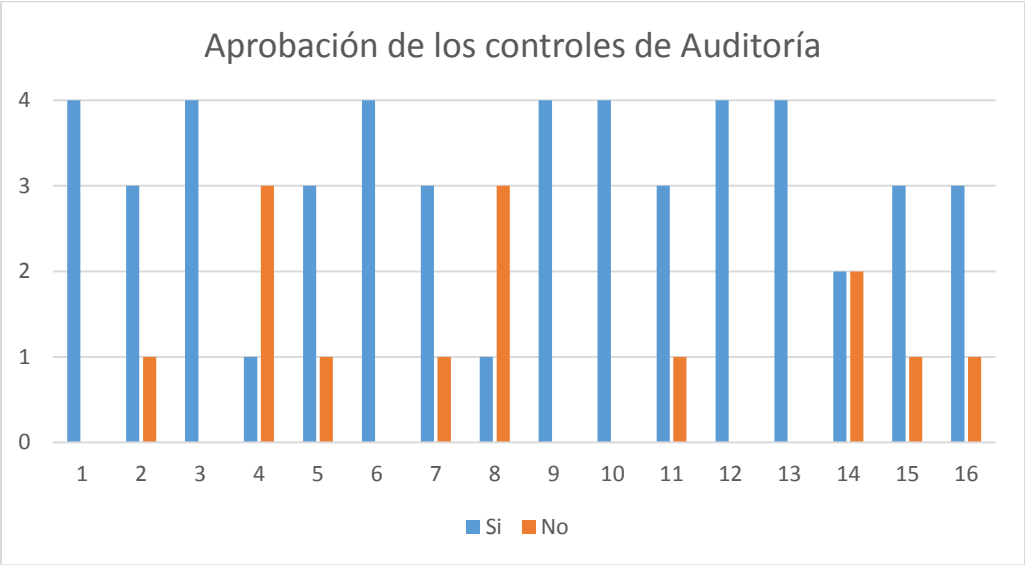

Gráfico 4.5. Aprobación de los controles

Fuente: Elaboración propia

Como se puede observar en el Gráfico 4.5 los controles 1, 3, 6, 9, 10, 12 y 13 de acuerdo al equipo de trabajo se encuentran de acuerdo a lo que se define en COBIT 5, además que se ajustan a las evaluaciones que se realizan en JM Auditores. Por su parte los demás controles recibieron algunas observaciones que se detallan a continuación.

- Para el control 2, un participante indica que se debe ajustar el control para tomar en cuenta el plan de continuidad que establece la actividad de COBIT 5. Por otra parte otro participante indica que la auditoría actual no lo toma en cuenta por un tema de alcance al tipo de auditoría que se realiza.

- Para el control 4, un 75% de los participantes no estuvieron de acuerdo, debido a que establecen que el control debe establecer criterios más medibles y verificables.
- Para el control 5, un participante indica que se debe mejorar la redacción del control, para ser medible y que brinde mayor entendimiento al auditor.
- Para el control 7, un participante indica que existe una diferencia entre la actividad que establece COBIT 5 y el control creado, por lo que se debe ajustar mejor a la actividad.
- El control 8 contó con que tres participantes indicaron que es importante también tomar en cuenta como se otorgan los permisos, además de apegarlo un poco más a la actividad que establece COBIT 5.
- Por su parte el control 11, un participante indica que es importante no solamente autorizar los cambios, sino que también debe contar con un proceso de revisión de la solicitud.
- Para el control 14, los dos participantes que establecieron la negatividad indican que se debe evaluar la existencia de un *tracking* de las solicitudes de cambios donde se puede observar todo el proceso y cambios de estado que ha tenido una solicitud de cambio.
- Por su parte el control 15, un participante describe que se debe mejorar la redacción del control para que brinde un mejor entendimiento al auditor.
- Por último, el control 16, un participante indica que el control debe ser claro en el tema que los cambios en la configuración debe llevarse mediante una solicitud de cambio.

Pregunta 2: ¿De acuerdo a su experiencia cuales controles cambiaría, eliminaría o agregaría? Incluir los cambios y el porqué.

De las respuestas brindadas por los participantes, un 75% establece que se debe agregar un control donde se evalúen los cambios realizados en el ambiente de producción, asimismo como quienes son los responsables de realizar dichos cambios. Por otro lado también agregan que se debe establecer un control para la segregación de funciones a nivel del Departamento de TI, para separar el personal encargado del desarrollo y el personal encargado de realizar la puesta en producción del cambio.

Finalmente, un 25% de los participantes comentan que se debe mejorar la redacción de los controles de forma que sean más detallados, medibles, verificables y entendibles para el auditor.

Pregunta 3: ¿Cree que con las modificaciones realizadas, ya se puede determinar si una Organización realiza una adecuada Gestión de Cambios? Indicar el porqué.

Esta es una pregunta que busca determinar si se está cubriendo la mayoría de los aspectos de una Gestión de Cambio adecuada, para lo cual el 100% de los participantes aprobaron los controles y los cambios realizados en la pregunta dos, entre los comentarios indicados, se destaca que por medio de la evaluación de dichos controles se busca que la empresa auditada trabaje en disminuir el riesgo asociado y busque una mejora continua en la gestión no solo de los cambios sino de TI en general.

4.1.6 Definición de los controles de auditorías para el proceso de Gestión del Cambio

Una vez obtenido las respuestas de las encuestas, en la cual el equipo de trabajo brindó observaciones sobre la definición de los controles de auditoría, se busca realizar una depuración de los controles a partir de las observaciones, de forma que estos sean más medibles, verificables y entendibles para el auditor.

Tras obtener los resultados de la encuesta se realizó un segundo análisis de los controles de auditoría definidos donde con ayuda de la supervisora del área (Ver Apéndice M) se determinó que el control con la siguiente descripción: “El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos” no será tomado en cuenta debido a que se consideró como un control que no que pone en riesgo la generación de estados financiero o el registro contable de las empresas auditadas, el cual es el enfoque de las auditorías realizadas.

Por otro lado, se estableció que es necesario definir un control de auditoría que evalué los cambios en los parámetros de los sistemas o aplicativos de la organización, los cuales se realizan de forma directa en el ambiente de producción, por tal razón y a pesar que COBIT no define ningún aspecto relacionado, se decidió incluir el siguiente control (Ver Apéndice N): “La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción”.

Tras un análisis realizado, gracias a que se cuenta con un conocimiento tanto de la gestión de Tecnología de Información, como en la creación de los estados financieros se realizó una clasificación de los controles de auditoría de forma que se estableció la secuencia con la que se deben evaluar dichos controles, dicha secuencia se describe en la Tabla 4.6, dicho controles fueron aprobados por el Gerente del área (Ver Apéndice N).

Tabla 4.6. Establecimiento de la Secuencia de Evaluación de los controles de Auditoría

Secuencia	Controles de Auditoría
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos, restricciones.
2	Todas las Solicitudes de Cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.
3	La Organización ha establecido un procedimiento para analizar las Solicitudes de Cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.
4	Todas las Solicitudes de Cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.
5	El Gestor del Cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.
6	Las Solicitudes de Cambio aprobadas son planificadas y programadas.

Secuencia	Controles de Auditoría
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.
9	El Departamento de TI cuenta con una bitácora de seguimiento de Solicitudes de Cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).
11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.
14	La Organización cuenta con un procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia.
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.
16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.

Fuente: Elaboración Propia

En el siguiente apartado de la metodología de trabajo se establecen las actividades de COBIT 5 consideradas para las pruebas sustantivas, mismas que se definirán para cada uno de los controles de auditoría definidos.

4.1.7 Establecimiento de las pruebas sustantivas

Como se mencionó en el apartado 4.1.5.1 Clasificación de las actividades, las cuales se dividieron en actividades para controles de auditoría y actividades para las pruebas sustantivas, estas últimas fueron las utilizadas para establecer las pruebas sustantivas ligadas a cada uno de los controles de auditoría definidos en el apartado 4.1.6 Definición de los controles de auditorías para el proceso de Gestión del Cambio.

Para algunos de los controles de auditoría definidos no se identificaron actividades de COBIT 5 que ayuden a establecer las pruebas sustantivas, por lo cual por medio del conocimiento obtenido por el estudiante en la carrera, se logró realizar un análisis de cada uno de los controles de forma que se definieron las pruebas sustantivas, mismas que se detallan en la Tabla 4.7.

Tabla 4.7. Establecimiento de pruebas sustantivas de acuerdo a COBIT 5

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la Gestión del Cambio es revisado y si es necesario actualizado al menos una vez al año.
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.
		Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.
2	Todas las Solicitudes de Cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las Solicitudes de Cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.
		Las Solicitudes de Cambio sobre la documentación oficial de la Gestión de TI se encuentran formalmente documentados y almacenados en un repositorio.

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
3	La Organización ha establecido un procedimiento para analizar las Solicitudes de Cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del cambio y su habilidad para adoptar el mismo.
		Para cada una de las Solicitudes de Cambio, se identifican los colaboradores que se resisten al cambio.
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.
4	Todas las Solicitudes de Cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las Solicitudes de Cambio son aprobadas por los niveles correspondientes.
		Se realiza una revisión de la Solicitud de Cambio para determinar que cuenta con los requerimientos mínimos solicitados.
		Los cambios más considerables son aprobados por un comité de cambio o por la gerencia de TI.
		Las Solicitudes de Cambios rechazadas son justificadas ante el solicitante y personal interesado.

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
5	El Gestor del Cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado se realiza en conjunto con los interesados del cambio.
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.
6	Las Solicitudes de Cambio aprobadas son planificadas y programadas.	Determinar la creación de un cronograma o programación de los cambios aprobados.
		Determinar si los cambios son realizados en el tiempo planificado.
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.	Los cambios aprobados son comunicados al personal interesado y al personal afectado por este.
		La documentación sobre el cambio se encuentra en un sitio accesible para el personal involucrado.
		Determinar que se comunican los beneficios y afectaciones del cambio al personal involucrado.

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.
9	El Departamento de TI cuenta con una bitácora de seguimiento de Solicitudes de Cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción), donde se involucran los roles, procedimiento y carga de datos de acuerdo a lo esperado.
		Determinar que las pruebas y los resultados preliminares se ajustan a los criterios de éxito establecidos para el cambio.
		Indagar sobre el establecimiento de un plan de pruebas, que permita realizar operaciones de acuerdo a las operaciones y condiciones reales.

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.	Los criterios de calidad son documentados para su revisión durante la etapa de desarrollo de la solución.
		Se documentan las revisiones a los criterios de calidad durante el desarrollo de la solución donde los usuarios solicitantes participan de la revisión.
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con todas las revisiones, resultados, excepciones y correcciones.
		Determinar si las pruebas se llevan a cabo en conjunto con los interesados del cambio en busca de su aprobación.
		Se registran y clasifican los errores presentados durante las pruebas.
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Indagar si los cambios planificados son cerrados en el tiempo establecido.
		Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
14	La Organización cuenta con un procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia.	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se haya aplicado el cambio.
		Se ha definido qué es un cambio de emergencia para la organización.
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.
		Se ha establecido los niveles de aprobación de los cambios de emergencia.
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.

	Controles de Auditoría Definitivos	Actividades para las pruebas sustantivas
16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción.
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos.
		Los cambios realizados en los parámetros de los aplicativos quedan registrados en un bitácora de monitoreo.
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.

Fuente: Elaboración propia

4.1.7.1 Análisis de la encuesta

A partir de lo anterior, se realizó una segunda encuesta (Ver Apéndice F) al equipo de trabajo del área de Administración de Riesgo de la Información, mismo que está conformado por un total de cuatro personas, población total que es posible realizarle la encuesta, misma que es aplicada debido a que son los encargados de realizar las evaluaciones de TI como apoyo a la auditoría financiera y brindan un criterio de experto, a partir del conocimiento y experiencia propia de cada uno. El fin de dicha encuesta es determinar si las pruebas sustantivas definidas en la Tabla 4.7 son suficientes para evaluar el control de auditoría en un 100%. A continuación, se presentan las preguntas realizadas en la segunda encuesta al equipo de trabajo y los resultados obtenidos de cada una (Ver Apéndice O).

Pregunta 1: En la casilla “Aplica” de la Tabla 1 marque con “Check” (✓) si las pruebas sustantivas definidas son suficientes para probar el control de auditoría; en caso contrario marque con una “Equis” (X).

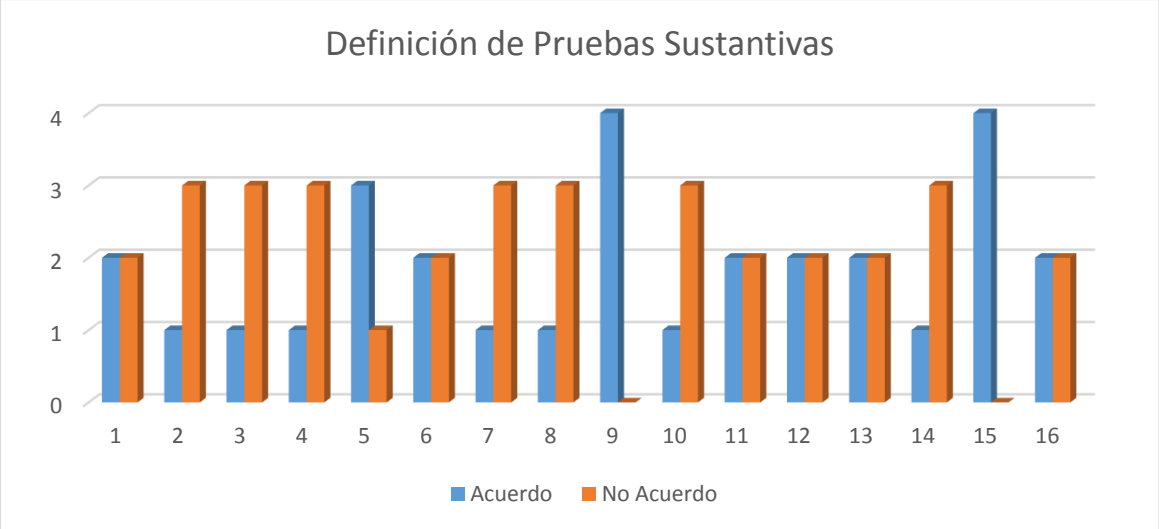

Gráfico 4.6. Establecimiento de pruebas sustantivas

Fuente: Elaboración propia

De acuerdo al Gráfico 4.6 se observa como solamente el control 9 y 15 establecen pruebas sustantivas que permiten evaluar el 100% del control definido. Para los restantes 14 controles recibieron observaciones por parte de los entrevistados mismas que se detallan como parte de la respuesta de la pregunta dos de la encuesta.

Pregunta 2: Para aquellos controles que fueron marcados con una “Equis” (X) indique las pruebas sustantivas que agregaría para cumplir en un 100% con el control de auditoría o que cambios le habría a las pruebas ya definidas.

El equipo de trabajo al cual se le aplicó la encuesta realizaron observaciones en las pruebas sustantivas definidas para los restantes 14 controles de auditoría, dichas observaciones se observan se detallan a continuación.

Control 1: El 50% de los entrevistados brindaron observaciones sobre las pruebas sustantivas definidas para este control, en la cual establecen que el revisar que la política funcione de acuerdo a lo establecido, no es una prueba que agregar valor a la auditoría.

Control 2: El 75% de los entrevistados establece que la prueba sustantiva “Las solicitudes de cambio sobre la documentación oficial de la gestión de TI se encuentran formalmente documentados y almacenados en un repositorio” no es una prueba sustantiva debido a que los cambios en la documentación no es parte de la Gestión de Cambio en TI, debido que en la mayoría de las organización ese es un proceso que se realizan en otros departamentos como control interno.

Control 3: El 75% de los participante de la entrevista establecen que la identificación del personal que se resiste al cambio se realiza luego de implementar el mismo y no antes, por lo que la prueba relacionada no corresponde como parte del control de auditoría, así mismo establecen que es necesario realizan mejoras en la redacción de las restantes pruebas realizadas.

Control 4: El 25% de los entrevistados establece que la prueba “Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.” Ya se ha verificado en las pruebas anteriores por lo cual se estaría redundando en las pruebas a realizar. Por su parte el 50% de los participantes establecen que las pruebas definidos para este control deben de mejorar su redacción para mejor entendimiento y claridad en lo que debe revisar el auditor.

Control 5: El participante que no estuvo de acuerdo con las pruebas sustantivas representa el 25% de los entrevistados, brinda la recomendación en agregar el responsable a la segunda prueba de este control, además que para la tercera prueba se defina que se realicen sobre las solicitudes de cambio para que brinde un mayor entendimiento al auditor.

Control 6: El 50% de los entrevistas establecen que se tiene que mejorar la redacción de las pruebas de forma que se entienda mejor lo que se solicita y la evidencia que tiene que buscar el auditor.

Control 7: Un total del 75% de los participantes se mostraron desacuerdo con las pruebas establecidas, para lo cual brindar la recomendación que unir la prueba tres y uno, mientras que la prueba dos no es parte del control. Así mismo se brindan recomendaciones de cómo mejorar la redacción de las pruebas para un mejor entendimiento de las mismas.

Control 8: Un 25% de los participantes, brindan la observación que una prueba debe ser capaz de verificar que el personal que tiene acceso al ambiente de desarrollo no tiene acceso al ambiente de producción y viceversa. Por otro lado, un 25% de los participantes establece que con determinar el personal que tiene acceso a los diferentes ambientes ya se estaría cumpliendo con el control definido. Y por último el otro 25% que se mostró en desacuerdo con las pruebas establecidas indica que es necesario verificar que el personal que tiene acceso a los diferentes ambientes, realmente no poseen el acceso.

Control 10: El 50% de los participantes establecen que las pruebas sustantivas definidas no son parte del control de auditoría, por su parte el 25% restante indica que es importante revisar que los cambios pasados al ambiente producción son registrados.

Control 11: Un 25% de los participantes, establecen que es necesario realizar un cambio en el control para que este tome en consideración los criterios de aceptación y los pases a producción de los cambios. Por otra parte el restante 25% de los participantes que no estuvieron de acuerdo con las pruebas sustantivas definidas, establecen que la primera prueba es suficiente para realizar la evaluación del control descrito.

Control 12: Un 25% de los participantes brindan la observación de restructurar las pruebas sustantivas para que están sean más específicas, mientras que el otro 25% en desacuerdo establece que dos de las tres pruebas descritas se pueden unir para establecer una sola prueba donde se revisen ambos aspectos.

Control 13: Un 50% de los entrevistas establece que una de las pruebas descritas para este control ya se encuentra considerada en el control 6 por lo que se debería eliminar.

Control 14: El 25% de los entrevistados establece que no es necesario verificar los accesos para los cambios de emergencia mientras se tengan los ambientes segregados, lo cual ya fue revisado en los controles anteriores. Mientras que el restante 50% de los participantes en desacuerdo establece que no es necesario un procedimiento que defina que es un cambio de emergencia, debido a que generalmente esto forma parte de la política de Gestión del Cambio.

Control 16: Un 25% de los participantes brindaron una mejora en la redacción para un mayor entendimiento de la prueba, mientras q el otro 25% establece una similitud con el control 15 el cual revisa los cambios en la configuración de los aplicativos.

4.1.7.2 Definición de las pruebas sustantivas

Tras las observaciones y recomendaciones recibidas de las encuestas realizadas al equipo de trabajo, se desarrollaron mejoras y en algunos casos se eliminaron pruebas sustantivas que no se relacionan con el control de auditoría definidos.

Entre los resultados obtenidos se realizó un segundo análisis donde se determinó que el control número 11 el cual indicaba: “El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.” no determinaba un mayor riesgo para la generación de estados financieros.

Y a su vez se estaba dejando de lado la aprobación de los cambios por parte del usuario solicitante y un control sobre los cambios que ya son puestos en el ambiente de producción, para lo cual dicho control (Control 11) fue modificado de la siguiente forma: “El Departamento de TI documenta los cambios que son puestos en el ambiente de producción.” Asimismo fueron modificadas las pruebas sustantivas para dicho control.

Por otro lado, este análisis llevó a realizar cambios en la redacción de las pruebas definidas en primera instancia, además que algunas pruebas fueron eliminadas porque se determinó que no se adaptaban al control establecido o no generaban un valor agregado para evaluarlo. En la Tabla 4.8 se muestran las pruebas sustantivas definidas para cada uno de los controles de auditoría, mismas que fueron aprobadas por la organización (Ver Apéndice P).

Tabla 4.8. Definición de Pruebas Sustantivas para los Controles de Auditoría

N°	Controles de Auditoría	Pruebas Sustantivas
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la Gestión del Cambio es revisado al menos una vez al año.
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del mismo.
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.

N°	Controles de Auditoría	Pruebas Sustantivas
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.
		Los cambios con mayor impacto son aprobados por un comité de cambio o por la gerencia de TI.
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.
5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado es realizado por el Departamento de TI en conjunto con los interesados del cambio.
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.
6	Las Solicitudes de Cambio aprobadas son planificadas y programadas.	Determinar si la Organización ha establecido un proceso para programar y/o priorizar las solicitudes de cambios.
		Determinar si los cambios aprobados son concluidos en el tiempo planificado.

N°	Controles de Auditoría	Pruebas Sustantivas
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.	Los cambios aprobados son comunicados al personal interesado.
		Determinar que se mantiene una comunicación constante con los interesados del cambio.
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.
		Verificar que el personal de TI que cuenta con acceso al ambiente de producción no tenga relación con el ambiente de desarrollo y viceversa.
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.

N°	Controles de Auditoría	Pruebas Sustantivas
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción).
		Determinar que las pruebas sobre la solución del cambio se realizan de acuerdo al plan de pruebas establecido para este fin.
11	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con el resultado de las pruebas y posibles excepciones.
		Las pruebas de aceptación son realizadas por el usuario solicitante.
		Determinar si la documentación de las pruebas fallidas son documentadas.
12	El Departamento de TI documenta los cambios que son puestos en el ambiente de producción.	Los criterios de aprobación son revisados en conjunto con los interesados del cambio antes de su pase a producción.
		Los pases a producción son documentados, en los cuales se indica el encargado, hora y fecha de la operación.

N°	Controles de Auditoría	Pruebas Sustantivas
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.
14	La Organización cuenta con un procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar, registrar los cambios de emergencia.	Se ha definido qué es un cambio de emergencia para la organización.
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.
		Se ha establecido los niveles de aprobación de los cambios de emergencia.
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.

N°	Controles de Auditoría	Pruebas Sustantivas
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.
16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción.
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos.
		Los cambios realizados en los paramentos de los aplicativos quedan registrados en un bitácora de monitoreo.
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.

Fuente: Elaboración propia

4.1.8 Comparación de los Controles de Auditoría para el proceso de Gestión del Cambio

Una vez obtenidos los resultados de la redefinición de los controles de auditoría y las pruebas sustantivas que corresponden a cada control, se realizará a continuación una comparación en relación con los controles que se evalúan actualmente en la Organización.

Actualmente JM Auditores cuenta con cinco controles de auditoría y un total de 15 pruebas sustantivas para evaluar el proceso de Gestión del Cambio, mismo que se definen en la Tabla 4.9.

Tabla 4.9. Controles y pruebas sustantivas actuales de JM Auditores

N°	Control	Prueba de Eficacia Operativa
1	La Organización ha establecido un proceso de administración del cambio formal que contenga los requisitos para realizar los cambios en los sistemas y aplicaciones que tienen control sobre el reporte financiero.	1. Los procesos se encuentran formalmente documentados y comunicados al personal de TI y al personal Usuario.
		2. El personal apropiado ha realizado la aprobación del proceso de control de cambios.
2	Todas las solicitudes de cambios para los sistemas de información y aplicaciones que brinden control sobre el reporte financiero están formalmente documentadas.	1. Las solicitudes de cambios están formalmente documentadas y almacenadas en un repositorio centralizado.
		2. Las solicitudes de cambios se encuentran aprobados por las personas correspondientes.
		3. Las solicitudes de cambios significativos aprobados por el comité de TI o una función similar.
		4. Cambios a la configuración / parametrización es documentada y evaluada para asegurar el logro de los requerimientos de control del negocio y las aplicaciones.

N°	Control	Prueba de Eficacia Operativa
3	La organización ha establecido un proceso formal de pruebas y firma que permite las pruebas tanto de los sistemas de información como de los usuarios.	1. El personal de TI realiza pruebas del sistema (pruebas de la unidad, el volumen, secuencia e interfaces).
		2. Por parte del personal de TI y usuarios es realizada una prueba de regresión.
		3. Las pruebas de aceptación de los cambios hechos son realizadas por cada uno de los usuarios.
		4. El desarrollo de los planes de implementación y evaluación son desarrollados antes de migrar los cambios a producción.
		5. El plan de implementación considera al menos los aspectos siguientes: *Plan de contingencia y procedimientos de “back-out”. * Procesos de actualización de librerías y directorios. * Lugares de implementación de los cambios. (Si hay múltiples localidades).
4	La Organización ha establecido una política que limita los cambios a producción del personal de administración de cambios.	1. Determinar si los cambios a producción de las librerías y/o directorios son registrados (bitácoras) por software de seguridad.
		2. Determinar y verificar el acceso de modificación en el ambiente de producción está limitado al personal adecuado.

N°	Control	Prueba de Eficacia Operativa
5	Todos los cambios de emergencia se registran para facilitar la revisión detallada del cambio.	1. Los resultados de las pruebas son documentados y almacenados en el repositorio de la documentación de pruebas.
		2. En lo posible, las pruebas de usuario se realizan también para los cambios de emergencia.

Fuente: Adaptado de (JM Auditores, 2014)

Como se puede mostrar en la Tabla 4.9, la Organización solamente toma en cuenta que el auditado tenga un procedimiento para la Gestión del Cambio, así como que se tengan documentados las solicitudes de cambios y las pruebas realizadas. Además de la revisión de los cambios de emergencia realizados y que estos cuenten con la documentación necesaria.

A partir de lo anterior se identificaron brechas entre los controles de auditoría, las cuales buscan ser solucionadas por medio de los nuevos 16 controles de auditoría definidos como desarrollo del presente proyecto y un total de 46 pruebas sustantivas (Ver Tabla 4.8), que se encuentran asociadas a las actividades descritas por COBIT 5.

4.1.9 Matriz de Controles Generales de TI

Actualmente la MCGTI es un documento en Excel que solamente indica los controles y pruebas a realizar por el auditor. Esta es una herramienta de uso interno y exclusivo del auditor como una guía de las pruebas que debe realizar al momento de aplicar una evaluación de Controles Generales en una organización. Los controles establecidos en la MCGTI se encuentran configurados en un sistema de información que posee JM Auditores para llevar a cabo toda la auditoría en una organización, por tal razón es que se establece la mejora de la MCGTI por medio de una plantilla de Excel y no por medio de un sistema de información.

Por medio de la información detallada en este capítulo de los controles de auditoría y pruebas sustantivas para el proceso de Gestión del Cambio, asimismo como los controles y pruebas de los demás procesos de la MCGTI, los cuales no sufrieron cambios tras el desarrollo de este proyecto, se realizó la Automatización de dicha matriz por medio de una plantilla en Microsoft Excel por medio del uso de macros y programación de celdas, la cual fue aprobada por la organización (Ver Apéndice Q).

En el siguiente capítulo se detallan los controles de auditoría que se proponen para la evaluación del proceso de Gestión del Cambio, de la misma forma se establece la elaboración y funcionamiento de la MCGTI una vez que fue modificada y automatizada por medio de una plantilla en Microsoft Excel.

5. Propuesta de Solución

En el presente capítulo se establece la solución brindada al problema descrito en el apartado 1.2 Planteamiento del problema, el cual se centra en la definición de controles de auditoría para el proceso de Gestión del Cambio.

5.1 Alineación de los procesos de la MCGTI con los procesos de COBIT 5

Como se estableció en los 1.3 Objetivos del proyecto y después realizar el análisis de las metodologías (ITIL v2011, COBIT 5) y de la norma (ISO/IEC 20000), se alineó cada uno de los procesos de la Matriz de Controles Generales de TI, a los procesos de COBIT 5.

En la Tabla 5.1, se muestra como el procesos de Entendimiento de TI, se alinea con los procesos de COBIT 5 descritos en la tabla, los cuales establecen que el Departamento de TI debe estar alineado a la estrategia de la organización y para lo cual se deben establecer políticas, procedimientos, procesos y operaciones acorde a los objetivos del negocio.

Tabla 5.1. Alineación del proceso de Entendimiento de TI a COBIT 5

Proceso de la MCGTI	Proceso de COBIT 5
Entendimiento de TI	APO01 Gestión del Marco de Administración de TI.
	APO02 Gestión de la Estrategia.

Fuente: Elaboración propia

Por otra parte, la Tabla 5.2 establece los procesos de COBIT 5 que se alinean al proceso de Acceso a Programas y Datos de la MCGTI, esto debido a que estos se centran en la seguridad de la información en los sistemas informativos, así como en la seguridad física en las instalaciones con las que cuenta la organización y por último porque indican que se debe definir cuál es el personal clave que tiene accesos privilegiados a los diferentes sistemas.

Tabla 5.2. Asociación del proceso “Acceso a Programas y Datos” a COBIT 5

Proceso de la MCGTI	Proceso de COBIT 5
Acceso a Programas y Datos	APO07 Gestión de Recursos Humanos.
	DSS01 Gestión de Operaciones.
	DSS05 Gestión de los Servicios de Seguridad.

Fuente: Elaboración propia

Por su parte la Tabla 5.3 indica la relación del proceso “Gestión del Cambio” con los procesos de COBIT 5, los cuales establecen que el cambio se debe gestionar por medio de tres fases: El pre cambio, donde se realiza un análisis del cambio, se identifican los actores y afectaciones principales; la construcción del cambio, donde se lleva a cabo el desarrollo de la solución del cambio; y por último la post implementación del cambio, donde se evalúan los resultados de haber hecho el cambio, así como la aceptación del personal de la organización.

Tabla 5.3. Alineación del proceso de Gestión del Cambio a COBIT 5

Proceso de la MCGTI	Proceso de COBIT 5
Gestión del Cambio	BAI05 Gestionar la Habilitación del Cambio.
	BAI06 Gestión del Cambio.
	BAI07 Gestión de la Aceptación del Cambio.

Fuente: Elaboración propia

La Tabla 5.4 describe cómo el proceso de Desarrollo de programas utilitarios se alinea a los procesos de COBIT que describen cómo se deben priorizar las inversiones que se desean realizar en la organización. De igual forma se establece que se debe contar con un proceso para realizar los desarrollos de programas y que estos al ser finalizados deben ser actualizados en la documentación oficial correspondiente.

Tabla 5.4. Alineación del proceso de Desarrollo de programas utilitarios a COBIT 5

Proceso de la MCGTI	Proceso de COBIT 5
Desarrollo de programas utilitarios	APD05 Gestión del Portafolio de Servicio.
	BAI01 Gestión de los Programas y Proyecto.
	BAI03 Gestión de la Construcción de Soluciones.

Fuente: Elaboración propia

Por último, la Tabla 5.5 establece los procesos de COBIT 5 que se asocian al proceso Operación Computacional de la MCGTI, estos se alinean debido a que estos definen la programación de respaldos en las bases de datos y de los sistemas que posee la organización. Además, se tiene que realizar pruebas sobre los respaldos para validar que estos son útiles en caso que se necesario su utilización.

Tabla 5.5. Alineación del proceso Operación Computacional a COBIT 5

Proceso de la MCGTI	Proceso de COBIT 5
Operación Computacional	DSS01 Gestión de Operaciones.
	DSS04 Gestión de la Continuidad.

Fuente: Elaboración propia

5.2 Definición de controles de auditoría

Tal y como se especificó en el apartado 4.1.6 Definición de los controles de auditorías para el proceso de Gestión del Cambio para el proceso de Gestión del Cambio, donde se definieron los resultados obtenidos de la metodología seleccionada, además de los resultados obtenidos de las encuestas realizadas, se establecieron los siguientes controles de auditoría para el proceso de Gestión del Cambio, mismos que se muestran en la Tabla 5.6 en el orden en que deben ser evaluados por los auditores.

Tabla 5.6. Definición de los controles de auditoría

Controles de Auditoría	
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de cambios, con los respectivos lineamientos, pasos y restricciones.
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.
5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.
6	Las Solicitudes de Cambio aprobadas son planificadas y programadas.

Controles de Auditoría	
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).
11	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.
12	El Departamento de TI documenta los cambios que son puestos en el ambiente de producción.
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.
14	La Organización cuenta con un procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia.
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.
16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.

Fuente: Elaboración propia

Por medio de los 16 controles definidos, JM Auditores se asegura realizar evaluaciones más detallas sobre la Gestión del Cambio, el cual de acuerdo a la metodología propia es uno de los procesos más críticos de evaluación. Asimismo estos controles de auditoría permiten realizar evaluaciones acorde a un marco de trabajo internacional como lo es COBIT 5, al mismo tiempo que su contraparte (Empresa auditada) entenderá mejor cada uno de los requisitos y pruebas a realizar por parte de los auditores.

5.3 Definición de pruebas sustantivas

A partir de esto se han definido una serie de pruebas sustantivas que los auditores deben realizar para garantizar que la organización auditada cumple con Gestión del Cambio en busca la disminución del riesgo. La Tabla 5.7 define cuales son las pruebas sustantivas definidas para cada uno de los 16 controles de auditoría que se definieron para el proceso de Gestión del Cambio.

Por medio de estas 47 pruebas sustantivas, se establece una revisión más detallada sobre la Gestión del Cambio que realizan las empresas auditadas. De forma que se busque disminuir el riesgo de realizar cambios indebidos en sistemas o aplicativos que se involucran en la generación de los estados financieros, por parte del personal de TI. Además, que se han establecidos controles de revisión durante los diferentes etapas del ciclo de vida de un cambio, lo que permite brindar un seguimiento en cada etapa e identificar alguna alteración que se pueden presentar durante el desarrollo de una solución al cambio presentado.

Tabla 5.7. Definición de Pruebas Sustantivas para cada uno de los Controles de Auditoría

N°	Controles de Auditoría	Pruebas Sustantivas
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la Gestión del Cambio es revisado al menos una vez al año.
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del mismo.
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.

N°	Controles de Auditoría	Pruebas Sustantivas
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.
		Los cambios con mayor impacto son aprobados por un comité de cambio o por la gerencia de TI.
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.
5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado es realizado por el Departamento de TI en conjunto con los interesados del cambio.
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.

N°	Controles de Auditoría	Pruebas Sustantivas
6	Las Solicitudes de Cambio aprobadas son planificadas y programadas.	Determinar si la Organización ha establecido un proceso para programar y/o priorizar las solicitudes de cambios.
		Determinar si los cambios aprobados son concluidos en el tiempo planificado.
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.	Los cambios aprobados son comunicados al personal interesado.
		Determinar que se mantiene una comunicación constante con los interesados del cambio.
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.
		Verificar que el personal de TI que cuenta con acceso al ambiente de producción no tenga relación con el ambiente de desarrollo y viceversa.

N°	Controles de Auditoría	Pruebas Sustantivas
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción).
		Determinar que las pruebas sobre la solución del cambio se realizan de acuerdo al plan de pruebas establecido para este fin.
11	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con el resultado de las pruebas y posibles excepciones.
		Las pruebas de aceptación son realizadas por el usuario solicitante.
		Determinar si la documentación de las pruebas fallidas son documentadas.
12	El Departamento de TI documenta los cambios que son puestos en el ambiente de producción.	Los criterios de aprobación son revisados en conjunto con los interesados del cambio antes de su pase a producción.
		Los pases a producción son documentados, en los cuales se indica el encargado, hora y fecha de la operación.

N°	Controles de Auditoría	Pruebas Sustantivas
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.
14	La Organización cuenta con un procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar, registrar los cambios de emergencia.	Se ha definido qué es un cambio de emergencia para la organización.
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.
		Se ha establecido los niveles de aprobación de los cambios de emergencia.
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.

N°	Controles de Auditoría	Pruebas Sustantivas
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.
16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción.
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos.
		Los cambios realizados en los paramentos de los aplicativos quedan registrados en un bitácora de monitoreo.
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.

Fuente: Elaboración propia

5.4 Automatización de la Matriz de Controles Generales de TI

Finalmente, como entregable a la organización se automatizó la Matriz de Controles Generales de TI, la cual es una herramienta interna para uso de los auditores para llevar el control sobre las pruebas que debe realizar. El objetivo de establecer una automatización de la MCGTI es brindar facilidad al auditor a la hora de definir el resultado de las pruebas realizadas, el hecho de automatizar la Matriz por medio de Excel se debe que ya JM Auditores cuenta con un sistema de información robusto para llevar a cabo toda la auditoría financiera y esta Matriz es que uso exclusivo para el auditor Especialista en TI. Por tal motivo, no se realizó la recomendación de incluir un sistema de información con los controles de auditoría y pruebas sustantivas definidas.

Por medio de esta automatización, se le permitirá al auditor también identificar cuáles de las pruebas han sido efectivas, cuáles posee oportunidades de mejora y cuáles son inefectivas.

La automatización de la Matriz se realizó por medio de una plantilla de Microsoft Excel, en la cual se definieron indicadores de colores, la Tabla 5.8 muestra el indicar de color, el significado establecido y el resultado a reportar.

Tabla 5.8. Indicadores de las pruebas de auditoría

Indicador (color)	Significado	Resultado
Verde	Prueba Efectiva.	Prueba Efectiva.
Amarillo	Prueba Efectiva, con una debilidad a mejorar.	Oportunidad de Mejora.
Rojo	Prueba Inefectiva.	Hallazgo de Auditoría.

Fuente: Elaboración Propia

Por otro lado, también se definió una lista de opciones que le permitirá al auditor precisar el resultado de la prueba sustantiva que se está evaluando, de forma que la seleccionar una de las opciones que se muestran en la Tabla 5.9 para el proceso de “Entendimiento de TI” o de las opciones que se muestran la Tabla 5.10 para los restantes procesos de la MCGTI, la matriz le indicará al auditor el resultado de la prueba indicada.

Tabla 5.9. Opciones para brindar resultado a las pruebas del proceso “Entendimiento de TI”

Opción	Resultado
Se tiene actualizado	Pruebas Efectiva
Se tiene sin actualizar	Oportunidad de Mejora
No se tiene	Hallazgo de Auditoría

Fuente: Elaboración propia

Tabla 5.10. Opciones para brindar resultado a las pruebas de los procesos de la MCGTI

Opción	Resultado
El funcionamiento de la prueba realizada es efectiva.	Pruebas Efectiva
Se mantiene un control sobre lo solicitado; sin embargo, se identificaron debilidades a reportar.	Oportunidad de Mejora
No se cuenta con lo solicitado por la prueba.	Hallazgo de Auditoría

Fuente: Elaboración propia

Tras la automatización, también se realizaron cambios en la estructura de la Matriz donde se incluyó una columna para que el auditor pueda colocar una situación identificada relacionada con una oportunidad de mejora o un hallazgo de auditoría, de forma que le permita tener descritos los resultados que debe emitir en una carta de resultados enviada al final de la evaluación. Asimismo, se incluyó un apartado donde se resumen la cantidad de pruebas sustantivas que han sido efectivas, las que se han reportado con oportunidades de mejora y las que son inefectivas, es decir, con un hallazgo de auditoría.

Una vez definida la estructura y los cambios a realizar en la MCGTI, se establecieron los controles de auditoría y las pruebas sustantivas que se tenían definidas para los procesos: “Entendimiento de TI”, “Acceso a Programas y Datos”, Desarrollo de Programas Utilitarios” y “Operación Computacional”. En la Tabla 5.11 se muestran la cantidad de pruebas que se realizan para cada uno de los procesos. Cabe destacar que estás pruebas no sufrieron cambios durante el desarrollo de este proyecto y por su lado se estableció a qué procesos del marco de COBIT se encuentran alineados.

Tabla 5.11. Cantidad de pruebas a realizar para cada proceso de la MCGTI

Proceso	Cantidad de pruebas a realizar
Entendimiento de TI	9 pruebas
Acceso a Programas y Datos	11 pruebas
Desarrollo de Programas Utilitarios	5 pruebas
Operación Computacional	2 pruebas

Fuente: Adaptado de (JM Auditores, 2014)

Por su parte, también se establecieron en la MCGTI los 16 Controles de Auditoría y las 45 pruebas sustantivas que se definieron como producto del presente proyecto para el proceso de Gestión de Cambio y como se explicó en el apartado 4 Análisis de Resultados del presente documento difieren de los cinco controles y 15 pruebas sustantivas que se tenían definidos anteriormente.

A continuación se presentan imágenes que muestran el resultado final de la automatización de la MCGTI y se explicará un ejemplo para comprender su funcionamiento, asimismo en el Apéndice R se puede observar la MCGTI completa.

Controles Generales de TI			
Entendimiento de TI			
Documento	**Cumplimiento**	**Estatus**	**Situación Identificada**
* Plan estratégico de Tecnología de Información	Se tiene sin actualizar	Oportunidad de Mejora	
* Listado de los sistemas y su plataforma tecnológica	Se tiene sin actualizar	Oportunidad de Mejora	
* Listado de los proyectos en vigencia	No se tiene	Hallazgo	
* Organigrama de Tecnología de Información	Se tiene actualizado	Efectivo	
* Diagrama de la red	Se tiene actualizado	Efectivo	
* Plan de Continuidad	Se tiene sin actualizar	Oportunidad de Mejora	
* Plan de Capacitación	Se tiene actualizado	Efectivo	
* Manuales y/o descripciones de puestos	No se tiene	Hallazgo	
* Políticas relacionadas con TI y/o acceso al sitio donde están publicadas	Se tiene sin actualizar	Oportunidad de Mejora	

Figura 5.1. Proceso de "Entendimiento de TI" de la nueva MCGTI

Fuente: Elaboración propia

Como se puede observar en la Figura 5.1 se establece en la columna "Documento" toda la documentación que debe solicitar el auditor para su revisión. Por su parte en la columna "Cumplimiento" se ha configurado las opciones que se definieron en la Tabla 5.9, en la columna "Estatus" la matriz de forma automática identifica si la prueba es efectiva, con una oportunidad de mejora o inefectiva con un hallazgo de auditoría a partir de lo seleccionado en la columna "Cumplimiento" y finalmente en la columna "Situación Identificada", el auditor ingresa la oportunidad de mejora o el hallazgo de auditoría identificado. Para comprender mejor el funcionamiento de la matriz se detalla el siguiente ejemplo:

> Un auditor Especialista en TI de JM Auditores, llega a la empresa “Productos Lácteos S.A” a brindar apoyo a la Auditoría Financiera en la revisión de los sistemas de información relacionados con el registro contable y la emisión de los estados financieros. Lo primero que debe revisar el auditor es el proceso de “Entendimiento de TI” para lo cual solicita los documentos indicados en la MCGTI, luego de la revisión de los mismo identifica que el Plan Estratégico de TI no ha sido revisado durante el último año, asimismo no se mantiene un registro de los proyectos de TI que se llevan cabo en la empresa durante el periodo de auditoría. Por otro lado, el Plan de Continuidad tampoco ha sido actualizado.

Cada uno de estos aspecto señalados en el ejemplo, el auditor los ingresa en la Matriz Automatizada y esta le va indicando si corresponde a una Oportunidad de Mejora o si es un Hallazgo de Auditoría tal y como lo muestra la Figura 5.1.

Controles Generales de TI					
Acceso a Programas y Datos					
No.	**Control**	**Pruebas de Eficacia Operativa**	**Cumplimiento**	**Estatus**	**Situación Identificada**
Políticas de seguridad de la información y concientización de usuarios					
1	La Organización ha establecido una función de seguridad de la información que está alineada apropiadamente con la organización.	1. Determinar si la función está apropiadamente posicionada y es independiente para el desarrollo y operación.	No se cuenta con lo solicitado por la prueba	Hallazgo	
		2. Indagar que el personal que conforma la función de seguridad de la información tiene la expertice técnica para comprender/entender conceptos de seguridad y su implementación.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
2	La Organización ha adoptado una política de seguridad formal que ofrece una guía para la seguridad de la información e incluye en su alcance todos los aspectos del ambiente de TI relevantes para las aplicaciones y datos del reporte financiero (p.e. redes, seguridad de perímetro, seguridad del sistema operativo, seguridad de aplicaciones, uso aceptable de sistemas).	1. La política de seguridad ha sido comunicada a todo el personal de la organización.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		2. La política ha sido aprobada por el personal adecuado dentro de TI y la organización.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		3. La política se revisa y actualiza apropiadamente	No se cuenta con lo solicitado por la prueba	Hallazgo	
Identificación y autenticación					
3	La Organización ha establecido un mecanismo de autenticación para los sistemas de información incluidos en el alcance que proporcione responsabilidad individual (cuentas individuales por usuario).	1.Cada empleado cuenta con un Usuario y Contraseña único, de cual es responsable.	Se mantiene un control sobre lo solicitado; sin embargo, se identificaron debilidades a reportar	Oportunidad de Mejora	
		2. Se utilizan contraseñas o métodos más robustos para determinandar la autenticidad de los usuarios.	El funcionamiento de la prueba realizada es efectiva	Efectivo	

Figura 5.2. Proceso de “Acceso a Programas y Datos” en la nueva MCGTI

Fuente: Elaboración propia

A diferencia del proceso de “Entendimiento de TI”, para lo demás procesos de la MCGTI se establecieron los controles de auditoría y las pruebas sustantivas de cada control (Ver Figura 5.2, Figura 5.3, Figura 5.4 y Figura 5.5), las cuales son las que posee un resultado final a partir de lo indicado por el auditor en la columna “Cumplimiento”, la cual tiene configurada las opciones definidas en la Tabla 5.10. Al continuar con el ejemplo.

El Especialista de TI continua con la evaluación en “Productos Lácteos”, donde evalúa el proceso de Acceso a Programas y Datos para lo cual se inicia con la primera prueba sustantiva que indica “Determinar si la función está apropiadamente posicionada y es independiente para el desarrollo y operación.”, para lo cual el auditor después de ejecutar la prueba establece que no se cuenta con lo solicitado en la misma.

Lo indicado por el auditor es ingresado a la matriz y está establece que se debe reportar un hallazgo de auditoría. Esta misma lógica de funcionamiento se establece para los demás procesos de MCGTI (Ver Figura 5.2, Figura 5.3, Figura 5.4 y Figura 5.5)

Controles Generales de TI					
Gestión del Cambio					
No.	**Control**	**Pruebas de Eficacia Operativa**	**Cumplimiento**	**Estatus**	**Situación Identificada**
Proceso Formal de la Gestión del Cambio					
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	1. Determinar si la política y/o procedimiento de la Gestión del Cambio es revisado y si es necesario actualizado al menos una vez al año.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		2. La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		3. Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		4. Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		5. La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.	Se mantiene un control sobre lo solicitado; sin embargo, se identificaron debilidades a reportar	Oportunidad de Mejora	
2	Todas las Solicitudes de Cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	1. Las Solicitudes de Cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.	No se cuenta con lo solicitado por la prueba	Hallazgo	

Figura 5.3. Proceso de “Gestión del Cambio” en la nueva MCGTI

Fuente: Elaboración propia

Controles Generales de TI					
Desarrollo de Programas Utilitarios					
No.	**Control**	**Pruebas de Eficacia Operativa**	**Cumplimiento**	**Estatus**	**Situación Identificada**
Metodología de Desarrollo y Adquisición					
1	La organización ha adoptado un proceso formal para la adquisición o desarrollo de la infraestructura de TI y los sistemas de información.	1. La administración ha establecido niveles de autorización de compras para TI que incluye las aprobaciones basadas en impacto del negocio y nivel de gastos.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		2. La administración ha adoptado una metodología de ciclo de vida de desarrollo de los sistemas.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
2	El desarrollo de sistemas significativos y proyectos de infraestructura son aprobados por TI y la alta gerencia.	1. Determinar y verificar que la Compañía cuenta con un Comité de TI.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		2. Determinar y verificar si la Compañía cuenta con aprobaciones especiales cuando los proyectos sobrepasan la cantidad de presupuesto.	Se mantiene un control sobre lo solicitado; sin embargo, se identificaron debilidades a reportar	Oportunidad de Mejora	
		3. La capitalización y requerimientos de gastos es establecida en base a el tamaño y alcance del proyecto.	No se cuenta con lo solicitado por la prueba	Hallazgo	

Figura 5.4. Proceso de “Desarrollo de Programas Utilitarios” en la nueva MCGTI

Fuente: Elaboración propia

Controles Generales de TI					
Operación Computacional					
No.	**Control**	**Pruebas de Eficacia Operativa**	**Cumplimiento**	**Estatus**	**Situación Identificada**
Procedimientos de respaldos y recuperación					
1	Se ha implementado un horario de respaldo y requerimientos de retención proporcionales con el riesgo de la pérdida de datos, basandose en la criticidad del sistema y el costo de la recuperación manual.	1. Verificar la existencia de horarios, diarios, semanales y mensuales.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		2. Determinar si ha habido definición de periodos de retención basados en las regulaciones del negocio.	El funcionamiento de la prueba realizada es efectiva	Efectivo	
		3. Determinar si el equipo adecuado o capaz de realizar la lectura de los datos que son almacenados.	Se mantiene un control sobre lo solicitado; sin embargo, se identificaron debilidades a reportar	Oportunidad de Mejora	
2	Los procedimientos de respaldo y de recuperación son probados periódicamente para los sistemas incluidos dentro del alcance.	1. Determinar y verificar si la Compañía evalúa periódicamente los procedimientos de respaldo y de recuperación para los sistemas incluidos dentro de nuestro alcance.	No se cuenta con lo solicitado por la prueba	Hallazgo	

Figura 5.5. Proceso “Operación Computacional” en la nueva MCGTI

Fuente: Elaboración propia

Luego de establecer los controles de auditoría y pruebas sustantivas para el proceso de Gestión del Cambio, asimismo de haber alineado cada proceso de la MCGTI a lo que establece COBIT y la automatización de la misma, se realizó una reunión con la Organización para realizar la presentación de la nueva MCGTI y brindarle a ellos un informe con los procesos de COBIT 5 a los que se relacionan los procesos establecidos en la Matriz (Ver Apéndice S).

Una vez realizado la presentación a la Organización y haber establecidos los entregables a la misma se procede en el siguiente capítulo a definir las conclusiones y posteriormente las recomendaciones a partir del análisis de la información y el desarrollo de la metodología de trabajo.

6. Conclusiones

En el presente capítulo se detallan las conclusiones derivadas del trabajo realizado, el análisis llevado a cabo sobre la información obtenida y el desarrollo de la metodología de trabajo propuesta. Previo a cada una de las conclusiones se indica el objetivo específico al que se hace referencia.

1. **Objetivo 1:** Realizar un análisis de dos metodologías internacionales (ITIL v2011, COBIT 5) y una norma (ISO/IEC 20000) basado en el proceso de Gestión del Cambio, con el propósito de recomendar la metodología que mejor se adapta a la organización.

   1. De la evaluación realizada por medio de la rúbrica donde se analizaron las metodologías, COBIT 5 e ITIL v2011 y la norma ISO/IEC 20000, se determinó lo siguiente:

   - ITIL v2011, permite capacitar al personal por un bajo costo y en un tiempo menor en comparación a COBIT 5 e ISO/IEC 20000.
   - ITIL v2011 posee una descripción más detalla del proceso de Gestión del Cambio, donde especifica cada una de las tareas que se deben ejecutar para establecer una Gestión de Cambio adecuada, mientras de COBIT 5 es más escueto en este aspecto, debido a que no entra en detalle en la implementación e indica las actividades necesarias para el control.

- Tanto ITIL v2011 como COBIT 5, establecen un proceso específico para cada uno de los cinco procesos que evalúa JM Auditores, mientras que la ISO/IEC 20000 describe dos de estos procesos.
- Tanto ITIL v2011 como COBIT 5, establecen que las solicitudes de cambio deben ser documentadas, mientras que ISO/IEC 20000, establece esta actividad como un hecho y no la define.
- COBIT 5 establece con claridad y define un proceso detallado sobre la ejecución de pruebas sobre el desarrollo de la solución, mientras que ITIL v2011 solamente establece que se tiene que realizar pruebas a los desarrollo sin entrar en detalle.
- Como producto del proceso definido en COBIT 5 para la ejecución de las pruebas se establece que el usuario solicitante debe realizar la aprobación de la solución y de las pruebas realizadas, mientras de ITIL v2011 no establece este aspecto en toda su documentación.
- ITIL v2011, establece que se debe mantener un registro de cada uno de los cambios que son colocados en el ambiente de producción, mientras de ISO/IEC 20000, no establece dicho registro.

- Tanto ITIL v2011 como COBIT 5, le brinda a la organización un valor agregado mayor al que brinda ISO/IEC 20000, esto debido a que ITIL v2011 mantiene una gestión para los activos, además que por medio de una gestión de TI adecuado por medio de ITIL se busca la madurez de los servicios brindados y que los mismos se encuentren alineados al 100% a la estrategia del negocio, mientras que COBIT 5 busca gestionar los riesgos para que estos no se materialicen, así como establecer que toda actividad de la Gestión de TI debe alinear a los objetivos de la organización; ISO/IEC 20000 es más escueto en estos aspecto lo que disminuye el valor que le agrega a una organización a pesar que se enfoca en el cumplimiento.

2. Se determinó que las operaciones y evaluaciones que realiza JM Auditores se alinean a los establecido en COBIT 5 por su orientación hacia el control y tras analizar su contenido por medio de las tres categorías de la rúbrica de evaluación (Información General, Descripción del proceso de Gestión del Cambio y Valor agregado); no obstante, se identificó que ITIL v2011 mantiene una cercanía por la forma que los clientes implementan los procesos auditados.

3. Se identificó que COBIT 5 mantiene una definición escueta sobre el proceso de Gestión del Cambio, sin embargo, por medio de los 37 procesos establecidos y la relación entre ellos permitió que esta metodología se adaptara a las evaluación de JM Auditores, además, que su orientación hacia en control sobre la Gestión de TI permitió que se alineará más que las otras metodología estudiadas.

2. **Objetivo 2:** Definir los controles generales de TI que establece la metodología seleccionada para evaluar la Gestión de Cambios.
    1. A partir del estudio realizado sobre los 37 procesos definidos en COBIT 5, se identificaron un total de 52 actividades distribuidas en 7 de los procesos definidos.
    2. Se definieron un total de 16 controles de auditoría para la revisión del proceso de Gestión del Cambio. Estos 16 controles permitirán evaluar el proceso desde la creación de una política que determine como se realiza un cambio en los aplicativos y sistemas de la organización auditada, hasta la colocación del cambio en producción, en contraste a los cinco controles definidos anteriormente.
    3. Se establecieron controles de auditoría más específicos donde inicialmente la organización contaba solamente con cinco controles para evaluar el proceso de Gestión del Cambio y tras el desarrollo del proyecto se transformaron en 16 controles de auditoría para este proceso.

3. **Objetivo 3:** Desarrollar de forma detallada las pruebas sustantivas para cada uno de los controles de auditoría identificados para evaluar la gestión de cambios.
    1. Se establecieron un total de 46 pruebas sustantivas que responden a los 16 controles de auditoría definidos, en contraste a las 15 pruebas establecidas inicialmente por JM Auditores.
    2. A partir de las entrevistas realizadas, al personal del área de Administración de Riesgo de la Información, se establecieron que las pruebas sustantivas debían ser medibles y concretas en lo que solicitaba cada una, con el fin de no establecer ambigüedades en las mismas que dieran como resultados pruebas diferentes en cada auditor.
    3. Un 80% de las pruebas sustantivas definidas, se encuentran asociadas a las actividades descritas por COBIT 5, mientras que el 20% restante se consideró a partir del conocimiento del personal consultado y conocimiento del estudiante tanto a nivel técnico, como a nivel administrativo.

4. **Objetivo 4:** Alinear la Matriz de Controles Generales de TI de acuerdo a los procesos identificados en la metodología seleccionada que cumplen con los procesos definidos actualmente por la organización.
    1. Por medio del estudio de COBIT 5, cada proceso de la MCGTI se alineó en promedio a tres procesos establecidos en COBIT 5; sin embargo, esto no implica que todas las actividades definidas en dichos procesos se ajusten a la evaluación y operación de JM Auditores, en específico a lo realizado por el área de Administración del Riesgo de la Información.
5. **Objetivo 5:** Modificar la matriz de controles generales de TI mediante la automatización de los controles y las pruebas sustantivas, basada en macros de Microsoft Excel, de forma que indique el resultado obtenido de la evaluación realizada.
    1. Se estableció una escala de tres indicadores para establecer si cada una de las pruebas sustantivas es efectiva (Verde), inefectiva (Rojo) o cuenta con oportunidades de mejora (Amarillo) para cumplir con el 100% de lo solicitado.
    2. Producto de la mejora realizada a la MCGTI le permite al auditor ingresar el resultado obtenido por medio de opciones ya predefinidas y esta le indica si la prueba es efectiva, inefectiva o con oportunidades de mejora.

3. Se eliminó el criterio del auditor para establecer si una prueba es efectiva o no, debido a que a partir de los resultados obtenidos se establece el resultado del control, el cual debe estar respaldado por la documentación incluida en el sistema de auditoría con el que cuenta JM Auditores.
4. Se automatizó la MCGTI mediante el uso de Macros y programación de celdas en Microsoft Excel, la cual cuenta con todos los controles de auditoría y pruebas sustantivas definidas por JM Auditores para los procesos “Entendimiento de TI”, “Acceso a Programas y Datos”, “Desarrollo de Programas Utilitarios”, “Operación Computaciones”. Además de los controles de auditoría y pruebas sustantivas definidas en este proyecto para el proceso de “Gestión del Cambio”.
5. Se estableció una herramienta de fácil uso donde puede centralizar los resultado obtenidos de cada una de las pruebas y facilite la generación del reporte de resultados que es emitido al auditado al final de la evaluación.

7. Recomendaciones

En este apartado se establecen las recomendaciones identificadas a partir del desarrollo del proyecto en busca de brindar oportunidades de mejora en las actividades que se realizan en la organización.

1. Realizar la alineación de los demás procesos de la MCGTI a una metodología internacional, de forma que se establezcan controles de auditoría y pruebas sustantivas de acuerdo a la metodología. Por medio del presente proyecto se establecieron los procesos de COBIT 5 a los que se alinean cada uno, sin embargo, es importante considerar el uso de otras metodologías como parte de la definición de los controles de auditoría.
2. Valorar el uso de ITIL en combinación con COBIT 5 para establecimiento de controles de auditoría como parte de la mejora continua, esto debido a que en muchas de las empresas auditadas buscan la implementación de ITIL para la gestión de los servicios de TI.
3. Capacitar al personal del área de Administración del Riesgo de la Información en el manejo de COBIT 5, de manera tal que estos pueda realizar las pruebas con mayor criterios y respaldados por lo indicado en una metodología reconocida internacionalmente. Además le brinda al auditor un conocimiento para mantener fundamentos en las observaciones brindadas a los auditados.
4. Establecer a nivel del área de Administración del Riesgo de la Información un proceso para la mejora continua de las evaluaciones y procesos que se realizan.

5. Establecer un proceso de revisión de las pruebas realizadas por los auditores para determinar que la ejecución de las pruebas son las correctas y se mantiene una similitud entre todos los auditores.
6. Desarrollar un documento que establezca los requerimientos necesarios para realizar cada uno de las pruebas sustantivas establecidas.
7. Desarrollar una herramienta o documento complementario a la MCGTI que le indique al auditor la evidencia mínima que debe solicitar para cumplir con cada una de las pruebas.

8. Apéndice

8.1 Apéndice A: Plantilla de Minutas

Minuta # – Trabajo Final de Graduación

Título de la minuta

Fecha:	
Lugar:	

Presentes

Estudiante practicante	
Profesor Asesor	
Representante de la Organización	

1. Objetivo

1.1

2. Temas tratados

2.1

3. Compromisos asumidos

3.1 Estudiante:

3.1.1

3.2 Profesor:

3.2.1

4. Próxima reunión

Día, Mes

5. Firmas de los presentes

_____ _____

Profesor Asesor Estudiante practicante

_____

Representante de la Organización

8.2 Apéndice B: Plantilla de Solicitud de Cambio

Plantilla de Solicitud de Cambio

1. Datos de la solicitud de cambio

Fecha	
Nombre del solicitante	

2. Categoría del Cambio

Marque todas las opciones que apliquen

	Alcance
	Documentación

	Cronograma
	Otros

3. Descripción de la propuesta del cambio

4. Justificación de la propuesta del cambio

5. Impacto del cambio en la línea base del proyecto

Describa el impacto que tendrá el cambio en los aspectos descritos

Alcance
Cronograma
Recursos

Procedimientos
Documentación
Otros

6. Riesgos de implementación del cambio solicitado

7. Comentarios

8. Aprobado/Rechazado

Se indican las razones del rechazo o las pautas de la aceptación.

9. Firma del comité de cambios

Nombre	Rol	Firma

8.3 Apéndice C: Plantilla para el control de los cambios

Plantilla de control de cambios

Proyecto: _Propuesta de mejora y definición de controles de auditoría y pruebas sustantivas___

Encargado del proyecto: _Adán Josué Masís Alvarez_____

Profesor tutor: _Isaac Alpízar_____

ID	Descripción del Cambio	Solicitante	Fecha de Solicitud	Aprobado / Rechazado	Fecha de Aprobación / Rechazo	Aprobado por:	Observaciones

8.4 Apéndice D: Rúbrica de evaluación de las metodologías

Tabla D.1. Rúbrica de evaluación de metodologías

Rúbrica de evaluación de metodologías							
		Escala de Calificación					Comentarios
		Malo	Deficiente	Regular	Bueno	Excelente	
Puntuación	100%	0 Puntos	1 Punto	2 Puntos	3 Puntos	4 Puntos	
Información General (25%)							
Criterios de Evaluación							
Permite Certificación	**4%**	No permite certificación.	Certifica solo el conocimiento y no la práctica.	Posee solo un nivel de certificación, es decir, posee una sola certificación para toda la metodología.	Posee entre 2 y 3 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	Posee más de 4 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	

Valor de capacitación para el personal	**3%**	Capacitar al persona tiene un valor superior a los 1300 dólares por persona, lo que se sale del presupuesto de la organización.	Capacitar al personal tiene un valor entre 976 y 1300 dólares por persona.	Capacitar al personal tiene un valor entre 651 y 975 dólares por persona.	Capacitar al personal tiene un valor entre 326 y 650 dólares por persona.	Capacitar al personal tiene un valor entre 0 y 325 dólares por persona.	
Tiempo de capacitación para el personal	**3%**	No es posible definir el tiempo exacto de la capacitación del personal.	Duración entre 20 y 24 horas de capacitación.	Duración entre 19 y 15 horas.	Duración entre 14 y 10 horas.	Duración menor a 10 horas de capacitación.	
Cantidad de procesos definidos para la gestión de TI	**5%**	No define procesos relacionados con la Gestión de TI.	Define entre 1 a 10 procesos de la Gestión de TI.	Define entre 11 y 20 procesos de la Gestión de TI.	Define entre 21 y 30 procesos de la Gestión de TI.	Define entre 31 y 40 procesos de la Gestión de TI.	

Descripción del proceso de Gestión del Cambio	**5%**	No se define el Proceso de Gestión del Cambio.	Realiza una mención superficial del proceso de Gestión del Cambio.	Define la Gestión del Cambio sin entrar en detalles.	Define la Gestión del Cambio y da algunos detalles sobre su implementación.	Se define de forma clara el proceso de Gestión del Cambio y se detalla ampliamente su implementación.	
La metodología toma en cuenta los demás procesos que evalúa la organización	**5%**	No define los procesos que realiza la organización.	Define 1 de los 5 procesos que evalúa la organización.	Define 2 de los 5 procesos que evalúa la organización.	Define 3 de los 5 procesos que evalúa la organización.	Define 4 o 5 de los 5 procesos que evalúa la organización.	
Criterios de Evaluación de Gestión del Cambio (40%)							
Criterios de Evaluación							
Registro de solicitudes de cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26% y 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% y 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% y 100% con las evaluaciones que realiza JM Auditores.	

Aprobación de las solicitudes de Cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26% y 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% y 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% y 100% con las evaluaciones que realiza JM Auditores.	
Mantiene un proceso de pruebas para los cambios	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26% y 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% y 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% y 100% con las evaluaciones que realiza JM Auditores.	
Aprobación del cambio por parte del usuario solicitante	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26% y 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% y 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% y 100% con las evaluaciones que realiza JM Auditores.	

Registro de los cambios puestos en producción	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26% y 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% y 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% y 100% con las evaluaciones que realiza JM Auditores.	
Valor agregado en su aplicación (35%)							
Criterios de Evaluación							
Mejora la administración de los activos	**7%**	No hace mención de la Gestión de los Activos.	Realiza una mención superficial de la administración de los activos.	Define la Gestión de los Activos sin entrar en detalles.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara y la gestión de los activos y da amplios detalles sobre su implementación.	
Administración del Riesgo en los diferentes procesos	**7%**	No se hace mención de la Gestión del Riesgo.	Realiza una mención superficial de la Gestión del Riesgo.	Define la Gestión del Riesgo sin entrar en detalle.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión del Riesgo y da amplios detalles sobre su implementación.	

Gestiona la Madurez de los procesos	**7%**	No hace mención de la Gestión de la Madurez de los procesos.	Realiza una mención superficial de la Gestión de la Madurez de los procesos.	Define la Gestión de la Madurez de los procesos sin entrar en detalle.	Define la Gestión de la Madurez de los procesos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión de la Madurez de los procesos y da amplios detalles sobre su implementación.	
Alineamiento de los procesos de TI con la estrategia organizacional	**7%**	No hace mención de como alinear los procesos de TI con la estrategia de la organización.	Realiza una mención superficial de cómo alinear los procesos de TI con la estrategia organizacional.	Define como alinear los procesos de TI con la estrategia organizacional sin entrar en detalle.	Define cómo alinear los procesos de TI con la estrategia organizacional y da algunos detalles sobre su implementación.	Define de forma clara de cómo alinear los procesos de TI con la estrategia organizacional y da amplios detalles sobre su implementación.	
Maximiza la calidad y eficiencia de los procesos de TI	**7%**	No hace mención de cómo maximizar la calidad y eficiencia de los procesos de TI.	Realiza una mención superficial de cómo maximizar la calidad y eficiencia de los procesos de TI.	Define cómo maximizar la calidad y eficiencia de los procesos de TI sin entrar en detalle.	Define cómo maximizar la calidad y eficiencia de los procesos de TI y da algunos detalles sobre su implementación.	Define de forma clara de cómo maximizar la calidad y eficiencia de los procesos de TI y da amplios detalles sobre implementación.	

Fuente: Elaboración propia

8.5 Apéndice E: Encuesta sobre controles generales de Gestión del Cambio

Definición de Controles para la Gestión del Cambio

Nombre: _____

Indicaciones

Lea cuidadosamente cada una de las tablas. La Tabla 1 define las actividades que establece COBIT 5 para la Gestión del Cambio y la Tabla 2 establece los controles relacionados con la actividad de COBIT 5.Basado en la información de las tablas y de acuerdo a su experiencia responda las siguientes preguntas.

1. De la Tabla E.1 y Tabla E.2 indique cuales procesos se ajustan adecuadamente a la actividad que establece COBIT y las evaluaciones que se realizan en la firma. ¿Justifique su respuesta para aquello controles que no se ajustan?

N° de Control	Justificación		N° de Control	Justificación
1			9	
2			10	
3			11	
4			12	
5			13	
6			14	
7			15	
8			16	

2. ¿De acuerdo a su experiencia cuales controles cambiaría, eliminaría o agregaría? Incluir los cambios y el porqué

_____

_____

_____

_____

_____

_____

_____

_____

3. ¿Cree que con las modificaciones realizadas, ya se puede determinar si una Organización realiza una adecuada Gestión de Cambios? Indicar el porqué.

_____

_____

_____

_____

_____

_____

_____

_____

Tabla E.1. Actividades de COBIT 5

Actividades de COBIT 5	
1	Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
2	Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.
3	Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
4	Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.
5	Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.
6	Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados.
7	Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
8	Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.
9	Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.
10	Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.

Tabla E.2. Controles de auditoría

Controles de Auditoría		¿Aplica?
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de cambios, con los respectivos lineamientos, pasos, restricciones.	
2	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio presentadas por los colaboradores, dicho análisis incluye evaluar el alcance e impacto en componentes de TI como en el personal de la empresa.	
3	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio.	
4	El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos.	
5	Los desarrollos a la solución del cambio presentado, se realizan basado en un plan de calidad que toma en cuenta las expectativas de los interesados.	
6	Se realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo, se confirman los criterios de aceptación.	
7	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	
8	Los accesos otorgados para el desarrollo de la solución son revocados al momento del cierre de la solicitud de cambio	
9	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	
10	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	

Actividades de COBIT 5		Controles de Auditoría		¿Aplica?
11	Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.	11	Todas las solicitudes de cambios son aprobadas por los niveles correspondientes de aprobación.	
12	Planificar y programar todos los cambios aprobados.	12	Las Solicitudes de Cambio aprobadas son planificadas y programadas	
13	Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.	13	La Organización cuenta con una procedimiento formal para declarar, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	
14	Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.	14	Se han establecido bitácoras de seguimiento de las solicitudes de cambios presentadas	
15	Crear una base de datos de pruebas que sea representativa del entorno de producción.	15	Las pruebas se realizan bajo un ambiente similar a las condiciones del ambiente de producción.	
16	Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.	16	Todo cambio de configuración a los sistemas o aplicativos es administrado y aprobado por la Gestión de Cambio.	

Fuente: Elaboración propia

8.6 Apéndice F: Encuesta sobre la definición de Pruebas Sustantivas

Definición de Pruebas Sustantivas

Nombre: _____

Indicaciones

Lea cuidadosamente la Tabla 1, la cual muestra los controles de auditoría y las pruebas sustantivas definidas para cada uno de estos controles y responda las siguientes preguntas.

1. En la casilla “Aplica” de la Tabla 1 marque con “Check” (✓) si las pruebas sustantivas definidas son suficientes para probar el control de auditoría; en caso contrario marque con una “Equis” (X).
2. Para aquellos controles que fueron marcados con una “Equis” (X) indique las pruebas sustantivas que agregaría para cumplir en un 100% con el control de auditoría o que cambios le habría a las pruebas ya definidas.

No. Control	Prueba Sustantiva

Tabla 1: Definición de pruebas sustantivas			
Controles de Auditoría a partir de la encuesta		**Actividades para las pruebas sustantivas**	**¿Aplica?**
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la gestión del cambio es revisado y si es necesario actualizado al menos una vez al año.	
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.	
		Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.	
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.	
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.	
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.	
		Las solicitudes de cambio sobre la documentación oficial de la gestión de TI se encuentran formalmente documentados y almacenados en un repositorio.	
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.	
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del cambio y su habilidad para adoptar el mismo.	
		Para cada una de las solicitudes de cambio, se identifican los colaboradores que se resisten al cambio.	
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.	

4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.	
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.	
		Los cambios más considerables son aprobados por un comité de cambio o por la gerencia de TI.	
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.	
5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.	
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado se realiza en conjunto con los interesados del cambio.	
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.	
6	Las Solicitudes de Cambio aprobadas son planificados y programados	Determinar la creación de un cronograma o programación de los cambios aprobados.	
		Determinar si los cambios son realizados en el tiempo planificado.	
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	Los cambios aprobados son comunicados al personal interesado y al personal afectado por este.	
		La documentación sobre el cambio se encuentra en un sitio accesible para el personal involucrado.	
		Determinar que se comunican los beneficios y afectaciones del cambio al personal involucrado.	
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.	
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.	
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.	
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.	

9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.	
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción), donde se involucran los roles, procedimiento y carga de datos de acuerdo a lo esperado.	
		Determinar que las pruebas y los resultados preliminares se ajustan a los criterios de éxito establecidos para el cambio.	
		Indagar sobre el establecimiento de un plan de pruebas, que permita realizar operaciones de acuerdo a las operaciones y condiciones reales.	
11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.	Los criterios de calidad son documentados para su revisión durante la etapa de desarrollo de la solución.	
		Se documentan las revisiones a los criterios de calidad durante el desarrollo de la solución donde los usuarios solicitantes participan de la revisión.	
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con todas las revisiones, resultados, excepciones y correcciones.	
		Determinar si las pruebas se llevan a cabo en conjunto con los interesados del cambio en busca de su aprobación.	
		Se registran y clasifican los errores presentados durante las pruebas.	
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Indagar si los cambios planificados son cerrados en el tiempo establecido.	
		Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.	
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.	
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.	

14	La Organización cuenta con una procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se haya aplicado el cambio.	
		Se ha definido qué es un cambio de emergencia para la organización.	
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.	
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.	
		Se ha establecido los niveles de aprobación de los cambios de emergencia.	
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.	
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.	
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.	
16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción.	
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos	
		Los cambios realizados en los parámetros de los aplicativos quedan registrados en un bitácora de monitoreo.	
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.	

8.7 Apéndice G: Rúbrica de Evaluación de ITIL v2011

Tabla G1. Rúbrica de Evaluación de ITIL v2011

Rúbrica de evaluación de metodologías								
		Escala de Calificación					Puntos Asignados	Comentarios
		Malo	Deficiente	Regular	Bueno	Excelente		
Puntuación	100 %	0 Puntos	1 Punto	2 Puntos	3 Puntos	4 Puntos	83	
Información General (25%)								
Criterios de Evaluación								
Permite Certificación	**4%**	No permite certificación.	Certifica solo el conocimiento y no la práctica.	Posee solo un nivel de certificación, es decir, posee una sola certificación para toda la metodología.	Posee entre 2 y 3 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	Posee más de 4 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	4	Posee 5 niveles de certificación: Foundation Level, Pactitioner Level, Intermediate Level, Expert Level, Master Level.

Valor de capacitación para el personal	**3%**	Capacitar al persona tiene un valor superior a los 1300 dólares por persona, lo que se sale del presupuesto de la organización.	Capacitar al personal tiene un valor entre 976 y 1300 dólares por persona.	Capacitar al personal tiene un valor entre 651 y 975 dólares por persona.	Capacitar al personal tiene un valor entre 326 y 650 dólares por persona.	Capacitar al personal tiene un valor entre 0 y 325 dólares por persona.	1	Tiene un valor de 1000 dólares por persona
Tiempo de capacitación para el personal	**3%**	No es posible definir el tiempo exacto de la capacitación del personal.	Duración entre 20 y 24 horas de capacitación.	Duración entre 19 y 15 horas.	Duración entre 14 y 10 horas.	Duración menor a 10 horas de capacitación.	1	Un curso de capacitación tiene una duración de 24 horas
Cantidad de procesos definidos para la gestión de TI	**5%**	No define procesos relacionados con la Gestión de TI.	Define entre 1 a 10 procesos de la Gestión de TI.	Define entre 11 y 20 procesos de la Gestión de TI.	Define entre 21 y 30 procesos de la Gestión de TI.	Define entre 31 y 40 procesos de la Gestión de TI.	3	Se definen 23 procesos en las 5 faces del ciclo de vida del proceso

Descripción del proceso de Gestión del Cambio	**5%**	No se define el Proceso de Gestión del Cambio.	Realiza una mención superficial del proceso de Gestión del Cambio.	Define la Gestión del Cambio sin entrar en detalles.	Define la Gestión del Cambio y da algunos detalles sobre su implementación.	Se define de forma clara el proceso de Gestión del Cambio y se detalla ampliamente su implementación.	4	Define un total de 8 actividades y un ciclo de vida del cambio, así como se debería clasificar, priorizar y llevar a cabo toda la Gestión de cambio para un proceso, sistema o código de una aplicación.
La metodología toma en cuenta los demás procesos que evalúa la organización	**5%**	No define los procesos que realiza la organización.	Define 1 de los 5 procesos que evalúa la organización.	Define 2 de los 5 procesos que evalúa la organización.	Define 3 de los 5 procesos que evalúa la organización.	Define 4 o 5 de los 5 procesos que evalúa la organización.	4	Se define un proceso que se liga cada uno de los evaluados por la Organización, asimismo en los demás procesos habla sobre algunos temas que son vinculantes.

Criterios de Evaluación de Gestión del Cambio (40%)								
Criterios de Evaluación								
Registro de solicitudes de cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	La metodología establece que todas las solicitudes de cambio deben ser registradas. La Organización evalúa que se tenga registro de todos los cambios realizados a sistemas y aplicaciones.
Aprobación de las solicitudes de Cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	ITIL establece una jerarquía para realizar las aprobaciones de los cambios. La empresa indica que toda solicitud de cambio debe ser aprobada por el personal correspondiente.

Mantiene un proceso de pruebas para los cambios	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	3	Se establece una etapa de pruebas y un proceso de desarrollo y entrega; no obstante no se establece un proceso para llevar a cabo las pruebas de un cambio. Por su parte la Organización establece que se debe seguir todo un proceso de pruebas antes de pasar el cambio a un ambiente de producción.
Aprobación del cambio por parte del usuario solicitante	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	2	Al igual que el punto anterior es establece una etapa de pruebas y un proceso de desarrollo y entrega, pero no se describe en el mismo que debe haber una aprobación por parte del usuario solicitante, aspecto que evalúa la organización.

Registro de los cambios puestos en producción	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% y 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Se establece una revisión y documentación de cierre una vez que el cambio se ha realizado y se ha pasado al ambiente de producción. La Organización evalúa que todo cambio en producción sea documentado.
Valor agregado en su aplicación (35%)								
Criterios de Evaluación								
Mejora la administración de los activos	**7%**	No hace mención de la Gestión de los Activos.	Realiza una mención superficial de la administración de los activos.	Define la Gestión de los Activos sin entrar en detalles.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara y la gestión de los activos y da amplios detalles sobre su implementación.	4	Define un proceso específico para la gestión de los activos, el cual incluye tanto activos fijos o activos relacionados con los procesos de TI.

Administración del Riesgo en los diferentes procesos	**7%**	No se hace mención de la Gestión del Riesgo.	Realiza una mención superficial de la Gestión del Riesgo.	Define la Gestión del Riesgo sin entrar en detalle.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión del Riesgo y da amplios detalles sobre su implementación.	2	Define el proceso de seguridad, en el cual se menciona la gestión de riesgos, sin mucho detalle.
Gestiona la Madurez de los procesos	**7%**	No hace mención de la Gestión de la Madurez de los procesos.	Realiza una mención superficial de la Gestión de la Madurez de los procesos.	Define la Gestión de la Madurez de los procesos sin entrar en detalle.	Define la Gestión de la Madurez de los procesos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión de la Madurez de los procesos y da amplios detalles sobre su implementación.	3	Establece que por medio de todo el ciclo de vida de los procesos la organización puede llegar a gestionar la madurez de los mismos, obteniendo mayor eficiencia en la Gestión de TI.
Alineamiento de los procesos de TI con la estrategia organizacional	**7%**	No hace mención de como alinear los procesos de TI con la estrategia de la organización.	Realiza una mención superficial de cómo alinear los procesos de TI con la estrategia organizacional.	Define como alinear los procesos de TI con la estrategia organizacional sin entrar en detalle.	Define cómo alinear los procesos de TI con la estrategia organizacional y da algunos detalles sobre su implementación.	Define de forma clara de cómo alinear los procesos de TI con la estrategia organizacional y da amplios detalles sobre su implementación.	4	Establece la fase de Estrategia del Servicio el cual busca que todo proceso de TI, se encuentre alineado a la estrategia y necesidades de la empresa.

Maximiza la calidad y eficiencia de los procesos de TI	**7%**	No hace mención de cómo maximizar la calidad y eficiencia de los procesos de TI.	Realiza una mención superficial de cómo maximizar la calidad y eficiencia de los procesos de TI.	Define cómo maximizar la calidad y eficiencia de los procesos de TI sin entrar en detalle.	Define cómo maximizar la calidad y eficiencia de los procesos de TI y da algunos detalles sobre su implementación.	Define de forma clara de cómo maximizar la calidad y eficiencia de los procesos de TI y da amplios detalles sobre implementación.	4	Establece que por medio del apego de las buenas prácticas y lo estipulado por estas se logró una mejor calidad y eficiencia a la hora de entregar los procesos a los usuarios finales.

Fuente: Elaboración propia

8.8 Apéndice H: Rúbrica de Evaluación de COBIT 5

Tabla H.1. Rúbrica de Evaluación de COBIT 5

Rúbrica de evaluación de metodologías								
		Escala de Calificación					Puntos Asignados	Comentarios
		Malo	Deficiente	Regular	Bueno	Excelente		
Puntuación	100 %	0 Puntos	1 Punto	2 Puntos	3 Puntos	4 Puntos	86	
Información General (25%)								
Criterios de Evaluación								
Permite Certificación	**4%**	No permite certificación.	Certifica solo el conocimiento y no la práctica.	Posee solo un nivel de certificación, es decir, posee una sola certificación para toda la metodología.	Posee entre 2 y 3 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	Posee más de 4 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	4	Posee más de 4 niveles de certificación. Foundation, Implementation, Assessor, Assessor for Security, Implementing the NIST Standart.

Valor de capacitación para el personal	**3%**	Capacitar al persona tiene un valor superior a los 1300 dólares por persona, lo que se sale del presupuesto de la organización.	Capacitar al personal tiene un valor entre 976 y 1300 dólares por persona.	Capacitar al personal tiene un valor entre 651 y 975 dólares por persona.	Capacitar al personal tiene un valor entre 326 y 650 dólares por persona.	Capacitar al personal tiene un valor entre 0 y 325 dólares por persona.	1	Tiene un costo de 1000 dólares por persona
Tiempo de capacitación para el personal	**3%**	No es posible definir el tiempo exacto de la capacitación del personal.	Duración entre 20 y 24 horas de capacitación.	Duración entre 19 y 15 horas.	Duración entre 14 y 10 horas.	Duración menor a 10 horas de capacitación.	1	El curso de capacitación tiene una duración de 20 horas.
Cantidad de procesos definidos para la gestión de TI	**5%**	No define procesos relacionados con la Gestión de TI.	Define entre 1 a 10 procesos de la Gestión de TI.	Define entre 11 y 20 procesos de la Gestión de TI.	Define entre 21 y 30 procesos de la Gestión de TI.	Define entre 31 y 40 procesos de la Gestión de TI.	4	Posee definidos un total de 37 procesos.

Descripción del proceso de Gestión del Cambio	**5%**	No se define el Proceso de Gestión del Cambio.	Realiza una mención superficial del proceso de Gestión del Cambio.	Define la Gestión del Cambio sin entrar en detalles.	Define la Gestión del Cambio y da algunos detalles sobre su implementación.	Se define de forma clara el proceso de Gestión del Cambio y se detalla ampliamente su implementación.	2	Define la Gestión del Cambio en el proceso BAI 06, no obstante, no entra en detalle y brinda la sugerencia de consultar otros marcos de referencia.
La metodología toma en cuenta los demás procesos que evalúa la organización	**5%**	No define los procesos que realiza la organización.	Define 1 de los 5 procesos que evalúa la organización.	Define 2 de los 5 procesos que evalúa la organización.	Define 3 de los 5 procesos que evalúa la organización.	Define 4 o 5 de los 5 procesos que evalúa la organización.	4	Define procesos relacionados con la estrategia, la seguridad de accesos, la gestión del cambio, gestión de la configuración y gestión del conocimiento.
Criterios de Evaluación de Gestión del Cambio (40%)								
Criterios de Evaluación								
Registro de solicitudes de cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	La metodología establece que las solicitudes de cambio deben ser documentadas para proceder a su evaluación y aprobación correspondiente.

Aprobación de las solicitudes de Cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Se define que toda solicitud de cambio debe ser aprobada por los niveles apropiados. La Organización evalúa que las solicitudes sean aprobadas por el personal que corresponde.
Mantiene un proceso de pruebas para los cambios	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Define un proceso Aceptación del Cambio, el cual establece que se debe planificar y establecer un entorno de pruebas. La Organización evalúa que se cuente con un proceso de pruebas para todos los cambios y que este proceso sea documentado.

Aprobación del cambio por parte del usuario solicitante	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Se define que se debe contar con un plan de pruebas el cual debe ser aprobado por las partes interesadas en el cambio. La Organización evalúa que el usuario solicitante del cambio realice la aprobación de las pruebas realizadas.
Registro de los cambios puestos en producción	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Se realiza una revisión post-implementación del cambio, una vez que este es pasado al ambiente de producción. La Organización evalúa que todo cambio en el ambiente de producción se encuentre documentado.

Valor agregado en su aplicación (35%)								
Criterios de Evaluación								
Mejora la administración de los activos	**7%**	No hace mención de la Gestión de los Activos.	Realiza una mención superficial de la administración de los activos.	Define la Gestión de los Activos sin entrar en detalles.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara y la gestión de los activos y da amplios detalles sobre su implementación.	4	Define con claridad el proceso de Gestión de los Activos por medio del proceso BAI 09, el cual establece un total de 5 actividades.
Administración del Riesgo en los diferentes procesos	**7%**	No se hace mención de la Gestión del Riesgo.	Realiza una mención superficial de la Gestión del Riesgo.	Define la Gestión del Riesgo sin entrar en detalle.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión del Riesgo y da amplios detalles sobre su implementación.	4	Establece un proceso para optimizar el Riesgo a nivel estratégico, además, define el proceso APO 12 el cual Gestiona los Riesgos desde el punto de vista de la Gestión de TI.

Gestiona la Madurez de los procesos	**7%**	No hace mención de la Gestión de la Madurez de los procesos.	Realiza una mención superficial de la Gestión de la Madurez de los procesos.	Define la Gestión de la Madurez de los procesos sin entrar en detalle.	Define la Gestión de la Madurez de los procesos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión de la Madurez de los procesos y da amplios detalles sobre su implementación.	0	No establece como alcanzar la madurez de los procesos a lo largo del ciclo de vida
Alineamiento de los procesos de TI con la estrategia organizacional	**7%**	No hace mención de como alinear los procesos de TI con la estrategia de la organización.	Realiza una mención superficial de cómo alinear los procesos de TI con la estrategia organizacional.	Define como alinear los procesos de TI con la estrategia organizacional sin entrar en detalle.	Define cómo alinear los procesos de TI con la estrategia organizacional y da algunos detalles sobre su implementación.	Define de forma clara de cómo alinear los procesos de TI con la estrategia organizacional y da amplios detalles sobre su implementación.	4	Establece que los procesos y la Gestión de TI deben ir alineada a los objetivos y estrategia de Marco de Gobierno Corporativo de la Organización.
Maximiza la calidad y eficiencia de los procesos de TI	**7%**	No hace mención de cómo maximizar la calidad y eficiencia de los procesos de TI.	Realiza una mención superficial de cómo maximizar la calidad y eficiencia de los procesos de TI.	Define cómo maximizar la calidad y eficiencia de los procesos de TI sin entrar en detalle.	Define cómo maximizar la calidad y eficiencia de los procesos de TI y da algunos detalles sobre su implementación.	Define de forma clara de cómo maximizar la calidad y eficiencia de los procesos de TI y da amplios detalles sobre implementación.	4	Establece que el Objetivo del Gobierno de TI es Crear Valor al usuario por medio de la entrega de procesos eficientes que cubren las necesidades de los mismos.

Fuente: Elaboración propia

8.9 Apéndice I: Rúbrica de Evaluación de ISO/IEC 20000

Tabla I.1. Rúbrica de Evaluación de ISO/IEC 20000

Rúbrica de evaluación de metodologías								
		Escala de Calificación					Puntos Asignados	Comentarios
		Malo	Deficiente	Regular	Bueno	Excelente		
Puntuación	100 %	0 Puntos	1 Punto	2 Puntos	3 Puntos	4 Puntos	62.5	
Información General (25%)								
Criterios de Evaluación								
Permite Certificación	**4%**	No permite certificación.	Certifica solo el conocimiento y no la práctica.	Posee solo un nivel de certificación, es decir, posee una sola certificación para toda la metodología.	Posee entre 2 y 3 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	Posee más de 4 niveles de certificación de acuerdo a la madurez de la empresa o experiencia laboral de la persona.	4	Se establecen 5 niveles de certificación. Fundamentos, dos niveles de Profesional y dos niveles de Expertos

Valor de capacitación para el personal	**3%**	Capacitar al persona tiene un valor superior a los 1300 dólares por persona, lo que se sale del presupuesto de la organización.	Capacitar al personal tiene un valor entre 976 y 1300 dólares por persona.	Capacitar al personal tiene un valor entre 651 y 975 dólares por persona.	Capacitar al personal tiene un valor entre 326 y 650 dólares por persona.	Capacitar al personal tiene un valor entre 0 y 325 dólares por persona.	2	El curso de capacitación tiene un valor de 800 dólares por persona
Tiempo de capacitación para el personal	**3%**	No es posible definir el tiempo exacto de la capacitación del personal.	Duración entre 20 y 24 horas de capacitación.	Duración entre 19 y 15 horas.	Duración entre 14 y 10 horas.	Duración menor a 10 horas de capacitación.	3	El curso de capacitación tiene una duración de 12 horas.
Cantidad de procesos definidos para la gestión de TI	**5%**	No define procesos relacionados con la Gestión de TI.	Define entre 1 a 10 procesos de la Gestión de TI.	Define entre 11 y 20 procesos de la Gestión de TI.	Define entre 21 y 30 procesos de la Gestión de TI.	Define entre 31 y 40 procesos de la Gestión de TI.	2	Define un total de 13 procesos para la Gestión de TI.

Descripción del proceso de Gestión del Cambio	**5%**	No se define el Proceso de Gestión del Cambio.	Realiza una mención superficial del proceso de Gestión del Cambio.	Define la Gestión del Cambio sin entrar en detalles.	Define la Gestión del Cambio y da algunos detalles sobre su implementación.	Se define de forma clara el proceso de Gestión del Cambio y se detalla ampliamente su implementación.	4	Define de forma detalla el proceso de Gestión del Cambio, por medio del soporte que obtiene del Marco de ITIL.
La metodología toma en cuenta los demás procesos que evalúa la organización	**5%**	No define los procesos que realiza la organización.	Define 1 de los 5 procesos que evalúa la organización.	Define 2 de los 5 procesos que evalúa la organización.	Define 3 de los 5 procesos que evalúa la organización.	Define 4 o 5 de los 5 procesos que evalúa la organización.	2	Describe solamente los procesos de Seguridad, Configuración y Gestión del Cambio, deja de lado los demás procesos que considera la Organización.

Criterios de Evaluación de Gestión del Cambio (40%)								
Criterios de Evaluación								
Registro de solicitudes de cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Establece que todo cambio se debe solicitar por medio de un RFC que realiza el usuario. La Organización revisa que toda solicitud de cambio sea documentada.

Aprobación de las solicitudes de Cambio	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Establece un comité de cambios para que realice la aprobación de los mismos. La Organización revisa que los cambios sean aprobados por el personal que corresponde.
Mantiene un proceso de pruebas para los cambios	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	4	Establece que se debe llevar a cabo donde un plan de pruebas, las cuales simulen el entorno de producción. La Organización evalúa que todo cambio pase por un proceso de pruebas para verificar su correcto funcionamiento.

Aprobación del cambio por parte del usuario solicitante	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	3	La autorización de las pruebas realizadas, las realiza el encargado del proceso de Gestión de Cambio. La Organización evalúa que las pruebas sean autorizadas y firmadas como efectivas, sin embargo, busca que esta acción sea realizada por el usuario solicitante del cambio
Registro de los cambios puestos en producción	**8%**	Lo establecido en la metodología se alinea en un 0% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 1% al 25% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 26 al 50% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 51% al 75% con las evaluaciones que realiza JM Auditores.	Lo establecido en la metodología se alinea en un 76% al 100% con las evaluaciones que realiza JM Auditores.	3	Define una revisión y documentación Post-Implementación de los cambios, una vez que el mismo ha sido puesto en el ambiente de producción. La Organización evalúa que todo cambio en el ambiente de producción es documentado.

Valor agregado en su aplicación (35%)								
Criterios de Evaluación								
Mejora la administración de los activos	**7%**	No hace mención de la Gestión de los Activos.	Realiza una mención superficial de la administración de los activos.	Define la Gestión de los Activos sin entrar en detalles.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara y la gestión de los activos y da amplios detalles sobre su implementación.	2	Se menciona la Gestión de Activos, dentro del proceso de Gestión de la Configuración, sin entrar en mayor detalle
Administración del Riesgo en los diferentes procesos	**7%**	No se hace mención de la Gestión del Riesgo.	Realiza una mención superficial de la Gestión del Riesgo.	Define la Gestión del Riesgo sin entrar en detalle.	Define la Gestión de Activos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión del Riesgo y da amplios detalles sobre su implementación.	2	Define el proceso de Seguridad, en el cual se menciona la gestión de riesgos sin entrar en mayor detalle en cómo realizar dicha gestión.
Gestiona la Madurez de los procesos	**7%**	No hace mención de la Gestión de la Madurez de los procesos.	Realiza una mención superficial de la Gestión de la Madurez de los procesos.	Define la Gestión de la Madurez de los procesos sin entrar en detalle.	Define la Gestión de la Madurez de los procesos y da algunos detalles sobre su implementación.	Define de forma clara la Gestión de la Madurez de los procesos y da amplios detalles sobre su implementación.	0	No establece como se debe alcanzar la madurez de los procesos que se brindan

Alineamiento de los procesos de TI con la estrategia organizacional	**7%**	No hace mención de como alinear los procesos de TI con la estrategia de la organización.	Realiza una mención superficial de cómo alinear los procesos de TI con la estrategia organizacional.	Define como alinear los procesos de TI con la estrategia organizacional sin entrar en detalle.	Define cómo alinear los procesos de TI con la estrategia organizacional y da algunos detalles sobre su implementación.	Define de forma clara de cómo alinear los procesos de TI con la estrategia organizacional y da amplios detalles sobre su implementación.	1	Establece que la Gestión de TI brindará procesos que mejoren y brinden beneficios a toda la Organización, sin embargo, no establece como estos procesos, procedimiento o políticas que se creen deben ir alineados a los objetivos y estrategia del negocio.
Maximiza la calidad y eficiencia de los procesos de TI	**7%**	No hace mención de cómo maximizar la calidad y eficiencia de los procesos de TI.	Realiza una mención superficial de cómo maximizar la calidad y eficiencia de los procesos de TI.	Define cómo maximizar la calidad y eficiencia de los procesos de TI sin entrar en detalle.	Define cómo maximizar la calidad y eficiencia de los procesos de TI y da algunos detalles sobre su implementación.	Define de forma clara de cómo maximizar la calidad y eficiencia de los procesos de TI y da amplios detalles sobre implementación.	0	No se establece como maximizar la calidad y eficacia de los procesos de TI, para llevar a cabo una mejor gestión de TI.

Fuente: Elaboración propia

8.10 Apéndice J: Minuta 1 – Presentación de los resultados de la Rúbrica a la Organización

Minuta 1 – Trabajo Final de Graduación

Presentación de los resultados de la rúbrica de evaluación de metodologías.

Fecha:	18/04/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Gerente Senior	Eric Mora

1. Objetivo

1.1 Presentar los resultados obtenido de la evaluación de metodologías por medio de la rúbrica creada para tal fin.

1.2 Discutir los resultados obtenidos.

1.3 Seleccionar la metodología para la definición de los controles de auditoría.

2. Temas tratados

2.1 El estudiante presentó los resultados obtenido de la rúbrica por medio de los números otorgados para cada metodología.

2.2 Seguidamente, se realizó la presentación de los resultados por medio de diagramas donde se presentaron las diferencias identificadas entre las metodologías y la norma estudiadas para tal fin.

2.3 El gerente consultó sobre los criterios utilizados para entender la modalidad de la evaluación.

2.4 El gerente brinda algunas observaciones sobre las calificaciones dadas, principalmente en la categoría relacionada con las operaciones de la empresa.

2.5 El estudiante explica cuál fue el procedimiento utilizado para brindar las calificaciones.

2.6 Finalmente el Gerente establece que el desarrollo del proyecto, se realice bajo la marco de COBIT 5, debido a que se apega más a las operaciones de la empresa, así como que las futuras evaluaciones se realizarán bajo esta metodología y que el personal actual de la organización será capacitado para el entendimiento, uso y aplicación de COBIT.

3. Compromisos asumidos

N/A

4. Próxima reunión

Jueves 27 de Abril en conjunto con el profesor Asesor

5. Firma de los presentes

8.11 Apéndice K: Minuta 2 – Clasificación de actividades de COBIT 5

Minuta 2 – Trabajo Final de Graduación

Clasificación de las actividades de COBIT 5

Fecha:	19/04/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Supervisora	Angélica Sánchez

1. Objetivo

1.1 Clasificar las actividades de COBIT 5, para luego determinar los controles de auditoría.

2. Temas tratados

2.1 Se presentó la lista de las actividades identificadas en COBIT 5 que se asocia a la Gestión del Cambio a la supervisora del área.

2.2 En forma conjunta, se fueron identificando las actividades que establecían la idea principal para identificarlas como actividades que permitirán definir el control de auditoría.

2.3 Una vez identificadas las actividades más potenciales, se analizaron de forma conjunta las actividades restantes para identificar si se relacionaban entre si y ser utilizada para establecer una prueba sustantiva o si establecía un control extra.

2.4 Con la ayuda de la experiencia de la supervisora, se lograba identificar cuales actividades.

2.5 A partir de la división que se iban realizando de las actividades, se iba realizando una tabla para establecer las actividades definidas para un control y las actividades para las pruebas sustantivas.

3. Compromisos asumidos

Estudiante:

3.1 Definir los controles de auditoría a partir de las actividades identificadas para este fin.

4. Próxima reunión

Por definir

5. Firmas de los presentes

8.12 Apéndice L: Respuesta a la encuesta de la Definición de Controles de Auditoría del equipo de trabajo

8.12.1 Encuesta #1

Definición de Controles para la Gestión del Cambio

Nombre: Angélica Sánchez González

Indicaciones

Lea cuidadosamente cada una de las tablas. La Tabla 1 define las actividades que establece COBIT 5 para la Gestión del Cambio y la Tabla 2 establece los controles relacionados con la actividad de COBIT 5.

Basado en la información de las tablas y de acuerdo a su experiencia responda las siguientes preguntas.

1. De la Tabla 1 y Tabla 2 indique cuales procesos se ajustan adecuadamente a la actividad que establece COBIT y las evaluaciones que se realizan en la firma. ¿Justifique su respuesta para aquello controles que no se ajustan?

N° de Control	Justificación
1	
2	
3	
4	El control definido se entiende más como una actividad.
5	
6	
7	Con el control definido no hay manera de comprobar (asegurar) la participación de las partes interesadas.
8	El control definido no cumple del todo la actividad requerida por COBIT 5.

N° de Control	Justificación
9	
10	
11	
12	
13	
14	
15	
16	

2. ¿De acuerdo a su experiencia cuales controles cambiaría, eliminaría o agregaría? Incluir los cambios y el porqué

1. Incluiría un control que permita evaluar los planes de mejora identificados en el proceso de Gestión de cambios.
2. Incluiría un control que permita evaluar la segregación de funciones de modo que se limiten los cambios en producción del personal de administración de combios.

3. ¿Cree que con las modificaciones realizadas, ya se puede determinar si una Organización realiza una adecuada Gestión de Cambios? Indicar el porqué.

Sí, considero que el alcance de los controles definidos permiten evaluar el proceso de combios de una Organización de forma completa, permitiéndole poder identificar aspectos de mejora que los apoye a las diferentes metodologías de cambios.

Tabla 1: Actividades de COBIT 5	
1	Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
2	Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.
3	Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
4	Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.
5	Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.
6	Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados.
7	Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
8	Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.
9	Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.
10	Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.
11	Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
12	Planificar y programar todos los cambios aprobados.
13	Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
14	Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.
15	Crear una base de datos de pruebas que sea representativa del entorno de producción.
16	Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.

Tabla 2: Controles de Auditoría basados en COBIT 5		Aplica?
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de cambios, con los respectivos lineamientos, pasos, restricciones.	✓
2	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio presentadas por los colaboradores, dicho análisis incluye evaluar el alcance e impacto en componentes de TI como en el personal de la empresa.	✓
3	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	✓
4	El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos.	X
5	Los desarrollos a la solución del cambio presentado, se realizan basado en un plan de calidad que toma en cuenta las expectativas de los interesados.	✓
6	Se realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo, se confirman los criterios de aceptación.	✓
7	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	X
8	Los accesos otorgados para el desarrollo de la solución son revocados al momento del cierre de la solicitud de cambio	X
9	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	✓
10	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	✓
11	Todas las solicitudes de cambios son aprobadas por los niveles correspondientes de aprobación.	✓
12	Las Solicitudes de Cambio aprobadas son planificadas y programadas	✓
13	La Organización cuenta con una procedimiento formal para declarar, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	✓
14	Se han establecido bitácoras de seguimiento de las solicitudes de cambios presentadas	✓
15	Las pruebas se realizan bajo un ambiente similar a las condiciones del ambiente de producción.	✓
16	Todo cambio de configuración a los sistemas o aplicativos es administrado y aprobado por la Gestión de Cambio.	✓

8.12.2 Encuesta #2

Definición de Controles para la Gestión del Cambio

Nombre: Esteban Carmona Loría

Indicaciones

Lea cuidadosamente cada una de las tablas. La Tabla 1 define las actividades que establece COBIT 5 para la Gestión del Cambio y la Tabla 2 establece los controles relacionados con la actividad de COBIT 5.

Basado en la información de las tablas y de acuerdo a su experiencia responda las siguientes preguntas.

1. De la Tabla 1 y Tabla 2 indique cuales procesos se ajustan adecuadamente a la actividad que establece COBIT y las evaluaciones que se realizan en la firma. ¿Justifique su respuesta para aquello controles que no se ajustan?

N° de Control	Justificación
1	
2	
3	
4	El tema es más revisar si TI evalua y dá seguimiento a las solicitudes del negocio. Porque ese control se cae con una explicación
5	Igual, me parece que el control debería ser algo más fácil de medir. Pedir evidencia puntual sobre eso.
6	
7	
8	No es solo importante si son revocados, sino también como se otorgan. Es más definir un procedimiento a los ambientes.

N° de Control	Justificación
9	
10	
11	No es tanto si se aprueban. Sino también si se tiene definido un procedimiento de revisión y aprobación.
12	
13	
14	Aquí es más sobre si se va documentando el avance del proyecto o cambio no solo la bitácora que eso es solo al final
15	
16	Y documentada

2. ¿De acuerdo a su experiencia cuales controles cambiaría, eliminaría o agregaría? Incluir los cambios y el porqué

Buscaría mejorar los controles 4, 5, 8, 11, 14 y 16 para que cubran del todo la actividad.

Los controles deberían ser más fáciles de medir y puntuales, que se pueda dar un criterio de si o no con facilidad. Y que indique la evidencia que se debe pedir.

3. ¿Cree que con las modificaciones realizadas, ya se puede determinar si una Organización realiza una adecuada Gestión de Cambios? Indicar el porqué.

Si porque se va de la mano con las actividades establecidas por COBIT5 y se definen controles para evaluar si estas actividades se están realizando

Tabla 1: Actividades de COBIT 5	
1	Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
2	Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.
3	Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
4	Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.
5	Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.
6	Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados.
7	Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
8	Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.
9	Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.
10	Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.
11	Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
12	Planificar y programar todos los cambios aprobados.
13	Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
14	Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.
15	Crear una base de datos de pruebas que sea representativa del entorno de producción.
16	Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.

Tabla 2: Controles de Auditoría basados en COBIT 5		Aplica?
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de cambios, con los respectivos lineamientos, pasos, restricciones.	✓
2	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio presentadas por los colaboradores, dicho análisis incluye evaluar el alcance e impacto en componentes de TI como en el personal de la empresa.	✓
3	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	✓
4	El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos.	X
5	Los desarrollos a la solución del cambio presentado, se realizan basado en un plan de calidad que toma en cuenta las expectativas de los interesados.	✓
6	Se realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo, se confirman los criterios de aceptación.	✓
7	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	✓
8	Los accesos otorgados para el desarrollo de la solución son revocados al momento del cierre de la solicitud de cambio	X
9	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	✓
10	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	✓
11	Todas las solicitudes de cambios son aprobadas por los niveles correspondientes de aprobación.	✓
12	Las Solicitudes de Cambio aprobadas son planificadas y programadas	✓
13	La Organización cuenta con una procedimiento formal para declarar, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	✓
14	Se han establecido bitácoras de seguimiento de las solicitudes de cambios presentadas	X
15	Las pruebas se realizan bajo un ambiente similar a las condiciones del ambiente de producción.	✓
16	Todo cambio de configuración a los sistemas o aplicativos es administrado y aprobado por la Gestión de Cambio.	✓

8.12.3 Encuesta #3

Definición de Controles para la Gestión del Cambio

Nombre: Josué Chaves

Indicaciones

Lea cuidadosamente cada una de las tablas. La Tabla 1 define las actividades que establece COBIT 5 para la Gestión del Cambio y la Tabla 2 establece los controles relacionados con la actividad de COBIT 5.

Basado en la información de las tablas y de acuerdo a su experiencia responda las siguientes preguntas.

1. De la Tabla 1 y Tabla 2 indique cuales procesos se ajustan adecuadamente a la actividad que establece COBIT y las evaluaciones que se realizan en la firma. ¿Justifique su respuesta para aquello controles que no se ajustan?

N° de Control	Justificación
1	
2	
3	
4	El control del objetivo A no define una actividad de revisión palpable. Debería ir enfocada en verificar la creación de propuestas de mejora.
5	
6	
7	
8	

N° de Control	Justificación
9	
10	
11	
12	
13	
14	
15	
16	

2. ¿De acuerdo a su experiencia cuales controles cambiaría, eliminaría o agregaría? Incluir los cambios y el porqué

En el control #8 de la matriz, añadiría un procedimiento que verifique la segregación de funciones del personal de TI en cuanto al desarrollo e implementación de los cambios en el ambiente productivo. Lo anterior dado que el personal de desarrollo no debería contar con acceso al entorno de producción.

3. ¿Cree que con las modificaciones realizadas, ya se puede determinar si una Organización realiza una adecuada Gestión de Cambios? Indicar el porqué.

Considero que con los controles propuestos, se revisa de manera consistente el proceso de cambios, ya que se han establecido controles desde el registro del caso, hasta la aprobación del pase a producción.

Asimismo, se han definido procedimientos para revisar las actividades post-implementación de cambios

Tabla 1: Actividades de COBIT 5	
1	Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
2	Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.
3	Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
4	Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.
5	Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.
6	Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados.
7	Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
8	Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.
9	Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.
10	Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.
11	Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
12	Planificar y programar todos los cambios aprobados.
13	Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
14	Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.
15	Crear una base de datos de pruebas que sea representativa del entorno de producción.
16	Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.

Tabla 2: Controles de Auditoría basados en COBIT 5		Aplica?
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de cambios, con los respectivos lineamientos, pasos, restricciones.	✓
2	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio presentadas por los colaboradores, dicho análisis incluye evaluar el alcance e impacto en componentes de TI como en el personal de la empresa.	✓
3	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	✓
4	El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos.	⚠
5	Los desarrollos a la solución del cambio presentado, se realizan basado en un plan de calidad que toma en cuenta las expectativas de los interesados.	✓
6	Se realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo, se confirman los criterios de aceptación.	✓
7	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	✓
8	Los accesos otorgados para el desarrollo de la solución son revocados al momento del cierre de la solicitud de cambio	✓
9	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	✓
10	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	✓
11	Todas las solicitudes de cambios son aprobadas por los niveles correspondientes de aprobación.	✓
12	Las Solicitudes de Cambio aprobadas son planificadas y programadas	✓
13	La Organización cuenta con una procedimiento formal para declarar, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	✓
14	Se han establecido bitácoras de seguimiento de las solicitudes de cambios presentadas	✓
15	Las pruebas se realizan bajo un ambiente similar a las condiciones del ambiente de producción.	✓
16	Todo cambio de configuración a los sistemas o aplicativos es administrado y aprobado por la Gestión de Cambio.	✓

8.12.4 Encuesta #4

Definición de Controles para la Gestión del Cambio

Nombre: Natalia Rodríguez.

Indicaciones

Lea cuidadosamente cada una de las tablas. La Tabla 1 define las actividades que establece COBIT 5 para la Gestión del Cambio y la Tabla 2 establece los controles relacionados con la actividad de COBIT 5.

Basado en la información de las tablas y de acuerdo a su experiencia responda las siguientes preguntas.

1. De la Tabla 1 y Tabla 2 indique cuales procesos se ajustan adecuadamente a la actividad que establece COBIT y las evaluaciones que se realizan en la firma. ¿Justifique su respuesta para aquello controles que no se ajustan?

N° de Control	Justificación
1	
2	El control no contiene la evaluación de un plan de continuidad.
3	
4	
5	
6	
7	
8	En el control es importante evaluar un registro o bitácora de la actividad de los Usuarios

N° de Control	Justificación
9	
10	
11	
12	
13	
14	Sería importante no delimitar el control a solamente bitácoras Sino cualquier mecanismo que me
15	permita consultar el estado del cambio. Le cambiaría la redacción al control.
16	Estás dejando por fuera el tema de que los cambios deben estar enlazados ~~es~~ con una solicitud de cambio.

2. ¿De acuerdo a su experiencia cuales controles cambiaría, eliminaría o agregaría? Incluir los cambios y el porqué

Control 2: La Organización ha establecido un Plan de Continuidad de Negocio además de un procedimiento para analizar las solicitudes de cambio presentadas...

Control 8: Yo agregaría "La Organización ha implementado algún mecanismo que permita monitorear continuamente la actividad de los usuarios."

Control 14: Se han establecido mecanismos (ej: bitácoras de seguimiento de las solicitudes) que permiten evaluar el estado del cambio.

Control 15: Las pruebas se realizan bajo un ambiente que representa => el ambiente de producción.

3. ¿Cree que con las modificaciones realizadas, ya se puede determinar si una Organización realiza una adecuada Gestión de Cambios? Indicar el porqué.

Pienso que si ya que se abarcan todos los aspectos que solicita Cobit 5.

Control 16: Yo agregaría el siguiente control "Todo cambio a la configuración del Sistema tiene su respectiva Solicitud de Cambio."

Tabla 1: Actividades de COBIT 5	
1	Crear un conjunto de políticas para conducir las expectativas de control de TI en temas clave relevantes, como calidad, seguridad, confidencialidad, controles internos, uso de activos de TI, ética y derechos de propiedad intelectual.
2	Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio (BCPs) y proveedores de servicios para asegurar que todos los componentes afectados han sido debidamente identificados.
3	Coordinar y comunicar cambios y actividades de transición tales como proyectos, planes de cambio, planificaciones, políticas de lanzamiento, errores conocidos y concienciación sobre formación.
4	Trabajar conjuntamente para identificar, comunicar e implementar iniciativas de mejora.
5	Integrar las prácticas de gestión de la calidad en los procesos y prácticas de desarrollo de soluciones.
6	Durante todo el proyecto, obtener, analizar y confirmar que los requerimientos de todas las partes interesadas, incluyendo los criterios de aceptación relevantes, son considerados.
7	Registrar las peticiones de cambio y revisar el diseño, rendimiento y calidad, asegurando una participación activa de las partes interesadas afectadas.
8	Asegurar que las responsabilidades por usar una alta seguridad o acceso restringido a los componentes de la infraestructura están claramente definidas y son comprendidas por todos aquellos que desarrollan e integran los componentes de la infraestructura. Su uso debería ser supervisado y evaluado.
9	Registrar los resultados de las pruebas y comunicar los resultados a las partes interesadas conforme al plan de pruebas.
10	Llevar a cabo una revisión post-implantación de acuerdo al proceso de gestión del cambio en la organización. Involucrar a los propietarios de procesos de negocio y a terceras partes, según sea apropiado.
11	Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio, partes interesadas de los departamentos de TI, según sea apropiado. Los cambios relativamente frecuentes con niveles de riesgo bajo deberían ser pre-aprobados como cambios estándar.
12	Planificar y programar todos los cambios aprobados.
13	Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.
14	Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la Dirección del detalle del estado de los cambios y del estado global (ej. análisis de antigüedad de las peticiones de cambio). Asegurar que los informes de estado sirven como pista de auditoría, de forma que pueda seguirse el historial de un cambio desde su concepción hasta su cierre.
15	Crear una base de datos de pruebas que sea representativa del entorno de producción.
16	Enlazar todos los cambios de configuración con las peticiones de cambio aprobadas para identificar cualquier cambio no autorizado. Informar de cambios no autorizados a la gestión de cambios.

Tabla 2: Controles de Auditoría basados en COBIT 5		Aplica?
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de cambios, con los respectivos lineamientos, pasos, restricciones.	✓
2	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio presentadas por los colaboradores, dicho análisis incluye evaluar el alcance e impacto en componentes de TI como en el personal de la empresa.	X
3	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	✓
4	El Departamento de TI trabaja de forma conjunta con las demás unidades de negocio de la empresa para determinar e identificar mejoras en los sistemas y aplicativos.	✓
5	Los desarrollos a la solución del cambio presentado, se realizan basado en un plan de calidad que toma en cuenta las expectativas de los interesados.	✓
6	Se realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo, se confirman los criterios de aceptación.	✓
7	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	✓
8	Los accesos otorgados para el desarrollo de la solución son revocados al momento del cierre de la solicitud de cambio	X
9	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	✓
10	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	✓
11	Todas las solicitudes de cambios son aprobadas por los niveles correspondientes de aprobación.	✓
12	Las Solicitudes de Cambio aprobadas son planificadas y programadas	✓
13	La Organización cuenta con una procedimiento formal para declarar, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	✓
14	Se han establecido bitácoras de seguimiento de las solicitudes de cambios presentadas	X
15	Las pruebas se realizan bajo un ambiente similar a las condiciones del ambiente de producción.	X
16	Todo cambio de configuración a los sistemas o aplicativos es administrado y aprobado por la Gestión de Cambio.	X

8.13 Apéndice M: Minuta 3 – Depuración de los Controles de Auditoría

Minuta 3 – Trabajo Final de Graduación

Depuración de los Controles de Auditoría

Fecha:	28/04/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Supervisora	Angélica Sánchez

1. Objetivo

1.1 Depurar los controles de auditoría a partir de los resultados y observaciones brindadas en la encuesta 1.

1.2 Mejorar la redacción de los controles para que estos sean entendibles para todo el equipo de trabajo.

2. Temas tratados

2.1 El estudiante muestra los controles establecidos luego de analizar las respuestas de las encuestas y de modificar los mismos a partir de las observaciones brindadas.

2.2 De forma conjunta, inician leyendo uno a uno los controles de auditoría para establecer y entender cada uno de ellos, de forma que permita establecer un mismo entendimiento por ambas partes.

2.3 La supervisora va indicando cambios a realizar en los diferentes controles, donde el estudiante de forma inmediata realiza los cambios.

2.4 En algunos controles ambos discuten sobre los diferentes puntos de vista, donde el fin único era llegar a un acuerdo donde ambos entendieran el mismo significado del control y lograr trasmitir el mismo entendimiento al resto del equipo de trabajo.

3. Compromisos asumidos

3.1. Estudiante:

3.1.1. Presentar los controles finales al Gerente para el visto bueno u observaciones del caso.

4. Próxima reunión

Por definir

5. Firmas de los presentes

8.14 Apéndice N: Minuta 4 – Aprobación de los Controles de Auditoría

Minuta 4 – Trabajo Final de Graduación

Aprobación de los controles de auditoría por parte de la Organización

Fecha:	28/04/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Gerente Senior	Eric Mora

1. Objetivo

1.1 Presentar los controles de auditoría definidos a partir de las actividades de COBIT 5 y de las observaciones obtenidas por medio de la encuesta 1.

1.2 Recibir la aprobación de los controles de auditoría por medio de la Organización.

2. Temas tratados

2.1 El estudiante le presenta los controles de auditoría que se han definido a partir de las actividades que define COBIT 5 en sus diferentes procesos, asimismo indica que los controles sufrieron modificaciones a partir de las observaciones brindadas por el equipo de trabajo.

2.2 El Gerente lee cada uno de los controles de auditoría donde va brindando observaciones para que se modifique la redacción para un mayor entendimiento.

2.3 Por medio de un análisis realizado por ambas partes se determina que el control que posee la siguiente descripción: “El Departamento de TI documenta formalmente las revisiones periódicas que realiza con el negocio a los sistemas para identificar oportunidades de mejoras sobre los mismos.” No es relevante para el tipo de evaluaciones que se realizan, debido a que se centran en la parte financiera y no como se gestiona TI.

2.4 El gerente estableció que es necesario tener controles sobre el ambiente de producción y de segregación de funciones, a partir de lo cual se establece un control extra, el cual se definió de la siguiente forma: “La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción”

2.5 Tras los cambios realizados, el gerente realiza la aprobación de los controles de auditoría para el proceso de gestión del cambio.

3. Compromisos asumidos

N/A

4. Próxima reunión

Por definir

5. Firmas de los presentes

8.15 Apéndice O: Respuesta a la encuesta de Pruebas Sustantivas por parte del equipo de trabajo

8.15.1 Encuesta #1

Definición de Pruebas Sustantivas

Nombre: Angelica Sanchez

Indicaciones

Lea cuidadosamente la Tabla 1, la cual muestra los controles de auditoría y las pruebas sustantivas definidas para cada uno de estos controles y responda las siguientes preguntas.

1. En la casilla "Aplica" de la Tabla 1 marque con "Check" (✓) si las pruebas sustantivas definidas son suficientes para probar el control de auditoría; en caso contrario marque con una "Equis" (X).
2. Para aquellos controles que fueron marcados con una "Equis" (X) indique las pruebas sustantivas que agregaría para cumplir en un 100% con el control de auditoría o que cambios le habría a las pruebas ya definidas.

No. Control	Prueba Sustantiva
1	Determinar si la política y/o procedimiento de la Gestión es revisado.
1	El proceso de validar si se encuentra funcionando de acuerdo a la política no se revisa en este control.
2	No es una prueba sustantiva, debido a que el cambio o un cambio en el procedimiento requiere pasar por el proceso de Gestión del cambio.
3	La resistencia al cambio se da hasta que el cambio haya sido puesto en producción, no es parte del análisis inicial.
7	Los cambios aprobados son comunicados a todo el personal relacionado con el cambio.
7	Con el control anterior se valida que todo el personal involucrado en el cambio conozca del mismo
10	Determinar que las pruebas se realizan en un ambiente que simule el ambiente de producción
10	Las pruebas sustantivas 2 y 3 del control 10 no son pruebas sustantivas del control definido.
11	Con el fin de validar que se cumpla lo solicitado por el usuario ajustar el control de manera que se revisen los criterios de aceptación antes de ser puestos en producción.

12. Se mantiene un registro con el resultado de las pruebas y posibles excepciones.
   - Las pruebas de aceptación son realizadas por el usuario solicitante
   - Determinar si la documentación de las pruebas fallidas es documentada.

6. ~~Identi~~ Determinar si la Organización ha establecido un proceso para la programación / priorización de las solicitudes de cambio.

13. Misma prueba sustantiva del control 6.

14. No es necesario que se acuerden accesos para solicitudes de emergencia, siempre y cuando el acceso al ambiente de producción este bien segregado y controlado.

Tabla 1: Definición de pruebas sustantivas			
Controles de Auditoría a partir de la encuesta		**Actividades para las pruebas sustantivas**	**¿Aplica?**
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la gestión del cambio es revisado y si es necesario actualizado al menos una vez al año.	X
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.	✓
		Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.	X
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.	✓
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.	✓
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.	✓
		Las solicitudes de cambio sobre la documentación oficial de la gestión de TI se encuentran formalmente documentados y almacenados en un repositorio.	X
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.	✓
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del cambio y ~~su habilidad para adoptar el mismo.~~	✓
		Para cada una de las solicitudes de cambio, se identifican los colaboradores que se resisten al cambio.	X
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.	✓
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.	✓
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.	✓
		Los cambios más considerables son aprobados por un comité de cambio o por la gerencia de TI.	✓
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.	✓

5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.	✓
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado se realiza en conjunto con los interesados del cambio.	✓
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.	✓
6	Las Solicitudes de Cambio aprobadas son planificados y programados	Determinar la creación de un cronograma o programación de los cambios aprobados.	✓
		Determinar si los cambios son realizados en el tiempo planificado.	✓
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	Los cambios aprobados son comunicados al personal interesado y al personal afectado por este.	✓
		La documentación sobre el cambio se encuentra en un sitio accesible para el personal involucrado.	✓
		Determinar que se comunican los beneficios y afectaciones del cambio al personal involucrado.	✓
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.	✓
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.	✓
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.	✓
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.	✓
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.	✓
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción), donde se involucran los roles, procedimiento y carga de datos de acuerdo a lo esperado.	✓
		Determinar que las pruebas y los resultados preliminares se ajustan a los criterios de éxito establecidos para el cambio.	✓
		Indagar sobre el establecimiento de un plan de pruebas, que permita realizar operaciones de acuerdo a las operaciones y condiciones reales.	✓

11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.	Los criterios de calidad son documentados para su revisión durante la etapa de desarrollo de la solución.	X
		Se documentan las revisiones a los criterios de calidad durante el desarrollo de la solución donde los usuarios solicitantes participan de la revisión.	X
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con todas las revisiones, resultados, excepciones y correcciones.	X
		Determinar si las pruebas se llevan a cabo en conjunto con los interesados del cambio en busca de su aprobación.	X
		Se registran y clasifican los errores presentados durante las pruebas.	X
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Indagar si los cambios planificados son cerrados en el tiempo establecido.	X
		Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.	✓
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente ~~de la solución~~ nuevo que está siendo transferido al entorno de producción.	✓
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.	✓
14	La Organización cuenta con una procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se haya aplicado el cambio.	X
		Se ha definido qué es un cambio de emergencia para la organización.	✓
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.	✓
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.	✓
		Se ha establecido los niveles de aprobación de los cambios de emergencia.	✓
		Se realizan pruebas sobre el cambio antes de ~~ponerlo en funcionamiento~~ ser puesto en el ambiente de producción.	✓
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.	✓
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.	✓

16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ~~ese~~ cambios desde el aplicativo que afectan directamente en el ambiente de producción.	✓
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos	✓
		Los cambios realizados en los parámetros ~~de los aplicativos~~ quedan registrados en un bitácora de monitoreo.	✓
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.	✓

8.15.2 Encuesta #2

Definición de Pruebas Sustantivas

Nombre: Esteban Carmona Loría

Indicaciones

Lea cuidadosamente la Tabla 1, la cual muestra los controles de auditoría y las pruebas sustantivas definidas para cada uno de estos controles y responda las siguientes preguntas.

1. En la casilla "Aplica" de la Tabla 1 marque con "Check" (✓) si las pruebas sustantivas definidas son suficientes para probar el control de auditoría; en caso contrario marque con una "Equis" (X).
2. Para aquellos controles que fueron marcados con una "Equis" (X) indique las pruebas sustantivas que agregaría para cumplir en un 100% con el control de auditoría o que cambios le habría a las pruebas ya definidas.

No. Control	Prueba Sustantiva
10	Determinar que los cambios pasados a producción cumplieron los criterios de aceptación establecidos
8	Determinar que los usuarios de TI tiene acceso a las áreas de producción son los indicados

Tabla 1. Definición de pruebas sustantivas

	Controles de Auditoría a partir de la encuesta	Actividades para las pruebas sustantivas	¿Aplica?
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la gestión del cambio es revisado y si es necesario actualizado al menos una vez al año.	✓
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.	✓
		Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.	✓
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.	✓
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.	✓
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.	✓
		Las solicitudes de cambio sobre la documentación oficial de la gestión de TI se encuentran formalmente documentados y almacenados en un repositorio.	✓
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.	✓
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del cambio y su habilidad para adoptar el mismo.	✓
		Para cada una de las solicitudes de cambio, se identifican los colaboradores que se resisten al cambio.	✓
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.	✓
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.	✓
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.	✓
		Los cambios más considerables son aprobados por un comité de cambio o por la gerencia de TI.	✓
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.	✓

5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.	✓
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado se realiza en conjunto con los interesados del cambio.	✓
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.	✓
6	Las Solicitudes de Cambio aprobadas son planificados y programados	Determinar la creación de un cronograma o programación de los cambios aprobados.	✓
		Determinar si los cambios son realizados en el tiempo planificado.	
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	Los cambios aprobados son comunicados al personal interesado y al personal afectado por este.	
		La documentación sobre el cambio se encuentra en un sitio accesible para el personal involucrado.	
		Determinar que se comunican los beneficios y afectaciones del cambio al personal involucrado.	
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.	✗
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado. (4)?	✗
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.	✓
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.	✓
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.	
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción), donde se involucran los roles, procedimiento y carga de datos de acuerdo a lo esperado.	✓
		Determinar que las pruebas y los resultados preliminares se ajustan a los criterios de éxito establecidos para el cambio.	✗
		Indagar sobre el establecimiento de un plan de pruebas, que permita realizar operaciones de acuerdo a las operaciones y condiciones reales.	✗

11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.	Los criterios de calidad son documentados para su revisión durante la etapa de desarrollo de la solución.	✓
		Se documentan las revisiones a los criterios de calidad durante el desarrollo de la solución donde los usuarios solicitantes participan de la revisión.	✓
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con todas las revisiones, resultados, excepciones y correcciones.	✓
		Determinar si las pruebas se llevan a cabo en conjunto con los interesados del cambio en busca de su aprobación.	✓
		Se registran y clasifican los errores presentados durante las pruebas.	✓
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Indagar si los cambios planificados son cerrados en el tiempo establecido.	✓
		Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.	✓
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.	✓
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.	✓
14	La Organización cuenta con una procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se haya aplicado el cambio.	✓
		Se ha definido qué es un cambio de emergencia para la organización.	✓
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.	✓
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.	✓
		Se ha establecido los niveles de aprobación de los cambios de emergencia.	✓
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.	✓
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.	✓
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.	✓

16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Se tiene identificados Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción. ??	X
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos	✓
		Los cambios realizados en los parámetros de los aplicativos quedan registrados en un bitácora de monitoreo.	✓
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.	✓

8.15.3 Encuesta #3

Definición de Pruebas Sustantivas

Nombre: Josué Chaves V.

Indicaciones

Lea cuidadosamente la Tabla 1, la cual muestra los controles de auditoría y las pruebas sustantivas definidas para cada uno de estos controles y responda las siguientes preguntas.

1. En la casilla "Aplica" de la Tabla 1 marque con "Check" (✓) si las pruebas sustantivas definidas son suficientes para probar el control de auditoría; en caso contrario marque con una "Equis" (X).
2. Para aquellos controles que fueron marcados con una "Equis" (X) indique las pruebas sustantivas que agregaría para cumplir en un 100% con el control de auditoría o que cambios le habría a las pruebas ya definidas.

No. Control	Prueba Sustantiva
3,4,5	Los controles 3,4 y 5 tienen criterios de evaluación muy similares. Se podrían consolidar en un sólo control, y así poder evaluar los requerimientos, alcance y aprobación de las solicitudes de cambio.
8	Con determinar el personal que desarrolló el cambio y quién tiene acceso al ambiente de pruebas, no se está evaluando un criterio concreto. Sería mejor definir en la prosa, verificar que el personal con acceso a producción, no tiene acceso en el ambiente de desarrollo ó vice versa.
16	El objetivo 16, está muy relacionado al numero 15. Propondría unificar pruebas y consolidar en único control.

Tabla 1: Definición de pruebas sustantivas			
Controles de Auditoría a partir de la encuesta		**Actividades para las pruebas sustantivas**	**¿Aplica?**
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la gestión del cambio es revisado y si es necesario actualizado al menos una vez al año.	✓
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.	✓
		Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.	✓
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.	✓
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.	✓
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.	✓
		Las solicitudes de cambio sobre la documentación oficial de la gestión de TI se encuentran formalmente documentados y almacenados en un repositorio.	✓
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.	✓
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del cambio y su habilidad para adoptar el mismo.	✓
		Para cada una de las solicitudes de cambio, se identifican los colaboradores que se resisten al cambio.	✓
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.	✓
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.	
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.	
		Los cambios más considerables son aprobados por un comité de cambio o por la gerencia de TI.	
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.	

5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.	
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado se realiza en conjunto con los interesados del cambio.	
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.	
6	Las Solicitudes de Cambio aprobadas son planificados y programados	Determinar la creación de un cronograma o programación de los cambios aprobados.	✓
		Determinar si los cambios son realizados en el tiempo planificado.	✓
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	Los cambios aprobados son comunicados al personal interesado y al personal afectado por este.	✓
		La documentación sobre el cambio se encuentra en un sitio accesible para el personal involucrado.	✓
		Determinar que se comunican los beneficios y afectaciones del cambio al personal involucrado.	✓
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.	
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.	
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.	✓
		Los accesos al ambiente de producción son registrados por medio de una bitácora de monitoreo.	✓
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.	✓
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción), donde se involucran los roles, procedimiento y carga de datos de acuerdo a lo esperado.	✓
		Determinar que las pruebas y los resultados preliminares se ajustan a los criterios de éxito establecidos para el cambio.	✓
		Indagar sobre el establecimiento de un plan de pruebas, que permita realizar operaciones de acuerdo a las operaciones y condiciones reales.	✓

11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.	Los criterios de calidad son documentados para su revisión durante la etapa de desarrollo de la solución.	✓
		Se documentan las revisiones a los criterios de calidad durante el desarrollo de la solución donde los usuarios solicitantes participan de la revisión.	✓
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con todas las revisiones, resultados, excepciones y correcciones.	✓
		Determinar si las pruebas se llevan a cabo en conjunto con los interesados del cambio en busca de su aprobación.	✓
		Se registran y clasifican los errores presentados durante las pruebas.	✓
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Indagar si los cambios planificados son cerrados en el tiempo establecido.	✓
		Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.	✓
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.	✓
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.	✓
14	La Organización cuenta con una procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se haya aplicado el cambio.	✓
		Se ha definido qué es un cambio de emergencia para la organización.	✓
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.	✓
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.	✓
		Se ha establecido los niveles de aprobación de los cambios de emergencia.	✓
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.	✓
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.	✓
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos.	✓

16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción.	
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos	
		Los cambios realizados en los parámetros de los aplicativos quedan registrados en un bitácora de monitoreo.	
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.	

8.15.4 Encuesta #4

Definición de Pruebas Sustantivas

Nombre: Natalia Rodriguez

Indicaciones

Lea cuidadosamente la Tabla 1, la cual muestra los controles de auditoría y las pruebas sustantivas definidas para cada uno de estos controles y responda las siguientes preguntas.

1. En la casilla "Aplica" de la Tabla 1 marque con "Check" (✓) si las pruebas sustantivas definidas son suficientes para probar el control de auditoría; en caso contrario marque con una "Equis" (X).
2. Para aquellos controles que fueron marcados con una "Equis" (X) indique las pruebas sustantivas que agregaría para cumplir en un 100% con el control de auditoría o que cambios le habría a las pruebas ya definidas.

No. Control	Prueba Sustantiva
1	La forma de validar que el proceso de Gestión del Cambio está funcionando es por medio de la revisión de [illegible] por lo que el control está orientado a efectuar si se encuentra ocurre se ejecuta
2	Cambios de la Gestión de TI no intervienen para el control descrito.
3	Modificar redacción (2). La manera de identificar antes se resisten es posteriores de llevar a cabo el cambio (3).
4	Con las pruebas anteriores ya se van identificando antes con rechazadas
5	Indicar que el listado de requerimientos los realiza personal de TI. (2) Indicar que corresponde a las solicitudes de cambio (3)
6	Modificar redacción
7	Con la prueba sustantiva 3 se realiza la 1. La prueba 2 no está relacionada a este control.
8	Con los pasos (y 2 se realiza [illegible] la prueba
9	Incluir el personal encargado de revisar dichas bitácoras.
10	No son pruebas sustantivas para el control definido.
11	Prueba 2 es igual a la 1
13	Prueba 2 se encuentra relacionada.

Tabla 1: Definición de pruebas sustantivas			
Controles de Auditoría a partir de la encuesta		**Actividades para las pruebas sustantivas**	**¿Aplica?**
1	La Organización cuenta con una política y/o procedimiento que establezca el proceso de Gestión de Cambios, con los respectivos lineamientos, pasos y restricciones.	Determinar si la política y/o procedimiento de la gestión del cambio es revisado y si es necesario actualizado al menos una vez al año.	✓
		La política y/o procedimiento de Gestión del Cambio se encuentra comunicada al personal de la Organización.	✓
		Determinar que el proceso de Gestión del Cambio se encuentra funcionando de acuerdo a lo establecido en la política y/o procedimiento.	✗
		Se tienen definidos los roles, responsabilidades del personal de Gestión del Cambio.	✓
		La política y/o procedimiento se encuentra aprobada por las autoridades correspondientes.	✓
2	Todas las solicitudes de cambios, tanto en los sistemas y aplicativos de la empresa como en la documentación oficial que regula la gestión de TI, se encuentran formalmente documentados.	Las solicitudes de cambio sobre los aplicativos o sistemas se encuentran formalmente documentados y almacenados en un repositorio.	✓
		Las solicitudes de cambio sobre la documentación oficial de la gestión de TI se encuentran formalmente documentados y almacenados en un repositorio.	✗
3	La Organización ha establecido un procedimiento para analizar las solicitudes de cambio, el cual incluye evaluar el alcance e impacto tanto en componentes de TI como en el personal de la empresa, asimismo la afectación en la continuidad del negocio.	Indagar e inspeccionar si se realiza un análisis del impacto del cambio para todas las solicitudes de cambio presentadas.	✓
		Determinar si se lleva a cabo una evaluación del alcance del cambio que permita identificar los principales afectados del cambio y su habilidad para adoptar el mismo.	✗
		Para cada una de las solicitudes de cambio, se identifican los colaboradores que se resisten al cambio.	✗
		Las solicitudes cambio son priorizadas y categorizadas de acuerdo al análisis del alcance e impacto.	✓
4	Todas las solicitudes de cambios son evaluadas, revisadas y aprobadas por los niveles correspondientes de aprobación, de acuerdo a la política y/o procedimiento de Gestión del Cambio establecido por la Organización.	Las solicitudes de cambio son aprobadas por los niveles correspondientes.	✓
		Se realiza una revisión de la solicitud de cambio para determinar que cuenta con los requerimientos mínimos solicitados.	✓
		Los cambios más considerables son aprobados por un comité de cambio o por la gerencia de TI.	✓
		Las solicitudes de cambios rechazadas son justificadas ante el solicitante y personal interesado.	✗

5	El Gestor del cambio realiza una confirmación con las partes interesadas de los requerimientos presentados en la Solicitud de Cambio; asimismo se confirman los criterios de aceptación.	Determinar si se lleva a cabo un proceso de validación de los requerimientos con el usuario solicitante y parte interesadas.	✓
		Se establece un listado o documentación de los requerimientos técnicos, funcionales, además de los riesgos asociados con el cambio. Dicho listado se realiza en conjunto con los interesados del cambio.	✓
		Los criterios de aceptación para el cambio son documentados y confirmados por parte de los interesados del cambio.	✓
6	Las Solicitudes de Cambio aprobadas son planificados y programados	Determinar la creación de un cronograma o programación de los cambios aprobados.	X
		Determinar si los cambios son realizados en el tiempo planificado.	✓
7	Se tiene establecido un proceso para comunicar los cambios a realizar en sistemas o aplicaciones de la organización, de forma que el personal conozca de las afectaciones y mejoras relacionadas con el cambio	Los cambios aprobados son comunicados al personal interesado y al personal afectado por este.	X
		La documentación sobre el cambio se encuentra almacenada en un sitio accesible para el personal involucrado.	X
		Determinar que se comunican los beneficios y afectaciones del cambio al personal involucrado.	✓
8	Los accesos a los componentes de TI son otorgados de forma que limita los cambios en el ambiente de producción del personal de Gestión de Cambios.	Determinar el personal de TI que tiene acceso a realizar cambios en el ambiente de producción.	✓
		Determinar el personal de TI encargado de realizar el desarrollo a la solución del cambio presentado.	✓
		Indagar e inspeccionar como se otorgan los permisos al personal de gestión del cambio.	X
		Los accesos al ambiente de producción son registrados ~~por medio de una~~ en bitácora de monitoreo.	✓
9	El Departamento de TI cuenta con una bitácora de seguimiento de solicitudes de cambios, la cual muestra el seguimiento (Cambio de Estado) que ha tenido la misma durante todo el ciclo del cambio.	Determinar si se cuenta con una bitácora o mecanismo que permita monitorear los cambios de estado de las solicitudes de cambio.	✓
10	Las pruebas se realizan en un ambiente de desarrollo que simula las mismas condiciones de un ambiente real (producción).	Determinar que las pruebas se realizan en un ambiente que simula el ambiente real (producción), donde se involucran los roles, procedimiento y carga de datos de acuerdo a lo esperado. modificar eliminar	✓
		Determinar que las pruebas y los resultados preliminares se ajustan a los criterios de éxito establecidos para el cambio.	X
		Indagar sobre el establecimiento de un plan de pruebas, que permita realizar operaciones de acuerdo a las operaciones y condiciones reales.	X

11	El Departamento de TI realiza revisiones a los criterios de calidad establecidos para el cambio durante el desarrollo de la solución.	Los criterios de calidad son documentados para su revisión durante la etapa de desarrollo de la solución.	✓
		Se documentan las revisiones a los criterios de calidad durante el desarrollo de la solución donde los usuarios solicitantes participan de la revisión.	✗
12	Los resultados de las pruebas realizadas a la solución del cambio, se encuentran formalmente documentados y comunicados a los interesados.	Se mantiene un registro con todas las revisiones, resultados, excepciones y correcciones.	✓
		Determinar si las pruebas se llevan a cabo en conjunto con los interesados del cambio en busca de su aprobación. * matriz rol. para q?!	✓
		Se registran y clasifican los errores presentados durante las pruebas.	✓
13	Se lleva a cabo una validación post implementación, que involucra la evaluación del mismo, adaptación del personal y actualización de documentos relacionados con el cambio.	Indagar si los cambios planificados son cerrados en el tiempo establecido.	✗
		Determinar que se actualiza la documentación sobre sistemas y procesos de negocio relevantes, información de configuración y documentación del plan de contingencia, según sea apropiado.	✓
		Determinar que todas las bibliotecas de medios son actualizadas con la versión del componente de la solución que está siendo transferido al entorno de producción.	✗
		Se ha establecido un plan de capacitación del personal a partir del cambio realizado.	✓
14	La Organización cuenta con una procedimiento formal para definir, evaluar, aprobar de forma preliminar, así como para autorizar y registrar los cambios de emergencia	Verificar que los accesos de emergencia acordados para realizar los cambios están debidamente autorizados y documentos y son revocados una vez se haya aplicado el cambio.	✓
		Se ha definido qué es un cambio de emergencia para la organización.	✗
		El procedimiento se encuentra actualizado y aprobado por los altos mandos de la organización.	✓
		Todo cambio de emergencia solicitado se encuentra formalmente documentado.	✓
		Se ha establecido los niveles de aprobación de los cambios de emergencia. para q? para	✓
		Se realizan pruebas sobre el cambio antes de ponerlo en funcionamiento en el ambiente de producción.	✗
15	Todo cambio de configuración a los sistemas o aplicativos son gestionados, aprobados y monitoreados por medio de la Gestión de Cambio.	Determinar que los cambios en la configuración de los aplicativos posee una solicitud de cambio.	✓
		Se ha implementado una bitácora de monitoreo donde se registran todos los cambios en la configuración de los aplicativos. quien la revisa?	✓

16	La Organización ha establecido una política y/o procedimiento para establecer los cambios en parámetros de los sistemas o aplicativos en el ambiente de producción.	Indagar sobre los parámetros que permiten ser cambios desde el aplicativo que afectan directamente en el ambiente de producción.	✓
		Determinar el personal que tiene acceso a realizar cambios en los parámetros de los aplicativos	✓
		Los cambios realizados en los parámetros de los aplicativos quedan registrados en un bitácora de monitoreo.	✓
		La política y/o procedimiento se encuentran actualizados y aprobados por altos mandos en la organización.	✓

8.16 Apéndice P: Minuta 5 – Aprobación de las pruebas sustantivas por parte de la Organización

Minuta 5 – Trabajo Final de Graduación

Aprobación de las pruebas sustantivas por parte de la Organización

Fecha:	08/05/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Gerente Senior	Eric Mora

1. Objetivo

1.1 Presentar las pruebas sustantivas definidas para cada uno de los controles de auditoría.

1.2 Recibir retroalimentación sobre el establecimiento de las pruebas sustantiva.

1.3 Recibir la aprobación por parte de la organización.

2. Temas tratados

2.1 El estudiante presenta las pruebas sustantivas definidas para cada uno de los controles de auditoría que se establecieron anteriormente.

2.2 El Gerente procedió a realizar la lectura de cada una de las pruebas, para lo cual iba brindando observaciones que fueron corregidas en el momento por el estudiante.

2.3 Se establecieron que algunas de las pruebas establecidas ya eran tomadas en cuenta por otras por lo que había una redundancia, para lo cual se determinó eliminar dichas pruebas.

2.4 Tras los cambios realizados, el gerente realiza la aprobación de los controles de auditoría para el proceso de gestión del cambio.

3. Compromisos asumidos

N/A

4. Próxima reunión

Por definir

5. Firmas de los presentes

8.17 Apéndice Q: Minuta 6 – Presentación de la MCGTI automátizada a la Organización

Minuta 6 – Trabajo Final de Graduación

Presentación de la MCGTI final ante la Organización

Fecha:	16/05/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Gerente Senior	Eric Mora

1. Objetivo

1.1 Presentación de la Matriz de Controles Generales de TI automática ante la Organización.

2. Temas tratados

2.1 El estudiante inicia explicando la definición de los tres indicadores utilizados y configurados en la Matriz.

2.2 Seguidamente, el estudiante indica las columnas que fueron ingresadas, que no se encontraban en la Matriz original.

2.3 Luego inició dando un ejemplo y como dependiendo del resultado y de las opciones que se establecieron la Matriz de forma automática va brindando los indicadores y estableciendo si la prueba es efectiva, inefectiva o mantiene una oportunidad de mejora que debe ser reportada.

2.4 También se presentó el cuadro resumen desarrollado para establecer la cantidad de controles que han sido efectivos, inefectivos y los que cuentan con oportunidades de mejora.

2.5 El gerente establece que le parece bien lo desarrollado y brinda el visto bueno de la MCGTI.

3. Compromisos asumidos

N/A

4. Próxima reunión

Por definir

5. Firmas de los presentes

8.19 Apéndice R: Minuta 7 - Presentación de la MCGTI final y entrega de los documentos finales a la Organización.

Minuta 7 – Trabajo Final de Graduación

Presentación de la MCGTI final y entrega de los documentos finales a la Organización.

Fecha:	25/05/2017
Lugar:	Oficinas Centrales de JM Auditores

Presentes

Estudiante practicante	Josué Masís
Gerente Senior	Eric Mora

1. Objetivo

1.1 Presentación y entrega de la Matriz de Controles Generales de TI automática ante la Organización.

1.2 Entrega del informe sobre la asociación de los procesos de la MCGTI con lo establecido por COBIT 5.

2. Temas tratados

2.1 El estudiante expone los cambios en estructura que se realizó a la Matriz de Controles Generales.

2.2 Seguidamente, el estudiante presenta como es el funcionamiento de los indicadores de color que se implementaron en la nueva Matriz, asimismo se muestran como por medio de la programación la matriz indica el resultado de la prueba a partir de lo indicado por el auditor.

2.3 Asimismo, el estudiante expone que la Matriz cuenta ya con los nuevos controles de evaluación para el proceso de Gestión del Cambio y las pruebas sustantivas de cada uno.

2.4 El Gerente aprueba los cambios realizados a la Matriz de Controles Generales de TI, e indica que los cambios realizados fueron apropiados para iniciar un proceso de mejora a nivel del área.

2.5 Por otro lado el estudiante entrega y explica el informe sobre como los demás procesos de MCGTI se asocian a los procesos de COBIT 5.

2.6 El gerente recibe el documento para su revisión y aprobación posterior.

3. Compromisos asumidos

N/A

4. Próxima reunión

Por definir

5. Firmas de los presentes

9. Glosario

En esta sección se muestra un conjunto de definiciones y conceptos utilizados durante el presente trabajo.

Término	Definición
Auditado	Empresa que recibe una auditoría por parte de una firma auditora.
CAB	Comité encargado de aprobación de los cambios, el término CAB procede por sus siglas en inglés.
COBIT 5	Última versión del marco de trabajo aprobado por la industria a nivel internacional, basado en definición de controles sobre la gestión de la tecnología.
Diagrama del Rio	Diagrama que permite la comparación de rúbricas, a partir de puntos máximos y mínimos.
Empresa Cliente	Empresa que está siendo evaluada por el equipo de auditoría de la firma.
Especialista de TI	Auditor encargado de realizar el apoyo a la auditoría financiera para la evaluación de los componentes tecnológicos.
Firma	Organización donde se llevará a cabo el trabajo final de graduación, se define como firma, al tratarse de una organización auditora.
IRM	*Information Risk Management,* nombre del área de negocio donde se llevará a cabo el trabajo final de graduación.
ITIL v2011	Última versión del marco de referencia sobre la Gestión de los Servicios de TI.
ISO/IEC 20000	Estándar que normaliza un marco de referencia para la gestión de TI.
JM Auditores	Nombre con utilizado para hacer referencia a la organización donde se llevará a cabo el trabajo final de graduación.
MCGTI	Matriz de Controles Generales de Tecnología de Información.
Metodología Propia	Metodología establecida por la organización que dicta la forma y las reglas para llevar a cabo las auditorías.
Pruebas de eficacia operativa	Pruebas que establece la organización para obtener evidencia sobre el control de auditoría que se está evaluando, en COBIT 5, es conocido como pruebas sustantivas.
TI: Tecnología de Información	Utilización de componentes tecnológicos para el procesamiento de información.
TFG	Trabajo Final de Graduación

10. Bibliografía

IT Governance Ltd. (2017). *IT Governance*. Obtenido de IT Governance: https://www.itgovernance.co.uk/itil

Basu, S. K. (2009). *Fundamentals of Auditing.* India: Dorling Kindersley.

Better Evaluation. (s.f). *The River Chart*. Obtenido de Better Evaluation: http://www.betterevaluation.org/resources/tools/rubrics/river_chart

Bon, J. V. (2011). *ITIL 2011 Edition - A Pocket Guide.* U.K: Van Haren Publishing.

Brookhart, S. (2013). *How to Create and Use Rubrics for Formative Assessment and Grading.*

Cabinet Office. (2011). *ITIL Service Strategy.* Gran Bretaña: The Stationery Office.

Cabinet Office. (2011). *ITIL Service Transition .* Gran Bretaña: The Stationery Office.

Certificación PM. (2017). *Certificación PM*. Obtenido de Certificación PM: http://pmbok.certificacionpm.com/proceso/47/realizar-el-control-integrado-de-cambios

CEVALLOS, M. A. (2015). *PLAN DE CONTINUIDAD DE LOS SERVICIOS CRÍTICOS DE RED.* PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR, Quito.

Costa, M., & Valley, I. (2014). *Choosing the Right Assessment Method.* Obtenido de http://www.lbcc.edu: http://www.lbcc.edu/outcomesassessment/documents/coursemethods/Rubric-Information.pdf

De Haes, S., & Van Grembergen, W. (2015). *Enterprose Governance of Information Technology.* Switzerland: Springer International Publishing.

Echenique, J. A. (s.f). *Auditoría en Informática.* México: McGraw-Hill.

Eyssautier de la Mora, M. (2006). *Metodología de la Investigación Desarrollo de la Inteligencia.* Thomson.

Gantz, S. (2014). *The Basics of IT Audit.* USA: Elsevier.

Garraza, T. R. (2017). *PDCA.* Instituto Navarro de Administración Pública.

ISACA. (2012). *COBIT 5 Enabling Processes.* USA: ISACA.

ISACA. (2014). *IS Audit and Assurance Standard.* Obtenido de ISACA: https://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2205-Evidence_gui_Eng_0614.pdf

ISACA. (2015). *ISACA.* Obtenido de ISACA: https://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

ISO. (2011). *ISO 19011.* Obtenido de ISO: http://www.umc.edu.ve/pdf/calidad/normasISO/Norma_ISO_19011-2011_Espanol.pdf

ISO/IEC. (2007). *ISO 20000.* España: AENOR.

IT Governance Institute. (2008). *ISACA.* Obtenido de ISCA: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-COBIT-4-1-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa_res_Spa_0108.pdf

JM Auditores. (2014). *Metodología propia.*

JM Auditores. (2016). *Documentación de Recursos Humanos.* Costa Rica.

JM Auditores. (2016). *Plan Estratégico Organizacional.*

KPMG. (2017). *KPMG*. Obtenido de KPMG: http://auditoria-auditores.com/directorio/auditores-kpmg

Latorre, A. (2007). *La investigación-acción, Conocer y cambiaar la práctiva educativa.* Barcelona: Publidisa.

Moreno, N. A. (s.f.). *AUDITORÍA FINANCIERA A LOS ESTADOS FINANCIEROS AL 31 DEDICIEMBRE DE 2010 DE LA EMPRESA DE SEGURIDAD OMEGA.* Escuela politécnica del Ejécito, Ecuador.

Parcell, G., & Collison, C. (2009). *No More Consultants - We know More Than We Think.* United Kingdom: John Wiley & Sons.

Real Academia Española. (2017). *Diccionario de la Lengua Española*. Obtenido de Real Academia Española: http://dle.rae.es/?id=4NVvRTc

Sampieri, R. H. (2014). *Metodología de la Investigación.* Mexico: Ma Graw Hill Education.

Sánchez, A. (2015). *Mejora de los controles de auditoría para la revisión de la seguridad de TI.* San Jose.

Scribano, A. O. (2007). *El proceso de investigación social culitativo.* Buenos Aires: Prometeo Libros.