TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en el marco de referencia COBIT 2019

Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información

Elaborado por: María Jesús Calvo Bolaños

Prof. Tutor :MSc. Laura Alpízar Chaves

Cartago, Costa Rica

I Semestre

Junio, 2022

ÁREA ACADÉMICA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN

GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador del Área Académica de Administración de Tecnologías de Información, recomendamos que el siguiente informe del Trabajo Final de Graduación de la estudiante María Jesús Calvo Bolaños sea aceptado como requisito parcial para optar al grado académico de Licenciatura de Administración de Tecnología de Información.

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)

Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2022.06.21 10:21:47 -06'00'

Laura Alpízar
Tutora

ANGELA VANESSA TENCIO CHACON (FIRMA)

Ángela Tencio
Lectora

TEC | Tecnológico de Costa Rica

Firmado digitalmente por SONIA ANGELICA MORA GONZALEZ (FIRMA)
Fecha: 2022.06.18 21:13:44 -06'00'

Sonia Mora
Lectora

TEC | Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2022.06.21 18:32:35 -06'00'

Yarima Sandoval
Coordinación Trabajo Final de Graduación

Dedicatoria

A mis papás, Victoria y Carlos, quienes desde el primer día de mi carrera universitaria han estado presentes con su cariño y motivación y quienes me enseñaron que el éxito proviene de paciencia y esfuerzo.

También a mis hermanos, José Eduardo y Francisco, quienes han sido un apoyo incondicional en esta y otras etapas de mi vida.

Agradecimientos

A mi familia. A mis papás, Victoria y Carlos, por inculcarme la importancia del estudio y apoyarme en todas las decisiones relacionadas con mi profesión. A mis hermanos, José Eduardo y Francisco, por ser un apoyo incondicional en toda mi carrera universitaria, así como en otras etapas de mi vida.

A mis amigos y personas cercanas, aquellos que vivieron esta etapa conmigo y aquellos que me apoyaron durante el proceso; gracias por su motivación y cariño.

A mi profesora tutora, Laura Alpízar, por ser mi guía en este proceso y brindarme la realimentación, apoyo y motivación necesarias para culminar el trabajo de forma exitosa.

Al equipo de TI, especialmente a Angélica y Yeiny, por brindarme la oportunidad de realizar el trabajo y formarme como profesional dentro de su equipo.

Resumen

Calvo, M. (2022). *Propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en el marco de referencia COBIT 2019*. Área Académica de Administración de Tecnología de Información. Instituto Tecnológico de Costa Rica.

El equipo de TI del área de *Management Consulting* de la empresa KPMG S.A., presenta una problemática de desactualización de su matriz de requerimientos de procesos tecnológicos y desestandarización de sus herramientas de gestión utilizadas en la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma. Todas estas herramientas son utilizadas en las actividades de su proceso de auditoría. La matriz de requerimientos de procesos tecnológicos tiene un alto nivel de detalle y no está alineada con el marco de referencia COBIT 2019, mientras que las herramientas de gestión son utilizadas de acuerdo con el criterio de cada auditor, al carecer de una guía o manual para desarrollarlas. Según el equipo de TI, esta problemática ocasiona documentación ambigua y confusiones en la información, lo cual dificulta cumplir con el tiempo final de la auditoría y aumenta sus cargas laborales.

A raíz de esto, surge el presente Trabajo Final de Graduación, el cual propone una actualización de la matriz de requerimientos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019. Con la realización de este proyecto se pretende brindarle al equipo herramientas actualizadas y estandarizadas para facilitar la comprensión y pactar una misma línea de trabajo en las actividades. Asimismo, se pretende evaluar la factibilidad de este proyecto como una respuesta para disminuir las cargas laborales pactadas y por tanto, disminuir la dificultad de cumplir con el tiempo de auditoría.

Palabras clave: Auditoría de TI, matriz de requerimientos de procesos tecnológicos, herramientas de gestión de auditoría, instructivo de gestión, COBIT 2019.

Abstract

Calvo, M. (2022). *Propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en el marco de referencia COBIT 2019*. Área Académica de Administración de Tecnología de Información. Instituto Tecnológico de Costa Rica.

The IT team of the Management Consulting area of KPMG S.A. presents a problem of non-updating of its technological process requirements matrix and non-standardization of its management tools used in the documentation of meetings of understanding, risk documentation, and development of the schedule. All these tools are used in the activities of its audit process. The technology process requirements matrix has a high level of detail and is not aligned with the COBIT 2019 framework, while the management tools are used according to the criteria of each auditor as they do not have a guide or manual to develop them. According to the IT team, this problem causes ambiguous documentation and confusion in the information, which makes it difficult to comply with the final time of the audit and increases their workload.

As a result of this, the present Final Graduation Project arises, which proposes an update of the technological requirements matrix and an audit execution management instruction based on the COBIT 2019 reference framework. The purpose of this project is to provide the team with updated and standardized tools to facilitate understanding and agree on the same line of work in the activities. It is also intended to evaluate the feasibility of this project as a response to reduce the agreed workloads and thus reduce the difficulty of meeting the audit time.

Keywords: IT audit, technology process requirements matrix, audit management tools, management manual, COBIT 2019.

Nota Aclaratoria

Género [1]:

La actual tendencia al desdoblamiento indiscriminado del sustantivo en su forma masculina y femenina va contra el principio de economía del lenguaje y se funda en razones extralingüísticas. Por tanto, deben evitarse estas repeticiones, que generan dificultades sintácticas y de concordancia, que complican innecesariamente la redacción y lectura de los textos.

Este documento se redacta de acuerdo con las disposiciones actuales de la Real Academia Española en relación con el uso del "género inclusivo". Al mismo tiempo se aclara la posición de la suscrita investigadora, a favor de la igualdad de derechos entre los géneros.

[1] Recuperado de: http://www.rae.es/consultas/los-ciudadanos-y-las-ciudadanas-los-ninos-y-las-ninas

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

1. INTRODUCCIÓN

La presente sección abarca una contextualización del proyecto. Se describen los antecedentes de la organización, el área y el equipo de trabajo para el desarrollo del proyecto, proyectos similares, la situación problemática con sus respectivos beneficios, objetivo general y objetivos específicos. También, se detallan las actividades del alcance, supuestos, limitaciones, exclusiones y entregables de producto, académicos y de gestión.

1.1. Descripción General

Este documento describe el proyecto de Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información, del Instituto Tecnológico de Costa Rica. El proyecto consiste en la propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019. Es llevado a cabo dentro del equipo de Tecnología de Información (TI), del área de *Management Consulting*, en la firma KPMG, S.A, durante el primer semestre del año 2022.

La propuesta de este proyecto surge para solventar la problemática del equipo de TI asociada a la desactualización de la matriz de requerimientos de procesos tecnológicos y desestandarización de las herramientas de gestión para la ejecución de las auditorías de tecnología de información, especialmente aquellas utilizadas en las actividades del proceso de auditoría de realización de cronograma, reuniones de entendimiento y documentación de fichas de trabajo.

En las siguientes secciones se detalla primeramente una descripción de la firma auditora y el equipo de trabajo involucrado en el desarrollo del proyecto. Luego, se explica la problemática por la cual surge la propuesta, la justificación y los beneficios de esta, así como los objetivos. Finalmente, alineado a los objetivos, se desglosan las diferentes actividades que abarcan el alcance del proyecto, así como los respectivos entregables, supuestos, limitaciones y exclusiones.

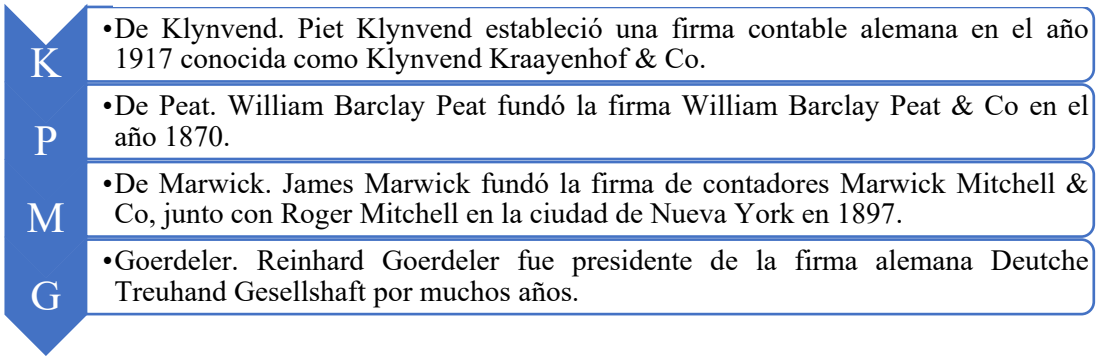
1.2. Antecedentes

1.2.1. Descripción de la organización

KPMG es una red de firmas fundada en 1870. De acuerdo con KPMG (2021), el origen de la compañía fue a partir de cuatro fundadores, los cuales, por medio de la fusión entre sus firmas, crearon el nombre de KPMG. Estos fundadores se establecen en la **Figura 1**.

Figura 1

Fundadores de KPMG



Nota. Información obtenida de KPMG (2021).

Actualmente, KPMG cuenta con 174 000 profesionales y tiene presencia en 155 países, al ofrecer servicios en las siguientes áreas (KPMG, s.f):

- Auditoría: La firma cuenta con un equipo multidisciplinario con alta experiencia en el sector, supervisado por líderes del área, que participan en la comunicación oportuna de hallazgos, áreas de oportunidad, mejora continua y valor agregado, con altos estándares de calidad.
- Impuestos: La firma tiene una red de especialistas en temas jurídicos y tributarios los cuales ofrecen una amplia gama de soluciones de asesoramiento en impuestos y servicios legales, tales como: asesoría tributaria, cumplimiento de impuestos, precios de transferencia, resolución de disputas tributarias, servicios legales, infraestructura y gobierno, aduanas y comercio exterior, y derecho laboral.
- Asesoría/Consultoría: La firma cuenta con asesores de confianza destinados a orientar organizaciones para mejorar el desempeño de la compañía y sus colaboradores, optimizar procesos, incursionar en nuevos mercados, reestructurar, y gestionar sus riesgos.

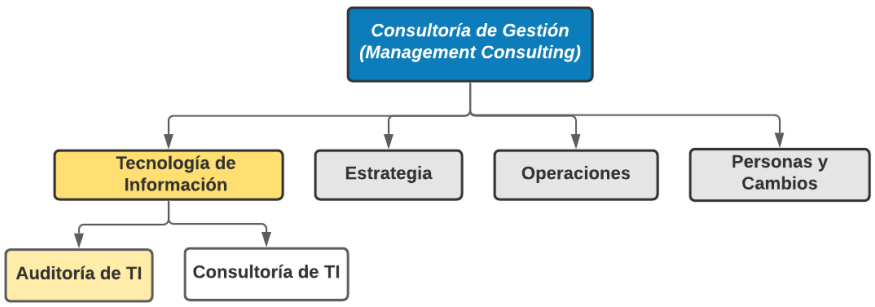
El proyecto se desarrolla en KPMG Costa Rica, empresa dentro de la unidad de negocio llamada KPMG Centroamérica S.A, conocida como KCA. Esta unidad inició sus operaciones en el año 2005, y la integran otros países como Guatemala, Honduras, El Salvador, Nicaragua, Panamá y República Dominicana (KPMG, 2021).

KPMG Costa Rica fue fundada en 1958 y es actualmente una de las firmas profesionales de servicios más importantes en el país, con experiencia en el área por más de 60 años. Cuenta con profesionales de diferentes ramas, agrupados en equipos interdisciplinarios para responder ante las necesidades del mercado costarricense en organizaciones públicas, privadas, o sin fines de lucro, por medio del conocimiento del marco regulatorio local, formación continua, gestión de riesgos, generación de valor y la dedicación total al servicio brindado al cliente (KPMG, 2021).

El área específica donde se desarrolla el proyecto dentro de KPMG Costa Rica es Consultoría de Gestión, comúnmente conocida en inglés como *Management Consulting* (MC). El área de *Management Consulting* está dividida en los siguientes equipos: Tecnología de Información (TI), Estrategia, Operaciones, y, Personas y Procesos; al equipo de Tecnología de Información le corresponde trabajar el proyecto, específicamente en el ámbito de Auditoría de TI, tal como se representa en la **Figura 2**.

Figura 2

Organigrama del área de Consultoría de Gestión



Nota. Elaboración propia a partir de información brindada por el equipo de TI del área de *Management Consulting*.

1.2.1.1. Misión

La misión de KPMG es la siguiente:

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 (KPMG, 2021).

1.2.1.2. Visión

La visión de KPMG es la siguiente:

Ser la mejor firma en dónde trabajar, para nuestros clientes, para nuestra gente y para nuestra comunidad (KPMG, 2021).

1.2.1.3. Valores

Los valores de KPMG se señalan a continuación (KPMG, 2021):

- Integridad
- Excelencia
- Coraje
- Juntos
- Para mejorar

1.2.1.4. Equipo de trabajo

El equipo de trabajo involucrado en el desarrollo del proyecto está conformado por los siguientes miembros:

- *Socio del área:* Esta persona participa activamente brindando respuestas concretas orientadas a nivel de negocio relacionadas con la problemática del proyecto.
- *Gerente de TI:* Esta persona se considera como patrocinador del proyecto. Se encarga de atender las reuniones y firmar los documentos relacionados con la gestión del proyecto, tales como la carta de aceptación, evaluaciones por parte de la organización,

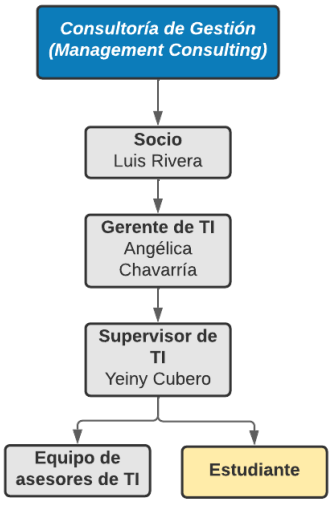
documentos de control de cambios, entre otros. También, provee la información necesaria para el desarrollo del proyecto, además, revisa, aprueba y brinda realimentación a los distintos entregables durante el periodo de ejecución del proyecto.

- *Supervisor de TI:* Esta persona se encarga de proveer la información necesaria para el desarrollo del proyecto de acuerdo con sus diferentes entregables. Junto con el gerente de TI, se encarga de atender las reuniones y consultas, firmar documentos y brindar realimentación durante el desarrollo del proyecto.
- *Equipo de asesores de TI:* Estas personas brindan apoyo durante el desarrollo del proyecto por medio de observaciones, documentación y entrega de cualquier información relacionada con la ejecución del proyecto.
- *Estudiante:* El estudiante forma parte del equipo de asesores de TI. Para el periodo definido de ejecución del proyecto es la persona encargada de desarrollarlo y presentar los resultados tanto a la academia (ATI) como al equipo de TI.

En la **Figura 3** se describe el organigrama del equipo descrito.

Figura 3

Organigrama del equipo de Management Consulting



Nota. Elaboración propia a partir de información brindada por el equipo de TI del área de *Management Consulting*.

1.2.2. Trabajos similares realizados dentro y fuera de la organización

En esta sección se describen detalladamente los trabajos realizados dentro y fuera de la organización, los cuales están relacionados con este proyecto.

Con respecto a trabajos realizados dentro del equipo de TI del área de *Management Consulting* con tema similar al presente proyecto, se consulta al gerente de TI. Chavarría indica que hubo un trabajo final de graduación desarrollado en el año 2019 por un estudiante de ATI (comunicación personal, noviembre, 2021). Este proyecto se llamó Propuesta de una metodología para las auditorías de tecnología de información para entidades reguladas por CONASSIF y fue elaborado por José Gabriel Vargas. El fin de este proyecto fue proponer una metodología que permitiera estandarizar todas las actividades del proceso de auditoría para el área de *Management Consulting*, por medio de la incorporación de mejores prácticas de la industria, así como prácticas basadas en marcos de referencia globales como COBIT 5, ITIL v3 e ISO, para velar por el cumplimiento de la gestión de la tecnología de información en organizaciones públicas y privadas (Vargas, 2019). Actualmente, lo desarrollado por Vargas corresponde al proceso y prácticas actuales que utiliza el equipo de TI para ejecutar las auditorías.

Con respecto a trabajos realizados fuera de la organización, se procede a indagar en la comunidad de ATI, donde se encuentran documentos de trabajos finales de graduación de años anteriores. Entre los trabajos relacionados con el presente proyecto están los siguientes:

- Propuesta de mejora de los controles generales de auditoría de TI en el tema de la seguridad de la Información, elaborado por Cristopher Fabián Inces. El fin de este proyecto fue plantear un proceso de mejora de los controles generales de TI, para responder con lo definido en el acuerdo 14-17 emitido por SUGEF. El proceso de mejora abarcaba el fortalecimiento de los controles existentes, así como la definición de nuevos controles y pruebas para la revisión eficiente de los procesos implementados en las organizaciones financieras, con el propósito de asegurar la integridad y confidencialidad de la información correspondiente para las auditorías de tecnología de información según COBIT 5 (Inces, 2019).
- Propuesta de un Manual de Auditoría de Tecnologías de Información, elaborado por Carlos Alberto Ramírez. El fin de este proyecto fue elaborar un manual de auditoría de TI alineado según el proceso de auditoría establecido por ISO 19011. Este manual incorpora una

introducción sobre la historia y servicios que brinda la empresa, así como una explicación del proceso de auditoría de TI, en donde se definen y especifican los procedimientos y atributos respectivos para evaluar cada tema abarcado. Esto para estandarizar el ciclo de auditoría utilizado por la empresa respectiva (Ramírez, 2018).

1.3. Planteamiento del problema

En esta sección se describe la situación problemática identificada dentro del equipo de Tecnología de Información del área *Management Consulting*, la cual motiva el desarrollo del proyecto. Además, se mencionan los beneficios esperados con la solución del problema identificado.

1.3.1. Situación problemática

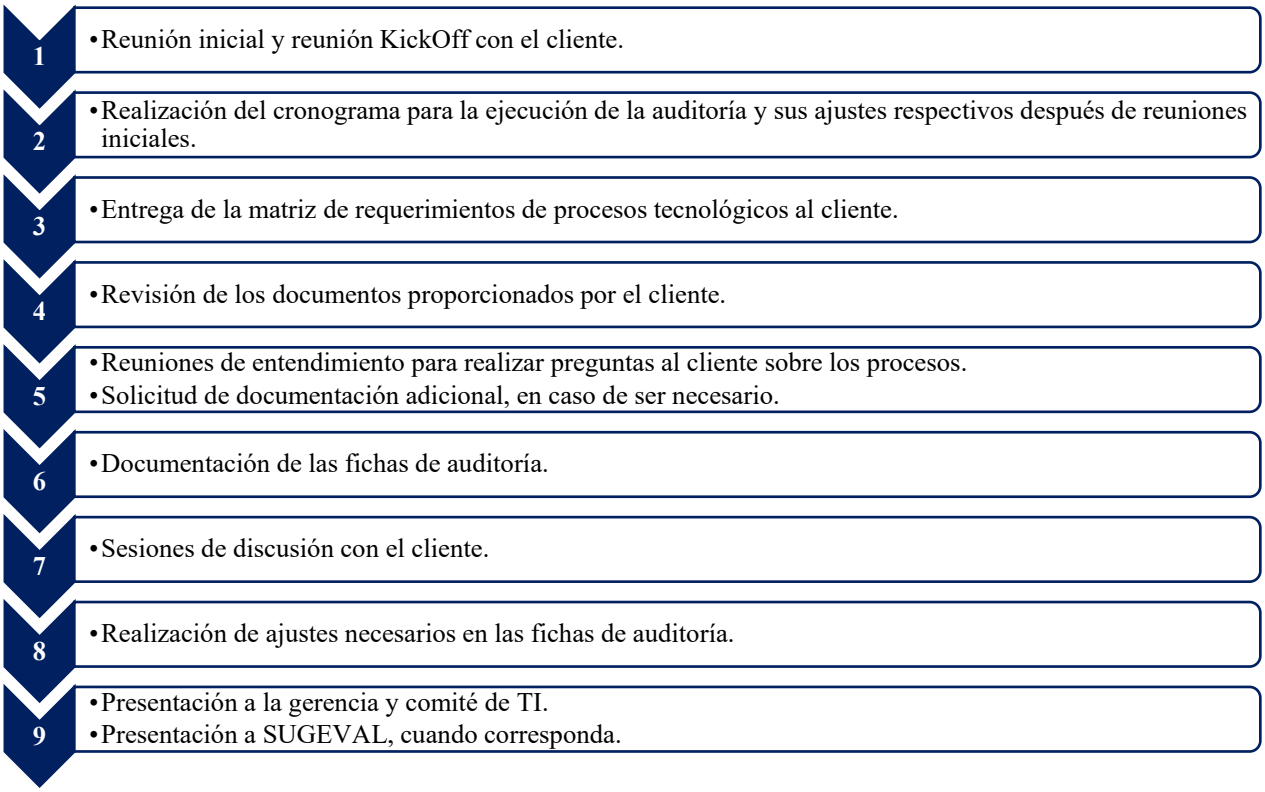
El equipo de Tecnología de Información (TI) del área de *Management Consulting* es el encargado del desarrollo de auditorías y consultorías de tecnología de información. Sus tareas se basan en la ejecución y gestión de proyectos que involucran la implementación del marco de referencia COBIT, seguridad de TI, gobierno digital y transformación digital.

Con respecto a las auditorías de tecnología de información que elabora el equipo, se identifica que algunos clientes solicitan las auditorías de TI para el cumplimiento del acuerdo 14-17 emitido por SUGEF, mientras que otros piden para únicamente evaluar su nivel y desempeño con respecto al marco de referencia COBIT.

El proceso actual para realizar auditorías de tecnología de información utilizado por el equipo de TI contiene las actividades definidas en la **Figura 4**.

Figura 4.

Proceso para realizar auditorías de tecnología de información



Nota. Elaboración propia a partir de información brindada por el equipo de TI del área de *Management Consulting*.

En las diferentes actividades del proceso, los auditores utilizan un conjunto de herramientas para la documentación y gestión de la auditoría. Dado a que la mayoría de las auditorías son basadas en COBIT 5, porque el acuerdo 14-17 de la SUGEF así lo indica, las herramientas utilizadas se obtienen del conocimiento en este marco de referencia. No obstante, muchas de estas no están estandarizadas. A esto se le suma la llegada de la nueva versión del marco de referencia, COBIT 2019. El equipo debe mantenerse alineado con la última versión del marco de referencia para brindar alta calidad y cumplir con la misión de la organización. Por estas razones, al equipo de TI le surge la necesidad de actualizar y estandarizar sus herramientas basándose en esta nueva versión del marco de referencia.

A continuación, se lista con más detalle las situaciones problemáticas relacionadas con las herramientas de auditoría:

- La primer problemática identificada se encuentra en la siguiente actividad del proceso: "3. Entrega de la matriz de requerimientos de proceso tecnológicos al cliente". La problemática es la desactualización de la matriz de requerimientos de procesos tecnológicos, la cual es utilizada para recopilar la información por solicitar al auditado. Por un lado, el listado de requerimientos por solicitar de cada proceso dentro de la matriz es de alto nivel. Usualmente, se debe solicitar documentación repetidamente después de haber entregado la matriz, porque en la lista inicial de requerimientos estos no se encuentran definidos. Esto genera que el equipo de auditores tenga dificultad para cumplir con las fechas establecidas para la ejecución de la auditoría, dado que solicitar documentación repetidamente ocasiona un aumento del tiempo de ejecución de las actividades previamente definidas en el cronograma y compromete las cargas de trabajo de los auditores. Por otro lado, la matriz está basada en COBIT 5, por lo cual omite información relevante que pueda tener el nuevo marco de referencia COBIT 2019 con respecto a los controles.
- La segunda problemática identificada es la desestandarización de las herramientas utilizadas para la ejecución de la auditoría, en especial aquellas utilizadas en las siguientes actividades del proceso: "2. Realización de cronograma", "5. Reuniones de entendimiento para realizar preguntas al cliente sobre los procesos" y "6. Documentación de las fichas de auditoría". Las problemáticas son las siguientes:
    - Las reuniones de entendimiento son ambiguas. Las preguntas por realizar a la parte auditada son planteadas de acuerdo con el criterio del auditor responsable de ejecutar la auditoría, basado en su conocimiento de COBIT 5. Las anotaciones son escuetas dado que no existe una herramienta estándar para realizarlas. Estas dependen del juicio del auditor; cada auditor elige la herramienta que le parece conveniente para documentar la información que a su criterio es relevante. Esto ocasiona confusión en los auditores para entender la reunión, lo cual también genera una dificultad en la comunicación entre estos.
    - En la documentación de las fichas de auditoría se identifica una escritura informal de los riesgos. Por un lado, la definición del riesgo es planteada por cada auditor. Por otro lado, la definición del impacto de los riesgos identificados depende del juicio de

experto de cada auditor. El no tener un criterio estandarizado, con base en marcos de referencia o políticas relevantes para los riesgos causa ambigüedad en la documentación de estas fichas.

- Planificación desorganizada del cronograma, dado que no existe una duración promedio por cada proceso. Las fechas establecidas por cada proceso dependen del criterio del auditor responsable. Esto genera confusiones entre los auditores o atrasos en el tiempo de ejecución de las actividades para cumplir la auditoría, lo cual afecta las cargas de trabajo y, dificulta el cumplimiento de las fechas de auditoría.

Estas situaciones problemáticas descritas causan un problema central definido como *desactualización de la matriz de requerimientos de procesos tecnológicos y desestandarización de las herramientas de gestión utilizadas para la ejecución de las auditorías de tecnología de información*, el cual se detalla mediante un árbol del problema en la **Figura 5**.

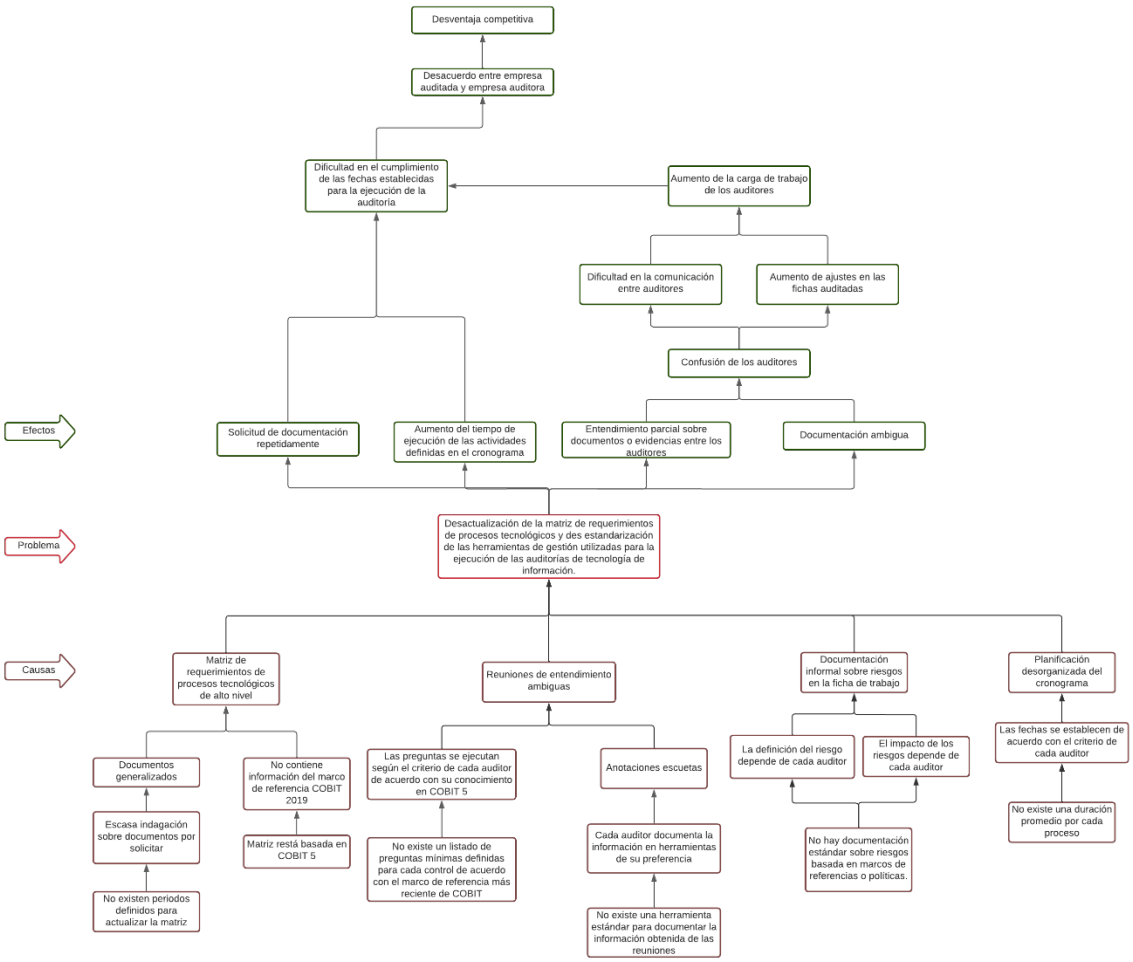
A raíz de este problema central, sus causas y efectos, se formulan las siguientes hipótesis:

I. La desactualización de la matriz de requerimientos de procesos tecnológicos y la desestandarización de las herramientas de gestión utilizadas para la ejecución de las auditorías de tecnología de información dificultan el tiempo de ejecución y aumentan las cargas de trabajo de los auditores en el cumplimiento del proceso de la auditoría.

II. Una propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en COBIT 2019 solventa la problemática de desactualización de la matriz de requerimientos de procesos tecnológicos y desestandarización de las herramientas de gestión utilizadas para la ejecución de las auditorías de tecnología de información que enfrenta actualmente el equipo de TI del área de *Management Consulting*.

Figura 5

Árbol del problema



Nota. Elaboración propia

1.3.2. Justificación del proyecto

Para la justificación del proyecto se procede a brindar una respuesta detallada y precisa a las siguientes preguntas:

- ¿Por qué el proyecto es factible dentro del área de la organización?
- ¿Por qué el proyecto es apto para un profesional de la carrera de ATI?

Primeramente, para responder a la pregunta "¿Por qué el proyecto es factible dentro del área de la organización?" se consideran los siguientes dos aspectos. Por una parte, con respecto a por qué es factible una actualización de la matriz de requerimientos de procesos tecnológicos, se enfatiza que la matriz de requerimientos actual utilizada por el equipo de TI fue desarrollada a un alto nivel de detalle utilizando el marco de referencia COBIT 5. Esto ocasiona no solo omitir información relevante del nuevo marco de referencia COBIT 2019, sino omitir datos importantes del marco de referencia COBIT 5.

Si bien las auditorías para cumplir con el acuerdo 14-17 se realizan basándose en COBIT 5, se debe recordar que el equipo también realiza auditorías para organizaciones que únicamente quieren evaluar su nivel y desempeño en el marco de referencia, sea COBIT 5 o COBIT 2019, dependiendo de las peticiones de sus clientes. El equipo de TI, al ser parte de una firma auditora destacada que siempre busca el cumplimiento en temas de alta calidad en el trabajo de las auditorías, está en la obligación de actualizar su matriz de requerimientos de procesos tecnológicos con el nuevo marco de referencia. Esto no solo les genera ventaja competitiva como equipo auditor, sino que cumplen con la misión de la organización de realizar auditorías de alta calidad.

Por otra parte, con respecto a por qué es factible un instructivo de gestión de ejecución de la auditoría, se enfatiza que el equipo de TI se encuentra en formación. Si bien el proceso de auditoría especificado en la **Figura 4** es el que siguen todos los miembros del equipo, las herramientas utilizadas para la ejecución de este quedan a criterio de cada auditor de acuerdo con su conocimiento en COBIT 5 y su forma de trabajar la auditoría. Esto hace que los nuevos miembros entiendan estas herramientas bajo el conocimiento del auditor encargado únicamente, dada la inexistencia de un conjunto de herramientas de gestión que sean de entendimiento común para todos los miembros del equipo.

Asimismo, las auditorías de la firma se rigen bajo la guía llamada *KPMG Audit Execution Guide* (KAEG), donde se detallan las normas, responsabilidades, herramientas y procedimientos importantes para elaborar auditorías. No obstante, KAEG no contempla esas características para las auditorías de tecnología de información, lo cual genera que el proceso esté sujeto a la percepción del equipo de TI y se incurra en problemáticas de desactualización o no estandarización de

herramientas de trabajo, que involucran consecuencias de aumentos de cargas de trabajo y dificultad para cumplir con las metas o fechas de las auditorías.

Considerando lo anterior, la elaboración de este proyecto le permite al equipo de TI tener herramientas, tanto la matriz de requerimientos de procesos tecnológicos como el instructivo de gestión, basadas en el marco de referencia más reciente de COBIT, de entendimiento común para todos los miembros. Por medio de este proyecto, el equipo obtiene las actividades de entrega de la matriz de requerimientos de procesos, realización del cronograma, reuniones de entendimiento y documentación de las fichas de auditoría ordenadas, lo cual les facilita tener el control sobre la información gestionada durante el proceso de auditoría. Este orden y control puede erradicar la dificultad para cumplir con las fechas pactadas con el cliente. Esto mantiene la imagen de la compañía como empresa auditora, posicionándola en gran ventaja competitiva con respecto a otras.

Luego, para responder a la pregunta "¿Por qué el proyecto es apto para un profesional de la carrera de ATI?", se desafía al estudiante a poner en ejecución la teórica, práctica y experiencia obtenida en los cursos de la carrera, para desarrollar el proyecto orientado a las áreas de investigación que caracterizan el perfil de un egresado de ATI. Este proyecto se desenvuelve en el área de auditoría de tecnologías de información, pues el propósito es brindar una propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el nuevo marco de referencia COBIT 2019.

Por un lado, parte de la propuesta de solución es hacer una actualización de la matriz de requerimientos de procesos; se pretende poner en práctica lo visto en el curso de Auditoría de Tecnologías de Información. Este curso establece las bases teóricas sobre el proceso de auditoría, sus diferentes involucrados, fases y actividades por realizar. También establece las bases para desarrollar una matriz de requerimientos de procesos tecnológicos y utilizarla al momento de auditar. Además, introduce el conocimiento y la puesta en práctica del marco de referencia COBIT 2019, a través de un proyecto que requiere la participación de una organización. Todo esto, para experimentar a nivel general una auditoría de TI y posicionar al estudiante como un auditor de TI.

Utilizar el marco de referencia de COBIT 2019 tiene una serie de ventajas a la hora de realizar la auditoría, según lo descrito por Svatá (2018):

- Flexibilidad y apertura para adaptarse y alinearse al contexto particular que el usuario necesite, lo cual permite añadir nuevas áreas de enfoque y modificar las actuales.
- Permite la referencia y la alineación de conceptos relacionados con los últimos estándares de tecnología de información y regulaciones de cumplimiento.
- Contribuye con la gestión de las tecnologías de información, al introducir conceptos de madurez y alineación.

Por otro lado, dado que la propuesta de solución también involucra generar un instructivo de gestión para la auditoría, se desafía al estudiante a poner en práctica el conocimiento adquirido en cursos relacionados con Administración de Proyectos. En estos cursos se aprende, por medio de teoría y elaboración de proyectos que involucren una organización, a identificar hallazgos u oportunidades de mejora para solventar una problemática. También, a desarrollar herramientas de gestión que puedan servir como orientación al proyecto en cuestión de definición de etapas o procedimientos, tales como herramientas para documentar información, cronogramas, informes, entre otros.

1.3.3. Beneficios esperados o aportes del Trabajo Final de Graduación

A continuación, se especifican explícitamente los beneficios directos e indirectos que conlleva la realización del proyecto dentro del equipo de TI, con el propósito de resolver la situación problemática.

1.3.3.1. Beneficios directos

Entre los beneficios directos que conlleva la realización de este proyecto para resolver la situación problemática, se señalan los siguientes:

- Validación de la factibilidad de una solución para actualizar y estandarizar las herramientas utilizadas en ciertas actividades del proceso de auditoría de TI efectuado por el equipo de TI.
- Validación de beneficios para el equipo de TI mediante una solución para actualizar y estandarizar las herramientas utilizadas en este.

- Cumplimiento exitoso y ordenado de las actividades del proceso de auditoría, acorde con el cronograma planteado con el cliente.
- Incremento de la calidad de las auditorías, lo cual les asegura su alineamiento con la misión de la organización.
- Alineación de las herramientas de auditoría, tanto matriz de requerimientos tecnológicos como herramientas para documentación de reuniones de entendimiento, fichas de auditoría y cronograma, con el nuevo marco de referencia COBIT 2019.
- Entendimiento común de las herramientas de gestión para la ejecución de la auditoría entre todos los miembros del equipo.
- Mejoras en la comunicación entre los auditores, al existir un entendimiento común de las herramientas de gestión.
- Validación de la efectividad de una disminución de pérdidas de tiempo en la ejecución de las actividades de la auditoría, minimización de las cargas de trabajo de los auditores y reducción del pago de horas extra por las cargas de trabajo.

1.3.3.2. Beneficios indirectos

Entre los beneficios indirectos que conlleva la realización de este proyecto para resolver la situación problemática, se enlistan los siguientes:

- Mantenimiento de la credibilidad de la empresa con respecto a las auditorías de tecnología de información.
- Aumento de la ventaja competitiva tanto para el equipo de TI del área de *Management Consulting* como para la empresa en general.

1.4. Objetivos del Trabajo Final de Graduación

A continuación, se detalla el objetivo general y los objetivos específicos del proyecto, con el propósito de resolver la problemática.

1.4.1. Objetivo general

Proponer una actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019, para la implementación de mejoras en las herramientas utilizadas por el equipo de TI del área de *Management Consulting*, en la firma KPMG S.A, durante el primer semestre de 2022.

1.4.2. Objetivos específicos

- Analizar la situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión utilizadas por el equipo de TI, para la identificación de hallazgos y oportunidades de mejora de estas herramientas.
- Aplicar un análisis de brecha, considerando la situación actual y la situación deseada, para la delimitación de la propuesta de solución que solvente la problemática.
- Elaborar una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión, basados en el marco de referencia COBIT 2019, para la promoción de la actualización y estandarización de estas herramientas utilizadas por el equipo de TI.
- Desarrollar un análisis financiero para la comprobación de los beneficios y viabilidad de la propuesta de solución.
- Validar la pertinencia de la propuesta de solución, por medio de un plan piloto, para el cumplimiento de esta como respuesta a la problemática.

1.5. Alcance

El alcance de este proyecto está estrictamente relacionado con la entrega de una propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019.

Primeramente, antes de describir las actividades del alcance, se procede a listar las herramientas involucradas:

- Matriz de requerimientos de procesos tecnológicos.
- Herramienta para las reuniones de entendimientos.
- Herramienta para la definición de riesgos de auditoría.

- Cronograma de auditoría.

Para el alcance de este proyecto, el concepto de herramientas de gestión, abarcado a lo largo del documento, corresponde únicamente a las siguientes tres herramientas: la herramienta para las reuniones de entendimiento, la herramienta para la definición de riesgos de auditoría, y al cronograma.

Seguidamente, para la elaboración de esta propuesta el alcance abarca cinco actividades. La primeras dos actividades dentro del alcance consisten en efectuar un análisis de la situación actual y un análisis de brecha con respecto a la matriz de requerimientos de procesos tecnológicos y herramientas de gestión para las actividades de realización de cronograma, documentación de reuniones de entendimiento y documentación de las fichas de auditoría. Primeramente, se pretende realizar el análisis de la situación actual para identificar el contexto de estas herramientas, tanto la matriz como las herramientas de gestión para documentar las reuniones de entendimiento, documentar los riesgos y elaborar el cronograma, y así visualizar las oportunidades de mejora. Posteriormente, se busca comparar el estado actual con el deseado de estas herramientas con respecto a COBIT 2019, para así proponer la solución apropiada a las oportunidades de mejora identificadas.

Luego, la tercera actividad dentro del alcance conlleva dos aspectos. El primero es la actualización de la matriz de requerimientos de procesos siguiendo lo establecido por el marco de referencia COBIT 2019. Se pretende seleccionar un total de diez procesos, dos por cada dominio definido en el marco de referencia, descritos de forma general en la **Tabla 1**. Esta elección se realiza mediante el criterio de experto sobre los procesos más comunes que son auditados por el equipo de TI. Una vez obtenido el listado respectivo de procesos comunes a auditar, se toman dos procesos aleatorios por cada dominio. Posteriormente, se procede a estudiar y desglosar cada proceso para posteriormente crear la matriz con la información respectiva.

Tabla 1

Selección de los procesos por cada dominio de COBIT 2019

Dominio	Proceso	Descripción
Evaluar, Dirigir y Monitorizar (EDM)	EDM01: Asegurar el establecimiento y el mantenimiento del marco de gobierno.	Analizar y articular los requisitos para el gobierno de TI de la empresa. Establecer y mantener componentes de gobierno claros con respecto a la autoridad y las responsabilidades para lograr la misión, las metas y los objetivos de la empresa.

Dominio	Proceso	Descripción
	EDM03: Asegurar la optimización del riesgo	Asegurar que el apetito y la tolerancia al riesgo de la empresa se entiendan, articulen y comuniquen, y que se identifique y gestione el riesgo para el valor de negocio relacionado con el uso de TI.
Alinear, Planificar y Organizar (APO)	APO009: Gestionar los acuerdos de servicio	Alinear los productos y servicios habilitados por TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluidos la identificación, especificación, diseño, publicación, acuerdo y monitorización de los productos y servicios de TI, niveles de servicio e indicadores de rendimiento.
	APO13: Gestionar la seguridad	Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.
Construir, Adquirir e Implementar (BAI)	BAI06: Gestionar los cambios de TI	Gestionar todos los cambios de una manera controlada, incluidos los cambios estándar y los mantenimientos de emergencia en relación con los procesos de negocio, las aplicaciones y la infraestructura. Esto incluye estándares y procedimientos de cambio, evaluación del impacto, priorización y autorización, cambios de emergencia, seguimiento, informes, cierre y documentación.
	BAI09: Gestionar los activos	Gestionar los activos de TI a través de su ciclo de vida para asegurarse de que su uso aporta valor a un coste óptimo, continúan operativos (adecuados a su propósito), y se tienen en cuenta y están físicamente protegidos. Asegurar que aquellos activos que son críticos para soportar la capacidad del servicio son confiables y están disponibles. Gestionar las licencias de software para asegurarse de que se adquiere, retiene y despliega la cantidad óptima en relación con el uso que requiere el negocio, y que el software instalado cumpla con los acuerdos de licencia.
Entregar, Dar Servicio y Soporte (DSS)	DSS02: Gestionar las peticiones y los incidentes de servicio	Proporcionar una respuesta oportuna y efectiva a las solicitudes de los usuarios y la resolución de todos los tipos de incidentes. Restaurar el servicio normal, registrar y completar las solicitudes de usuario; y registrar, investigar, diagnosticar, escalar y resolver los incidentes.
	DSS03: Gestionar los problemas	Identificar y clasificar los problemas y su causa raíz. Ofrecer una solución oportuna para evitar incidentes recurrentes. Ofrecer recomendaciones de mejoras.
Monitorizar, Evaluar y Valorar (MEA)	MEA02: Gestionar el sistema de control interno	Supervisar y evaluar continuamente el entorno de control, incluyendo autoevaluaciones y auto concienciación. Habilitar a la gerencia para identificar deficiencias e ineficiencias de control e iniciar acciones de mejora. Planificar, organizar y mantener estándares para la evaluación del control interno y la eficacia del control de procesos.
	MEA03: Gestionar el cumplimiento de los requisitos externos	Evaluar si los procesos de TI y los procesos de negocio apoyados por TI cumplen con las leyes, regulaciones y requisitos contractuales. Asegurar que los requisitos se han identificado y cumplido; integrar el cumplimiento de TI con el cumplimiento general de la empresa.

Nota. Información tomada de COBIT 2019.

El segundo aspecto es la elaboración de un instructivo de gestión para las siguientes actividades:

- Realización del cronograma.
- Reuniones de entendimiento para realizar preguntas al cliente sobre los procesos.
- Guión para documentar los riesgos de auditoría dentro de las fichas de auditoría.

Dado que las herramientas para realizar el cronograma, documentar la información de las reuniones de entendimiento y documentar los riesgos dentro de las fichas de auditoría quedan a criterio de cada auditor responsable de la auditoría, esta propuesta de instructivo de gestión busca brindar un guion al equipo de TI, el cual contenga la definición de las herramientas para desarrollar y gestionar el cronograma, las reuniones de entendimiento y la documentación de los riesgos dentro de la ficha de auditoría. De esta manera, todos los miembros utilizarán las mismas herramientas, lo cual promueve la estandarización de estas y disminuye los problemas de comunicación entre los auditores en el entendimiento de la información. La realización de este instructivo considera los procesos de COBIT 2019 seleccionados en la **Tabla 1**.

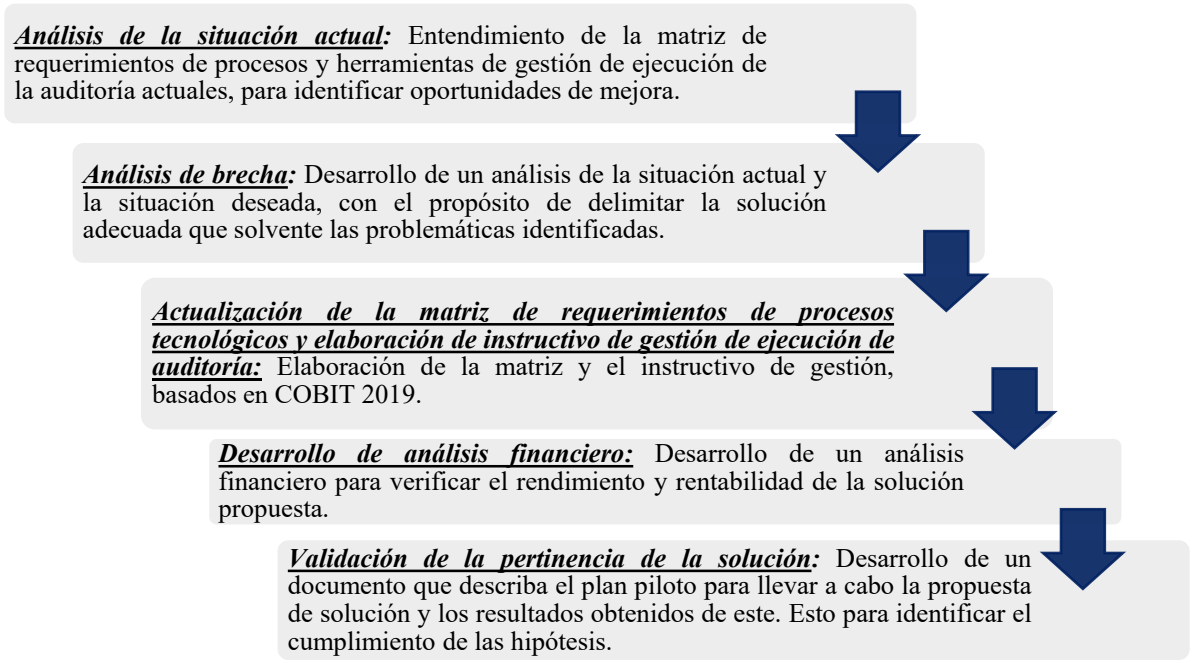
La cuarta actividad dentro del alcance consiste en desarrollar un análisis financiero para validar la propuesta de solución en términos económicos. Se busca determinar el nivel de rendimiento y viabilidad que tiene la propuesta de solución para las labores que realiza el equipo de TI.

Finalmente, la quinta actividad dentro del alcance consiste en desarrollar un análisis de validación de la pertinencia de la solución. Se pretende evaluar, por medio de un plan piloto, si la solución planteada en la tercera actividad es la respuesta ideal para resolver la problemática identificada y la consecuencia del aumento de cargas de trabajo. Esto para dar respuesta a las hipótesis planteadas.

Para desarrollar estas actividades, en la **Figura 6** se establecen las etapas para la ejecución del proyecto.

Figura 6

Proceso de ejecución del proyecto



Nota. Elaboración propia.

1.6. Supuestos

En esta sección se indican explícitamente cuáles son los factores y elementos que se presume se cumplirán con la realización del proyecto. Estos son los siguientes:

- Apoyo por parte del equipo de TI para la realización completa y exitosa del proyecto propuesto.
- Disposición del gerente de TI y el supervisor de TI para atender reuniones y consultas relacionadas con el proyecto.
- La información necesaria para la realización del proyecto será entregada al estudiante a tiempo conforme esta sea solicitada.
- Exactitud y confiabilidad de la información brindada por el equipo de TI para la realización del proyecto.
- Consideración de auditorías en desarrollo a la fecha de ejecución del proyecto, para validar la pertinencia de la propuesta de solución.

1.7. Entregables

En esta sección se describen los entregables del proyecto, tomando en cuenta los entregables del producto solicitados por la organización, los entregables académicos y los entregables de gestión.

1.7.1. Entregables del producto

A continuación, se describen los entregables asociados a cada objetivo del proyecto.

1. *Análisis de la situación actual:* Este entregable pretende describir, de forma explícita, la situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de la auditoría, para identificar las diferentes debilidades y oportunidades de mejora.
2. *Análisis de brecha:* Este entregable pretende comparar la situación actual y la situación deseada de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de la auditoría, para identificar las brechas y delimitar la propuesta de solución para solventarlas.
3. *Matriz de requerimientos actualizada e instructivo de gestión de la ejecución de la auditoría basados en COBIT 2019*: Este entregable corresponde dos aspectos. El primero es la matriz de requerimientos de procesos actualizada con los diez procesos previamente seleccionados. El segundo aspecto es el instructivo de gestión, el cual es el guion para el equipo de TI y contiene la definición y estructura para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma.
4. *Análisis financiero:* Este entregable corresponde a la formulación de un análisis económico para determinar el nivel de rentabilidad y rendimiento de la propuesta de solución para las actividades que realiza el equipo de TI.
5. *Validación de la propuesta:* Este entregable corresponde al análisis de validación de la pertinencia de la solución, la cual incorpora la actualización de la matriz y el instructivo de gestión, como respuesta a la problemática. Primeramente, se pretende describir el plan piloto para realizar la validación correspondiente. Seguido de esto, se pretende desglosar los diferentes resultados encontrados y dar respuesta a las hipótesis planteadas.

1.7.2. Entregables académicos

Los entregables correspondientes al Trabajo Final de Graduación para optar al grado de Licenciatura en Administración de Tecnología de Información, son los siguientes:

- Capítulo 1: Introducción
- Capítulo 2: Marco Teórico
- Capítulo 3: Marco Metodológico
- Capítulo 4: Análisis de Resultados
- Capítulo 5: Propuesta de Solución
- Capítulo 6: Conclusiones
- Capítulo 7: Recomendaciones

1.7.3. Entregables de gestión

A continuación, se describen los artefactos asociados con la gestión del proyecto.

1.7.3.1. Cronograma

El cronograma se detalla en la **Figura 7**.

1.7.3.2. Minutas

La plantilla para las minutas que se realizarán a lo largo de la ejecución del proyecto se encuentra en el **Anexo I**.

1.7.3.3. Gestión del cambio

La plantilla para el control de los cambios durante la ejecución del proyecto se encuentra en el **Anexo II**.

Figura 7

Cronograma para la ejecución del proyecto

Cronograma																		
Actividad	**Semanas**																	
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
Reunión con profesor tutor	■																	
Reunión con empresa	■																	
Ajustes del anteproyecto		■																
Elaboración del capítulo de Introducción		■	■															
Entrega del primer avance				■														
Elaboración del capítulo de Marco Conceptual				■	■													
Correcciones del primer avance					■													
Entrega del segundo avance						■												
Elaboración del capítulo de Metodología						■	■											
Correcciones del primer avance							■											
Entrega del tercer avance								■										
Elaboración del capítulo de Resultados y Propuesta de Solución								■	■									
Correcciones del tercer avance									■									
Entrega del cuarto avance										■								
Elaboración del capítulo de Conclusiones y Recomendaciones										■	■							
Correcciones del cuarto avance											■							
Entrega del quinto avance												■						
Correcciones del quinto avance													■					
Entrega de informe final														■				
Defensa																	■	
Correcciones finales																	■	
Entrega final																		■

Nota. Elaboración propia.

1.8.Limitaciones

En esta sección se indican explícitamente los factores o elementos que en alguna medida restringen la realización del proyecto. Estos son:

- Disponibilidad inmediata del gerente de TI o supervisor para atender consultas del proyecto.
- Inexistencia de documentación sobre el proceso de auditoría de TI, herramientas actuales para la auditoría, u otra información necesaria para la realización del proyecto.
- Acceso de información considerada como confidencial para la elaboración de este proyecto.

1.9. Exclusiones

En esta sección se describen los entregables o productos que podrían esperarse del proyecto pero que por alguna razón específica quedarán fuera del alcance. Estos entregables son los siguientes:

- Actualización completa de la matriz de requerimientos. El resto de los procesos que no fueron seleccionados quedarán fuera de la actualización de esta matriz.
- No se incluyen los otros equipos del área de *Management Consulting*, ni las otras áreas de la organización (Auditoría e Impuestos), dado que estas no ejecutan auditorías en temas de tecnología de información.

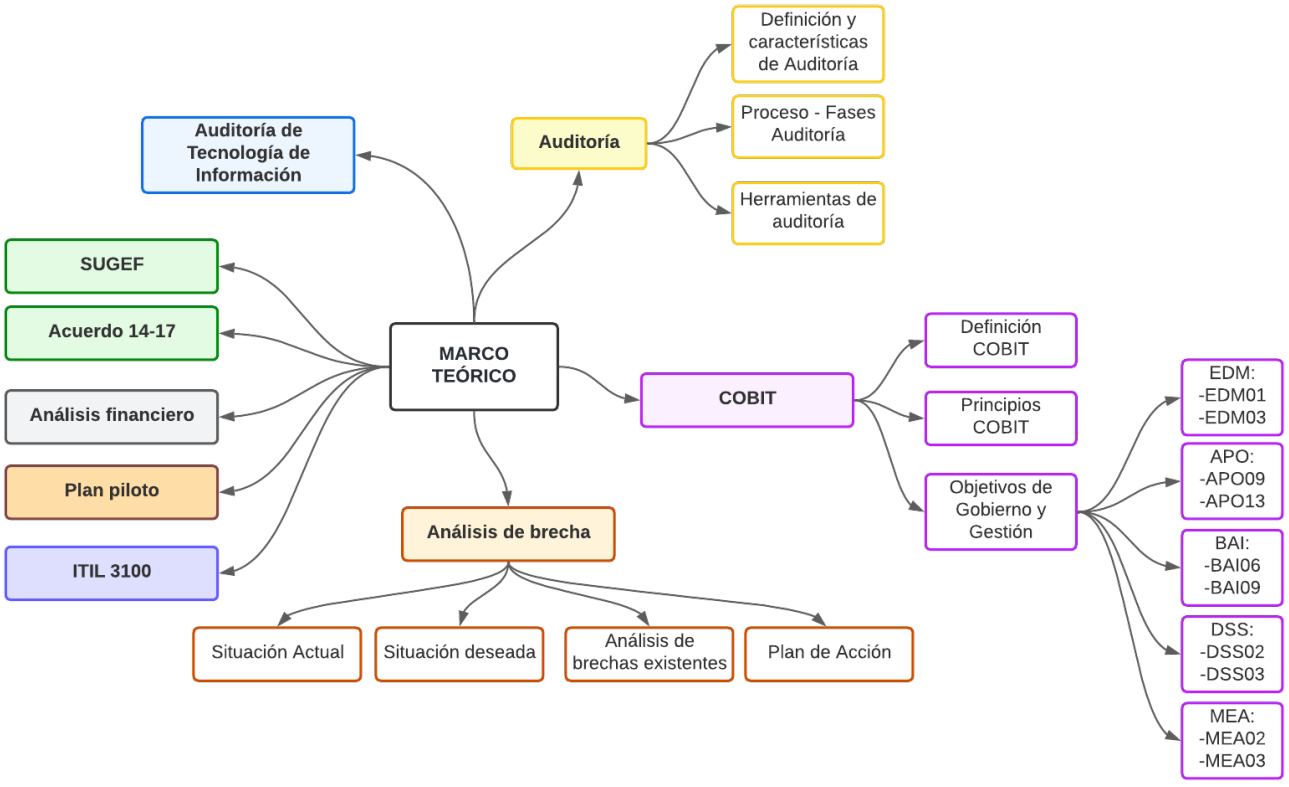
2. MARCO CONCEPTUAL

En el presente capítulo se procede con la definición de las bases conceptuales relevantes, ya sea teóricas o prácticas, para sustentar el problema identificado y la propuesta de solución de este proyecto. Se indagan conceptos relacionados con auditoría, entes regulatorios, acuerdos, fases y herramientas; se explora el marco de referencia COBIT 2019, el cual es la base para el desarrollo de la propuesta de solución; y se describen términos relacionados con análisis financieros y plan piloto, los cuales serán ejecutados como parte de la propuesta de solución.

La **Figura 8** establece un mapa mental de los conceptos abarcados en esta sección.

Figura 8

Mapa de conceptos



Nota. Elaboración propia.

2.1. Auditoría

El concepto de auditoría es comúnmente conocido a nivel contable o financiero. Sin embargo, este término se ha desenvuelto a través de los años en múltiples áreas que no solo involucran la económica, sino áreas a nivel administrativo, operativo, tecnológico, riesgos, entre otros. Por esta razón, se determina su definición general aplicada a cualquier área o actividad que pueda ser auditada.

La Organización Internacional de Normalización (ISO) (2011) define auditoría como: "proceso sistemático, independiente y documentado para obtener evidencias objetivas (…) y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría (…)".

De igual manera, Tapia et al (2019) consideran a la auditoría como una revisión sistemática de una actividad o situación, que tiene como fin evaluar el cumplimiento de las reglas o criterios objetivos a los cuales está sometida dicha actividad o situación. En general, la auditoría busca obtener y evaluar de forma objetiva todas las evidencias relacionadas con dichas actividades o acontecimientos, para determinar su grado de correspondencia con los criterios previamente establecidos. En otras palabras, la auditoría trata de:

- Revisar que los hechos, fenómenos y operaciones se ejecuten de la forma planteada.
- Verificar que las políticas, reglas o procedimientos establecidos hayan sido observados y respetados.
- Evaluar la forma de administración y operación para aprovechar al máximo los recursos.

2.1.1. Características de la auditoría

Como parte de las características de la auditoría, se enfatiza primeramente en que la persona encargada de realizar y conducir la auditoría se llama auditor. Tapia et al (2019) establecen las características de un auditor, las cuales se centran en tener una perspectiva global, agudeza para los negocios, orientación basada en riesgos, comunicación asertiva, pensamiento crítico, entre otras.

Luego, como su definición lo menciona, la auditoría busca obtener evidencias objetivas para determinar el cumplimiento de estas de acuerdo con los criterios de auditoría previamente establecidos. ISO (2011) define criterios de auditoría como aquellos requisitos usados como

referencia para comparar las evidencias. También, recalca que las evidencias objetivas son todo material o información que respalda la existencia y/o veracidad de lo acontecido. Espino (2014) menciona algunos ejemplos de evidencia de auditoría, los cuales son: evidencia documental, declaraciones de terceros como confirmaciones, cartas, o declaraciones de clientes y evidencia física, como inventarios.

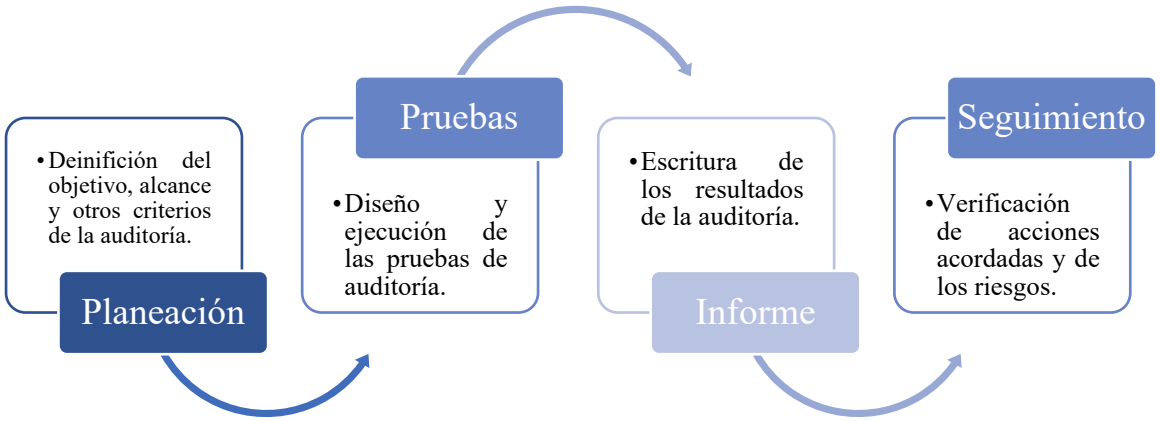
2.1.2. Proceso o Fases de auditoría

El proceso de auditoría está compuesto por las fases presentadas en la **Figura 9**. Estas son descritas a partir de información proporcionada por Frett (2019) del sitio oficial Auditool, así como información académica elaborada por Alpízar (2020):

- *Planeación:* En esta fase se procede con la definición de los objetivos de la auditoría, así como la descripción del alcance y enfoques de esta. También, se establece el equipo de trabajo involucrado en la auditoría y la delimitación de los criterios o métricas por utilizar, los cuales pueden ser estándares, marcos de referencia, o políticas.
- *Pruebas:* Esta fase corresponde al diseño y ejecución de las pruebas de auditoría. Se diseñan las pruebas sustantivas y de cumplimiento. Durante la ejecución de las pruebas se procede con la recolección de evidencia, documentación de resultados y determinación de hallazgos. Se utilizan técnicas como: consulta, observación, inspección, revisión de comprobantes, indagación, rastreo, entre otras.
- *Informe:* En esta fase se procede con la documentación de los resultados de la auditoría, para posteriormente comunicarlos a las partes interesadas e involucrados. Los posibles formatos para este tipo de informes son: impreso, digital, verbal o por medio audiovisual.
- *Seguimiento:* Esta fase corresponde al proceso de verificación que deben hacer los auditores para validar que se estén efectuando las acciones acordadas con el auditado para solucionar los hallazgos establecidos. También, validan que los riesgos identificados hayan sido mitigados a un nivel aceptable para la organización auditada.

Figura 9

Proceso de auditoría



Nota. Elaboración propia a partir de información tomada de Frett (2019) y Alpízar (2020).

2.1.3. Herramientas de auditoría

Para entender correctamente el término de *herramientas de auditoría* es importante responder a la incógnita *¿Cuál es la diferencia entre técnicas y herramientas de auditoría?* Por un lado, las técnicas de auditoría hacen referencia a los métodos prácticos o procedimientos de investigación y prueba de empleados por el auditor para analizar la información y hacer sus respectivas comprobaciones con miras a emitir su criterio. Ejemplos de técnicas pueden ser observación, inspección, confirmación, investigación, análisis o muestreos. Por otro lado, las herramientas de auditoría son los elementos que permiten llevar a cabo las acciones indicadas en las técnicas (Alatrista, 2019; Auditool, 2019).

Existen múltiples herramientas de auditoría, las cuales responden a actividades específicas según la auditoría por desarrollar. Auditool (2021) y Morales (2021) mencionan herramientas básicas como cuestionarios de entendimiento de proceso o cronogramas, hasta herramientas elaboradas tales como aquellas para la planeación estratégica de auditorías, investigación de fraudes, modelos de gobierno,

factores de riesgos, evaluación de implementaciones, otros. La **Tabla 2** delimita y describe algunas de las herramientas de auditoría de interés para la propuesta de solución de este proyecto, de acuerdo con lo establecido por este sitio oficial y autor.

Tabla 2

Herramientas de auditoría

Herramienta	Descripción
Cuestionarios	Son utilizados para el entendimiento de procesos. Contienen preguntas estructuradas que sirven de guía para obtener la mayor cantidad de información posible de acuerdo con el criterio establecido para la auditoría.
Entrevistas	Son utilizados para el entendimiento de procesos. Contienen preguntas estructuradas más específicas que los cuestionarios para obtener información concreta y concisa de las evidencias según los criterios establecidos para la auditoría.
Hojas de cálculo	Se ha convertido en la herramienta esencial en las auditorías. Es utilizada para realizar matrices, cronogramas u otras herramientas como por ejemplo, las de identificación de riesgos, las cuales tienen la finalidad de especificar aquellos riesgos a las que se expone el área auditada o los diferentes procesos por evaluar en la auditoría. Para mantener su orden y control, suele contener marcas propias de cada auditoría para establecer las versiones, participantes y estado de la auditoría.
Cronograma de actividades de auditoría	Su funcionalidad es programar y dar seguimiento a las actividades, al planificar las tareas de cada colaborador. Esto permite el cumplimiento de las actividades y la detección de posibles desviaciones.

Nota. Información tomada de Auditool (2021) y Morales (2021).

2.2. Auditoría de Tecnologías de Información

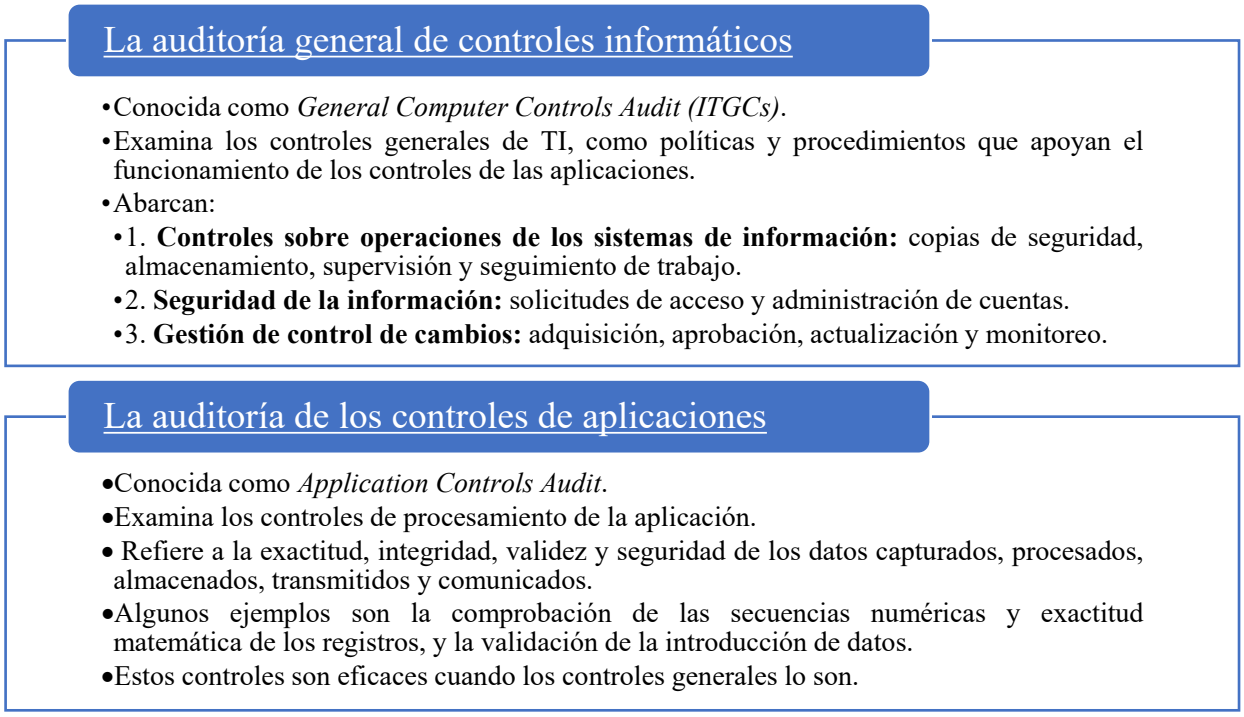
Antes de iniciar con la descripción del concepto de auditoría de tecnologías de información es importante aclarar: *¿Cuál es la diferencia entre sistema de información y tecnología de información?* Por una parte, un sistema de información es la combinación de las actividades directivas, estratégicas y operativas que intervienen en la gestión de la información. Se compone por personas, procesos y tecnología de información. Por otra parte, la tecnología de información es un componente de un sistema de información, el cual incluye hardware, software, comunicación y demás aspectos para almacenar, procesar, transmitir y producir información (Otero, 2019).

Ahora bien, una vez aclarado el concepto de tecnología de información, se procede con la descripción de auditorías de tecnologías de información. Si el término de *auditoría* hace referencia a aquel proceso o revisión sistemática de obtener evidencias objetivas y evaluarlas para determinar su grado de cumplimiento según los criterios establecidos, entonces la auditoría de tecnologías de información es un examen de los controles de la infraestructura de tecnología de información (TI) de una organización. Tienen el fin de evaluar las evidencias obtenidas para determinar si la tecnología de información está salvaguardando los activos, manteniendo la integridad y seguridad de los datos y operando efectivamente para alcanzar las metas u objetivos de la organización (Acuña, 2018).

Este tipo de auditoría garantiza de forma razonable que la información generada por las aplicaciones o programas sea precisa, completa y apoye la toma de decisiones. De acuerdo con Otero (2019), la auditoría de tecnologías de información se agrupa en dos dominios mostrados en la **Figura 10**.

Figura 10

Grupos de la auditoría de tecnologías de información



Nota. Información tomada de Otero (2019).

2.3.COBIT

Control Objetives for Information and Related Technologies, conocido por sus siglas en inglés como COBIT, es un marco de gobierno y gestión de las tecnologías de información de una empresa. Fue desarrollado *Information System Audit and Control Association*, conocido como ISACA.

Este marco de gobierno y gestión comprende la información y tecnología que utiliza toda la empresa para lograr sus objetivos, independientemente de dónde ocurra, es decir, que la información y la tecnología no se limitan únicamente a que el departamento de TI esté incluido (ISACA, 2018, p.13).

De acuerdo con ISACA (2018, p. 13), COBIT se encarga de las siguientes actividades:

- Definir los componentes para crear y sostener un sistema de gobierno: procesos, estructuras organizativas, políticas, procedimientos, flujos de información, cultura, comportamientos, habilidades, e infraestructura.
- Definir los factores de diseño que la empresa debería considerar para crear un sistema de gobierno.
- Tratar asuntos de gobierno mediante la agrupación de componentes de gobierno dentro de los objetivos de gobierno y gestión, los cuales pueden gestionarse según niveles de capacidad requeridos.

2.3.1. COBIT 2019

COBIT 2019 es la nueva versión de este marco de gobierno y gestión. Se basó en su versión anterior, COBIT 5. Está alineado con una serie de estándares y marcos relacionados para sustentar su posición consolidada como marco de gobierno de la tecnología y la información.

En primera instancia, de acuerdo con ISACA (2018), COBIT hace una distinción sobre gobierno y gestión. Ambas disciplinas abarcan diferentes actividades, requieren distintas estructuras organizativas y sirven para diferentes propósitos. Por un lado, el gobierno asegura:

- Las necesidades, condiciones y opciones de las partes interesados se evalúan para determinar objetivos empresariales equilibrados y acordados.
- La dirección se establece a través de la priorización y la toma de decisiones.

- El desempeño y el cumplimiento se monitorean en relación con la dirección y los objetivos acordados.

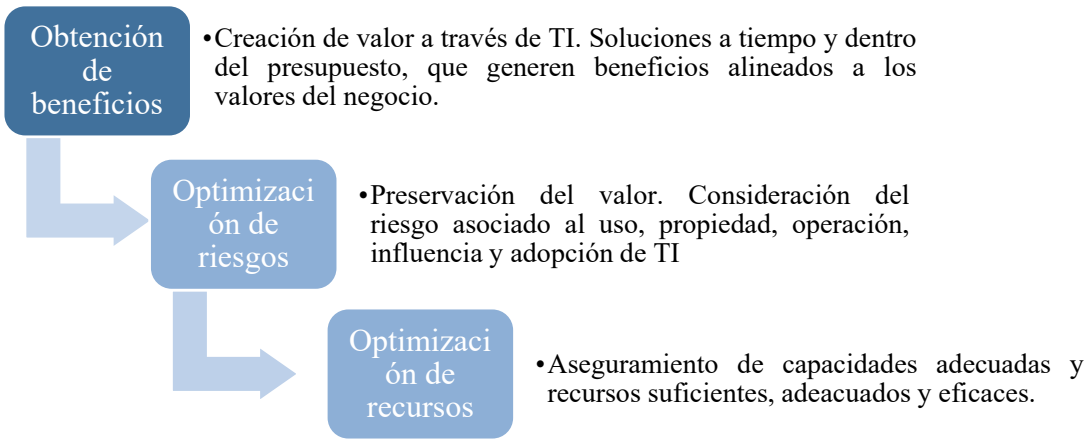
Por otro lado, la Gerencia planifica, construye, ejecuta y monitorea actividades en línea con la dirección establecida por el órgano de gobierno para alcanzar los objetivos de la empresa.

Seguidamente, COBIT 2019 implementa el concepto de *Gobierno Empresarial de la Información y Tecnología*, conocido como GETI. Este supervisa la definición e implementación de procesos, estructuras y mecanismos en la organización, para permitir a la empresa y al personal de TI desempeñar sus responsabilidades de soporte al negocio, alineación de TI y creación de valor de negocio. El contexto GETI se basa en una relación entre el Gobierno Empresarial de TI, alineación del negocio y TI, y creación de valor (ISACA, 2018).

No existe una fórmula para diseñar, implementar y mantener una GETI dentro de una organización. Por esta razón, el consejo y la Alta Gerencia adoptan las medidas GETI de acuerdo con su contexto y necesidades. Los tres principales beneficios de GETI se describen en la **Figura 11**.

Figura 11

Beneficios del GETI



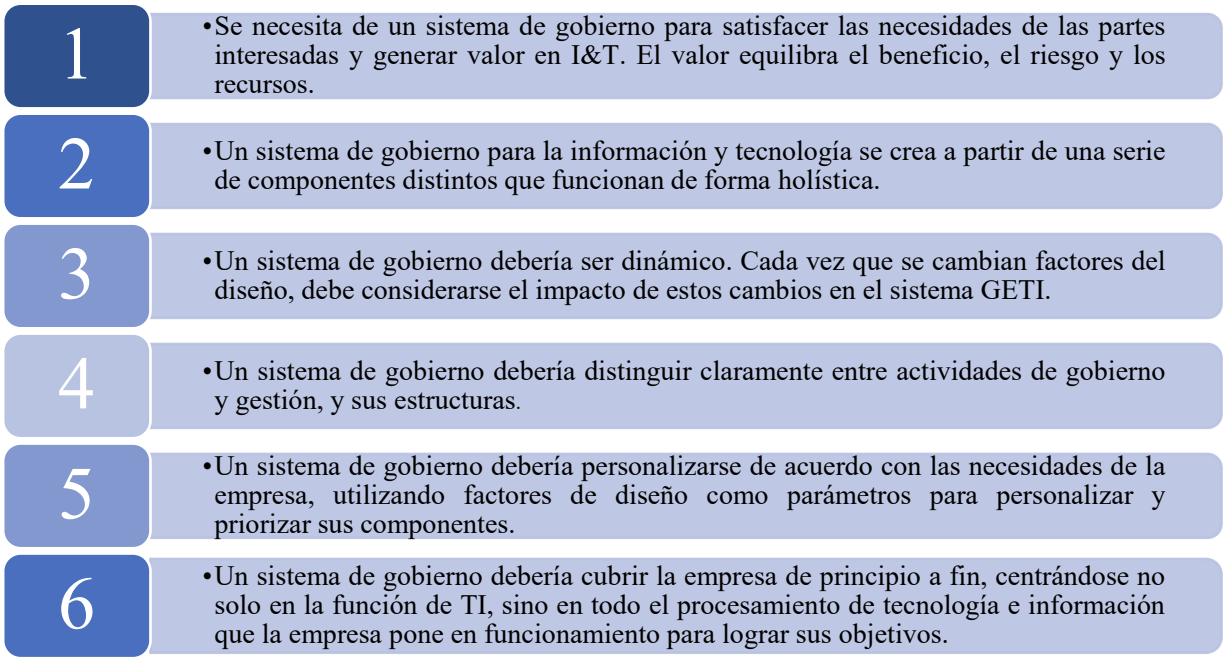
Nota. Información tomada de ISACA (2018).

2.3.2. Principios COBIT 2019

COBIT 2019 se desarrolló con base en dos series de principios. La primera serie son aquellos principios que describen los requisitos fundamentales de un sistema de gobierno para la información y tecnología de la empresa, reflejados en la **Figura 12**. La segunda serie son los principios para un marco de gobierno, el cual puede usarse para crear un sistema de gobierno en la empresa. Estos son reflejados en la **Figura 13**.

Figura 12

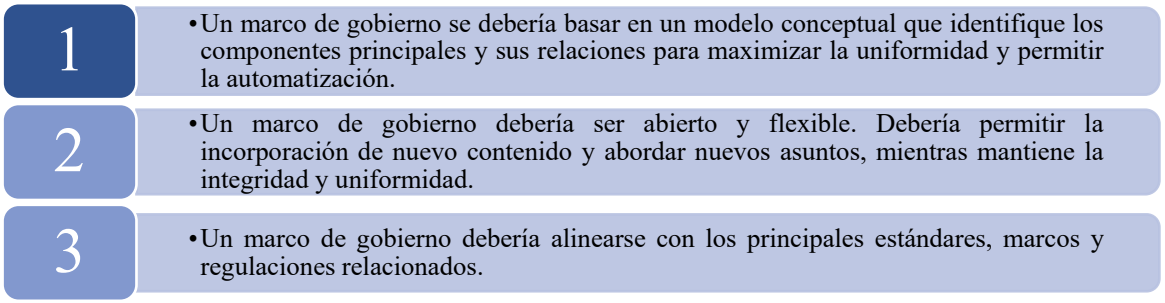
Principios para un sistema de gobierno



Nota. Información tomada de ISACA (2018).

Figura 13

Principios para un marco de gobierno



Nota. Información tomada de ISACA (2018).

2.3.3. Objetivos de gobierno y de gestión

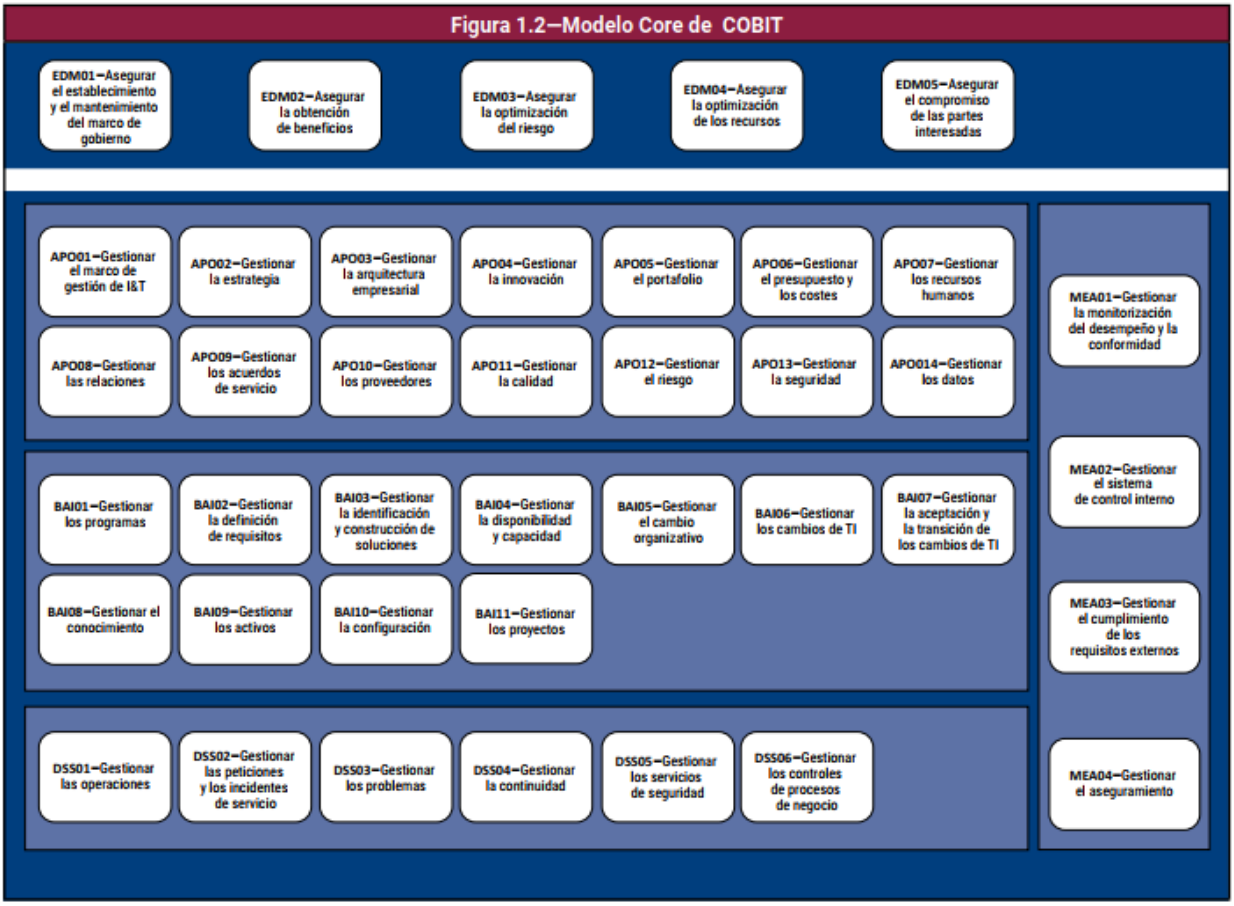
COBIT establece objetivos de gobierno y gestión para que la información y la tecnología contribuyan con los objetivos de la entidad. Cada uno de estos objetivos está relacionado con un proceso, ya sea de gobierno o de gestión, según corresponda.

Estos objetivos se agrupan en cinco dominios, tal y como lo muestra la **Figura 14**. Los objetivos de gobierno se agrupan en el dominio llamado Evaluar, Dirigir y Monitorizar (EDM). Los objetivos de gestión se agrupan en los siguientes cuatro dominios: Alinear, Planificar y Organizar (APO), Construir, Adquirir e Implementar (BAI), Entregar, Dar Servicio y Soporte (DSS), Monitorizar, Evaluar y Valorar (MEA).

En las secciones **2.3.4**, **2.3.5**, **2.3.6**, **2.3.7**, y **2.3.8** se detalla la descripción general de cada dominio, y, por cada dominio se describen los procesos considerados para el desarrollo de este proyecto.

Figura 14

Modelo Core de COBIT 2019



Nota. Tomado de ISACA (2018).

2.3.4. Evaluar, Dirigir y Monitorizar (EDM)

En el dominio Evaluar, Dirigir y Monitorizar (EDM) se evalúan las opciones estratégicas, se direcciona a la Alta Gerencia en opciones estratégicas y se monitoriza la consecución de la estrategia. Los procesos considerados para el desarrollo de este proyecto dentro de este dominio son *EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno*, y *EDM03. Asegurar la optimización del riesg*o.

2.3.4.1. EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno

El propósito de este proceso es:

> Proporcionar un enfoque consistente integrado y alineado con el enfoque de gobierno de la empresa. Las decisiones relacionadas con I&T deben hacerse en línea con las estrategias y objetivos de la empresa y para alcanzar el valor deseado. En este sentido, debe asegurarse de que los procesos relacionados con la I&T se supervisen de forma eficaz y transparente; que se cumpla con los requisitos legales, contractuales y regulatorios; y que se cumplan los requisitos de gobierno para los miembros del consejo de dirección (ISACA, 2018, p.29).

Este proceso dentro de COBIT 2019 define tres prácticas, descritas en la **Tabla 3**.

Tabla 3.

Prácticas EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno

Práctica	Descripción
EDM01.01 Evaluar el sistema de gobierno	Identificar e involucrarse continuamente con las partes interesadas, documentar los requisitos y evaluar el diseño actual y futuro del gobierno de I&T. Para ello, consta de ocho actividades.
EDM01.02 Dirigir el sistema de gobierno	Informar a los líderes sobre los principios de gobierno de I&T, obtener su apoyo, aprobación y compromiso. Guiar las estructuras, procesos y prácticas alineadas con los principios de gobierno, modelos de toma de decisiones y los niveles de autoridad acordados. Definir la información para la toma de decisiones. Para ello, consta de siete actividades.
EDM01.03 Monitorizar el sistema de gobierno	Monitorizar la eficacia y el rendimiento del gobierno de I&T de la empresa. Evaluar si el sistema de gobierno y los mecanismos están operando de forma efectiva y ofrecen una supervisión apropiada para la creación de valor. Para ello, consta de seis actividades.

Nota. Información tomada de ISACA (2018).

2.3.4.2. EDM03. Asegurar la optimización del riesgo

Este proceso tiene el siguiente propósito:

> Asegurarse de que el riesgo de negocio relacionado con la I&T no exceda el apetito y tolerancia al riesgo de la empresa, que se identifique y gestione el impacto del riesgo de I&T para el valor de negocio y que se minimicen los posibles fallos de cumplimiento (ISACA, 2018, p.41).

Este proceso dentro de COBIT 2019 define tres prácticas, descritas en la **Tabla 4**.

Tabla 4

Prácticas EDM03. Asegurar la optimización del riesgo

Práctica	Descripción
EDM03.01 Evaluar la gestión de riesgos	Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las I&T en la empresa. Considerar si el apetito al riesgo es apropiado e identificar y gestionar el riesgo para el valor de la empresa relacionado I&T. Para ello, consta de siete actividades.
EDM03.02 Dirigir la gestión de riesgos	Dirigir el establecimiento de prácticas de gestión de riesgos para ofrecer seguridad de que las prácticas de gestión de riesgos son apropiadas y que el riesgo no sobrepasa al apetito al riesgo. Para ello, consta de cinco actividades.
EDM03.03 Monitorizar la gestión de riesgos	Monitorizar las metas y las métricas clave de los procesos de gestión de riesgos. Establecer cómo las desviaciones o los problemas se identificarán, se les dará seguimiento y se comunicarán para su solución. Para ello, consta de cuatro actividades.

Nota. Información tomada de ISACA (2018).

2.3.5. Alinear, Planificar y Organizar (APO)

Alinear, Planificar y Organizar (APO) aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología. Los procesos considerados para el desarrollo de este

proyecto dentro del dominio son *APO09. Gestionar los acuerdos de servicio*, y *APO13. Gestionar la seguridad*.

2.3.5.1. APO09. Gestionar los acuerdos de servicio

Este proceso tiene el siguiente propósito: "Asegurarse de que los productos, servicios y niveles de servicio de I&T satisfagan las necesidades actuales y futuras de la empresa" (ISACA, 2018, p. 113).

Este proceso dentro de COBIT 2019 considera cinco prácticas, las cuales se describen en la **Tabla 5**.

Tabla 5

Prácticas APO09. Gestionar los acuerdos de servicio

Práctica	Descripción
APO09.01. Identificar los servicios de TI	Analizar los requisitos del negocio y hasta qué punto los servicios habilitados por TI y los niveles de servicio apoyan los procesos del negocio. Analizar y acordar los servicios y niveles de servicio potenciales con el negocio. Comparar los niveles de servicio potenciales con el portafolio actual de servicios; identificar opciones nuevas o modificadas de servicios o de nivel de servicio.
APO09.02. Catalogar los servicios habilitados por TI	Definir y mantener uno o más catálogos de servicios para grupos objetivos relevantes. Publicar y mantener servicios activos habilitados por I&T en los catálogos de servicios.
APO09.03. Definir y preparar acuerdos de servicio	Definir y preparar acuerdos de servicio basados en las opciones de los catálogos de servicio. Incluir acuerdos operativos internos.
APO09.04. Monitorizar y reportar los niveles de servicio	Monitorizar los niveles de servicio, informar sobre los logros e identificar tendencias. Ofrecer información gerencial apropiada para ayudar a la gestión del rendimiento.
APO09.05. Revisar los acuerdos y los controles de servicio	Realizar revisiones periódicas de los acuerdos de servicio y revisarlos cuando sea necesario.

Nota. Información tomada de ISACA (2018).

2.3.5.2. APO13. Gestionar la seguridad

El propósito de este proceso es: "Mantener el impacto y la ocurrencia de incidentes de seguridad de la información dentro de los niveles de apetito de riesgo de la empresa" (ISACA, 2018, p.139).

Este proceso dentro de COBIT 2019 considera tres prácticas, descritas en la **Tabla 6**.

Tabla 6

Prácticas APO13. Gestionar la seguridad

Práctica	Descripción
APO13.01. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)	Establecer y mantener un sistema de gestión de seguridad de la información (SGSI) que proporcione un enfoque estándar, formal y continuo para la gestión de la seguridad de la información, mediante la habilitación de tecnología segura y procesos de negocio alineados con los requisitos del negocio.
APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	Mantener un plan de seguridad de la información que describa cómo debe manejarse el riesgo de seguridad de la información y cómo se debe alinear con la estrategia y la arquitectura de la empresa. Asegurar que las recomendaciones para implementar mejoras a la seguridad se basen en casos de negocio aprobados, implementados como parte integral del desarrollo de servicios y soluciones, y que operen como parte integral de la operación del negocio.
APO13.03 Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	Mantener y comunicar periódicamente la necesidad y los beneficios de una mejora continua de seguridad de la información. Recopilar y analizar datos sobre el sistema de gestión de seguridad de la información (SGSI) y mejorar su efectividad. Corregir los incumplimientos para evitar la recurrencia.

Nota. Información tomada de ISACA (2018).

2.3.6. Construir, Adquirir e Implementar (BAI)

Construir, Adquirir e Implementar (BAI) se encarga de la definición, adquisición e implementación de las soluciones de información y tecnología, y su integración en los procesos de

negocio. Los procesos considerados para el desarrollo de este proyecto dentro del dominio son *BAI06. Gestionar los cambios de TI*, y *BAI09. Gestionar los activos*.

2.3.6.1. BAI06. Gestionar los cambios de TI

El propósito de este proceso es: "Facilitar una ejecución de cambios rápida y confiable para el negocio. Mitigar el riesgo de afectar negativamente la estabilidad o integridad del entorno que se ha modificado" (ISACA, 2018, p.193).

Este proceso dentro de COBIT 2019 considera cuatro prácticas, las cuales se describen en la **Tabla 7**.

Tabla 7

Prácticas BAI06. Gestionar los cambios de TI

Práctica	Descripción
BAI06.01 Evaluar, priorizar y autorizar solicitudes de cambio	Evaluar las solicitudes de cambio para determinar su impacto en procesos de negocio y de I&T; evaluar si el cambio afectará negativamente e introducirá riesgos. Asegurarse de que los cambios se registran, priorizan, clasifican, evalúan, autorizan, planifican y programan. Para ello, consta de siete actividades.
BAI06.02 Gestionar cambios de emergencia	Gestionar cuidadosamente los cambios de emergencia. Asegurar que el cambio de emergencia está controlado y seguro. Verificar que los cambios de emergencia se evalúan y se autorizan. Para ello, consta de cuatro actividades.
BAI06.03 Hacer seguimiento e informar sobre cambios de estado	Mantener un sistema de seguimiento e informes para documentar los cambios rechazados y comunicar el estado de los cambios aprobados, en proceso y finalizados. Asegurarse de que los cambios aprobados se implementan según lo previsto. Para ello, consta de cuatro actividades.
BAI06.04 Cerrar y documentar los cambios	Siempre que se implementen cambios, actualizar la solución, la documentación del usuario y los procedimientos afectados por el cambio. Para ello, consta de tres actividades.

Nota. Información tomada de ISACA (2018)

2.3.6.2. BAI09. Gestionar los activos

El propósito de este control es: "Tener en cuenta todos los activos de I&T y optimizar el valor proporcionado por su uso" (ISACA, 2018, p. 209).

Este proceso dentro de COBIT 2019 considera cinco prácticas, las cuales se describen en la **Tabla 8**.

Tabla 8

Prácticas BAI09. Gestionar los activos

Práctica	Descripción
BAI09.01 Identificar y registrar los activos actuales	Mantener un registro actualizado y preciso de todos los activos de TI requeridos para ofrecer servicios y que son propiedad o están controlados por la organización a la espera de un futuro beneficio (incluidos recursos con valor económico, como hardware o software). Asegurar el alineamiento con la gestión de configuración y la gestión financiera.
BAI09.02 Gestionar activos críticos	Identificar los activos que son críticos para garantizar la capacidad de prestación del servicio. Maximizar su confiabilidad y disponibilidad para apoyar las necesidades de negocio.
BAI09.03: Gestionar el ciclo de vida del activo	Gestionar los activos desde su adquisición hasta su disposición. Asegurar que los activos se usen con la mayor eficacia y eficiencia posible y se puedan contabilizar y proteger físicamente hasta su correcta retirada.
BAI09.04 Optimizar el valor de los activos	Revisar periódicamente la base de activos para identificar formas de optimizar valor y mantener el alineamiento con las necesidades del negocio.
BAI09.05 Gestionar las licencias	Gestionar las licencias de software para mantener el número de licencias óptimo y respaldar las necesidades del negocio. Garantizar que el número de licencias en propiedad sea suficiente para cubrir el software instalado en uso.

Nota. Información tomada de ISACA (2018).

2.3.7. Entregar, Dar Servicio y Soporte (DSS)

Entregar, Dar Servicio y Soporte (DSS) aborda la ejecución operativa y el soporte de los servicios de información y tecnología. Los procesos considerados para el desarrollo del proyecto son *DSS02. Gestionar las peticiones y los incidentes de servicio,* y *DSS03. Gestionar los problemas*.

2.3.7.1. DSS02. Gestionar las peticiones y los incidentes de servicio

Este proceso tiene el propósito de:

> Lograr una mayor productividad y minimizar las interrupciones mediante la resolución rápida de consultas e incidencias de los usuarios. Evaluar el impacto de los cambios y hacer frente a los incidentes del servicio. Resolver las solicitudes de los usuarios y restaurar el servicio como respuesta ante incidentes (ISACA, 2018, p. 237).

Este proceso dentro de COBIT 2019 considera cinco prácticas, descritas en la **Tabla 9**.

Tabla 9

Prácticas DSS02. Gestionar las peticiones y los incidentes de servicio

Práctica	Descripción
DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio	Definir esquemas de clasificación y modelos de incidentes y de peticiones de servicio.
DSS02.02 Registrar, clasificar y priorizar las peticiones e incidentes	Identificar, registrar y clasificar las peticiones de servicio y los incidentes y asignarles una prioridad, de acuerdo con la criticidad para el negocio y los acuerdos de servicio.
DSS02.03 Verificar, aprobar y resolver peticiones de servicio	Seleccionar los procedimientos apropiados para peticiones y verificar que las solicitudes de servicio cumplan con los criterios de solicitud definidos. Obtener aprobación, si se requiere, y satisfacer las solicitudes.
DSS02.04 Investigar, diagnosticar y asignar incidentes	Identificar y registrar los síntomas de los incidentes, determinar las causas posibles y asignarlos para su resolución.
DSS02.05 Resolver y recuperarse de los incidentes	Documentar, aplicar y probar las soluciones definitivas o temporales (workarounds) identificadas. Realizar acciones de recuperación para restaurar el servicio relacionado con I&T.
DSS02.06 Cerrar las peticiones de servicio y los incidentes	Verificar la solución satisfactoria del incidente y/o el cumplimiento de la petición y su cierre.
DSS02.07 Hacer seguimiento al estado y producir informes	Hacer seguimiento, analizar e informar regularmente sobre los incidentes y el cumplimiento de las solicitudes. Examinar tendencias para proporcionar información para la mejora continua.

Nota. Información tomada de ISACA (2018).

2.3.7.2. DSS03. Gestionar los problemas

Este proceso tiene el propósito de:

> Aumentar la disponibilidad, mejorar los niveles de servicio, reducir los costes y atender mejor las necesidades del cliente y lograr su satisfacción mediante una reducción del número de problemas operativos, e identificar las causas raíz como parte de la resolución de problemas (ISACA, 2018, p. 243).

Este proceso dentro de COBIT 2019 considera cinco prácticas, descritas en la **Tabla 10**.

Tabla 10

Prácticas DSS03. Gestionar los problemas

Práctica	Descripción
DSS03.01 Identificar y clasificar los problemas	Definir e implementar criterios y procedimientos para identificar e informar sobre los problemas. Incluir clasificación, categorización y priorización del problema. Para ello, consta de seis actividades.
DSS03.02 Investigar y diagnosticar problemas	Investigar y diagnosticar problemas con la ayuda de expertos en la materia, para evaluar y analizar su causa raíz. Para ello, consta de tres actividades.
DSS03.03 Presentar los errores conocidos	Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores, documentar soluciones temporales e identificar soluciones potenciales. Para ello, consta de dos actividades.
DSS03.04 Resolver y cerrar los problemas	Identificar e iniciar soluciones sostenibles dirigidas a la causa raíz del problema. Presentar solicitudes de cambio a través del proceso de gestión de cambio establecido, si es necesario, para resolver los errores. Asegurarse de que el personal afectado conoce las medidas adoptadas y los planes desarrollados. Para ello, consta de seis actividades.
DSS03.05 Realizar una gestión proactiva de los problemas	Recopilar y analizar los datos operacionales para identificar las tendencias que están emergiendo que puedan indicar problemas. Guardar los registros de problemas para su evaluación. Para ello, consta de seis actividades.

Nota. Información tomada de ISACA (2018).

2.3.8. Monitorizar, Evaluar y Valorar (MEA)

Monitorizar, Evaluar y Valorar (MEA) aborda la monitorización y la conformidad de la información y la tecnología con los objetivos de desempeño y de control interno, así como los requerimientos externos. Los procesos considerados para el desarrollo del proyecto son *MEA02. Gestionar el sistema de control interno*, y *MEA03. Gestionar el cumplimiento de los requisitos externos*.

2.3.8.1. MEA02. Gestionar el sistema de control interno

El propósito de este proceso es:

> Dar información transparente a las partes interesadas clave sobre la idoneidad del sistema de controles internos que permita, proporcionar confianza en las operaciones, confianza en el logro de los objetivos de la empresa y una comprensión adecuada del riesgo residual (ISACA, 2018, p.279).

Este proceso dentro de COBIT 2019 tiene cuatro prácticas, descritas en la **Tabla 11**.

Tabla 11.

Prácticas MEA02. Gestionar el sistema de control interno

Práctica	Descripción
MEA02.01 Supervisar los controles internos	Supervisar, hacer benchmarking y mejorar continuamente el entorno y marco de control de I&T, para alcanzar los objetivos de la organización. Para ello, consta de siete actividades.
MEA02.02 Revisar la eficacia de los controles del proceso de negocio	Revisar la operación de los controles. Incluir actividades para mantener evidencia de su operación efectiva. Estas evidencias garantizan el cumplimiento con requisitos de negocio, regulatorios y sociales. Para ello, consta de cinco actividades.
MEA02.03 Realizar autoevaluaciones de control	Alentar a la gerencia y dueños de procesos para que mejoren los controles mediante un programa continuo de autoevaluación que evalúe la integridad y efectividad del control. Para ello, consta de siete actividades.

Práctica	Descripción
MEA02.04 Identificar e informar las deficiencias de control	Identificar las deficiencias de control y analizar e identificar sus causas raíz. Escalar las deficiencias de control e informar a las partes interesadas. Para ello, consta de seis actividades.

Nota. Información tomada de ISACA (2018).

2.3.8.2. MEA03. Gestionar el cumplimiento de los requisitos externos

Este proceso tiene el propósito de: "Asegurarse de que la empresa cumpla con todos los requisitos externos aplicables" (ISACA, 2018, p. 285).

Este proceso dentro de COBIT 2019 tiene cuatro prácticas, descritas en la **Tabla 12**.

Tabla 12

Prácticas MEA03. Gestionar el cumplimiento de los requisitos externos

Práctica	Descripción
MEA03.01 Identificar los requisitos externos de cumplimiento	Supervisar de forma continua los cambios en las leyes y regulaciones locales e internacionales, así como otros requisitos externos. Identificar las obligaciones para el cumplimiento desde una perspectiva de I&T. Para ello, consta de siete actividades.
MEA03.02 Optimizar la respuesta a los requisitos externos	Revisar y ajustar políticas, principios, estándares, procedimientos y metodologías para asegurarse de abordar requisitos legales, regulatorios y contractuales. Considerar la adopción y adaptación de los estándares de industria, códigos y guías de buenas prácticas. Para ello, consta de dos actividades.
MEA03.03 Confirmar el cumplimiento externo	Confirmar el cumplimiento de las políticas, principios, estándares, procedimientos y metodologías con los requisitos legales, regulatorios y contractuales. Para ello, consta de cinco actividades.
MEA03.04 Obtener aseguramiento de cumplimiento externo	Obtener e informar del aseguramiento del cumplimiento y adherencia a las políticas, principios, estándares, procedimientos y metodologías. Confirmar que las acciones correctivas para abordar las brechas de cumplimiento se cierren de manera oportuna. Para ello, consta de seis actividades.

Nota. Información tomada de ISACA (2018).

2.4. SUGEF

Dado que las auditorías que realiza el equipo de TI del área de *Management Consulting*, pueden ser relacionadas con el acuerdo 14-17(abordado en la sección **2.5**) de la SUGEF, es importante dar una descripción general de qué se tratan estos dos aspectos.

La Superintendencia de Entidades Financieras, conocida como SUGEF es un ente supervisor modelo que tiene como objetivo: "Velar por la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional, con estricto apego a las disposiciones legales y reglamentarias y de conformidad con las normas, directrices y resoluciones que dicte la propia institución, todo en salvaguarda del interés de la colectividad" (SUGEF, s.f, sitio oficial).

La SUGEF supervisa y fiscaliza, mediante un enfoque basado en riesgos, a los intermediarios financieros de Costa Rica, así como a personas físicas y jurídicas encomendadas por ley, en donde demuestra cumplimiento de los requisitos de su Sistema de Gestión de la Calidad y mejora continua de sus procesos en línea con su estrategia (SUGEF, s.f).

Entre las funciones que realiza esta entidad destacan las siguientes definidas por SUGEF (s.f):

- Velar por la estabilidad, solidez y funcionamiento eficiente del sistema financiero nacional.
- Fiscalizar las operaciones y actividades de las entidades bajo su control
- Dictar normas generales necesarias para el establecimiento de prácticas bancarias sanas.
- Establecer categorías de intermediarios financieros de acuerdo con el tipo, tamaño y riesgo.
- Fiscalizar operaciones de los entes autorizados por el Banco Central de Costa Rica que participan en el mercado cambiario.
- Dictar normas generales y directrices necesarias para promover la estabilidad, solvencia y transparencia en las operaciones de las entidades fiscalizadas.
- Presentar informes de sus actividades de supervisión y fiscalización al Consejo Nacional de Supervisión del Sistema Financiero.
- Cumplir con otras funciones y atributos que le correspondan, según las leyes, reglamentes y demás disposiciones.

2.5. Acuerdo SUGEF 14-17

El acuerdo SUGEF 14-17 hace referencia al Reglamento sobre la Gestión de la Tecnología de Información, el cual: "…define los criterios y metodología para la evaluación y calificación de la gestión de la tecnología de información para las entidades fiscalizadas por la Superintendencia General de Entidades Financieras (SUGEF)" (Acuerdo SUGEF 14-17, 2020, p.1).

El objetivo del reglamento sobre la gestión de la tecnología de información es establecer los requerimientos mínimos para la gestión de la tecnología de información que deben ser acatados por las entidades supervisadas y reguladas del sistema.

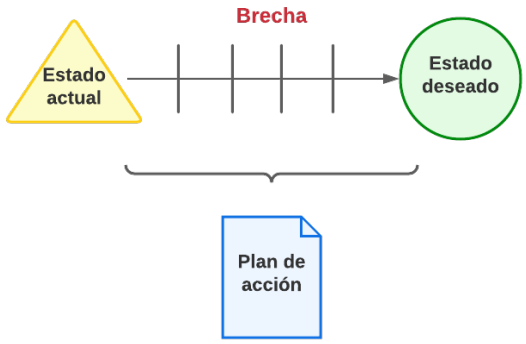
2.6. Análisis de brecha

El análisis de brecha, conocido en inglés como *GAP Analysis*, es una herramienta de evaluación que le permite a una organización comparar su situación actual con la que desea alcanzar en un futuro, de manera que proporciona a la organización un visión de las áreas de mejora, tal y como lo muestra la **Figura 15.** Es útil para establecer una diferencia entre las preguntas "¿Qué queremos?" y "¿Qué necesitamos?" (*ITIL® Continual Service Improvement,* 2011, p.79).

De acuerdo con lo establecido por *ITIL® Continual Service Improvement* (2011), el análisis de brecha determina, documenta y aprueba la diferencia entre los requisitos o expectativas de la empresa y sus capacidades actuales. Una vez entendida la expectativa de la empresa, es posible compararla con su nivel de rendimiento y funcionamiento actual. El análisis de brecha puede realizarse a partir de diferentes perspectivas, tales como la organización, la dirección de la empresa, los procesos empresariales, y la tecnología de información.

Figura 15

Descripción general del análisis de brecha



Nota. Elaboración propia a partir de información tomada de *ITIL® Continual Service Improvement* (2011).

De acuerdo con Kim y Ji (2018), el proceso de análisis de brecha consta de cuatro pasos claves, mostrados en la **Figura 16**. Cada paso es descrito en las **2.6.1**, **2.6.2**, **2.6.3**, **2.6.4**, según lo establecido por Kim y Ji (2018), y Leonard y Bottorff (2022).

Figura 16

Proceso del análisis de brecha

Nota. Elaboración propia a partir de información tomada de Kim y Ji (2018), y Leonard y Bottorff (2022).

2.6.1. Identificación de la situación actual

Antes de ejecutar un plan, es importante identificar la situación actual de los procesos, tecnologías, personas, áreas, o cualquier otro elemento sometido al análisis de brecha. Este paso busca describir, de forma detallada y concisa, los componentes y formas de operar de los elementos involucrados en el análisis de brecha. Responde a la pregunta *¿Cómo se realiza actualmente?*

2.6.2. Determinación de la situación deseada

Este paso consiste en definir la situación deseada de los elementos involucrados en el análisis de brecha. Se procede a establecer objetivos o metas sobre cómo deben ser, operar o desarrollarse los elementos identificados. Responde a la pregunta *¿Hacia dónde se quiere llegar?*

2.6.3. Análisis de brechas existentes

Este paso consiste en identificar y analizar las brechas existentes entre la situación actual y la situación deseada, con el propósito reconocer y comprender las oportunidades de mejora o factores claves del cambio, para determinar el plan de acción adecuado.

2.6.4. Establecimiento de un plan de acción

Este es el último paso y consiste en elaborar un listado de las acciones correctivas o acciones de mejora consideradas para cerrar las brechas previamente identificadas entre la situación actual y la situación deseada. Cada acción debe ser específica y objetiva con el análisis de brecha desarrollado. De acuerdo con Alexander (2019), un plan de acción puede contener secciones como: descripción del elemento al cual se aplicará el análisis, descripción del estado actual y deseado, desglose de las brechas identificadas, explicación de las acciones correctivas, dependencias, prioridades, estados, y otras consideraciones como limitaciones, suposiciones o riesgos.

2.7. Análisis financiero

El análisis financiero es un proceso que comprende la recopilación, interpretación, comparación y estudio de los estados financieros y datos operacionales de un negocio. Implica el cálculo y la interpretación de inversiones, porcentajes, tasas, tendencias e indicadores, los cuales sirven para evaluar el desempeño financiero y operacional de una organización para la posterior toma de decisiones relacionadas a actividades financieras (Ortiz, 2018).

Un análisis financiero puede incluir una serie de indicadores para garantizar la viabilidad y rentabilidad de las operaciones evaluadas. Un ejemplo común de indicador financiero es el Retorno de Inversión, conocido en inglés como *Return on Investment (ROI)*. Es utilizado para comprender la rentabilidad de una inversión al calcular cuánta utilidad genera el dinero invertido dentro de una organización (Ferrell et al, 2010).

2.8. Plan piloto

Para de responder a *¿Qué es un plan piloto?*, es importante comprender los dos términos que lo componen, según lo establecido por la Real Academia Española:

- Plan: “Intención, proyecto… Escrito en que sumariamente se precisan los detalles para realizar una obra”.
- Piloto: “En aposición, indica que la cosa designada por el nombre que le precede funciona como modelo o con carácter experimental”.

Entonces, un plan piloto puede ser considerado como un documento o escrito en donde se desglosan los detalles para desarrollar una obra con carácter experimental.

De acuerdo con Microsoft (2022), una prueba piloto es una oportunidad para proporcionar evidencia de que una solución propuesta resuelve los problemas empresariales identificados. Sirve para aumentar la probabilidad de la correcta adopción de una solución. Los proyectos o pruebas piloto pueden aplicarse a múltiples oportunidades, tales como: nuevos conceptos, productos o servicios de innovación, iniciativas punteras o de vanguardia, determinación de viabilidades. Estos pueden dirigirse a sectores o áreas específicas dentro de una organización (Zbrodoff, 2012; Blackburn et al, 2020).

Las pruebas o proyectos piloto requieren de una debida planeación, ejecución y documentación de resultados. Microsoft (2022) establece que se debe realizar una preparación y recomienda la creación de una especificación o plan. *Google for Education* (s.f) ha definido una guía para realizar pruebas o proyectos piloto de sus herramientas o tecnologías, donde destaca la definición de los objetivos, tiempos de duración, selección de alcance, lugar, involucrados, y definición de métricas para evaluar la información resultante de la prueba o proyecto piloto. Además de estos aspectos, Microsoft (2022) destaca la realización de un informe final para documentar el cumplimiento o no de la solución como viable para responder a la problemática, lecciones aprendidas, así como resultados valiosos de la prueba piloto.

Dado lo anterior, en la **Figura 17** se describen algunos aspectos por considerar en el desarrollo de un plan piloto.

Figura 17

Documentación de un plan piloto

Objetivos	Duración	Selección	Medición	Informe
•Definición de objetivos claves para evaluar la efectividadde la actividad piloto. •Deben ser medibles, dirigios a los involucrados y proveer respuesta para la decisión final.	•Definición de los periodos de tiempo de inicio y de finalización de la actividad piloto.	•Descripción de cómo será la actividad piloto, es decir, el alcance de la misma. •Definición detallada del lugar y los involucrados.	•Definición sobre cómo se medirá la información y datos obtenidos de la actividad piloto. •Se pueden estbalecer métodos como encuestas, informes, observaciones, etc.	•Escritura de los resultados obtenidos y lecciones aprendidas de la prueba piloto. •Respuesta si la prueba piloto es viable o no para la orgnaización.

Nota. Información tomada de Microsoft (2022) y Google (s.f).

2.9. ISO 3100

Para la definición de los impactos de riesgos, los cuales son documentados en las fichas de auditoría, es importante utilizar estándares reconocidos como lo es ISO 3100. ISO 3100 define los términos y condiciones, principios, marco de referencia, y proceso relacionado con el riesgo, el cual se considera una desviación respecto a lo previsto. El objetivo es brindar directrices para gestionar el riesgos al que enfrentas las organizaciones, adaptadas al contexto y necesidades de la organización. (Organización Internacional de Normalización [ISO], 2018)

Para efectos de este proyecto, es importante a destacar en el marco de referencia de la gestión del riesgo, la comprensión de la organización y su contexto, dentro de la etapa de diseño. El análisis del contexto externo permite identificar factores sociales, culturales, políticos, leales, reglamentarios, financieros, tecnológicos, económicos y ambientales (Organización Internacional de Normalización [ISO], 2018), los cuales podrían ser considerados impactos dependiendo del alcance, contexto y necesidades del cliente auditado.

3. MARCO METODOLÓGICO

En este capítulo se desarrollan todos los elementos necesarios contemplados dentro del marco metodológico del proyecto planteado para el trabajo final de graduación. En el marco metodológico se desarrollan aspectos como el tipo, enfoque, alcance y diseño de la investigación, fuentes de información, sujetos de investigación, muestras, variables, e instrumentos llevados a cabo para completar la investigación. Asimismo, se define el procedimiento metodológico con una especificación de cada una de sus fases, el cual es utilizado para guiar el desarrollo del proyecto.

3.1. Tipo de Investigación

Existen dos tipos de investigación científica: la investigación pura y la investigación aplicada. A continuación, se describe cada uno de ellos de acuerdo con lo escrito por Ñaupas et al (2014), y se procede con la selección del tipo más apto para este proyecto.

3.1.1. Investigación pura

La investigación pura, también conocida como investigación básica o fundamental, surgió de la curiosidad científica por descubrir los misterios del origen del universo, la vida natural y humana, en donde se utilizaba la observación, la imaginación y el razonamiento lógico como métodos de investigación. Esta investigación recibe el nombre de *pura*, dado al efecto de desinterés por un objetivo adquisitivo, pues su motivación es la curiosidad. También, recibe el nombre de básica porque sirve de cimiento a la investigación aplicada o tecnológica. Y, recibe el nombre de fundamental porque es esencial para el desarrollo de la ciencia.

Esta investigación tiene tres niveles: exploratorio, descriptivo y explicativo. El nivel exploratorio tiene el fin de buscar información con el propósito de formular problemas e hipótesis para una investigación más profunda de nivel explicativo. El nivel descriptivo tiene como objetivo recopilar datos e información sobre características, propiedades, aspectos, dimensiones, clasificaciones, otros, sobre objetos, personas, agentes, instituciones y procesos naturales o sociales. El nivel explicativo es complejo, profundo y riguroso, cuyo objetivo es la verificación de hipótesis, descubrimiento de nuevas leyes científicas, leyes sociales y microteorías sociales que expliquen las relaciones causales de las propiedades de los hechos o eventos de un sistema o proceso.

3.1.2. Investigación aplicada

La investigación aplicada o tecnológica está orientada a resolver objetivamente los problemas de los procesos de producción, distribución, circulación y consumo de bienes y servicios, de cualquier actividad humana de carácter industrial, de infraestructura, comercial, servicios, de comunicación, entre otros. Recibe el nombre de aplicada porque, con la base en la investigación pura, se formulan problemas e hipótesis de trabajo para resolver los problemas de la vida productiva de la sociedad. Asimismo, recibe el nombre de tecnológica porque su producto no es un conocimiento puro, sino un conocimiento tecnológico.

Esta investigación surge de la necesidad de mejorar, perfeccionar u optimizar el funcionamiento de los sistemas, procedimientos, normas, reglas, entre otros aspectos, dado los avances relacionados con la ciencia y tecnología.

3.1.3. Tipo de investigación seleccionado

Para este trabajo se seleccionó la investigación aplicada. Esto porque el trabajo busca resolver de forma objetiva una problemática específica, relacionada con las herramientas utilizadas por el equipo de TI durante el proceso de auditoría de TI. De igual forma, el trabajo pretende entregar un producto en específico que responda a mejorar funcionamiento de las herramientas dentro del proceso respectivo.

3.2. Enfoque de Investigación

De acuerdo con Hernández et al (2014), existen enfoques tipos de investigación: la investigación cualitativa, cuantitativa y mixta. Estos son posibles elecciones para enfrentar problemas de investigación y generar conocimiento A continuación, se define cada enfoque de acuerdo con lo expuesto por Hernández et al (2014). Posteriormente, se justifica la selección del enfoque de investigación para este trabajo.

3.2.1. Investigación Cuantitativa

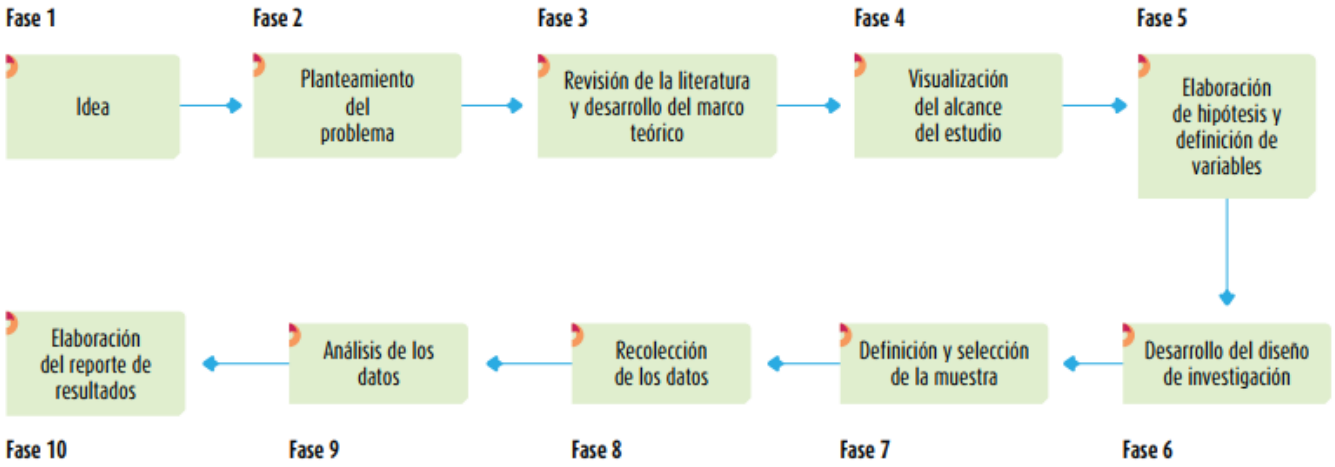
La investigación cuantitativa utiliza la recolección de datos para probar hipótesis utilizando la medición numérica y el análisis estadístico para establecer pautas de comportamiento y probar teorías. Es probatorio y secuencial, cada etapa precede a la siguiente y no se pueden saltar pasos.

Los estudios cuantitativos se interpretan por medio de predicciones iniciales, establecidas en las hipótesis, y de estudios o teorías previas.

La investigación cuantitativa sigue una serie de pasos representados en la **Figura 18**. Parte de una idea, la cual es delimitada. Luego, se derivan objetivos y preguntas, y se revisa la literatura para la perspectiva teórica. Seguido de esto, se establecen hipótesis y variables, y se define un plan para medirlas. Finalmente, las variables se analizan con métodos estadísticos y se extraen las conclusiones.

Figura 18

Proceso cuantitativo



Nota. Tomado de Hernández et al (2014).

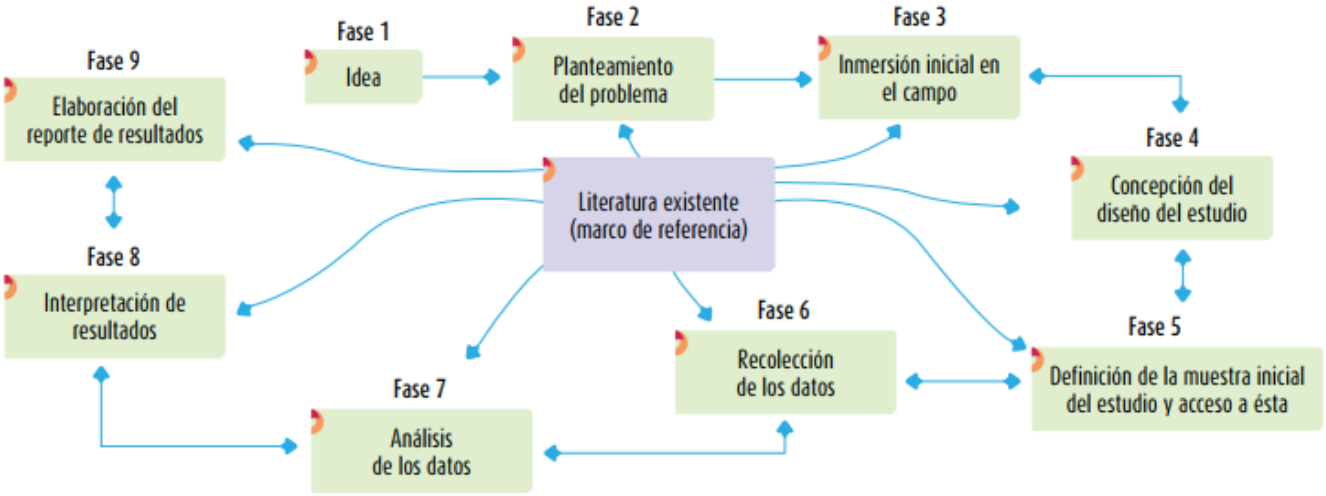
3.2.2. Investigación Cualitativa

La investigación cualitativa utiliza la recolección y análisis de datos para afinar las preguntas de investigación o revelar interrogantes en el proceso de interpretación. A diferencia de los estudios cuantitativos, en donde las preguntas e hipótesis preceden a la recolección y análisis de datos, la investigación cualitativa puede desarrollar preguntas antes, durante y después de la recolección y análisis de datos, lo cual da libertad al investigador de descubrir las preguntas de investigación más importantes y después perfeccionarlas para responderlas.

El proceso de la investigación cualitativa, representado en la **Figura 19**, es dinámico entre los hechos y su interpretación. Es un proceso circular en donde la secuencia no es siempre la misma. El investigador comienza examinando los hechos y en el proceso desarrolla una teoría coherente para representar lo observado. Se utilizan métodos de recolección de datos no estandarizados para obtener perspectivas de los involucrados en la investigación.

Figura 19

Proceso cualitativo



Nota. Tomado de Hernández et al (2014).

3.2.3. Investigación Mixta

La investigación mixta es la combinación entre la investigación cuantitativa y cualitativa. Son un conjunto de procesos sistemáticos, empíricos y críticos de investigación, los cuales implican la recolección y análisis de datos cuantitativos y cualitativos, con el objetivo de obtener una visión más completa y mayor entendimiento del fenómeno bajo estudio.

3.2.4. Enfoque de Investigación Seleccionado

El enfoque de investigación seleccionado para este trabajo fue la investigación cualitativa. Esto porque permite examinar los hechos y posteriormente desarrollar una teoría. Asimismo, permite utilizar distintos instrumentos de investigación no estandarizados para recolectar información y generar hipótesis antes, durante y después de la recolección de datos. Además, los resultados de la

investigación no son únicamente datos cuantitativos y por lo tanto, no requieren de recolección y análisis estadísticos para ser interpretados. La **Tabla 13** clarifica la justificación mencionada.

Tabla 13

Justificación del enfoque de investigación seleccionado

Enfoque	Selección	Justificación
Cuantitativo	✗	-La investigación no busca un análisis estadístico o numérico. -La investigación no trabaja con datos únicamente cuantitativos.
Cualitativo	✓	-La investigación busca comprender los hechos relacionados con las herramientas de auditoría, para posteriormente generar una teoría. -La investigación puede plantear hipótesis generales antes, durante o después de la recolección de datos. -Los métodos de recolección de datos son abiertos y no estandarizados.
Mixto	✗	-La investigación no busca un análisis estadístico o numérico. -La investigación no trabaja con datos únicamente cuantitativos.

Nota. Elaboración propia.

3.3. Alcance de la Investigación

De acuerdo con Hernández et al (2014), el alcance de la investigación resulta de la revisión literaria y de la perspectiva del estudio. Este depende de los objetivos del investigador para combinar los elementos de estudio. Más que ser una clasificación, el alcance constituye un continuo de causalidad que puede tener un estudio. El alcance de estudio depende de la estrategia de investigación, de esta manera, el diseño, los procedimientos y otros componentes del proceso son distintos de acuerdo con los cuatro tipos de alcance: exploratorio, explicativo, descriptivo y correlacional.

A continuación, se describen los alcances de investigación según lo establecido por Hernández et al (2014), y se selecciona el alcance apropiado para el proyecto.

3.3.1. Alcances de la investigación

La **Figura 20** describe los alcances de investigación descritos por Hernández et al (2014).

Figura 20

Alcances de la investigación

Exploratorio

- Su objetivo es examinar un tema o problema de investigación poco estudiado, del cual se tienen dudas o no ha sido abordado antes.
- Sirve para familiarizarse con fenómenos desconocidos. Determina e identifica tendencias, áreas, ambientes, contextos, relaciones, otros.

Descriptivo

- Busca especificar las propiedades, características y perfiles de las personas, grupos, comunidades, procesos, objetos o fenómenos.
- Pretende medir y recoger información sobre conceptos o información de las variables de estudio. No buscan indicar cómo se relacionan.

Correlacional

- Asocia variables mediante un patrón predecible para un grupo o población.
- Su finalidad es conocer la relación o grado de asociación que existe entre dos o más conceptos, categorías o variables, en un contexto particular

Explicativo

- Pretende establecer las causas de los sucesos o fenómenos en estudio.
- Se centra en explicar por qué ocurre un fenómeno, en qué condiciones se manifiesta, o por qué se relacionan las variables.

Nota. Tomado de Hernández et al (2014).

3.3.2. Alcance seleccionado

El alcance de investigación seleccionado para este trabajo fue el descriptivo. Esto porque el propósito del proyecto es buscar especificar las propiedades y características actuales de las herramientas de auditoría (matriz de requerimientos de procesos tecnológicos, y herramientas para documentar las reuniones de entendimiento, riesgos y cronograma), para proponer una solución de actualización y estandarización de estas. La **Tabla 14** justifica la selección tomada.

Tabla 14

Justificación del alcance de investigación seleccionado

Alcance	Seleccionado	Justificación
Exploratorio	✗	-El tema de investigación relacionado con herramientas de auditoría no es poco estudiado o desconocido.
Descriptivo	✓	-La investigación busca especificar las propiedades y características actuales de las herramientas de auditoría para proponer la solución adecuada.
Correlacional	✗	-La investigación no busca identificar las relaciones entre las variables seleccionadas para estudiar las herramientas de auditoría.
Explicativos	✗	-La investigación no se enfoca en justificar a fondo por qué ocurren ciertos fenómenos o contextos relacionados con las herramientas de auditoría.

Nota. Elaboración propia.

3.4. Diseño de la Investigación

Dado que el tipo de investigación seleccionado para el trabajo es la investigación cualitativa, se procede a conceptualizar los diseños dentro de este enfoque. Antes de describirlos, es importante responder *¿Qué es diseño dentro del enfoque cualitativo?* De acuerdo con Hernández et al (2014), el diseño dentro del enfoque cualitativo es el abordaje general que será utilizado en el proceso de investigación. Este va surgiendo desde el planteamiento del problema hasta la inmersión inicial y trabajo de campo y puede sufrir modificaciones.

3.4.1. Diseños de la investigación cualitativa

La **Tabla 15** define y caracteriza los diseños más comunes de la investigación cualitativa. Estos son: teoría fundamentada, etnográficos, narrativos, fenomenológicos, e investigación-acción.

Tabla 15

Diseños de la investigación cualitativa

Pregunta de Investigación	Diseño	Información que proporciona
Preguntas sobre procesos y relaciones entre conceptos que conforman un fenómeno.	**Teoría fundamentada**	-Categorías y vínculos del proceso o fenómeno. -Teoría que explica el proceso o fenómeno.
Preguntas sobre características, estructuras y funcionamiento de un sistema social, ya sea grupo, organización, comunidad, subcultura, cultura.	**Etnográfico**	-Descripción y explicación de los elementos y categorías del sistema social, tales como interacciones, lenguaje, reglas, mitos, normas, otros.
Preguntas para comprender la sucesión de eventos (catástrofes, elección, biografías), por medio de historias de quienes lo vivieron.	**Narrativo**	-Historia sobre procesos, hechos, eventos y experiencias siguiendo una línea de tiempo. -Categorías relacionadas con tales historias o narrativas.
Preguntas sobre la esencia de las experiencias, es decir, lo que personas experimentan respecto a un fenómeno o proceso.	**Fenomenológico**	-Experiencias comunes y distintas. -Categorías que se presentan frecuentemente en las experiencias.
Preguntas sobre problemáticas o situación de un grupo o comunidad.	**Investigación-acción**	-Diagnóstico de problemáticas sociales, políticas, laborales, económicas, de naturaleza colectiva. -Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones.

Nota. Tomado de Hernández et al (2014).

3.4.2. Diseño de la investigación seleccionado

Para el desarrollo de este proyecto, se escogió el diseño de investigación llamado investigación-acción. Esto porque el proyecto realiza preguntas asociadas a una problemática o situación de un grupo o comunidad. En este caso, a las problemáticas de las herramientas dentro del equipo de TI.

Asimismo, el proyecto busca categorizar esas problemáticas con la intención de dar un diagnóstico y un plan de resolución para lograr el cambio de dicha problemática.

3.5. Fuentes de datos e información

De acuerdo con Ulate y Vargas (2014), las fuentes de investigación son aquellas fuentes de información consultadas a lo largo del proyecto, las cuales son clasificadas en fuentes primarias, secundarias y terciarias. El propósito no es únicamente listar las fuentes, si no, proporcionar una clasificación mediante sus tipos y una conceptualización de su importancia en el proyecto.

3.5.1. Tipos de fuentes de investigación

A continuación, se describe cada tipo de fuente de investigación, de acuerdo con lo establecido por Ulate y Vargas (2014), Pimienta y de la Orden (2012) y Hernández et al (2014). La **Tabla 16** muestra algunos ejemplos de estas fuentes.

- Fuentes primarias: Aquellas fuentes de primera mano, que incluyen resultados, testimonio y/o vivencias de los estudios correspondientes sobre el tema de investigación.
- Fuentes secundarias: Fuentes que interpretan y analizan las fuentes primarias.
- Fuentes terciarias: Aquellas fuentes que reúnen información de segunda mano, tales como catálogos, directorios e índices.

Tabla 16

Ejemplos de fuentes de investigación

Fuentes primarias	Fuentes secundarias	Fuentes terciarias
-Consulta a un experto del tema. -Persona que observa un evento. -Escritos de la persona cuya biografía se está construyendo. -Libros. -Artículos de publicaciones periódicas. -Trabajos presentados en congresos o simposios. -Monografías. -Tesis académicas. -Disertaciones. -Documentos oficiales. -Reporte de asociaciones. -Testimonios de expertos. -Documentales.	-Comentarios de libros, tesis, disertaciones y otros documentos especializados. -Índices que incluyen los datos de las referencias y un breve resumen de cada una.	-Directorios de empresas. -Títulos de reportes con información gubernamental. -Catálogos de libros, revistas, etc. -Directorios y guías de índices.

Nota. Tomado de Ulate y Vargas (2014).

3.5.2. Fuentes seleccionadas

Las fuentes seleccionadas para el desarrollo de este proyecto se clasifican en fuentes primarias y secundarias. Estas son descritas en la **Tabla 17**.

Tabla 17

Fuentes primarias y secundarias seleccionadas

Tipos de Fuente	Nombre de Fuente	Importancia
Primarias	*Marco de referencia COBIT 2019*	Es el marco base para plantear la propuesta de solución ante la problemática.
	Libros académicos sobre auditoría, metodología de investigación y finanzas.	Proporcionan conceptualización, características, pasos y lineamientos para cumplir con los objetivos específicos del proyecto.
	Tesis académicas.	Aportan orientación en el desarrollo de la investigación.
	Consultas a expertos del tema.	Son los involucrados actuales en la problemática identificada, los cuales proporcionan respuestas y comentarios de primera mano relacionados con la problemática y propuesta de solución.
Secundarias	*Artículos científicos*	Sirven de guía para la comprensión e implementación de cada una de las acciones especificadas en los objetivos específicos, entre ellas, el análisis de brecha, la propuesta de solución, análisis financiero y plan piloto.
	Sitios webs	Aquellas páginas oficiales que ayuden a la comprensión de las temáticas y propuestas establecidas para el proyecto.
	Sitio web de TFG.	Proporciona documentos que guían la documentación de la investigación académica.
	Bases de datos suscritas dentro del TEC.	Proporcionan una serie de recursos bibliográficos relacionados con el objeto de investigación del proyecto.

Nota. Elaboración propia.

3.6. Población y selección de muestra

La muestra en el proceso de investigación cualitativa es un grupo de personas, eventos, sucesos, comunidades, entre otros, sobre el cual se habrán de recolectar los datos sin que necesariamente sea estadísticamente representativo del universo o de la población de estudio (Hernández et al, 2014).

Para este proyecto, la muestra corresponde a todos los miembros del equipo de TI y al socio del área de *Management Consulting*. El equipo de TI está conformado por un gerente de TI, un supervisor de TI y tres asesores. A estos miembros se les solicita el apoyo por medio de técnicas de investigación para que

provean la información requerida y así se puedan identificar los datos necesarios para desarrollar la propuesta de solución y responder a la problemática identificada.

3.7. Sujetos de Investigación

Si bien la muestra incluye, de acuerdo con Hernández et al (2014), a grupos de personas, comunidades, eventos, sucesos, entre otros, sobre los cuales se deben recolectar los datos, sin que sean estadísticamente representativos de la población de estudio, los sujetos de investigación son los individuos, grupos o comunidades involucradas en la investigación, los cuales aportan información de valor al estudio.

La **Tabla 18** muestra los sujetos de investigación seleccionados para el proyecto.

Tabla 18

Sujetos de investigación seleccionados

Rol	Años de experiencia	Caracterización	Importancia
Socio del área	27 años	Tiene responsabilidades ejecutivas y estratégicas correspondientes a proyectos de consultoría y de auditoría de TI.	Tiene experiencia en proyectos relacionados con auditoría y consultoría, por lo que, mediante sus expectativas y opiniones, contribuye a que la elaboración de la propuesta de solución se adapte a las herramientas del área de *Management Consulting* y el equipo de TI.
Gerente de TI	11 años	-Planificar el trabajo por desarrollar con el cliente mediante la elaboración de cronogramas y asignación de tareas. -Supervisar el trabajo realizado por el equipo para garantizar el cumplimiento de las expectativas y regulaciones.	Tiene experiencia en proyectos de auditoría de tecnología de información, por lo que conocer sus expectativas ayuda a que la propuesta de solución cumpla con los estándares de calidad, tanto para el equipo como para los clientes auditados. Además, se encarga de las revisiones y brinda observaciones a la propuesta de solución.

Rol	Años de experiencia	Caracterización	Importancia
Supervisor de TI	4 años	-Desarrollar propuestas e informarse mediante la investigación de metodologías, mejores prácticas, regulaciones, otros, con el fin de contar con las herramientas necesarias para la ejecución exitosa del proyecto. -Supervisar el avance y entregables de los trabajos que se realizan en el equipo. -Representar a la organización en eventos internos o externos.	Tiene experiencia en la supervisión de proyectos de auditoría de tecnología de información, por lo que brinda información sobre debilidades y oportunidades de mejora de las herramientas de auditoría. Además, al igual que el gerente de TI, brinda observaciones a la propuesta de solución.
Equipo de asesores (tres integrantes)	2 años	Se encargan de desarrollar, ejecutar y finalizar las tareas y entregables de cada proyecto, cumpliendo con los estándares de calidad y los tiempos de entrega preestablecidos.	Son los encargados de la ejecución de las revisiones de los diferentes procesos de auditoría, por lo que están más familiarizados con las herramientas de auditoría. Por ello, permiten conocer las debilidades y oportunidades de mejora sobre estas herramientas.

Nota. Elaboración propia.

3.8. Variables de la Investigación

Las variables de la investigación son aquellas propiedades medidas como atributos, cualidades, y características observables que poseen las personas, objetos, instituciones, otros. Expresan magnitudes que varían discretamente o de forma continua. Forman parte de las hipótesis, o pretenden desarrollar una descripción de estas (Ñaupas et al, 2014; Hernández et al, 2014).

Las variables de la investigación para el trabajo son identificadas y descritas en la **Tabla 19**.

Tabla 19

Variables de investigación identificadas

Variable	Importancia
Situación actual de la matriz de requerimientos de procesos tecnológicos.	La indagación y comprensión de la matriz de requerimientos actual ayuda a identificar problemáticas relacionadas con la versión, apartados de contenidos, detalle de información, estructuras, entre otros aspectos.
Situación actual de las herramientas de gestión de ejecución de la auditoría.	La comprensión de cuáles herramientas se dispone para gestionar las reuniones de entendimiento, documentar riesgos y realizar el cronograma, sus criterios, formas de uso, versiones, entre otros aspectos, ayudan a la identificación de problemáticas que afecten el rendimiento de la actividad que apoyan.
Brechas de las herramientas (matriz y herramientas de gestión para documentar reuniones de entendimiento, documentar riesgos y elaborar cronograma).	Proporciona la identificación de todas las oportunidades de mejora encontradas en el estudio de la situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de la auditoría. Asimismo, ayuda a delimitar las soluciones apropiadas para responder a las oportunidades de mejoras identificadas.
Matriz de requerimientos de procesos tecnológicos.	Producto realizado como parte de la propuesta de solución.
Herramientas de gestión de ejecución de auditoría.	Producto realizado como parte de la propuesta de solución.
Inversión	Inversión estimada del producto realizado como parte de la propuesta de solución.
Indicador de rendimiento económico	Sirve como indicador financiero para determinar la viabilidad en términos de costos y rentabilidad, de los productos realizados como parte de la propuesta de solución.
Nivel de cumplimiento.	Proporciona una verificación de que los productos desarrollados como parte de la propuesta de solución, respondan a las necesidades y criterios del equipo de trabajo.

Nota. Elaboración propia.

3.9. Técnicas e Instrumentos de Investigación

Antes de iniciar con la descripción de las técnicas e instrumentos, es importante responder *¿Cuál es la diferencia entre técnica de investigación e instrumento de investigación?* De acuerdo con Ñaupas et al (2014), las técnicas de investigación son métodos especiales o particulares que se aplican en cada etapa

de la investigación científica, cuantitativa o cualitativa, que varían de acuerdo con su enfoque. Estas técnicas se dividen en tres tipos:

- Técnicas conceptuales: Hacen posible las operaciones racionales, de abstracción, generalización, análisis, síntesis, clasificación, comparación y de reglas lógicas formales o dialécticas. Hacen referencia a conceptos como proyecto, problema y objetivos de investigación, marco teórico, hipótesis y variables. Sin estas técnicas es imposible formular un proyecto de investigación.
- Técnicas descriptivas: Sirven para la recolección de datos con el objeto de verificar hipótesis. Se destacan la observación, entrevistas, análisis de contenido, entre otras. Son la base para construir instrumentos de investigación, conducir experimentos, observar y controlar variables.
- Técnicas cuantitativas: Refieren a magnitudes o cantidades expresadas mediante números, fórmulas o algoritmos numéricos, tales como: determinar el universo, hallar muestras, técnicas matemáticas y estadísticas de procesamiento de datos, análisis estadísticos, otros.

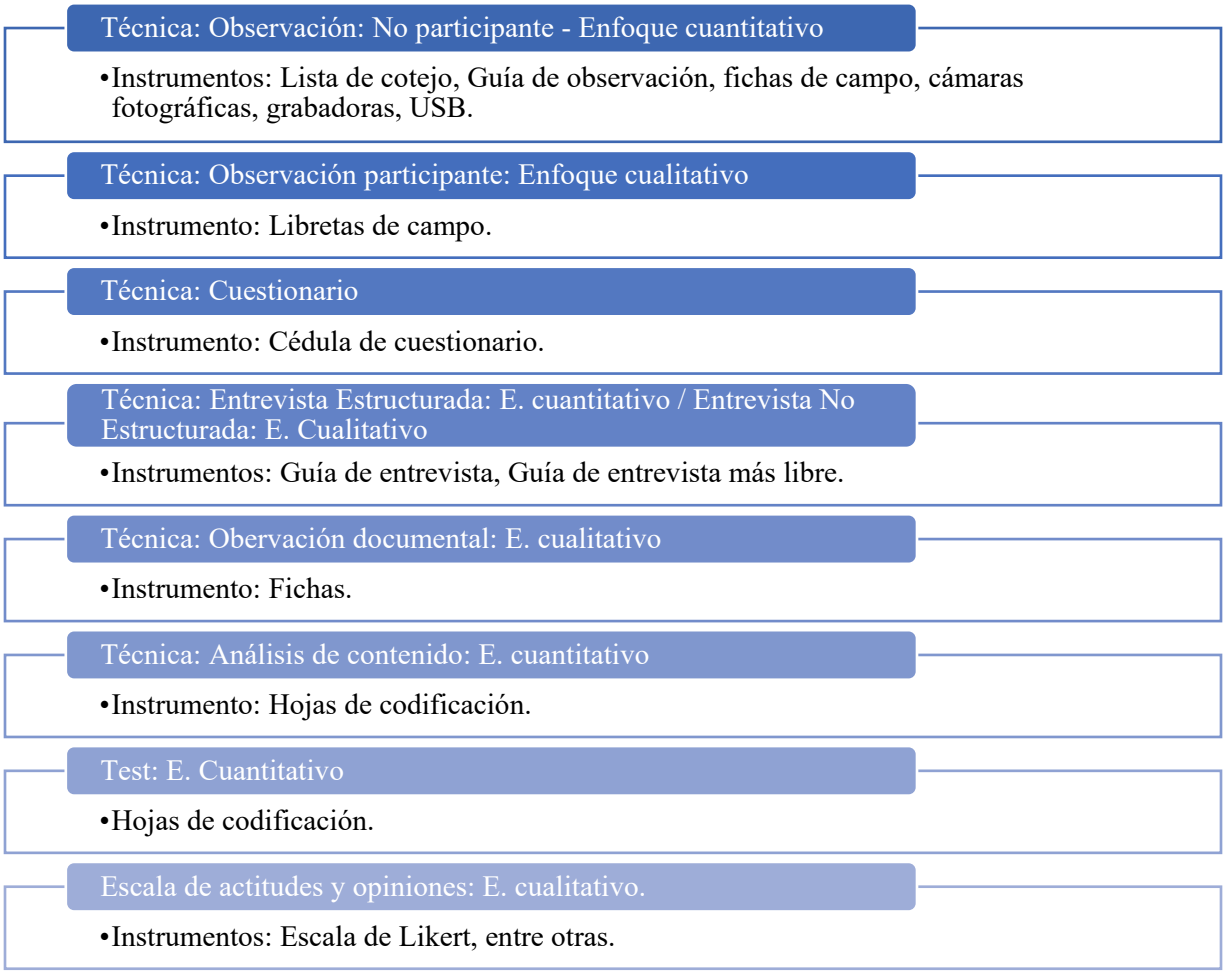
Luego, una vez comprendido el concepto de técnica, el instrumento de investigación corresponde a la herramienta conceptual o material que sirve a la técnica de investigación, en especial la de recolección de datos (Ñaupas et al, 2014). La **Figura 21** ejemplifica la relación entre estas.

Para efectos de este proyecto, se utilizaron las técnicas descriptivas. Esto porque el propósito es proceder con la recolección de datos por medio de observaciones, revisión documental, entrevistas, entre otros aspectos. El proyecto no pretendió realizar análisis estadísticos o aplicar métodos matemáticos con los resultados obtenidos.

A continuación, se definen y caracterizan las técnicas seleccionadas para la recolección de datos de este trabajo, así como los instrumentos que las apoyan.

Figura 21

Relación entre técnicas e instrumentos de investigación



Nota. Tomado de Ñaupas et al (2014).

3.9.1. Entrevista

La entrevista es una reunión para conversar e intercambiar información entre una persona, conocida como entrevistador, y otra, conocido como entrevistado. A través de las preguntas y respuestas, se obtiene una comunicación y una construcción de significados respecto a un tema en particular. Pueden hacerse preguntas sobre experiencias, opiniones, valores, creencias, percepciones, hechos, historias de vida, otros. La entrevista se puede clasificar en tres tipos:

estructurada, semiestructurada, y abierta. Estos son representados en la **Figura 22** (Hernández et al, 2014).

Para efectos de este proyecto, se realizaron entrevistas semiestructuradas para evaluar la situación actual de la problemática identificada, aplicadas al socio del área de *Management Consulting*, y al Gerente y Supervisor de TI. Los instrumentos respectivos para las entrevistas semiestructuradas se encuentran en el **Apéndice A**, y **Apéndice B**. Estos fueron compuestos por la siguiente estructura:

- Datos generales: Incluye información como el identificador de la entrevista, fecha de ejecución, entrevistado y entrevistador y tema de la entrevista.
- Sección de preguntas: En la sección se desglosan las preguntas previamente definidas para realizar a la parte entrevistada.

Figura 22

Tipos de entrevista

Nota. Información tomada de Hernández et al (2014).

3.9.2. Grupo focal

De acuerdo con Hernández et al (2014), el grupo focal corresponde a una especie de entrevistas grupales, las cuales consisten en reuniones de grupo pequeños o medianos, entre tres a diez personas, en donde los involucrados conversan a profundidad sobre un tema en particular.

En este proyecto se aplicó el grupo focal para evaluar la propuesta de solución y determinar si esta corresponde como solución a la problemática y consecuencias asociadas. Este se encuentra en el **Apéndice C**, y fue compuesto de la siguiente manera:

- Datos generales: Incluye información como el identificador del grupo focal, fecha de ejecución, participantes y responsable y objetivo general.
- Temas por abarcar: Lista los temas que serán contemplados durante la ejecución del grupo focal, los cuales están relacionados con el nivel de detalle, estructuración y estandarización, la comprensión de la propuesta y temas de cargas laborales.

3.9.3. Encuestas

Las encuestas son utilizadas para conocer la opinión de las personas sobre una situación o una problemática en que estén involucradas. Antes de iniciar con cualquier encuesta, es importante delimitar correctamente la muestra de personas que serán partícipes de esta (Ulate y Vargas, 2014).

Para el caso de este proyecto se aplicaron dos encuestas. La primera dirigida a los asesores de TI. Esta tuvo el objetivo de identificar la percepción sobre las herramientas (matriz de requerimientos de procesos tecnológicos y herramientas de gestión) actuales e identificar las expectativas sobre una propuesta de mejora sobre estas. El instrumento correspondiente se encuentra en el **Apéndice D**. La segunda encuesta, dirigida al gerente de TI, supervisor de TI y asesores, tuvo como fin valorar el cumplimiento de la propuesta de solución, para identificar si esta cumple con las expectativas planteadas. Esta se encuentra en el **Apéndice E**. Ambas encuestas fueron estructuradas de la siguiente manera:

- Párrafo introductorio: En este párrafo se especifica el fin de la encuesta por realizar, así como la explicación de la estructura por abarcar.

- Sección de preguntas: Se detallan las preguntas correspondientes al tema de interés. Pueden ser de selección única, selección múltiple, o respuesta corta/larga.

3.9.4. Revisión documental

Todo investigador tiene contacto con la información que percibe de la realidad de su foco de estudio. Por ello, la revisión documental hace referencia al proceso exploratorio de documentos, materiales y artefactos como cartas, diarios, documentos escritos de todo tipo, material audiovisual, expresiones artísticas, archivos, objetos, entre otros. Ayudan al investigador a entender el fenómeno central de estudio, al permitir conocer los antecedentes, vivencias, o situaciones que se producen en el funcionamiento cotidiano y anormal de estos elementos. Conforme se va realizando el proceso de revisión y análisis documental, la información básica se va incrementando y el investigador va logrando conocimiento cada vez más preciso sobre la idea o tema en estudio (Hernández et al, 2014; Ñaupas et al, 2014).

Para este proyecto, se procedió a realizar una revisión documental de la matriz de requerimientos de procesos tecnológicos, con el propósito de identificar y documentar los hallazgos, deficiencias y oportunidades de mejora de esta herramienta. El instrumento se encuentra en el **Apéndice F**, y se caracterizó de la siguiente manera:

- Datos generales: Información como la fecha de la revisión, persona encargada y tema.
- Identificador del hallazgo: Código o número del hallazgo identificado.
- Descripción del hallazgo: Escritura detallada del hallazgo, deficiencia u oportunidad de mejora identificada después de la revisión.

También, se realizó una revisión documental sobre los cronogramas de años anteriores dados por el equipo de TI, con el fin de determinar los promedios de duraciones de las actividades comunes. El instrumento se encuentra en el **Apéndice G**, y se estructuró de la siguiente forma:

- Datos generales: Información como la fecha de la revisión, persona encarga y tema.
- Hallazgos generales: Contiene identificador y descripción de los hallazgos generales identificados en todos o algunos de los cronogramas.

- Hallazgos en cada actividad: Contiene el listado de la actividad y un espacio para colocar los tiempos identificados.

3.9.5. Matriz de cobertura de las variables vs el diseño de los instrumentos

En la **Tabla 20**, se muestra la relación entre las variables y el diseño de los instrumentos de las técnicas de investigación seleccionadas.

Tabla 20

Matriz de cobertura de variables

Variable	Técnica			
	Entrevistas semiestructuradas	Grupo focal	Encuestas	Revisión documental
Situación actual de la matriz de requerimientos de procesos tecnológicos.	X		X	X
Situación actual de las herramientas de gestión de ejecución de la auditoría.	X		X	X
Brechas de las herramientas (matriz y herramientas de gestión para documentar reuniones de entendimiento, documentar riesgos y elaborar cronograma).	X		X	X
Matriz de requerimientos de procesos tecnológicos.	Es la propuesta de solución			
Herramientas de gestión de ejecución de auditoría.	Es la propuesta de solución			
Inversión	X			
Indicador de rendimiento económico	X			
Nivel de cumplimiento.		X	X	

Nota. Elaboración propia.

3.10. Procedimiento metodológico de la Investigación

Este apartado tiene como fin desglosar y explicar las fases que involucraron el proceso metodológico de este proyecto. En total se establecen cinco fases, representadas en la **Figura 23**, las cuales fueron

necesarias para cumplir con cada uno de los objetivos planteados para el desarrollo del trabajo. A continuación, se detallan los pasos y elementos importantes de cada fase definida.

Figura 23

Fases del proceso metodológico

Nota. Elaboración propia.

3.10.1. Fase I. Análisis de la situación actual

El análisis de la situación actual tuvo como objetivo identificar el contexto de las herramientas de auditoría, tanto la matriz de requerimientos de procesos tecnológicos como las herramientas de gestión para documentar las reuniones de entendimiento, los riesgos y el cronograma, para así visualizar las oportunidades de mejora.

En esta fase se aplicaron las técnicas de entrevistas y encuestas de situación actual a los miembros del equipo de TI, para conocer su perspectiva y opinión sobre las condiciones actuales de las herramientas y sobre cómo estas afectan el rendimiento de su trabajo durante el proceso de auditoría. Asimismo, se aplicó la técnica de revisión documental para la matriz de requerimientos

de procesos tecnológicos y el apartado de cronogramas, con el propósito de documentar posibles hallazgos o condiciones que pueden servir como oportunidades de mejora. Se buscó analizar los elementos relacionados con apartados, estructuras, contenidos, criterios, lineamientos, entre otros aspectos que ayuden a conocer por completo la situación actual.

3.10.2. Fase II. Análisis de brecha

La fase de análisis de brecha tuvo como fin comparar el estado actual con el estado deseado de las herramientas de matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de auditoría, para proponer la solución apropiada a las oportunidades de mejora identificadas.

En esta fase se utilizaron las entrevistas, encuestas y revisiones documentales (mencionadas en la Fase I) para documentar y detallar el estado actual de las herramientas en cuestión. Luego, se utilizó COBIT 2019 como punto de referencia para determinar el estado deseado. Una vez obtenida ambas partes de información, se procedió a listar las oportunidades de mejora que hacen la brecha de estas herramientas.

3.10.3. Fase III. Matriz de requerimientos de procesos tecnológicos e instructivo de gestión de ejecución de auditoría

Esta fase correspondió al desarrollo de la propuesta de solución, la cual fue dividida en dos aspectos:

- Actualización de la matriz de requerimientos de procesos tecnológicos: Se realizó una nueva matriz de requerimientos tomando como base el marco de referencia COBIT 2019 y las expectativas recopiladas de los miembros del equipo de TI. La matriz se realizó con un total de diez procesos, dos por cada dominio, los cuales fueron identificados en la sección del alcance, en la **Tabla 1**.
- Elaboración de un instructivo de gestión de ejecución de la auditoría: El instructivo de gestión contiene las herramientas para documentar las reuniones de entendimiento, documentar los riesgos y realizar el cronograma. Este instructivo de gestión buscó brindar un guion de referencia al equipo de TI, basado en sus expectativas sobre el tema para

promover la estandarización y disminuir las problemáticas de comunicación. Para este instructivo también se utilizaron los diez procesos de COBIT 2019 definidos en la **Tabla 1**.

3.10.4. Fase IV. Análisis financiero

Una vez desarrollada la propuesta de solución en la Fase III, se procedió a plantear un análisis financiero para identificar la viabilidad de la propuesta en términos económicos. Los aspectos importantes desarrollados en este análisis fueron la determinación de la inversión total del desarrollo del proyecto, considerando su planteamiento, análisis de resultados, propuesta de solución y conclusiones y recomendaciones, así como la capacitación que se requiere. Luego, se plantea analizar la viabilidad de esta inversión con el presupuesto establecido.

3.10.5. Fase V. Evaluación de la pertinencia de la solución

La última fase corresponde a la aplicación de un plan piloto para validar la propuesta de solución especificada en la fase III. Se evaluó si la solución planteada es la respuesta ideal para resolver las problemática identificadas y las consecuencias a raíz de esta. Para este plan piloto, se establecieron pruebas piloto para que el equipo de TI evaluara la propuesta de solución definida. Para ello, se utilizó el grupo focal y una encuesta de calificación. Después de ejecutada esta fase, se dieron respuesta a las hipótesis planteadas.

3.11. Operacionalización de las variables

La operacionalización de las variables identificadas para este proyecto se expresa en la **Tabla 21**.

Tabla 21

Operacionalización de las variables

Fase	Objetivo específico	Instrumentos	Variables	Sujetos
I. Análisis de situación actual	Analizar la situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión utilizadas por el equipo de TI, para la identificación de hallazgos y oportunidades de mejora.	• Revisión documental de la matriz de requerimientos y cronograma. • Entrevistas semiestructuradas de situación actual. • Encuesta de situación actual.	• Situación actual de la matriz de requerimientos de procesos tecnológicos. • Situación actual de las herramientas de gestión de ejecución de la auditoría.	• Socio del área. • Gerente de TI. • Supervisor de TI. • Asesores.
II. Análisis de brecha	Aplicar un análisis de brecha, considerando la situación actual y la situación deseada, para la delimitación de la propuesta de solución que solvente la problemática.	• Revisión documental de la matriz de requerimientos y cronograma. • Entrevistas semiestructuradas de situación actual. • Encuesta de situación actual.	• Brechas de las herramientas (matriz y herramientas de gestión para documentar reuniones de entendimiento, documentar riesgos y elaborar cronograma).	• Socio del área. • Gerente de TI. • Supervisor de TI. • Asesores.
III. Matriz de requerimientos de procesos tecnológicos e instructivo de gestión de ejecución de auditoría	Elaborar una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión basados en el marco de referencia COBIT 2019, para la promoción de la actualización y estandarización de estas herramientas utilizadas por el equipo de TI.	Es la propuesta de solución.		

Fase	Objetivo específico	Instrumentos	Variables	Sujetos
IV. Análisis financiero	Desarrollar un análisis financiero, para la comprobación de los beneficios y viabilidad de la propuesta de solución.	• Entrevista semiestructurada de situación actual	• Inversión • Indicador de rendimiento económico	• Gerente de TI. • Supervisor de TI.
V. Evaluación de la pertinencia de la solución	Validar la pertinencia de la propuesta de solución, por medio de un plan piloto, para el cumplimiento de esta como respuesta a la problemática.	• Grupo focal de evaluación de pertinencia de la solución. • Encuesta de evaluación de cumplimiento de la propuesta de solución.	• Nivel de cumplimiento.	• Gerente de TI. • Supervisor de TI. • Asesores.

Nota. Elaboración propia.

3.12. Tabla resumen del procedimiento metodológico de la investigación

A continuación, la **Tabla 22** refleja el resumen del procedimiento metodológico de la investigación por medio de la matriz de trazabilidad de los objetivos.

Tabla 22

Matriz de Trazabilidad

Objetivo	Marco Teórico	Metodología	Análisis de Resultados	Propuesta de solución	Conclusiones	Recomendaciones
1. Analizar la situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión utilizadas por el equipo de TI, para la identificación de hallazgos y oportunidades de mejora.	Sección 2.1 Sección 2.2	Sección 3.8 Sección 3.9.1 Sección 3.9.4 Sección 3.9.5 Sección 3.10.1	Sección 4.1.1 Sección 4.1.2	NA	Sección 6.1	Sección 7
2. Aplicar un análisis de brecha, considerando la situación actual y la situación deseada, para la delimitación de la propuesta de solución que solvente la problemática.	Sección2. 6	Sección 3.8 Sección 3.9.1 Sección 3.9.3 Sección 3.9.5 Sección 3.10.2	Sección 4.2.1 Sección 4.2.2	NA	Sección 6.2	Sección 7
3. Elaborar una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión basados en el marco de referencia COBIT 2019, para la promoción de la actualización y estandarización de estas herramientas utilizadas por el equipo de TI.	Sección2. 1.3 Sección 2.3	Sección 3.10.3	NA	Sección 5.1.1 Sección 5.1.2	Sección 6.3	Sección 7
4. Desarrollar un análisis financiero, para la comprobación de los beneficios y viabilidad de la propuesta de solución.	Sección 2.7	Sección 3.10.4	NA	Sección 5.2	Sección 6.4	Sección 7
5. Validar la pertinencia de la propuesta de solución, por medio de un plan piloto, para el cumplimiento de esta como respuesta a la problemática.	Sección 2.8	Sección 3.8 Sección 3.9.2 Sección 3.9.3 Sección 3.9.5 Sección 3.10.5	NA	Sección 5.3	Sección 6.5	Sección 7

Nota. Elaboración propia.

4. ANÁLISIS DE RESULTADOS

En este capítulo se pretende analizar toda la información recopilada a partir de las técnicas e instrumentos seleccionados para la Fase I y la Fase II del proceso metodológico. Esto con el propósito de identificar las oportunidades de mejora específicas y así abordar una propuesta de solución adecuada.

Las técnicas utilizadas para el análisis de resultados de la Fase I y Fase II son las siguientes:

- Entrevista al socio del área de *Management Consulting*, la cual se encuentra en el **Apéndice H**.
- Entrevista al gerente de TI y supervisor de TI, mostrada en el **Apéndice I**.
- Revisión documental de la matriz de requerimientos de procesos tecnológicos, la cual se encuentra en el **Apéndice J**.
- Encuesta a los tres asesores del equipo de TI, mostrada en el **Apéndice K**.
- Revisión documental sobre los cronogramas de auditorías, mostrada en el **Apéndice L**.

4.1. Fase I. Análisis de Situación Actual

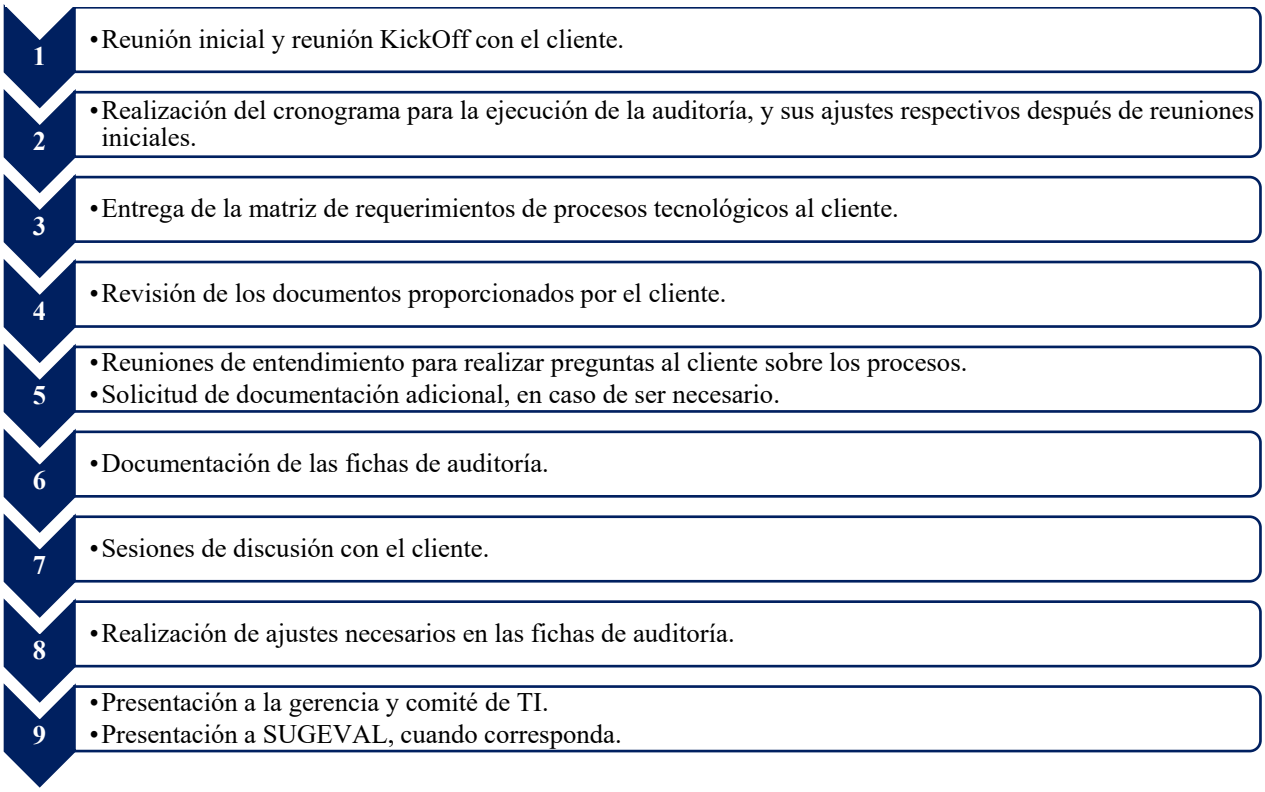
Como bien se mencionó en el Capítulo 1, el equipo de TI realiza auditorías de tecnologías de información para aquellas organizaciones que deban cumplir con el acuerdo SUGEF 14-17, o bien, para aquellas organizaciones que solo desean evaluar su desempeño en el marco de referencia correspondiente y tienen un proceso establecido para la ejecución de estas auditorías, mostrado en la **Figura 24**.

Este capítulo identifica y analiza las condiciones actuales de la herramienta matriz de requerimientos de procesos tecnológicos y herramientas de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y realización del cronograma, las cuales generan la problemática identificada y son insumos para elaborar una propuesta de solución apta a las necesidades y expectativas del equipo.

A continuación, se detalla la situación actual de cada una de las herramientas.

Figura 24

Proceso de auditoría de TI



Nota. Elaboración propia a partir de información brindada por el equipo de TI del área de *Management Consulting*.

4.1.1. Situación actual de la matriz de requerimientos de procesos tecnológicos

La matriz de requerimientos de procesos tecnológicos es conocida por el equipo de TI como matriz de requerimientos preliminares. Esta matriz tiene un listado de todos los documentos o requisitos por cada proceso a evaluar de acuerdo con lo establecido por COBIT 5, los cuales deben ser solicitados al cliente. Es enviada al cliente para que posteriormente entregue la documentación o los requisitos que actualmente tenga para proceder con la evaluación correspondiente.

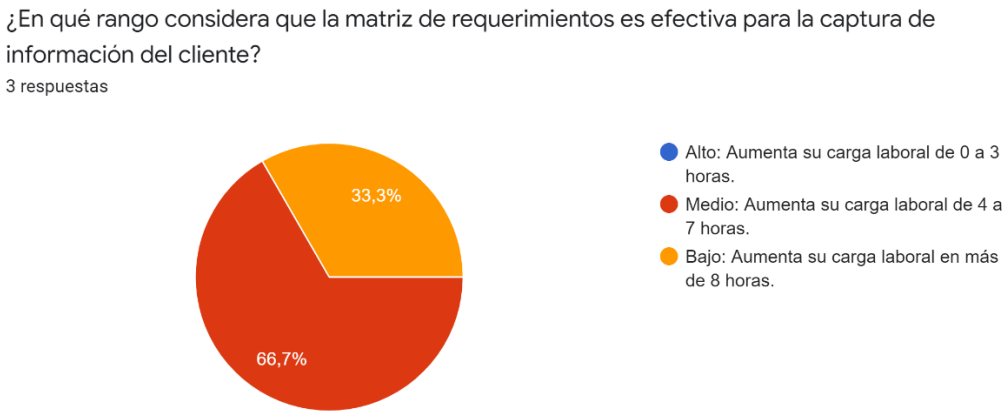
Según la revisión documental aplicada, la matriz de requerimientos de procesos tecnológicos contiene apartados para llevar el control de la documentación o requerimientos solicitados, apartados como fechas de entrega, responsables y observaciones. Si bien esto es importante para la gestión de documentos, se identifica en la revisión documental que la matriz de requerimientos está

estructurada únicamente por procesos y la documentación que solicita es para cada proceso en general, sin hacer distinción en algunos casos en las salidas establecidas dentro del marco de referencia sobre cada práctica de cada proceso. Como consecuencia, en esta identificación se puede considerar que el equipo de TI incurre en solicitar más documentación o requisitos que no contemplaban alguna práctica dentro del proceso. A su vez, puede generar confusiones para interpretar la completitud de cada práctica del proceso, con la documentación entregada. La solicitud de documentación extra se maneja con otra hoja de Excel llamada "Matriz de requerimientos adicionales", la cual tiene la misma estructura y formato que la matriz en cuestión.

Estas consecuencias justifican por qué la mayoría de los asesores del equipo de TI consideran que el uso de la matriz de requerimientos actual les aumenta sus cargas de trabajo extra, entre cuatro a siete horas en la actividad en la cual utilizan la herramienta; esto se muestra en la **Figura 25**. Únicamente una persona considera que sus extras son superiores a las siete horas.

Figura 25

Rango de efectividad de la matriz de requerimientos de procesos tecnológicos actual



Nota. Elaboración propia.

Asimismo, a partir de las entrevistas efectuadas al socio del área, gerente de TI y supervisor de TI, se puede notar que la matriz de requerimientos de procesos tecnológicos carece de formalidad a la hora ser entregada al cliente, ya que no contiene una portada o una guía de usuario que le sirva de

apoyo para entregar la documentación respectiva. Si bien la matriz de requerimientos es fácil de interpretar, la firma exige formalidad y la falta de esta hace que el cliente entregue la documentación bajo sus propios estándares, como por ejemplo, los nombres de los documentos, los cuales no hacen referencia al documento que se solicita, aunque su contenido sea el indicado. Esto puede causar confusión a la hora de evaluar la documentación por cada proceso y que se deba hacer consultas al cliente por aspectos de formas de entrega y no de contenido.

4.1.2. Situación actual de las herramientas de gestión de ejecución de la auditoría

En general, de acuerdo con la entrevista realizada al gerente y supervisor de TI y la encuesta efectuada al equipo de asesores, se logra identificar que el equipo de TI no posee un manual o un estándar que sirva de guía para desarrollar y utilizar las herramientas para documentar las reuniones de entendimiento, documentar los riesgos de auditoría y desarrollar el cronograma. Esto se muestra en la **Figura 26.**

Figura 26

Existencia de guía para desarrollo y documentación de herramientas de gestión

Nota. Elaboración propia.

No tener un manual o estándar genera como consecuencia que una actividad se trabaje de varias formas y se generen confusiones a la hora de su comprensión. Dentro del equipo de TI, se puede identificar que la mayoría del desarrollo y gestión de estas herramientas se hacen a partir del criterio de cada auditor.

A continuación, se analizan las condiciones actuales de las herramientas utilizadas para documentar las reuniones de entendimiento, documentar los riesgos de auditoría y desarrollar el cronograma.

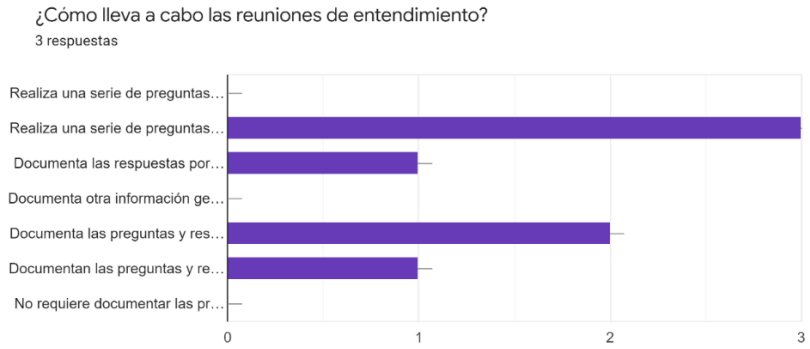
4.1.2.1. Documentación de las reuniones de entendimiento

De acuerdo con la entrevista realizada al gerente de TI y supervisor de TI, llevar a cabo la reunión de entendimiento y documentar la información obtenida de esta queda a total criterio del miembro o miembros responsables de ejecutarla. El equipo no tiene un estándar para ejecutar y documentar las reuniones de entendimiento. Tampoco maneja una guía de usuario sobre cómo se deben llevar a cabo las reuniones de entendimiento con el cliente en términos de tener una introducción, una agenda, preguntas base por considerar, sección para abarcar el tema, entre otros aspectos. Como consecuencia de esto, se interpreta que existen variedad de formas para gestionar la documentación y ejecución de las reuniones de entendimiento, pues cada miembro selecciona la herramienta que mejor considere, plantea las preguntas según su criterio profesional y experiencia en el proceso respectivo, documenta las respuestas como mejor considere y gestiona la reunión según su criterio.

De la encuesta realizada a los asesores, se puede confirmar en la **Figura 27** lo descrito en el párrafo anterior. Primeramente, todos realizan las preguntas de la reunión de entendimiento de acuerdo con su criterio profesional, todas basadas en el contenido del marco de referencia COBIT 5. Luego, la mayoría documenta sus respuestas por medios digitales como Word, Excel o One Note, sin embargo, también utilizan papel y lápiz para documentar sus respuestas. Finalmente, únicamente un miembro documenta las respuestas por proceso.

Figura 27

Actividades actuales para llevar a cabo las reuniones de entendimiento



Nota. Elaboración propia.

4.1.2.2. Documentación de los riesgos dentro de la ficha de auditoría

La documentación de los riesgos se efectúa dentro de las fichas de auditoría, las cuales son desarrolladas por medio de Word. La descripción de los riesgos y su respectiva recomendación se realiza por proceso. La estructura de los riesgos dentro de las fichas está dada por la firma y contiene los siguientes apartados:

- Condición: Es la descripción de los riesgos identificados en el proceso.
- Causa: Descripción de las causas que ocasionan los riesgos identificados.
- Impacto: Identificación del área que impacta el riesgo. Puede ser estratégico, operativo, económico o legal.
- Recomendaciones: Descripción de posibles recomendaciones para solventar los riesgos.

De acuerdo con la entrevista realizada al gerente y al supervisor de TI, la redacción del riesgo, causa, impacto y recomendación, queda a total criterio de cada miembro involucrado en la auditoría. Esto ocasiona que cada uno utilice sus propias técnicas o métodos para la redacción del apartado de riesgos y recomendaciones. Para confirmar esto, según la encuesta realizada a los asesores, en la **Figura 28**, se identifica que estos documentan el apartado de riesgos de auditoría de acuerdo con su experiencia en auditorías anteriores, o siguiendo los lineamientos de sus superiores. Asimismo, realizan las recomendaciones de acuerdo con su

criterio de experto como profesionales. Explicado lo anterior, se incurre en una variedad de formas para definir los riesgos, cuyo contenido lo define cada involucrado del proceso, lo cual puede causar confusión entre los miembros por la interpretación de estos.

Con respecto a los términos identificados en el apartado de impacto de los riesgos, estos son utilizados por formas de trabajo de la firma. El gerente de TI y el supervisor de TI afirman que no existe una definición sobre lo que abarca cada término, sin embargo, es fácil para todos los miembros del equipo de TI identificar cuando se trata del tema económico, legal, operativo o estratégico. A pesar de que estos términos sean de fácil entendimiento, el no tener una definición estándar de estos puede causar confusiones, sobre todo en personal nuevo que ingrese al equipo.

Figura 28

Actividades actuales para llevar a cabo la documentación de los riesgos de auditoría

Nota. Elaboración propia.

4.1.2.3. Elaboración del cronograma

De acuerdo con la entrevista efectuada al gerente y al supervisor de TI, así como la revisión documental sobre cuatro cronogramas de años anteriores, el cronograma siempre es elaborado en la herramienta Project. Los miembros responsables de la auditoría son los encargados de desarrollarlo. Generalmente, utilizan como base cronogramas de auditorías pasadas y ajustan la cantidad de actividades y los tiempos de los procesos respectivos. Esto se justifica en la

encuesta realizada a los asesores, donde expresaron que para el desarrollo del cronograma siguen su criterio de experto como profesional, los lineamientos de sus supervisores y lo realizado en cronograma de proyectos anteriores. Su respuesta se muestra en la **Figura 29**.

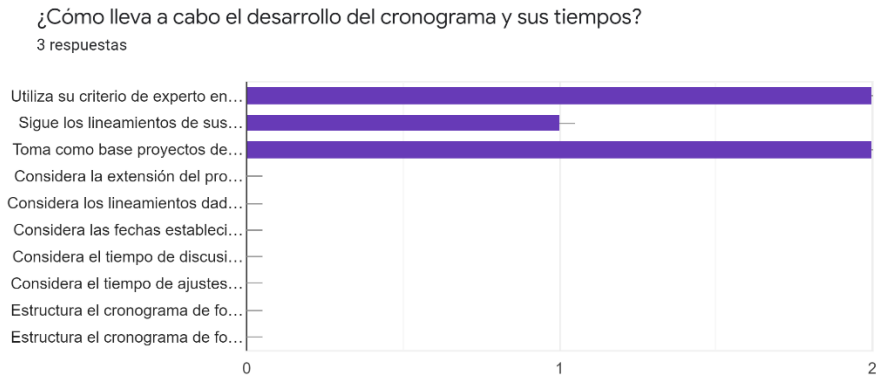
Con respecto a las duraciones de cada proceso, estas varían dependiendo del cliente, ya que un cliente puede no tener ninguna información del proceso en cuestión, lo cual hace que el tiempo para finalizar el proceso sea menor al pactado o pueden surgir preguntas o discusiones con respecto a la información de otros procesos y aumentar el tiempo pactado para estos.

A pesar de que el cronograma siempre sigue una estructura similar, se confirma que no involucra tiempos para consultas asociadas a la matriz de requerimientos, o espacios para analizar y validar requerimientos o evaluaciones de algunos temas, antes de proceder con las reuniones de discusión. Justifican que esto no se agrega por falta de tiempo.

A raíz de esto y a pesar de que cada auditoría es diferente, el no tener una guía aproximada de la duración de los procesos, así como espacios para efectuar consultas o validaciones, puede implicar atrasos posteriores del proceso de auditoría, porque cada auditor pactará los tiempos de acuerdo con su criterio y del cliente. También, porque se deberán abarcar consultas o aclaraciones que pudieron ser aclaradas en etapas tempranas del proceso y en el momento actual pueden dificultar la entrega a tiempo de la auditoría.

Figura 29

Actividades actuales para llevar a cabo el desarrollo del cronograma



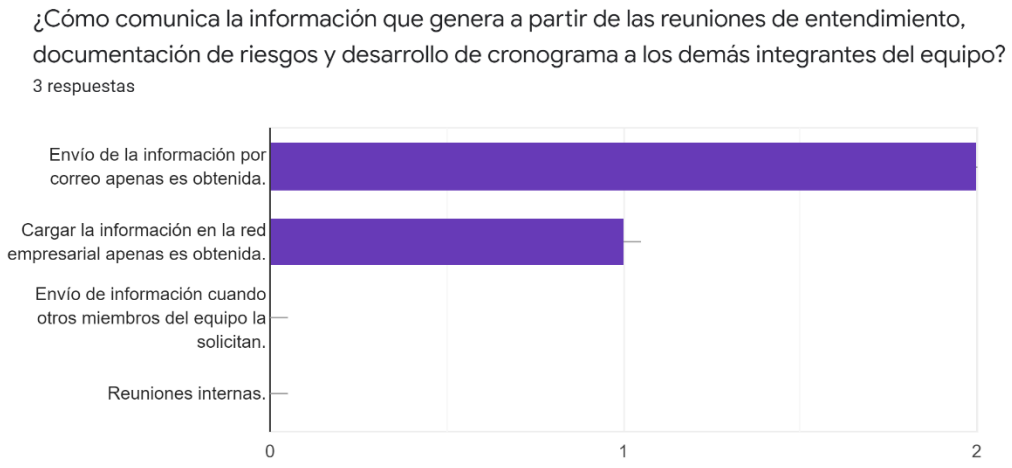
Nota. Elaboración propia.

Toda la información que es obtenida, procesada y analizada con el uso de estas herramientas descritas y analizadas, se comunica por medio de correo electrónico o es cargada a la red empresarial, según la encuesta realizada a los asesores, la cual muestra las respuestas en la **Figura 30**.

Para finalizar con la situación actual de estas herramientas, y de acuerdo con la encuesta efectuada, la mayoría de los asesores del equipo de TI consideran que estas herramientas aumentan sus cargas de trabajo, en las actividades respectivas para el uso de cada una, entre cuatro a siete horas; una sola persona expresa que sus cargas extras aumentan más de siete horas, dadas las consecuencias que estas presentan actualmente. Esto se refleja en la **Figura 31**.

Figura 30

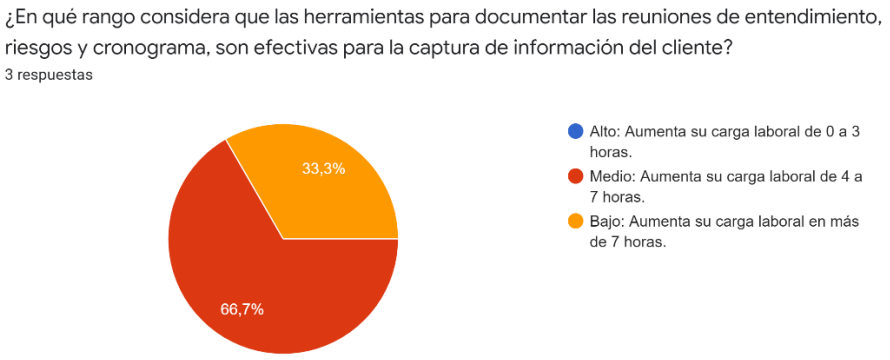
Medios de comunicación de la información obtenida de las herramientas de gestión



Nota. Elaboración propia.

Figura 31

Rango de efectividad de las herramientas de gestión de ejecución de auditoría



Nota. Elaboración propia.

En resumen, esta primera fase demostró que las herramientas en cuestión por el equipo de TI están desactualizadas y desestandarizadas. Por un lado, la matriz de requerimiento de procesos tecnológicos desglosa información por cada proceso en general y carece de formalidad a la hora de su entrega al cliente.

Estos aspectos hacen que se deba solicitar información en etapas posteriores del proceso y consultar aspectos de forma de estos, lo cual compromete las fechas inicialmente pactadas.

Por otro lado, en lo que respecta a la documentación de las reuniones de entendimiento, la documentación de riesgos y realización del cronograma, se encuentra que el equipo no cuenta con un guía o estándar para realizar, lo cual le da la libertad a cada miembro de trabajar dichos documentos de acuerdo con su criterio profesional después de conocer aquellos lineamientos o indicaciones de sus gerentes. Estas acciones causan ambigüedad, confusiones y atrasos en el proceso de auditoría pues cada uno tiene formas y ritmos diferentes de trabajar, independientemente de que estén cumplimiento con los objetivos de la auditoría.

4.2. Fase II. Análisis de brecha

Una vez analizada la situación actual de las herramientas mencionadas en la Fase I, se procede a aplicar un análisis de brecha para puntualizar las oportunidades de mejoras y la propuesta de solución. Este análisis de brecha consta de cuatro apartados: estado actual, estado deseado, brechas y plan de acción.

El análisis de brecha se realiza tanto para la herramienta de matriz de requerimientos como para las herramientas de gestión relacionadas con la documentación de reuniones de entendimiento, documentación de riesgos y cronograma. Los diferentes análisis de brecha se harán tomando en cuenta la información y el trabajo actual que maneja el equipo de TI y lo establecido en COBIT 2019 al respecto, para identificar los aspectos faltantes y favorecer su alineamiento.

4.2.1. Análisis de brecha matriz de requerimientos de procesos tecnológicos

El análisis de brecha de la matriz de requerimientos de procesos tecnológicos se realiza por cada proceso seleccionado en el alcance. El propósito es identificar, por cada proceso, las brechas entre los requerimientos de la matriz actual del equipo y la información definida, como salidas de los procesos, de acuerdo con COBIT 2019. Para ello, se toma como referencia la información obtenida en la situación actual así como la información contenida del proceso dentro de COBIT 2019.

4.2.1.1. Evaluar, Dirigir y Monitorizar (EDM)

A continuación, la **Tabla 23** y la **Tabla 24** establecen el análisis de brecha para los procesos *EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno*, y *EDM03. Asegurar la optimización del riesgo*.

Tabla 23

Análisis de brecha EDM01

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la gestión de Gobierno Corporativo. -Modelo de toma de decisiones. -Partes interesadas y obligaciones. -Informes de Gobierno Corporativo.	Requerimientos en COBIT 2019: -Principios rectores del gobierno empresarial. -Modelo de toma de decisiones. -Niveles de autoridad. -Comunicación del gobierno de la empresa. -Método de sistema de recompensa. -Retroalimentación del rendimiento y eficacia del gobierno.	No se contemplan los siguientes requerimientos: principios, niveles de autoridad, comunicación del gobierno, métodos de recompensa y realimentación del rendimiento y eficacia.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Nota. Elaboración propia.

Tabla 24

Análisis de brecha EDM03

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la gestión del riesgo. -Evidencia de aprobación del apetito,	Requerimientos en COBIT 2019: -Guía de apetito del riesgo. -Evaluación de actividades de gestión de riesgos.	No se contemplan los siguientes requerimientos: proceso para la medición de la gestión del riesgo, objetivos para monitorizar la gestión del riesgo, acciones	Actualización de la matriz de requerimientos, sección **5.1.1**.

Situación actual	Situación deseada	Brecha	Plan de Acción
tolerancia y perfil del riesgo. -Perfil del riesgo de la organización y de TI.	-Niveles aprobados de tolerancia al riesgo. -Proceso aprobado para la medición de la gestión de riesgos. -Objetivos clave a monitorizar para la gestión de riesgos. -Políticas de gestión de riesgos. -Acciones remediales para solucionar las desviaciones de gestión de riesgos. -Problemas de gestión de riesgos para el consejo de administración.	remediales, problemas de la gestión de riesgo, y la evaluación de las actividades de gestión de riesgos, o los niveles aprobados de riesgos.	

Nota. Elaboración propia.

4.2.1.2. Alinear, Planificar y Organizar (APO)

A continuación, la **Tabla 25** y **la Tabla 26** establecen el análisis de brecha para los procesos *APO09. Gestionar los acuerdos de servicio*, y *APO13. Gestionar la seguridad*.

Tabla 25

Análisis de brecha APO09

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados a la gestión de los acuerdos de servicio de TI. -Evidencia de revisiones periódicas del catálogo de servicios. -Catálogo(s) de servicios de TI.	Requerimientos en COBIT 2019: -Brechas identificadas en servicios de TI. -Definiciones de servicios estándar. -Catálogos de servicios. -Acuerdos de nivel de servicio (SLA). -Acuerdos de nivel operativo (OLAs).	-No se contemplan los siguientes requerimientos: brechas en servicios de TI, definición de servicios estándar, planes de acción de mejora y remediaciones, actualización de SLAs y OLAs.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Situación actual	Situación deseada	Brecha	Plan de Acción
-Acuerdos a nivel de servicios y evidencia de su aprobación por parte del negocio (SLA). -Informes de rendimiento de los SLAs vigentes.	-Planes de acción de mejora y remediaciones. -Informes de rendimiento del nivel de servicio. -SLA actualizados.		

Nota. Elaboración propia

Tabla 26

Análisis de brecha APO13

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la gestión del Sistema de Gestión de Seguridad de la Información (SGSI) -Organigrama de seguridad de la información. -Declaración del alcance de SGSI. -Plan de seguridad. -Informes de auditoría del SGSI.	Requerimientos en COBIT 2019: -Declaración del alcance de la SGSI. -Política de SGSI. -Plan de tratamiento del riesgo de seguridad de la información. -Casos de negocio de seguridad de la información. -Recomendaciones para la mejora de SGSI. -Informes de auditoría del SGSI.	No se contemplan los siguientes requerimientos: políticas, casos de negocio y recomendaciones de mejora para SGSI.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Nota. Elaboración propia.

4.2.1.3. Construir, Adquirir e Implementar (BAI)

A continuación, la **Tabla 27** y **la Tabla 28** establecen el análisis de brecha para los procesos *BAI06. Gestionar los cambios de TI* y *BAI09. Gestionar los activos*.

Tabla 27

Análisis de brecha BAI06

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados a la gestión de cambios y cambios de emergencia. -Listado de cambios durante el periodo auditado. -Listado de cambios de emergencia durante el periodo auditado. -Plan de cambios y cronograma. -Reglamento del comité de cambios.	Requerimientos en COBIT 2019: -Plan y cronograma de cambios. -Solicitudes de cambio aprobadas. -Evaluaciones del impacto. -Revisión posterior a la implementación. -Informes de estado de las solicitudes de cambio. -Cambio en la documentación.	No se contemplan los siguientes requerimientos: solicitudes de cambio aprobadas, evaluaciones del impacto, revisiones post implementación, informes de estado de las solicitudes y cambios en documentación.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Nota. Elaboración propia.

Tabla 28

Análisis de brecha BAI09

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la gestión de activos. -Registro de activos de TI. -Resultados de comprobaciones físicas de inventarios. -Listado de activos críticos. -Resultado de auditoría de licencias instaladas.	Requerimientos en COBIT 2019: -Resultados de revisiones de idoneidad. -Registro de activos. -Resultados de comprobaciones de inventario físicas. -Comunicaciones de suspensiones por mantenimiento planificado. -Contratos de mantenimiento.	No se contemplan los siguientes requerimientos: resultados de revisiones de idoneidad, comunicaciones de suspensiones, contratos de mantenimientos, retiradas de activos, actualización de activos, solitudes aprobadas de activos, oportunidades para reducir costes o aumentar el valor de	Actualización de la matriz de requerimientos, sección **5.1.1**.

Situación actual	Situación deseada	Brecha	Plan de Acción
-Registro de licencias de software. -Resultados de revisiones de optimización de costes de gestión de activos.	-Retiradas autorizadas de activos. -Registro actualizado de activos. -Solicitudes aprobadas de adquisiciones de activos. -Oportunidades para reducir los costes o aumentar el valor de los activos. -Resultados de las revisiones de optimización de costes. -Plan de acción para ajustar el número y asignaciones de licencias. -Registro de licencias de software. -Resultados de las auditorías a las licencias instaladas.	activos, y plan de acción para gestionar licencias.	

Nota. Elaboración propia.

4.2.1.4. Entregar, Dar Servicio y Soporte (DSS)

A continuación, la **29** y la **Tabla 30** establecen el análisis de brecha para los procesos *DSS02. Gestionar las peticiones y los incidentes de servicio* y *DSS03. Gestionar los problemas*.

Tabla 29

Análisis de brecha DSS02

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la gestión de peticiones de servicio e incidentes. -Criterio para registro de problemas. -Reglas de escalamiento de incidentes. -Listado de incidentes y peticiones de servicio. -Esquema de clasificación y priorización de incidentes. -Informes de estado de cumplimiento de atención de peticiones de servicio. -Informes de estado de cumplimiento de atención de incidentes.	Requerimientos en COBIT 2019: -Criterios para el registro de problemas. -Reglas para el escalamiento de incidentes. -Esquema y modelos de clasificación de peticiones de servicio e incidentes. -Peticiones de servicio e incidentes clasificadas y priorizadas. -Registro de solicitudes de servicio e incidentes. -Peticiones de servicio aprobadas. -Peticiones de servicios completadas. -Log de problemas. -Síntomas de incidente. -Resoluciones de incidentes. -Confirmación del usuario del cumplimiento y resolución satisfactoria. -Cierre de peticiones de servicio e incidentes. -Estado de incidentes e informe de tendencias. -Estado de cumplimiento de peticiones e informe de tendencias.	No se contemplan los siguientes requerimientos: registro de solicitudes de servicio e incidentes, log de problemas, síntomas del incidente, resolución de incidentes, confirmaciones de usuario, y cierre de peticiones e incidentes.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Nota. Elaboración propia.

Tabla 30

Análisis de brecha DSS03

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relaciones con la gestión de problemas. -Listado de problemas durante el periodo auditado. -Esquema de clasificación y priorización de problemas. -Informes de estado de cumplimiento de atención de problemas. -Base de datos de errores conocidos con todos los atributos disponibles en la base de datos.	Requerimientos en COBIT 2019: -Esquema de clasificación de problemas. -Informes de estado del problema. -Registro de problemas. -Informes de resolución de problemas. -Causas raíz de problemas. -Soluciones propuestas a errores conocidos. -Registro de errores conocidos. -Comunicación de conocimientos aprendidos. -Registro de problemas cerrados. -Soluciones sostenibles identificadas. -Informes de supervisión de resolución de problemas.	No se contemplan los siguientes requerimientos: informes de resolución de problemas, causa raíz de los problemas, soluciones propuestas, comunicación de conocimiento aprendido, registro de problemas cerrados, soluciones, e informes de supervisión.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Nota. Elaboración propia.

4.2.1.5. Monitorizar, Evaluar y Valorar (MEA)

A continuación, la **Tabla 31** y la **Tabla 32** establecen el análisis de brecha para los procesos *MEA02. Gestionar el sistema de control interno*, y *MEA03. Gestionar el cumplimiento de los requisitos externos*.

Tabla 31

Análisis de brecha MEA02

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la supervisión, evaluación y valoración del sistema de control interno. -Ejemplo de informes de control interno realizados dentro del periodo auditado. -Resultados de las auditorías de TI. -Plan de auditoría de TI. -Plan de control interno de TI. -Resultados de las autoevaluaciones de TI realizadas durante el periodo auditado. -Documentos de auditoría interna.	Requerimientos en COBIT 2019: -Resultados de benchmarking y otras evaluaciones. -Resultados de la supervisión del control interno y sus revisiones. -Evidencia de la efectividad de los controles. -Planes y criterios de autoevaluación. -Resultados de las autoevaluaciones. -Acciones correctivas. -Deficiencias del control.	No se contemplan los siguientes requerimientos: resultados de benchmarking y otras evaluaciones, acciones correctivas o deficiencias.	Actualización de la matriz de requerimientos, sección **5.1.1**.

Nota. Elaboración propia.

Tabla 32

Análisis de brecha MEA03

Situación actual	Situación deseada	Brecha	Plan de Acción
Requerimientos solicitados: -Documentos relacionados con la supervisión, evaluación y valoración de la conformidad de los requisitos externos.	Requerimientos en COBIT 2019: -Log de acciones de cumplimiento requeridas. -Registro de requisitos de cumplimiento.	No se contemplan los siguientes requerimientos: las comunicaciones de los cambios de requisitos, confirmaciones de cumplimiento, informes de aseguramiento e informes de los	Actualización de la matriz de requerimientos, sección **5.1.1**.

Situación actual	Situación deseada	Brecha	Plan de Acción
-Inventario de requisitos de cumplimiento (requisitos legales, regulatorios y contractual). -Deficiencias de incumplimiento identificadas. -Listado de legislaciones y regulaciones aplicadas.	-Comunicaciones de cambios en los requisitos de cumplimiento. -Políticas, principios, procedimientos y estándares actualizados. -Confirmaciones de cumplimiento. -Brechas de incumplimiento identificadas. -Informes de aseguramiento del cumplimiento. -Informes de los problemas de incumplimiento y sus causas raíz.	problemas de incumplimiento.	

Nota. Elaboración propia.

4.2.2. Análisis de brecha para las herramientas de gestión de la auditoría

El análisis de brecha para las herramientas de gestión de la auditoría se desarrolla para cada herramienta en cuestión. Para la situación actual se toma en cuenta lo descrito y analizado en el análisis de la situación actual. Para la situación deseada se plantea una acción alineada a las actividades de los procesos contenidos en COBIT 2019, según cada aspecto.

4.2.2.1. Reuniones de entendimiento

La **Tabla 33** muestra el análisis de brecha establecido para las reuniones de entendimiento. La situación actual es definida de acuerdo con las respuestas documentadas de la entrevista al gerente y supervisor de TI y encuesta a los asesores. La situación deseada se centra en buscar un guion de estructuras y preguntas alineado con las actividades de COBIT 2019.

Tabla 33

Análisis de brecha para reuniones de entendimiento

Situación actual	Situación deseada	Brecha	Plan de Acción
-No existe un estándar para la documentación y ejecución de reuniones de entendimiento. -La documentación de la reunión se hace en varias herramientas como Word, Excel, o One note, y papel. -Los auditores documentan las respuestas por cada proceso. -La generación de las preguntas queda a criterio de cada auditor, basándose en su conocimiento en COBIT 5. -Cada miembro gestiona la reunión según su criterio profesional.	Guion estandarizado para las reuniones de entendimiento basándose en las actividades de cada proceso de COBIT 2019.	Carencia de un guion estandarizado para gestionar las reuniones de entendimiento y documentar la preguntas y respuestas de la reunión, con base en los procesos, prácticas y actividades definidas en COBIT 2019.	Generación de un instructivo de gestión que formalice y estandarice la documentación de las reuniones de entendimiento, sección **5.1.2**.

Nota. Elaboración propia.

4.2.2.2. Documentación de riesgos

El análisis de brecha de la documentación de riesgos se refleja en la **Tabla 34**. La situación actual es definida de acuerdo con las respuestas documentadas de la entrevista al gerente y supervisor de TI y encuesta a los asesores. La situación deseada se centra en buscar un guion de la definición de riesgos, alineado con las actividades de COBIT 2019.

Tabla 34

Análisis de brecha documentación de riesgos

Situación actual	Situación deseada	Brecha	Plan de Acción
-No existe un estándar para guiar la documentación de los riesgos de auditoría en las fichas de trabajo. -El detalle del riesgo, causa, impacto y recomendación la define el auditor de acuerdo con su criterio y experiencia.	Estandarización en la definición de los apartados de los riesgos basándose en las actividades de cada proceso de COBIT 2019.	Carencia de un guion o catálogo de riesgos que sirva de base para la definición de estos en las fichas de auditoría, alineado a los procesos, prácticas y actividades definidas en COBIT 2019.	Generación de un instructivo de gestión que formalice y estandarice un listado de riesgos por proceso de COBIT 2019, sección **5.1.2**.

Nota. Elaboración propia.

4.2.2.3. Cronograma

El análisis de brecha para el desarrollo del cronograma se efectúa en la **Tabla 35**. La situación actual se determina mediante la revisión documental de los cronogramas de auditorías de TI anteriores, las entrevistas aplicadas al gerente y supervisor de TI y la encuesta aplicada a los asesores. La situación deseada se centra en buscar una estandarización y ponderado de los tiempos en las actividades del cronograma, según lo ya desarrollado por el equipo.

Tabla 35

Análisis de brecha cronograma

Situación actual	Situación deseada	Brecha	Plan de Acción
-Los tiempos en el cronograma son pactados por el criterio de cada auditor y tomando como base auditorías anteriores.	Establecer un guion estandarizado de las actividades y tiempos promedios del cronograma.	-No existen periodos aproximados para trabajar los procesos. -No se incorporan dentro del cronograma tiempos para validaciones o preguntas.	Generación de un instructivo de gestión que formalice los tiempos del cronograma, sección **5.1.2**.

Situación actual	Situación deseada	Brecha	Plan de Acción
-La solicitud de requerimientos dura entre 1 a 5 días. -La revisión de requerimientos dura entre 4 y 5 días. -La evaluación de cada procesos dura entre 1 a 4 días. -El tiempo promedio de preparación de documentos está entre 31 y 57 días. -Los miembros siguen los lineamiento de sus gerentes para realizar el cronograma. -No se definen periodos de tiempo para validaciones o consultas.			

Nota. Elaboración propia.

En resumen, la ejecución de esta segunda fase permitió identificar las brechas para cada herramienta en cuestión. Con respecto a la matriz de requerimientos de procesos tecnológicos, se identifica como brecha la necesidad de contemplar las salidas de cada práctica del proceso según COBIT 2019. Esto porque la documentación actualmente solicitada requiere de más especificación y alineamiento con el nuevo marco de trabajo COBIT 2019.

Para las herramientas de documentación de reuniones de entendimiento, documentación de riesgos y realización del cronograma, se identifica como brecha la carencia de una guía o estándar para llevar a cabo las documentaciones correspondientes. Esto provoca que cada auditor trabaje a su manera, lo cual incurre en confusiones sobre cómo gestionar las actividades correspondientes y provoca comprometer los tiempos de auditoría establecidos.

5. PROPUESTA DE SOLUCIÓN

En este capítulo se procede con el desarrollo de la propuesta de solución ante la problemática planteada para este trabajo. A partir de la información obtenida y analizada en el capítulo anterior, se desarrollan las siguientes tres fases: elaboración de la actualización de la matriz de requerimientos de procesos tecnológicos y el instructivo de gestión, el análisis financiero y la evaluación de la propuesta. Finalmente, una vez desarrolladas cada fase, se procede a contestar las hipótesis planteadas.

5.1. Fase III. Matriz de requerimientos de procesos tecnológicos e instructivo de gestión de ejecución de auditoría

En esta fase se desarrolla la propuesta de solución de una actualización de la matriz de requerimientos de procesos tecnológicos y se elabora un instructivo de gestión para la documentación de las reuniones de auditoría, documentación de riesgos y desarrollo del cronograma. El fin es proporcionar una actualización y estandarización de estas herramientas esenciales durante la ejecución de las auditorías. A continuación, se desglosa cada propuesta.

5.1.1. Matriz de requerimientos de procesos tecnológicos

De acuerdo con el estudio realizado de la matriz de requerimientos actual y mediante la revisión de la información de cada proceso dentro de COBIT, se plantea la matriz de requerimientos de procesos tecnológicos actualizada de acuerdo con COBIT 2019.

La matriz se detalla en el **Apéndice M**. Esta herramienta se desarrolla en Microsoft Excel y contiene seis hojas. La primera hoja, llamada “Inicio”, contiene la introducción formal de la matriz, donde se da una descripción general de esta y se establece el objetivo de guiar al auditado en la entrega de documentación o evidencia sobre los requerimientos solicitados para la auditoría. Asimismo, también indica las instrucciones de uso necesarias para trabajar en ella, las cuales son:

- Brindar la documentación existente que cumpla con el (los) requerimiento(s) definido(s) por cada práctica del proceso. La documentación puede abarcar: planes, políticas, metodologías, reglamentos, procedimientos, guías, manuales, instructivos, protocolos, formularios, o cualquier otro tipo de documentación formal asociada al proceso.

- Completar el apartado de "Documentos proporcionados" con el nombre de los documentos por entregar.
- En caso de requerir una aclaración, excepción, entre otros aspectos, debe indicarse en el apartado de "Comentario".

Las cinco hoja restantes, “EDM”, “APO”, “BAI”, “DSS”, “MEA”, corresponden a la matriz de requerimientos de procesos tecnológicos, de acuerdo con cada dominio de COBIT 2019. A continuación, se explican los apartados de esta.

- Dominio: Se indica el dominio en cuestión, ya sea EDM, APO, BAI, DSS o MEA.
- Proceso: Se listan los procesos de cada dominio, en este caso los diez procesos definidos en el alcance para este proyecto.
- Práctica: Por cada proceso señalado se listan todas las prácticas que este contenga.
- Actividad: Se listan todas las actividades que contiene cada práctica.
- Requerimiento: Se listan las salidas del proceso definidas por COBIT 2019. Se dividen por cada práctica listada.
- Documentación: Se listan algunos tipos de documentación que pueden ser entregados por el auditado para cumplir con el requerimiento. Este apartado es un apoyo para guiar al cliente auditado en la entrega de documentación. Se detallan documentos como políticas, procedimientos, informes, resultados, listados, catálogos, entre otros tipos de documentación necesaria para cumplir con los requerimientos listados.
- Documentos proporcionados: En esta sección, el cliente auditado debe colocar el nombre de los documentos o información que va a adjuntar como evidencia para responder al requerimiento.
- Estado de la solicitud: Esta sección mantiene un control sobre el envío y entrega de la documentación e información de evidencia al cumplimiento de los requerimientos. El auditor del equipo de TI debe colocar los siguientes estados con respecto:
    - *No iniciado:* No se ha enviado a solicitar la información o documentación de evidencia para el requerimiento.
    - *En proceso:* Se solicitó la información o documentación de evidencia al requerimiento al cliente y se está en espera de recibir respuesta y los archivos correspondientes.

- *Finalizado:* El cliente ya entregó la información correspondiente de evidencia para el requerimiento.

- Área: En este apartado, el auditor del equipo de TI debe colocar el nombre de las áreas responsables que deben brindar la documentación respectiva.
- Responsable: En este apartado, el auditor del equipo de TI debe colocar el nombre de la persona a cargo de gestionar la entrega de la documentación respectiva según cada requerimiento solicitado.
- Fecha de solicitud: En este apartado, el auditor del equipo de TI debe indicar la fecha en que se hizo la solicitud de la información.
- Fecha de entrega: En este apartado, el cliente auditado debe indicar la fecha en que está haciendo entrega de la información de evidencia de cada requerimiento.
- Comentarios: En esta sección, tanto el auditor como el cliente auditado deben colocar, en caso de ser necesario, de existir alguna excepción o aclaración, comentarios relacionados con la gestión de la entrega de información.

5.1.2. Instructivo de gestión de ejecución de la auditoría

Este instructivo de gestión de ejecución de la auditoría surge como un estándar para la documentación de las reuniones de entendimiento, la documentación de los riesgos de auditoría y para la realización del cronograma. Este se encuentra en el **Apéndice N**. A continuación, se desglosa el desarrollo de cada punto del instructivo.

- **Introducción:**

  Este apartado describe de forma general el instructivo de gestión para la ejecución de la auditoría; detalla el fin de este y desglosa los apartados que contiene al dar una descripción sobre las reuniones de entendimiento, riesgos de auditoría y cronograma.

- **Documentación de las reuniones de entendimiento**

  La primera sección del instructivo es la documentación de las reuniones de entendimiento. Esta sección contiene una descripción general sobre especificaciones e instrucciones para llevar a cabo las reuniones de entendimiento. Asimismo, contiene un guion de preguntas por cada práctica de los procesos definidos en el alcance. Este guion es

elaborado según lo indicado en las actividades de cada práctica de los procesos de COBIT 2019, y está estructurado de la siguiente manera:

- Práctica: Se indica el nombre de la práctica del proceso en cuestión.
- Preguntas: Se establece una serie de preguntas base tomadas de las actividades de la práctica. Es importante aclarar que la series de preguntas sirven de guion para que cada auditor las adapte de acuerdo con las necesidades y contexto de los clientes auditados.

- **Documentación de los riesgos de auditoría**

  La siguiente sección es la documentación de los riesgos de auditoría. Primeramente, contiene una descripción sobre las especificaciones generales a considerar en la documentación de los riesgos de auditoría. Dentro de estas especificaciones se detalla la estructura ya pactada por el equipo de TI para documentar los riesgos, y se definen los términos utilizados para el impacto de los riesgos. El impacto de los riesgos se detalla según lo establecido por ISO 31000 en el diseño de su marco de gobierno de gestión de riesgos, específicamente en la comprensión de la organización y de su contexto, y según lo mencionado en el artículo de la plataforma ISOTools (2021). Seguido de estas especificaciones, la sección procede con la presentación de posibles riesgos por cada proceso definido dentro del alcance, los cuales sirve como base para plantear los riesgos de acuerdo con el contexto de cada cliente. Para efectos de este proyecto, se definen tres riesgos por cada uno de los diez procesos definido dentro del alcance, siguiendo los apartados de condición, causa, impacto y recomendación.

- **Desarrollo del cronograma de auditoría**

  Esta última sección del instructivo establece un guion para la elaboración del cronograma. Si bien todos los cronogramas varían de acuerdo con cada auditoría, se establecieron duraciones promedio en días para cada actividad dentro del cronograma, considerando únicamente los procesos de COBIT 2019 establecidos en el alcance. Para la elaboración de dicho cronograma, se utiliza el criterio de experto en los siguientes aspectos:

  - Dado que todos los cronogramas poseen duraciones diferentes, se procede a calcular un promedio de los cuatro cronogramas revisados para establecer una duración para

efectos de este instructivo. Los cuatro cronogramas tienen una duración total de 70 a 90 días, con un promedio de 80 días para la elaboración del cronograma base del instructivo.

- Tomando como base los 80 días calculados, se procede a calcular el promedio de cada actividad, a partir de los cuatro cronogramas revisados. Los días resultantes del promedio se redondean para que sean número entero. Este cálculo se muestra en la **Tabla 36** y consume un total de 69 días.
- Los once días restantes serán abarcados para incorporar los espacios de consultas y validaciones. Se da un día para abarcar consultas o validaciones de la matriz de requerimientos y se da un día por cada proceso dentro del alcance para las aclaraciones y validaciones de consultas. Esto porque el máximo de horas que dura una reunión de entendimiento es cuatro, a pesar de que se deba colocar el día por estándar de la empresa, entonces, se puede aprovechar el resto del día para el envío de aclaraciones y validaciones de consultas. Así se completan los 80 días promedio del cronograma.

Tabla 36

Cálculo de promedios de duración por cada actividad del cronograma

Actividad	Cronograma 1	Cronograma 2	Cronograma 3	Cronograma 4	Promedio días	Redondeo días
Kick off	1	1	1	1	1	1
Solicitud y recolección de requerimientos	5	1	5	5	4	4
Revisión de requerimientos	5	4	1	1	4.75	5
Evaluación EDM01	1	4	1	1	1.75	2
Evaluación EDM03	1	4	1	1	1.75	2
Evaluación APO09	1	3	1	1	1.75	2
Evaluación APO13	1	4	1	1	1.75	2
Evaluación BAI06	1	4	1	1	1.75	2
Evaluación BAI09	1	3	1	1	1.75	2
Evaluación DSS02	1	3	1	1	1.75	2
Evaluación DSS03	1	3	1	1	1.75	2
Evaluación MEA02	1	4	1	1	1.75	2
Evaluación MEA03	NA	3	3	NA	2	2
Preparación productos de auditoría	25	26	25	20	24	24

Actividad	Cronograma 1	Cronograma 2	Cronograma 3	Cronograma 4	Promedio días	Redondeo días
Revisión y envío de fichas	2	6	2	3	3.25	3
Reuniones de discusión	4	5	4	5	4.5	5
Ajustes y envío de informe consolidado	6	3	6	5	5	5
Presentación a Comité de TI	1	1	1	1	1	1
Presentación a Órgano de Dirección	1	1	1	1	1	1
					Total	**69**

Nota. Elaboración propia.

Para recapitular lo contenido en esta fase, se efectúa el desarrollo de la propuesta de solución respectiva para la problemática. Por un lado, se plantea y desarrolla la matriz de procesos de requerimientos actualizada a la versión de COBIT 2019, que abarca bajo nivel de detalle y apartados de control de información. Por otro lado, se estructura y desarrolla el instructivo de gestión, el cual contiene tres apartados: uno para la documentación de reuniones de entendimiento, otro para la documentación de riesgos de auditoría, y otro para el desarrollo del cronograma de auditoría. Cada apartado contiene una descripción de la actividad y un guion para desarrollarlo.

5.2. Fase IV. Análisis Financiero

La presente sección corresponde al análisis financiero de la propuesta de solución desarrollada en la sección anterior. A partir de rangos de datos proporcionados por la empresa, se procede a calcular los montos necesarios para determinar la inversión de la propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019.

Es importante recalcar que este análisis se realizará con promedio de datos proporcionados por la empresa y revisiones en el Ministerio de Trabajo y Seguridad Social o Instituto Nacional de Seguros, dado que muchos son confidenciales y no pueden ser detallados.

5.2.1. Presupuesto del equipo de TI

De acuerdo con lo indicado por el gerente de TI:

- Una auditoría de TI consume entre 340 a 350 horas.
- El rango de cobro por hora ronda entre $60 y $70, el cual ya tiene considerado todos los gastos, costos y utilidades necesarias.
- Anualmente, se promedia una cantidad de siete auditorías.

Entonces, asumiendo como dato oficial el promedio de los rangos de horas y de cobros, se tiene que el equipo de TI cobra aproximadamente $22 425.00 por una auditoría de TI. Como el equipo desarrolla siete auditorías de TI por año, generalmente tienen un presupuesto anual de $156,975.00 para el desarrollo de proyectos de auditoría de TI, el cual es detallado en la **Tabla 37**.

Tabla 37

Presupuesto de auditoría

Concepto	Monto
Promedio de horas de auditoría (340 a 350 h)	345
Promedio de cobro por hora ($60 a $70)	$65
Monto aproximado de cobro de una auditoría	$22,425.00
Cantidad de auditorías por año	7
Presupuesto anual para auditorías de TI	**$156,975.00**

Nota. Elaboración propia.

5.2.2. Inversión inicial de la propuesta

Para la elaboración de la propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, según lo establecido por COBIT 2019, se destinó un total de 16 semanas en las cuales se trabaja 40 horas cada una. Luego, se destinaron cuatro semanas para la capacitación al equipo sobre estas herramientas. Como los salarios son información confidencial, se utilizó el salario mínimo de un licenciado universitario dado por el Ministerio de Trabajo y Seguridad Social, el cual es ₡696,873.72, para calcular los

costos de ambas actividades. A este salario se le reducen las cargas sociales del 10.50% que debe pagar todo trabajador, dando un total neto de ₡623,701.98.

A este salario del licenciado universitario, se le agregan los montos que la organización debe aportar, los cuales son tomados de fuentes como la Caja Costarricense del Seguro Social, Instituto Nacional de Seguros, y fuentes de certificaciones. Entre estos costos se encuentran:

- Aportes del patrono en Caja Costarricense del Seguro Social (CSSS), otras instituciones como cuota patronal Banco Popular, Asignaciones Familiares, IMAS, INA, y, ley de protección del trabajador, equivalente a un 26.50% del salario del licenciado universitario, dando como monto total ₡184,671.54.
- Póliza de riesgos del trabajador: Dado que este apartado suele ser calculado con la planilla total de la organización, y no se tiene acceso a esta por temas de confidencialidad, se toma como base únicamente el salario del licenciado universitario, para calcular la prima por una única persona de forma anual. En este caso el monto asegurado se obtiene con la cantidad de salarios a pagar durante el año, es decir, 12 salarios establecidos por el Ministerio de Trabajo de Seguridad Social, dando un monto de ₡8,362,484.64. Luego, se estima que la tarifa de la actividad económica de la organización, en este caso auditoría y consultoría, es de 0.37%. La multiplicación del monto por la tarifa da una prima anual de ₡30,941.19 anual, lo cual quiere decir que la organización incurre en un monto ₡2578.43 de forma mensual en un licenciado universitario para temas de riesgos de trabajo.
- Certificaciones en el marco de referencia COBIT 2019. Mediante un convenio con ISACA, una certificación de fundamentos de COBIT 2019 tiene el costo de $525 con examen incluido, es decir, ₡351 750, tomando como tipo de cambio ₡670.
- Dado que el desarrollo del proyecto se trabaja 100% en modalidad virtual, no se incluyen gastos de servicios como agua, luz, o acceso a internet.

De esta manera, el precio total mensual de un licenciado universitario como parte del equipo de TI es de ₡1,162,701.95. Debido a que el presupuesto del equipo de TI es en dólares, se estima el tipo de cambio del dólar en ₡670, lo cual da como resultado un monto de $1735.38.

Dada esta información, calcula la inversión inicial de la siguiente manera. Primeramente, como se muestra en la **Tabla 38**, se divide el precio del licenciado universitario entre 160 horas. Esto

surge porque se trabaja 40 horas semanales durante 16 semanas, para un total de 640 horas de trabajo. Estas horas de trabajo se dividen entre cuatro semanas (asumiendo que el mes tiene cuatro semanas), resultando 160 horas de trabajo al mes. De esta manera, el salario de un licenciado universitario por horas es de $10.85.

Posteriormente, ese costo por hora en dólares es multiplicado por el total de horas del desarrollo del proyecto y resulta así una inversión de $6,941.50

Luego, para las cuatro semanas de capacitación se estima invertir un 40% del salario mensual de un auditor, el cual será invertido en la elaboración de material de capacitación y ejecución de esta. Tomando como referencia el salario de un licenciado universitario, se obtiene que el 40% corresponde a $694.15.

Finalmente, la inversión total tiene un valor de **$7,635.65**.

Tabla 38

Inversión inicial

Investigación y Desarrollo de la Propuesta de Solución					
Concepto	**Monto colones**	**Monto dólares**	**Monto por hora en dólares**	**Plazo total horas**	**Inversión total**
Licenciado universitario	₡1,162,701.95	$1735.38	$10.85	640	$6,941.50
Capacitaciones de la propuesta de solución					
Concepto	**Salario mensual**		**40% del salario**	Plazo total semanas	**Inversión total**
Capacitación	$1735.38		$694.15	4	$694.15
				Total	**$7,635.65**

Nota. Elaboración propia.

5.2.3. Evaluación de rendimiento

Para calcular el rendimiento del desarrollo de esta propuesta, se estima que los ingresos del equipo en auditorías de TI a un año son de $156,975.00. Esto, asumiendo lo establecido en la sección

5.2.1. Asimismo, el gerente de TI indica que esperan un incremento de los ingresos de auditoría en un aproximado de 0.70% para un año.

Entonces, se estima que la propuesta de actualización de una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditorías, basados en COBIT 2019, contribuye a obtener mínimo ese 0.70% de crecimiento en los ingresos de forma anual durante tres años, para un total de $474,229.17, tal y como se muestra en la tabla **Tabla 39**.

Tabla 39

Ingresos por año

Concepto	Año 1	Año 2	Año 3	Total
Ingresos	$156,975.00	$158,073.83	$159,180.34	**$474,229.17**

Nota. Elaboración propia

Luego, se calcula la inversión total a tres años, la cual corresponde a la inversión inicial y tres años de operación, correspondientes al 70% de los salarios de los miembros del equipo de TI, dado que es el porcentaje aproximado que invierten en proyectos de auditoría. La inversión se muestra en la **Tabla 40**. Se estima que los salarios también aumenten un 0.70% anual.

Tabla 40

Estimación de la inversión a tres años

Costos de la Investigación y Desarrollo de la propuesta de solución					
Concepto	**Inversión inicial**	**Año 1**	**Año 2**	**Año 3**	**TOTAL**
Investigación, desarrollo e implementación de la propuesta de solución					
Salario licenciado universitario	$6,941.50				$6,941.50
Capacitaciones	$694.15				$694.15
Operación de la propuesta de solución					
Salarios equipo TI		$72,885.79	$73,395.99	$73,909.77	$220,191.55
				Total	**$227,827.21**

Nota. Elaboración propia.

Entonces, a partir de estos datos estimados se calcula el retorno de inversión de la siguiente manera:

ROI = ((Ingresos – Inversión) ÷ Inversión) * 100

ROI = (($474,229.17–$227,827.21) ÷ $227,827.21) * 100

ROI = 108%

Este resultado de ROI indica que a los tres años posteriores del desarrollo de la propuesta se ha recuperado la inversión 1.08 veces. Con un ROI positivo se estima que los resultados de la inversión como propuesta de actualización de una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de las auditorías, basados en COBIT 2019, son viables y satisfactorios.

5.2.4. Beneficios no financieros

Entre los beneficios no financieros generados a partir de esta propuesta, se detallan los siguientes:

- Herramienta de matriz de requerimientos de procesos tecnológicos actualizada y alineada al marco de referencia COBIT 2019.
- Herramientas para la documentación de reuniones de entendimiento, documentación de riesgos de auditoría, y elaboración del cronograma, estandarizadas y alineadas al marco de referencia COBIT 2019.
- A partir de la actualización y estandarización de estas herramientas, se promueve el entendimiento común sobre qué es cada herramienta y cómo debe utilizarse, lo cual le brinda al equipo de TI un orden para trabajarlas por medio de una única estructura e instrucciones de las actividades.
- El entendimiento común y orden de las herramientas propuestas, favorecen la comunicación entre los auditores, lo cual aumenta la calidad de las actividades de auditoría y por ende, mantiene la reputación del equipo de TI como ente auditor.

En resumen, el desarrollo de una propuesta de actualización de una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditorías, basados en COBIT 2019 genera un costo de $7,635.65. Si se incrementan los ingresos a un 0.70% y se consideran los costos de operación a tres años, se obtendría un ROI de 108% y resulta viable la solución propuesta.

5.3. Fase V. Evaluación de la pertinencia de la solución

Esta es la última fase y corresponde a la aplicación de un plan piloto para validar el cumplimiento de la propuesta de solución con respecto a la problemática definida. Este plan piloto está compuesto por cuatro pruebas piloto, una por cada herramienta propuesta, las cuales son aplicadas en dos sesiones virtuales dentro del equipo de auditoría (gerente TI, supervisor de TI y asesores). A continuación, se desglosa cada una de las etapas del plan piloto en cuestión.

1. Objetivo del plan piloto

El objetivo de la aplicación del plan piloto es identificar el nivel de cumplimiento de la propuesta de solución como parte de la actualización y estandarización de las herramientas utilizadas durante el proceso de auditoría por parte del equipo de TI del área de *Management Consulting*.

2. Duración

La duración del plan piloto es de aproximadamente dos horas.

3. Selección

El contexto del plan piloto hace referencia a una auditoría de TI realizada en el año 2021 donde el cliente corresponde a una entidad financiera dedicada al desarrollo del mercado bursátil y es participante activo en el mercado local de Costa Rica. La idea es tomar el contexto de esta auditoría para ejecutar las pruebas piloto y efectuar las evaluaciones y valoraciones correspondientes.

Definido el contexto del plan piloto, se procede a establecer cuatro pruebas piloto, las cuales se encuentran en el **Apéndice Ñ**. Estas se basan en dos apartados. El primer apartado corresponde a las indicaciones, donde por cada prueba se debe brindar una opinión sobre la

herramienta en términos de estructura, nivel de detalle, estandarización, comprensión, recomendaciones, ajustes, disminución de horas extra y luego deben calificar el cumplimiento en bajo, medio o alto. El segundo apartado es la descripción de las pruebas, donde se posiciona a los miembros en el contexto de una entidad financiera que está siendo auditada y ya ha sido auditada años anteriores por la firma y se les insta a evaluar las herramientas propuestas para que determinen si cumplen o no dentro de las actividades que ellos mismos realizan.

Para llevar a cabo lo anterior, se ejecuta un grupo focal y una encuesta. Para el grupo focal se agendan dos sesiones con los miembros del equipo de TI, en donde se les expone la prueba; posterior a esto se les realiza una serie de preguntas para que discutan y den su opinión, recomendaciones o ajustes. La encuesta se efectúa una vez finalizado el grupo focal, para que estos califiquen el nivel de cumplimiento de las herramientas de acuerdo con la escala de numeración propuesta.

Como se menciona en el párrafo anterior, estas pruebas son aplicadas a todos los integrantes del equipo de TI, los cuales corresponden al gerente de TI, el supervisor de TI y los tres asesores.

4. Medición

La determinación del nivel de cumplimiento se define a partir de escalas de evaluación. Se establecen dos escalas. La primera es mostrada en la **Tabla 41** y busca determinar el cumplimiento de la propuesta de solución en términos de la respuesta hacia problemática establecida. En esta escala se definen los niveles: alto, medio y bajo. La segunda escala numérica, mostrada en la **Tabla 42**, es para determinar el cumplimiento de la propuesta de solución con respecto a la disminución de horas extras laborales. Define tres niveles: alto, medio y bajo.

Para ambas escalas, los miembros del equipo de TI proceden a seleccionar el nivel posterior a la aplicación del grupo focal. Finalizada la calificación de las cuatro pruebas, estas se analizan para dar un nivel de la propuesta de solución en general.

Tabla 41

Niveles de cumplimiento: respuesta a problemática

Nivel	Descripción
Alto	La propuesta de solución, la cual corresponde a la matriz de requerimientos tecnológicos y un instructivo de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma, responde como solución ante la problemática de desactualización y desestandarización de herramientas utilizadas por el equipo de TI. Todas las herramientas cumplen con las expectativas para gestiona la actividad que apoyan.
Medio	La propuesta de solución, la cual corresponde a la matriz de requerimientos tecnológicos y un instructivo de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma, responde parcialmente como solución ante la problemática de desactualización y desestandarización de herramientas utilizadas por el equipo de TI. Esto debido a que algunos apartados de las herramientas no cumplen con las expectativas para gestionar la actividad a la que apoyan.
Bajo	La propuesta de solución, la cual corresponde a la matriz de requerimientos tecnológicos y un instructivo de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma, no responde como solución ante la problemática de desactualización y desestandarización de herramientas utilizadas por el equipo de TI. Esto debido a que todas las herramientas no cumplen con las expectativas para gestionar la actividad a la que apoyan.

Nota. Elaboración propia.

Tabla 42

Niveles de cumplimiento: respuesta a cargas laborales

Nivel	Descripción
Alto	La propuesta de solución, la cual corresponde a la matriz de requerimientos tecnológicos y un instructivo de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma, disminuye las cargas laborales en más de un 50%.
Medio	La propuesta de solución, la cual corresponde a la matriz de requerimientos tecnológicos y un instructivo de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma, responde como solución ante la problemática de desactualización y desestandarización de herramientas utilizadas por el equipo de TI, disminuye las cargas laborales actuales entre 20% a 50%.
Bajo	La propuesta de solución, la cual corresponde a la matriz de requerimientos tecnológicos y un instructivo de gestión para la documentación de reuniones de entendimiento, documentación de riesgos y desarrollo del cronograma, disminuye las cargas laborales actuales entre 10% a 20%, o las mantiene igual.

Nota. Elaboración propia.

5. Resultados

A continuación, se describen los resultados del grupo focal de la matriz de requerimientos tecnológicos en el **Apéndice O**, los resultados del grupo focal del instructivo de gestión en el, **Apéndice P**, **Apéndice Q**, **Apéndice R**, y la encuesta efectuada al equipo de TI, en el **Apéndice S**. Los resultados de la encuesta también se complementan en la **Figura 32** y la **Figura 33**.

a. Prueba #1: Matriz de requerimientos de procesos tecnológicos

Primeramente, de acuerdo con la encuesta efectuada, la matriz de requerimientos de procesos tecnológicos propuesta se considera con un nivel de cumplimiento alto en términos de solución a la problemática. Como parte de la conversión del grupo focal, la mayoría de los miembros afirman que la matriz cumple con un bajo nivel de detalle al contener la información de cada práctica, actividad, requerimiento de salida y ejemplos de documentación. Asimismo, contiene una portada e instrucciones de uso que facilita la comprensión del cliente para interpretar la herramienta. Como recomendación de formato, se solicitan dos aspectos: el primero corresponde a especificar una definición para los tipos de documentación, dado que los clientes tienen interpretaciones variadas sobre lo que es un procedimiento, política, metodología, otro. El segundo aspecto, solicitado por el gerente de TI, corresponde a agregar una hoja de guía de usuario que redacte los apartados de las columnas explicados al momento del grupo focal.

Luego, todas las respuestas en la encuestas apuntan a que la matriz de requerimientos propuesta tiene un nivel bajo con respecto al cumplimiento en disminución de cargas laborales. En el grupo focal el equipo en su totalidad enfatiza que la herramienta propuesta promueve un entendimiento sobre la funcionalidad y gestión de la matriz de requerimientos y facilita la comprensión no solo para el cliente sino para aquellos miembros no familiarizados con el proceso, tales como futuros integrantes del equipo. Ayuda que todo el equipo y los clientes estén en una misma línea de trabajo, no obstante, consideran que sus horas extras actuales, las cuales eran entre cuatro a siete, se mantienen.

b. Prueba #2 Instructivo de gestión - Documentación de las reuniones de entendimiento

Por un lado, en general el equipo indica que el guion y estructura realizada para las reuniones de entendimiento tiene un alto cumplimiento para resolver el problema de desactualización y desestandarización. Algunos miembros enfatizan como recomendación dentro del grupo focal la importancia de siempre colocar preguntas relacionadas con la ubicación de los documentos, cuál es el nombre y que muestren la evidencia, sobre todo para aquellas preguntas que describen si tienen un procedimiento, plan o protocolo. Esto para que cliente no solo conteste "sí", sino que brinde evidencia o pruebas de su respuesta.

Por otro lado, el grupo focal dio lugar a que el equipo indicara que con este guion ya todos los miembros seguirán la misma línea para plantear reuniones de entendimiento, además de que encontrarán ejemplos básicos que pueden utilizar para formular consultas. Sin embargo, las horas extras no dependen solo de ellos, sino también del tiempo de los clientes y cuánto dure cada uno en clarificar el proceso, por lo tanto consideran que actualmente sus cargas laborales se mantienen o disminuyen una hora máximo.

c. Prueba #3: Instructivo de gestión - Documentación de los riesgos de auditoría

Según el grupo focal y la encuesta realizada, el equipo queda satisfecho con la elaboración del guion y estructura para la documentación de riesgos. Afirman que los ejemplos de riesgos se adaptan y cumplen con la estructura y escritura que mantiene la firma, además de que brindan varios ejemplos de riesgos por proceso, lo cual hace que todos los miembros sepan cómo deben redactarlos y les facilite su documentación. Por esta razón tienen un nivel alto de cumplimiento como respuesta a la problemática.

No obstante, al igual que la matriz y las reuniones de entendimiento, el equipo indica que sus horas actualmente se mantienen o pueden disminuirse aproximadamente una hora. Esto porque no solo se documentan los riesgos en la ficha de auditoría, sino otros aspectos y a veces estos pueden generar atrasos por temas de aclaraciones, consultas o discusiones con los clientes.

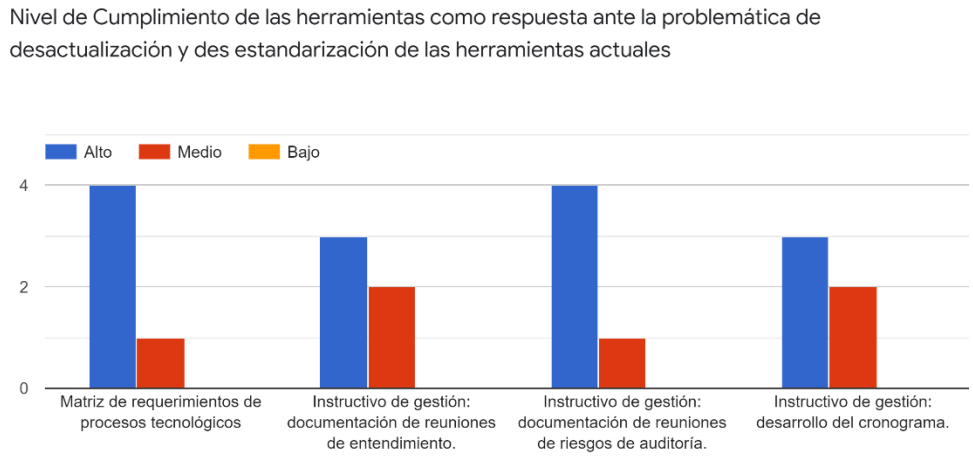
d. Prueba #4: Instructivo de gestión - Desarrollo del cronograma

El equipo de TI afirma que el cronograma propuesto tiene un alto nivel de cumplimiento para favorecer la actualización y estandarización. Si bien el cronograma es muy especializado para cada tipo de auditoría de TI que se realice, establece las actividades más comunes y ponderados de tiempo reales que pueden ser utilizados a la hora de formar un cronograma. A manera de formato, se recomienda colocar aquellas actividades de entrega de productos como hitos y separarlas de todo ajuste o consulta que deba realizarse. Asimismo, se recomienda que todas las actividades tengan predecesoras para facilitar la comprensión del orden del cronograma.

No obstante, como se ha indicado en secciones anteriores y nuevamente es descrito en el grupo focal, el equipo radica en que los tiempos son muy variables entre cliente y cliente, por lo cual pueden existir algunos para quienes el cronograma se vea comprometido y se deban asumir horas extras. Sin embargo, un miembro enfatiza en la recomendación de acortar aquellos tiempos relacionados con reuniones, pues estas no duran el día completo, de esta manera se pueden aprovechar los días y así hacer del cronograma un insumo principal para incentivar la disminución de cargas laborales.

Figura 32

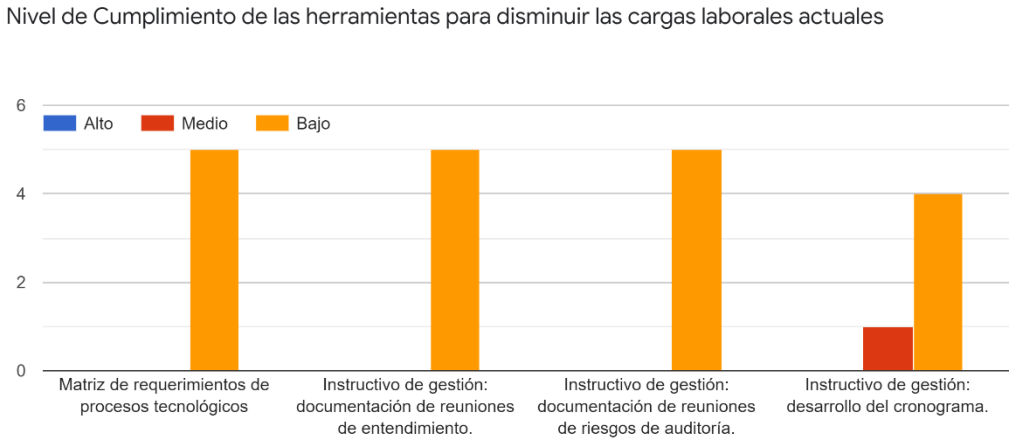
Nivel de cumplimiento de la propuesta de solución como respuesta a la problemática



Nota. Elaboración propia.

Figura 33

Nivel de cumplimiento de la propuesta de solución para disminuir cargas laborales



Nota. Elaboración propia.

7. Productos finales

Una vez efectuadas las pruebas, se procede a realizar los ajustes correspondientes dadas las recomendaciones del equipo, según cada herramienta. Es importante aclarar que para la documentación de riesgos, el equipo consideró el apartado apropiado, por lo cual no realizó ajustes.

- Matriz de requerimientos de procesos tecnológicos: Se incorpora la definición de los tipos de documentación de acuerdo con las definiciones planteadas por el equipo y lo establecido en la Real Academia Española, así como un apartado de guía de usuario en donde se detallan las secciones de la matriz de requerimientos. Su versión final se muestra en el **Apéndice T**.
- Instructivo de gestión-Documentación de reuniones de entendimiento: Se procede con la revisión de todas las preguntas propuestas para colocar las interrogantes relacionadas con el nombre y ubicación de documentos, así como la muestra de evidencia. Se observa en el **Apéndice U**.

- Instructivo de gestión-Desarrollo del cronograma: Se disminuyen los tiempos de las reuniones para que sean equivalentes a dos horas aproximadamente. Se separan las acciones de enviar productos de auditoría y se colocan como hitos para clarificar que es una entrega. Se muestra en el **Apéndice U**.

En resumen, esta fase de evaluación de la pertinencia de la propuesta de solución arroja dos resultados. El primero es que la propuesta de solución, correspondiente a la matriz de requerimientos de procesos tecnológicos y el instructivo de gestión, sí cumple como una respuesta ante la problemática de desactualización y desestandarización de las herramientas utilizadas en el proceso de auditoría. Esto porque promueven un conocimiento compartido que mantiene a todos los miembros del equipo de TI bajo una misma línea de trabajo. Además, facilita la comprensión de las estructuras y actividades para los miembros actuales y nuevos miembros del equipo, e incluso mejora la gestión de las consultas y documentación con el cliente, dado que todas las actividades se realizan con la misma estructura y luego se especializan entre cliente y cliente.

El segundo resultado es que la propuesta no es una respuesta para promover la disminución de las cargas laborales actuales del equipo de TI. El equipo de TI enfatiza que sus cargas laborales en general se mantendrían, disminuirá tal vez una hora o dos, aproximadamente. Se visualiza más la propuesta de solución como un insumo para compartir el conocimiento e instruir al personal de una forma sencilla, entendible y estructurada de cómo realizar las actividades y las herramientas respectivas para completar el proceso de auditoría de forma estandarizada y actualizada. Así, por medio de esta instrucción y aprendizaje se mejora el trabajo de cada auditor.

5.4. Respuesta a las hipótesis planteadas

Esta sección tiene como fin establecer una respuesta a las dos hipótesis planteadas, para confirmar o negar si la problemática identificada genera las consecuencias pactadas y si la propuesta de solución es respuesta a la problemática.

A continuación, se presentan las hipótesis:

- **Hipótesis I:** La desactualización de la matriz de requerimientos de procesos tecnológicos y la desestandarización de las herramientas de gestión utilizadas para la ejecución de las auditorías de tecnología de información dificultan el tiempo de ejecución y aumentan las cargas de trabajo de los auditores en el cumplimiento del proceso de la auditoría
- **Hipótesis II:** Una propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en COBIT 2019, solventan la problemática de desactualización de la matriz de requerimientos de procesos tecnológicos y desestandarización de las herramientas de gestión utilizadas para la ejecución de las auditorías de tecnología de información que enfrenta actualmente el equipo de TI del área de *Management Consulting*.

Por un lado, el análisis de resultados confirma, por medio de las entrevistas y encuestas aplicadas a los miembros del equipo, que existe un aproximado de cuatro a siete horas extra de trabajo con el uso de las herramientas en cuestión. Asimismo, se determina por medio de las entrevistas, encuestas, revisiones documentales y el análisis de brecha, que las herramientas están desactualizadas y desestandarizadas; esto causa confusión y variedad de formas de trabajo cuando debe existir únicamente una base general. Con estos puntos se puede identificar que sí existe la problemática de desactualización y desestandarización de las herramientas de auditorías y que sí existe aumento de las cargas laborales.

Por otro lado, al desarrollar la propuesta de solución y aplicar la evaluación de su pertinencia mediante los grupos focales y la encuesta a los miembros del equipo, se confirma que dicha propuesta de solución, la cual abarca la matriz de requerimientos de procesos actualizada y el instructivo de gestión para la documentación de reuniones de entendimiento, la documentación de riesgos y el desarrollo del cronograma, es una respuesta adecuada para solucionar la desactualización y estandarización de las herramientas. El equipo afirma que con la propuesta todos los miembros tendrán una misma base o línea

de trabajo, lo cual favorece la comprensión de las acciones por llevar a cabo y permite dar un mayor conocimiento para aquellos nuevos integrantes que se incorporen en proyectos de auditoría.

Sin embargo, los miembros afirman que sus horas extras, entre cuatro a siete, se mantendrían o disminuirían máximo una o dos horas. Justifican que los atrasos también dependen de la manera del cliente de llevar la auditoría y que si bien ellos como equipo ya tienen el insumo de la propuesta de solución que les permiten agilizar su trabajo en las actividades de auditoría, no pueden afirmar una reducción considerable, dada la variedad de los tiempos entre ellas.

Por lo anteriormente explicado, se puede confirmar la **Hipótesis II**, pues la propuesta de solución solventa la desactualización y desestandarización de las herramientas, lo cual proporciona una línea base de trabajo para todos los miembros del equipo de TI. No obstante, por lo indicado en la evaluación de la propuesta de solución, se rechaza la **Hipótesis I**, porque el equipo de TI afirma no tener disminución en las cargas laborales.

6. CONCLUSIONES

En este capítulo se especifican las conclusiones obtenidas a partir del trabajo realizado al equipo de TI del área de *Management Consulting*. A continuación, para cada objetivo planteado, se señalan las conclusiones correspondientes.

6.1. Conclusiones Objetivo específico 1

En referencia al objetivo específico 1: *Analizar la situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión utilizadas por el equipo de TI, para la identificación de hallazgos y oportunidades de mejora*, se concluye lo siguiente:

- La matriz de requerimientos de procesos tecnológicos utilizado por el equipo de TI, la cual es desarrollada en COBIT 5, tiene una estructura y detalle de alto nivel por cada proceso de COBIT 5, sin considerar sus prácticas y actividades. La entrega de este documento al cliente es informal, ya que carece de instrucciones de uso y entrega de los diferentes requerimientos. El estado actual descrito incurre en solicitar documentación repetidamente en otras etapas futuras del proceso de auditoría y confusiones a la hora de interpretar la herramienta y su información.
- El equipo de TI no cuenta con un manual o estándar para desarrollar y gestionar las herramientas para la documentación de reuniones de entendimiento, la documentación de riesgos de auditoría, y el desarrollo del cronograma de auditoría.
- Las reuniones de entendimiento son estructuradas y planteadas de acuerdo con el criterio de cada auditor, el cual establece las preguntas, selecciona las herramientas física o digital para su documentación y crea el guion para llevar a cabo la reunión.
- La documentación de los riesgos de auditoría sigue una estructura de condición, causa, impacto y recomendación, la cual es preestablecida por el equipo. Sin embargo, la documentación de esta estructura queda a criterio de cada auditor, el cual utiliza su experiencia o se guía con auditorías anteriores, siempre cumpliendo los lineamientos dado por los superiores.
- El desarrollo del cronograma de auditoría es por medio de Microsoft Project. Los miembros del equipo realizan el cronograma tomando como referencia cronogramas de auditorías anteriores así como pautas de su gerente o supervisor de TI.

- El equipo de TI considera que el uso actual de estas herramientas les aumenta sus cargas laborales entre cuatro y siete horas en las diferentes actividades del proceso de auditoría correspondientes.

6.2. Conclusiones Objetivo específico 2

En referencia al objetivo específico 2: *Aplicar un análisis de brecha, considerando la situación actual y la situación deseada, para la delimitación de la propuesta de solución que solvente la problemática*, se concluye lo siguiente:

- Los requerimientos actuales que solicita la matriz de requerimientos del equipo de TI están a alto nivel y requieren de alineamiento con las salidas establecidas por cada práctica de cada proceso de COBIT 2019.
- El equipo de TI carece de un guion estandarizado para documentar y gestionar la estructura y la recopilación de preguntas y respuestas para las reuniones de entendimiento, alineadas con los procesos, prácticas, actividades y salidas definidas en COBIT 2019.
- El equipo de TI carece de un guion o catálogo de riesgos alineado a los procesos, prácticas, actividades y salidas definidas en COBIT 2019, para estandarizar de forma básica la definición de los riesgos.
- El equipo de TI no tiene definido periodos aproximados para la evaluación de cada proceso así como periodos de validaciones o consultas dentro de los cronogramas de auditoría.

6.3. Conclusiones Objetivo específico 3

En referencia al objetivo específico 3: *Elaborar una matriz de requerimientos de procesos tecnológicos y un instructivo de gestión basados en el marco de referencia COBIT 2019, para la promoción de la actualización y estandarización de estas herramientas utilizadas por el equipo de TI*, se concluye lo siguiente:

- A partir del análisis de situación actual y un análisis de brecha se desarrolló una actualización de la matriz de requerimientos de procesos tecnológicos alineada a diez procesos de COBIT 2019. La matriz es estructurada por dominio, proceso, las prácticas de cada proceso con sus respectivas actividades y salidas. Contiene un apartado de ejemplos de documentación específica para

responder a los requerimientos, así como apartados para llevar el control de estos. Además, tiene un inicio y guía de usuario para aportar a la formalidad de la entrega.

- A partir del análisis de situación y análisis de brecha, se desarrolló un instructivo de gestión de ejecución de la auditoría, alineado a diez procesos de COBIT 2019 y a las actividades realizadas por el equipo de TI. Este contiene tres secciones: guion para documentar las reuniones de entendimiento, guion para documentar los riesgos de auditoría y guion para desarrollar el cronograma.
- El guion para la documentación de reuniones de entendimiento contiene una estructura y lineamientos generales sobre la actividad, así como un listado de posibles preguntas base que pueden ser adaptadas a cada cliente, estas preguntas son alineadas de acuerdo con las actividades de cada proceso.
- El guion para la documentación de los riesgos de auditoría contiene la estructura preestablecida del equipo y un listado de tres ejemplos de definición de riesgo por cada proceso establecido.
- El guion para el desarrollo del cronograma contiene las actividades predeterminadas en las auditorías de TI y un promedio de tiempos por cada actividad, el cual fue calculado por medio de los últimos cronogramas de auditoría realizados.

6.4. Conclusiones Objetivo específico 4

En referencia al objetivo específico 4: *Desarrollar un análisis financiero, para la comprobación de los beneficios y viabilidad de la propuesta de solución*, se concluye lo siguiente:

- La inversión en una propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019, es de $7,635.65. Esta inversión incluye el costo de desarrollo de la propuesta y la capacitación requerida sobre esta.
- El retorno de la inversión para un periodo de tres años, considerando el porcentaje de incremento de los ingresos y los salarios del equipo de TI en la operación, es de 108%, lo cual confirma la viabilidad de la propuesta.

6.5. Conclusiones Objetivo específico 5

En referencia al objetivo específico 5: *Validar la pertinencia de la propuesta de solución, por medio de un plan piloto, para el cumplimiento de esta como respuesta a la problemática*, se concluye lo siguiente:

- La propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019, cumple como solución ante la problemática de desactualización y desestandarización de las herramientas. De acuerdo con el grupo focal y encuesta efectuada, los miembros del equipo de TI consideran que se facilita la comprensión de las estructuras y actividades al pactar una única línea de trabajo para todos los miembros. Dado lo anterior, se confirma la hipótesis II del proyecto.
- No obstante, la propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019, no es una respuesta para promover la disminución de las cargas laborales descritas. De acuerdo con el grupo focal efectuado, los miembros del equipo de TI visualizan la propuesta como un insumo para instruir el conocimiento dentro del equipo, el cual puede contribuir a mejorar el trabajo de cada auditor dado el aprendizaje y guía que genera. Sin embargo, concluyen que los tiempos también dependen del tiempo extra que quiera invertir el cliente en la evaluación de los procesos y demás actividades de auditoría. Por esta razón, se rechaza la hipótesis I.

7. RECOMENDACIONES

En este capítulo se especifican las recomendaciones obtenidas a partir del trabajo realizado al equipo de TI del área de *Management Consulting*. A continuación, se señalan las recomendaciones correspondientes.

1. Utilizar la propuesta de solución para implementar sesiones de capacitación o instrucción acerca del conocimiento de las herramientas de auditoría, sus estructuras, lineamiento y guion de trabajo, de forma que todo el personal comprenda y se ajuste a la línea base de trabajo.
2. Utilizar la propuesta de solución para atender otras regulaciones o auditorías que apliquen como marco de referencia COBIT 2019.
3. Validar que, semanas posteriores a la capacitación, los miembros del equipo estén efectuando las actividades acorde con lo pactado y brindar apoyo en caso de consultas o problemas.
4. Incorporar a la matriz de requerimientos de procesos tecnológicos propuesta los procesos no incorporados en el alcance de este proyecto. Dado que son 30 procesos, se recomienda realizar una priorización sobre cuáles procesos requieren de una pronta actualización a COBIT 2019.
5. Incentivar la actualización y estandarización de cualquier otra herramienta que pueda ser utilizada en el proceso de auditoría de TI.
6. Fijar periodos para la revisión y la actualización de las herramientas de forma que aseguren la veracidad y calidad de la información que contienen.
7. Considerar las realimentaciones brindadas por los clientes o el equipo de TI así como cambios en el marco de referencia COBIT, para efectuar cualquier ajuste a las herramientas.
8. Comunicar las actualizaciones o ajustes realizados en las herramientas a todos los miembros de TI involucrados.
9. Mantener el repositorio del equipo actualizado con las últimas versiones de las herramientas y de acceso completo para todo el equipo de TI.
10. Dado que una consecuencia inicial de la problemática, establecida por el equipo de TI, fue el aumento de cargas laborales, y, dado que la evaluación de la pertinencia demostró que la propuesta de solución no promueve la reducción de cargas laborales, se recomienda al equipo de TI realizar una evaluación de cargas de trabajo para identificar cuáles son las causas del aumento de las horas extra y así solucionarlo de acuerdo con las necesidades y presupuesto del equipo de TI.

8. REFERENCIAS

Acuerdo SUGEF 14-17. *REGLAMENTO GENERAL DE GESTIÓN DE LA TECNOLOGÍA DE INFORMACIÓN*. https://www.sugef.fi.cr/normativa/normativa_vigente/SUGEF%2014-17%20(v%204_%2016%20de%20setiembre%20de%202020).pdf

Acuña, E. (12 de setiembre de 2018). *Auditoría de Tecnologías de Información*. http://www.imcpbc.org/wp-content/uploads/2018/09/Auditor%C3%ADa-de-Tecnolog%C3%ADas-de-Informaci%C3%B3n-compressed.pdf

Alatrista, M. (17 enero de 2019). *Técnicas y Procedimientos de Auditoría. Lo que todo auditor debe conocer*. Auditool. https://www.auditool.org/blog/auditoria-externa/2158-tecnicas-y-procedimientos-de-auditoria-lo-que-todo-auditor-debe-conocer

Alexander, M. (2019, July 17). *What is gap analysis? Uncovering the missing links to successful performance*. CIO. https://www.cio.com/article/220377/what-is-gap-analysis-uncovering-the-missing-links-to-successful-performance.html

Alpízar, L. (2020). *Proceso de auditoría*. [Diapositivas de Power Point].

Auditool. (2020). *Cronograma de actividades basado en el diagrama de Gantt*. https://www.auditool.org/herramientas/guias-practicas/7092-cronograma-de-actividades-basado-en-el-diagrama-de-gantt

Auditool. (4 de enero de 2021). *TOP 10: Herramientas para Auditores más descargadas en el 2020*. https://www.auditool.org/blog/desarrollo-personal/7558-top-10-herramientas-para-auditores-mas-descargadas-en-el-2020

Auditool. (22 de diciembre de 2021). *Las 10 herramientas para Auditores más descargadas en 2021*. https://www.auditool.org/blog/auditoria-interna/8249-las-10-herramientas-para-auditores-mas-descargadas-en-2021#:%7E:text=Auditool%20ofrece%20una%20completa%20biblioteca,modelos%20de%20auditor%C3%ADa%3B%20las%20herramientas

Arief, & I. H. A. Wahab. (2016). Information technology audit for management evaluation using COBIT and IT security (case study on dishubkominfo of north maluku provincial government, indonesia). Paper presented at the - *2016 3rd International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE)*, 388-392. doi:10.1109/ICITACEE.2016.7892477

Blackburn, C. J., Flowers, M. E., Matisoff, D. C., & Moreno, C. J. (2020). Do Pilot and Demonstration Projects Work? Evidence from a Green Building Program. *Journal of Policy Analysis & Management*, *39*(4), 1100–1132. https://doi-org.ezproxy.itcr.ac.cr/10.1002/pam.22218

Bonilla, M. (14 de enero de 2021). *Técnicas de Auditoría. Lo que todo Auditor debe saber*. Auditool. https://www.auditool.org/blog/auditoria-externa/6063-tecnicas-de-auditoria-lo-que-todo-auditor-debe-saber

Espino, M. (2014). *Fundamentos de auditoría* (1 ed.). Grupo Editorial Patria. https://www.editorialpatria.com.mx/pdffiles/9786074387247.pdf

Ferrel, O., Hirt, G., Ramos, L., Adrianséns, M. y Flores, M. (2010).*Introducción a los negocios* (7 ed.). McGraw Hill Educación.

Frett, N. (01 de julio de 2019). *El proceso de auditoría interna en 4 pasos*. Auditool. https://www.auditool.org/blog/auditoria-interna/6607-el-proceso-de-auditoria-interna-en-4-pasos

Google for Education. (s.f). *Pilot Framework*. https://static.googleusercontent.com/media/edu.google.com/es//pdfs/google-pilot-framework-design.pdf

Grupo INS. (s.f). *¿Cómo se calcula el precio del seguro?*. https://www.grupoins.com/seguro-de-riesgos-del-trabajo/calcular-precio-del-seguro/

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la Investigación* (6 ed.). McGraw Hill Education.

Hernández, R. y . (2018). *Metodología de la Investigación. Las rutas cuantitativa, cualitativa y mixta* (1 ed.). McGraw Hill Education.

Inces, C. (2019). *Propuesta de mejora de los controles generales de auditoría de TI en el tema de la seguridad de la Información*. [Trabajo Final de Graduación, Instituto Tecnológico de Costa Rica]. https://tecdigital.tec.ac.cr/dotlrn/clubs/Com.ATI/file-storage/view/documentos-trabajo-final-de-graduaci-n%2Fproyectos-finales-de-graduaci-n-p-blicos%2F2019%2FAuditor%C3%ADa_TI_pruebas_sustantiv_seguridad_Cristopher_Inces_I-2019

ISACA. (2018). *COBIT 2019*.

ISO 31000:2018. *Gestión del riesgo-Directrices*. https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es:sec:5.4.1

ISOTools. (13 agosto de 2021). *Tipos de riesgo según la norma ISO 31000 2018*. Software ISO. https://www.isotools.org/2021/08/13/tipos-de-riesgo-segun-la-norma-iso-31000-2018/

ITIL. (2011). *Continual Service Improvement*. TSO

Kim, S. y Ji, Y. (2018). Gap Analysis. *John Wiley & Sons, Inc*. DOI: 10.1002/9781119010722.iesc0079

KPMG. (2021). *Inducción*.

KPMG. (s.f). *¿Quiénes somos?*. https://home.kpmg/cr/es/home/about/quienes-somos.html

KPMG. (s.f). *KPMG en Costa Rica*. https://home.kpmg/cr/es/home/about/kpmg-costarica.html

KPMG. (s.f). *Our history*. https://home.kpmg/xx/en/home/about/who-we-are/our-history.html

KPMG. (s.f). *Audit*. https://home.kpmg/cr/es/home/Servicios/Audit.html

KPMG. (s.f). *Tax & Legal*. https://home.kpmg/cr/es/home/Servicios/Tax%20&%20Legal.html

KPMG. (s.f). *Advisory*. https://home.kpmg/cr/es/home/Servicios/Consultor%c3%ada.html

Leonard, K., & Bottorff, C. (2022, February 17). *Conducting A Gap Analysis: A Four-Step Template*. Forbes Advisor. https://www.forbes.com/advisor/business/gap-analysis-template/

Microsoft. (2022). *Prueba de concepto o piloto*. https://docs.microsoft.com/es-es/azure/architecture/serverless-quest/poc-pilot

Morales, F. (17 de enero de 2021). *Herramientas de TI para la ejecución de auditorías*. Auditool. https://www.auditool.org/blog/auditoria-externa/6818-herramientas-de-ti-para-la-ejecucion-de-la-auditorias

Ñaupas, H., Mejía, E., Novoa, E. y Villagómez, A. (2014). *Metodología de la Investigación. Cuantitativa – Cualitativa y Redacción de las Tesis* (4 ed.). Ediciones de la U.

Ramírez, C. (2018). *Propuesta de un Manual de Auditoría de Tecnologías de Información. Caso Despacho*. [Trabajo Final de Graduación, Instituto Tecnológico de Costa Rica]. https://tecdigital.tec.ac.cr/dotlrn/clubs/Com.ATI/file-storage/view/documentos-trabajo-final-de-graduaci-n%2Fproyectos-finales-de-graduaci-n-p-blicos%2F2018%2FManual_AuditoriaTI_Carlos_Ram%C3%ADrez_II-2018.pdf

Real Academia Española (RAE). https://www.rae.es/

SUGEF. (s.f). *Marco Estratégico*. https://www.sugef.fi.cr/sugef/marco_estrategico.aspx

SUGEF. (s.f). *Objetivos y funciones*. https://www.sugef.fi.cr/sugef/objetivos_funciones.aspx

Real Academia Española. (s.f). *Plan*. https://dle.rae.es/plan

Real Academia Española. (s.f). *Piloto*. https://dle.rae.es/piloto

Tapia, C., Mendoza, S., Castillo, S., & Guevara, E. (2019). *Fundamentos de auditoría. Aplicación práctica de las Normas Internacionales de Auditoría* (1 ed.). Google Books. https://books.google.co.cr/books?hl=en&lr=&id=4TLfDwAAQBAJ&oi=fnd&pg=PT2&dq=auditor%C3%ADa&ots=HebXBouD17&sig=J__cy4tmRxY2okitzl4HTFuwcME&redir_esc=y#v=onepage&q=auditor%C3%ADa&f=false

Organización Internacional de Normalización (ISO). (2011). *Directrices para la auditoría de los sistemas de gestión. (ISO 19011:2018)*. https://www.iso.org/obp/ui#iso:std:iso:19011:ed-3:v1:es

Ortiz Anaya, H. (2018). *Análisis financiero aplicado, bajo NIIF* (16a ed.). Universidad Externado de Colombia. https://www-digitaliapublishing-com.ezproxy.itcr.ac.cr/a/70953

Otero, A. (2018). *Information Technology Control and Audit*. Taylor & Francis Group, LLC. https://www.researchgate.net/publication/327312550_Information_Technology_Control_and_Audit

Pallerola Comamala, J. (2013). *Gestión financiera*. Rama Editorial. https://www-digitaliapublishing-com.ezproxy.itcr.ac.cr/a/109968

Pérez, A. (24 de abril de 2021). *VAN y TIR, dos herramientas para la viabilidad y rentabilidad de una inversión*. https://www.obsbusiness.school/blog/van-y-tir-dos-herramientas-para-la-viabilidad-y-rentabilidad-de-una-inversion

Pimienta, J. y de la Orden, A. (2012). *Metodología de la Investigación. Competencias + aprendizajes + vida* (1 ed.). Pearson.

SUGESE. (2017). *SEGURO DE RIESGOS DEL TRABAJO. TARIFAS AUTORIZADAS DEL SECTOR PRIVADO POR ACTIVIDAD ECONOMICA*. https://www.sugese.fi.cr/seccion-seguros-obligatorios/SegurosRT/Tarifas_RT_sector_privado_a_partir01_01_7.pdf

Ulate, I. y Vargas, E. (2014). *Metodología para elaborar una tesis* (1 ed.). Editorial Universidad Estatal a Distancia.

Universidad Estatal a Distancia (UNED) y Programa de Producción Electrónica Multimedial (PEM). (2017). *Instrumentos para la evaluación*. https://multimedia.uned.ac.cr/pem/recursos_pace/c-instrumentos-escala-calificacion.html

V. Svatá. (2019). COBIT 2019: Should we care? Paper presented at the - *2019 9th International Conference on Advanced Computer Information Technologies (ACIT),* 329-332. doi:10.1109/ACITT.2019.8779995

Vargas, J.G. (2019). *Propuesta de una Metodología para las Auditorías de Tecnología de Información para entidades reguladas por CONASSIF, Caso: KPMG S.A*. [Trabajo Final de Graduación, Instituto Tecnológico de Costa Rica]. https://tecdigital.tec.ac.cr/dotlrn/clubs/Com.ATI/file-

storage/view/documentos-trabajo-final-de-graduaci-n%2Fproyectos-finales-de-graduaci-n-p-blicos%2F2019%2FPropuesta_Metodologia_para_Auditorias_JoseGabriel_Vargas_II-2019.pdf

Zbrodoff, S. (2012). Pilot Projects—Making Innovations and New Concepts Fly. Paper presented at PMI® Global Congress 2012—EMEA, Marsailles, France. Newtown Square, PA: Project Management Institute. https://www.pmi.org/learning/library/pilot-projects-making-innovations-concepts-6260

9. APÉNDICES

Apéndice A. Plantilla de entrevista semiestructurada de análisis de situación actual para socio del área.

Datos Generales	
Entrevista #	
Fecha	
Entrevistado	Socio del área
Entrevistador	María Jesús Calvo Bolaños
Tema	Situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de auditoría.

Sección de preguntas:

¿Conoce la matriz de requerimientos preliminares y las herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma, utilizadas en el proceso de auditoría?

_____

_____

¿Qué opina de estas herramientas (matriz de requerimientos preliminares, herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma)?

_____

_____

¿Qué expectativas tiene de una propuesta de mejora de estas herramientas (matriz de requerimientos preliminares, herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma)?

_____

_____

Comentarios

_____

_____

Apéndice B. Plantilla de entrevista semiestructurada de análisis de situación actual para Gerente de TI y Supervisor de TI.

Datos Generales	
Entrevista #	
Fecha	
Entrevistado	Gerente de TI y Supervisor de TI
Entrevistador	María Jesús Calvo Bolaños
Tema	Situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de auditoría.

Sección de preguntas:

¿Qué opinan de la matriz de requerimientos preliminares y las herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma?

_____

_____

¿Qué expectativas tienen de una propuesta de mejora de estas herramientas (matriz de requerimientos preliminares, herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma)?

_____

_____

¿Consideran que las herramientas actuales permiten reducir las cargas laborales del equipo?

_____

_____

¿Cuál es el costo por hora de un asesor en este tipo de auditorías? ¿Cuál es el rango de costos de una auditoría de este tipo?

_____

Comentarios

_____

_____

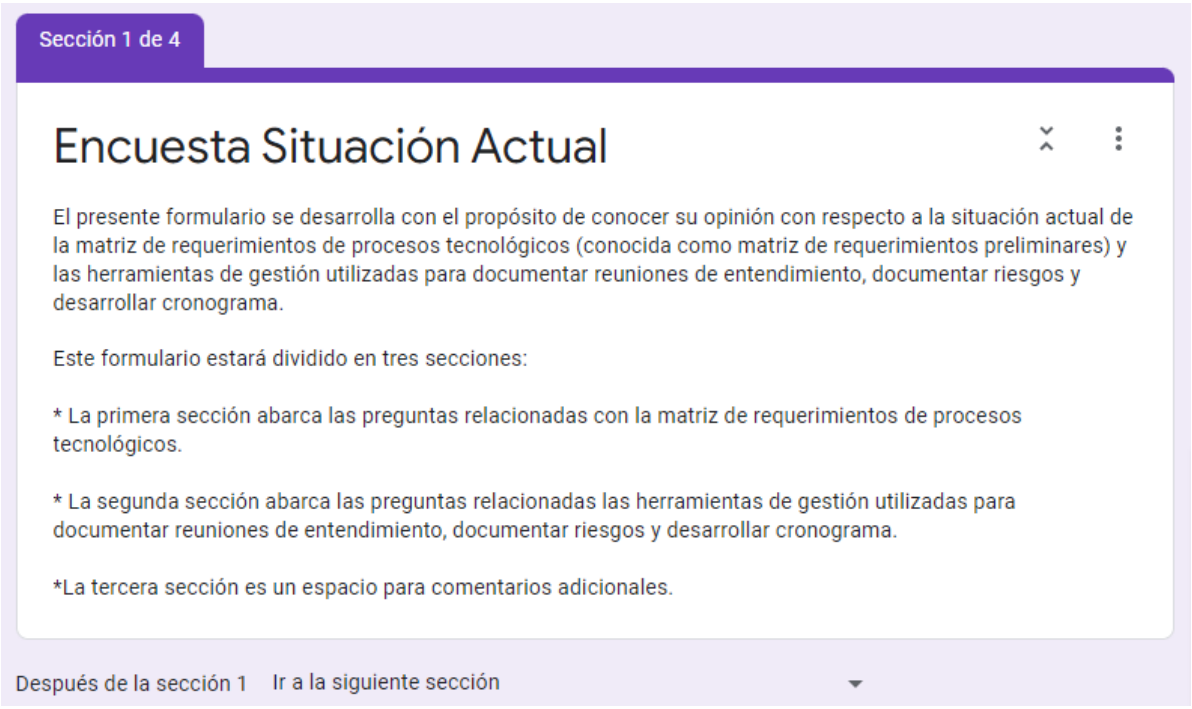
Apéndice C. Plantilla para grupo focal para la evaluación de la propuesta de solución.

Datos Generales	
Grupo focal #	
Fecha	
Participantes	Gerente de TI Supervisor de TI Asesores
Responsable	María Jesús Calvo Bolaños
Objetivo	

Temas por abarcar:

- Nivel de detalle, de estructuración y estandarización.
- Comprensión de la herramienta para el equipo y para el cliente (cuando corresponda).
- Recomendaciones o ajustes.
- Disminución de horas extras.

Apéndice D. Plantilla de encuesta de situación actual.


Sección 1 de 4

Encuesta Situación Actual

El presente formulario se desarrolla con el propósito de conocer su opinión con respecto a la situación actual de la matriz de requerimientos de procesos tecnológicos (conocida como matriz de requerimientos preliminares) y las herramientas de gestión utilizadas para documentar reuniones de entendimiento, documentar riesgos y desarrollar cronograma.

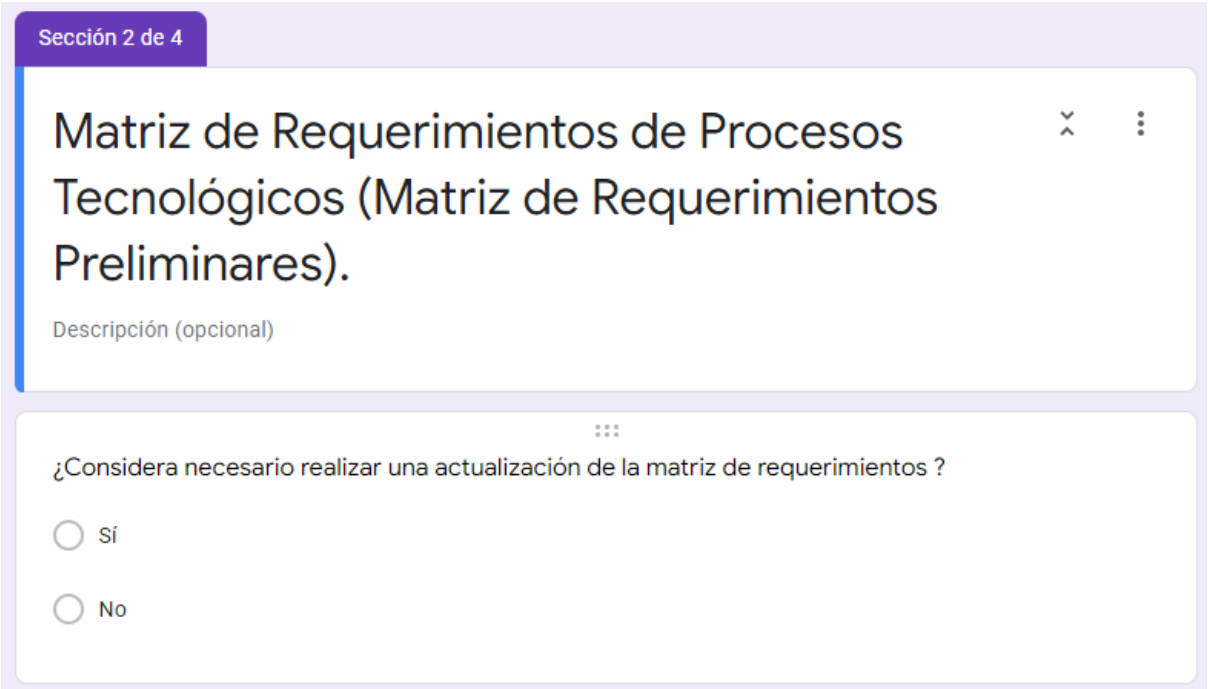
Este formulario estará dividido en tres secciones:

* La primera sección abarca las preguntas relacionadas con la matriz de requerimientos de procesos tecnológicos.

* La segunda sección abarca las preguntas relacionadas las herramientas de gestión utilizadas para documentar reuniones de entendimiento, documentar riesgos y desarrollar cronograma.

*La tercera sección es un espacio para comentarios adicionales.

Después de la sección 1 Ir a la siguiente sección


Sección 2 de 4

Matriz de Requerimientos de Procesos Tecnológicos (Matriz de Requerimientos Preliminares).

Descripción (opcional)

¿Considera necesario realizar una actualización de la matriz de requerimientos ?

Sí

No

¿Qué aspectos considera pertinentes para realizar una actualización de la matriz de requerimientos ?

- [ ] Mantener la versión de COBIT 5 para desarrollar la matriz.
- [ ] Utilizar la versión de COBIT 2019 para desarrollar la matriz.
- [ ] Listar la mayor cantidad de documentos para solicitar al cliente.
- [ ] Mantener la estructura actual de la matriz.
- [ ] Crear una estructura que involucre el proceso, las prácticas y las actividades que contiene cada práctica.
- [ ] Ordenar los documentos por solicitar al cliente según los procesos (como se encuentra actualmente).
- [ ] Ordenar los documentos por solicitar al cliente según las actividades de las prácticas de cada proceso.
- [ ] Fijar periodos de actualización de la matriz para cada año.
- [ ] Fijar periodos de actualización de la matriz para cada más de dos años.
- [ ] Realizar una portada de la matriz y una guía de usuario para orientar al cliente.
- [ ] Otra...

¿En qué rango considera que la matriz de requerimientos es efectiva para la captura de información del cliente?

- ○ Alto: Aumenta su carga laboral de 0 a 3 horas.
- ○ Medio: Aumenta su carga laboral de 4 a 7 horas.
- ○ Bajo: Aumenta su carga laboral en más de 8 horas.

¿Considera que una actualización de la matriz de requerimientos puede disminuir sus cargas laborales?

- ○ Sí
- ○ No
- ○ No se

Sección 3 de 4

Herramientas de Gestión de Ejecución de Auditoría

Herramientas para la documentación de reuniones de entendimiento, documentación de riesgos, y desarrollo del cronograma.

¿Utiliza una guía para el desarrollo y documentación de: las reuniones de entendimiento, los riesgos, y el cronograma?

- ○ Sí
- ○ No
- ○ Otra...

¿Cómo lleva a cabo las reuniones de entendimiento?

- ☐ Realiza una serie de preguntas al cliente, basadas en contenidos del marco de referencia COBIT 5.
- ☐ Realiza una serie de preguntas al cliente, basado en su criterio profesional.
- ☐ Documentan las respuestas por cada proceso.
- ☐ Documentan otra información general de la reunión como fecha de la reunión, entrevistado, acuerdos con ...
- ☐ Documenta las preguntas y respuestas por medios digitales (word, excel, one note, etc.).
- ☐ Documentan las preguntas y respuestas utilizando papel y lapiz.
- ☐ No requiere documentar las preguntas ni las respuestas.
- ☐ Otra...

¿Cómo lleva a cabo la documentación de los riesgos de auditoría?

- [ ] Documenta los riesgos de acuerdo con su experiencia en otras auditorías.
- [ ] Documenta los riesgos de acuerdo con los lineamientos de sus supervisores y gerentes.
- [ ] Documenta los riesgos de acuerdo a su criterio de experto, y considerando la información del proceso den...
- [ ] Documenta el impacto de los riesgos según impacto social, económico, legal, entre otros.
- [ ] Realiza las recomendaciones de los riesgos de acuerdo con su criterio profesional.
- [ ] Realiza las recomendaciones de los riesgos de acuerdo con su experiencia en otras auditorías.
- [ ] Realiza las recomendaciones de los riesgos de acuerdo a su criterio de experto, y considerando la informa...
- [ ] Obtiene los riesgos y las recomendaciones de un documento o estructura guía que especifica y estandariz...
- [ ] Otra...

¿Cómo lleva a cabo el desarrollo del cronograma y sus tiempos?

- [ ] Utiliza su criterio de experto en los procesos por evaluar.
- [ ] Sigue los lineamientos de sus supervisores y gerentes.
- [ ] Toma como base proyectos de auditorías anteriores.
- [ ] Considera la extensión del proceso.
- [ ] Considera los lineamientos dados por el cliente.
- [ ] Considera las fechas establecidas por el cliente.
- [ ] Considera el tiempo de discusión de las fichas de auditoría dentro del cronograma.
- [ ] Considera el tiempo de ajustes dentro del cronograma.
- [ ] Estructura el cronograma de forma secuencial.
- [ ] Estructura el cronograma de forma paralela.
- [ ] Otra...

¿En qué rango considera que las herramientas para documentar las reuniones de entendimiento, riesgos y cronograma, son efectivas para la captura de información del cliente?

- ○ Alto: Aumenta su carga laboral de 0 a 3 horas.
- ○ Medio: Aumenta su carga laboral de 4 a 7 horas.
- ○ Bajo: Aumenta su carga laboral en más de 7 horas.

¿Cómo comunica la información que genera a partir de las reuniones de entendimiento, documentación de riesgos y desarrollo de cronograma a los demás integrantes del equipo?

- ☐ Envío de la información por correo apenas es obtenida.
- ☐ Cargar la información en la red empresarial apenas es obtenida.
- ☐ Envío de información cuando otros miembros del equipo la solicitan.
- ☐ Reuniones internas.
- ☐ Otra...

¿Considera necesario estandarizar la documentación de las reuniones de entendimiento, los riesgos y el cronograma en un instructivo de gestión?

- ○ Sí
- ○ No

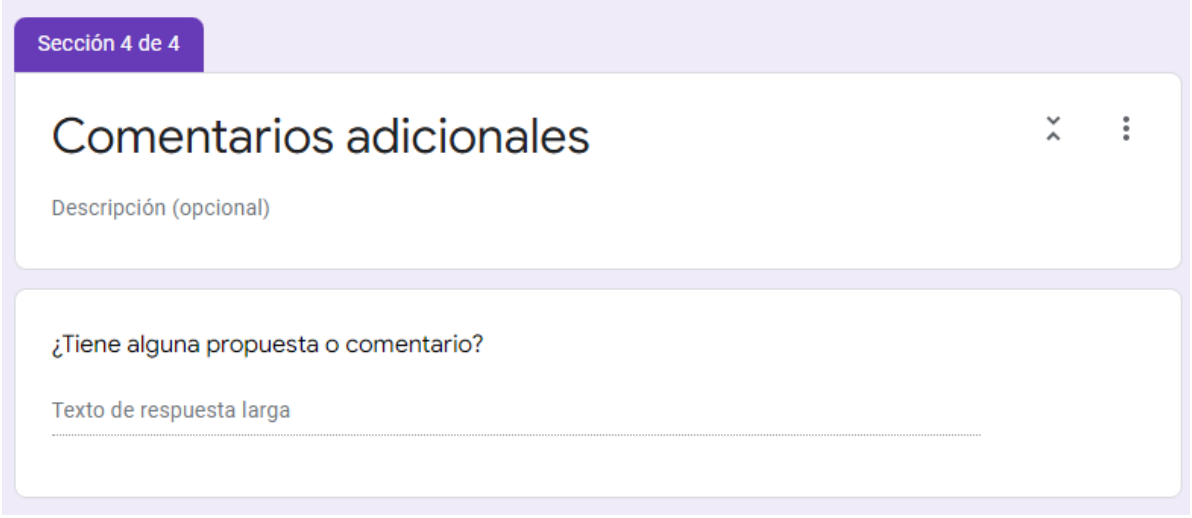
¿Qué expectativas tiene al realizar un instructivo de gestión que detalle las herramientas para documentar las reuniones de entendimiento, riesgos, y cronograma?

- [ ] Promoción de la estandarización de las herramientas.
- [ ] Herramientas de fácil uso y entendimiento.
- [ ] Herramientas basadas en el marco de referencia COBIT 5.
- [ ] Herramientas actualizadas según el marco de referencia COBIT 2019.
- [ ] Estructuración ordenada de cada herramienta para facilitar la lectura.
- [ ] Facilitación de la comunicación entre los miembros del equipo de trabajo.
- [ ] Disminución de las cargas de trabajo.
- [ ] Otra...

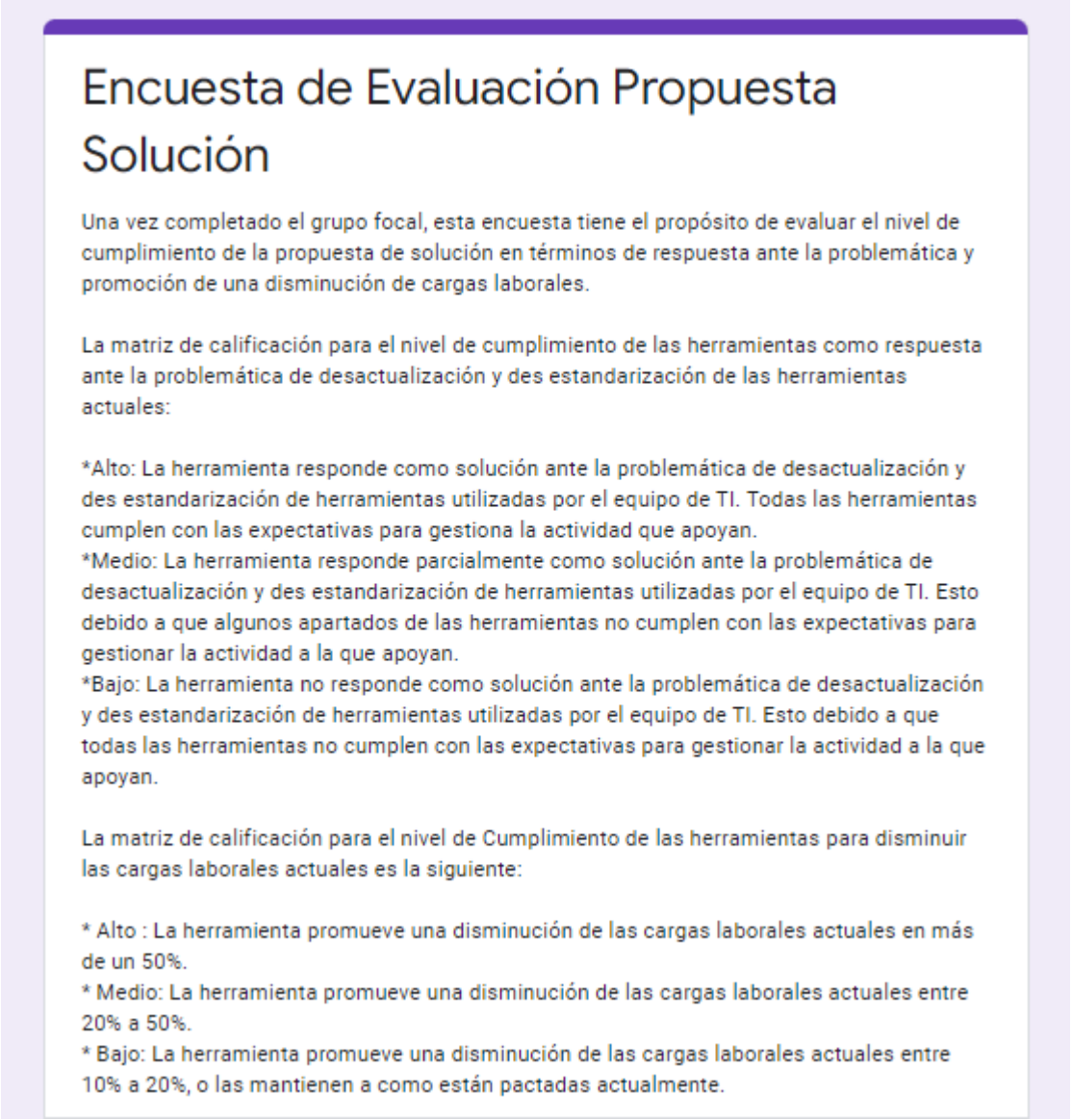
¿Considera que un instructivo de gestión sobre herramientas para las reuniones de entendimiento, riesgos y cronograma, puede disminuir sus cargas laborales?

- ( ) Sí
- ( ) No
- ( ) No se

Después de la sección 3 Ir a la siguiente sección


Sección 4 de 4
Comentarios adicionales
Descripción (opcional)
¿Tiene alguna propuesta o comentario?
Texto de respuesta larga

Apéndice E. Plantilla para encuesta de calificación de la evaluación de la propuesta de solución.



Encuesta de Evaluación Propuesta Solución

Una vez completado el grupo focal, esta encuesta tiene el propósito de evaluar el nivel de cumplimiento de la propuesta de solución en términos de respuesta ante la problemática y promoción de una disminución de cargas laborales.

La matriz de calificación para el nivel de cumplimiento de las herramientas como respuesta ante la problemática de desactualización y des estandarización de las herramientas actuales:

*Alto: La herramienta responde como solución ante la problemática de desactualización y des estandarización de herramientas utilizadas por el equipo de TI. Todas las herramientas cumplen con las expectativas para gestiona la actividad que apoyan.
*Medio: La herramienta responde parcialmente como solución ante la problemática de desactualización y des estandarización de herramientas utilizadas por el equipo de TI. Esto debido a que algunos apartados de las herramientas no cumplen con las expectativas para gestionar la actividad a la que apoyan.
*Bajo: La herramienta no responde como solución ante la problemática de desactualización y des estandarización de herramientas utilizadas por el equipo de TI. Esto debido a que todas las herramientas no cumplen con las expectativas para gestionar la actividad a la que apoyan.

La matriz de calificación para el nivel de Cumplimiento de las herramientas para disminuir las cargas laborales actuales es la siguiente:

* Alto : La herramienta promueve una disminución de las cargas laborales actuales en más de un 50%.
* Medio: La herramienta promueve una disminución de las cargas laborales actuales entre 20% a 50%.
* Bajo: La herramienta promueve una disminución de las cargas laborales actuales entre 10% a 20%, o las mantienen a como están pactadas actualmente.

Nivel de Cumplimiento de las herramientas como respuesta ante la problemática de desactualización y des estandarización de las herramientas actuales

	Alto	Medio	Bajo
Matriz de requerimientos de procesos tecnológicos	○	○	○
Instructivo de gestión: documentación de reuniones de entendimiento.	○	○	○
Instructivo de gestión: documentación de reuniones de riesgos de auditoría.	○	○	○
Instructivo de gestión: desarrollo del cronograma.	○	○	○

Nivel de Cumplimiento de las herramientas para disminuir las cargas laborales actuales

	Alto	Medio	Bajo
Matriz de requerimientos de procesos tecnológicos	○	○	○
Instructivo de gestión: documentación de reuniones de entendimiento.	○	○	○
Instructivo de gestión: documentación de reuniones de riesgos de auditoría.	○	○	○
Instructivo de gestión: desarrollo del cronograma.	○	○	○

Apéndice F. Plantilla de revisión documental para la matriz de requerimientos de procesos tecnológicos.

Datos Generales	
Revisión documental #	
Fecha	
Persona encargada	María Jesús Calvo Bolaños
Tema	Hallazgos de la matriz de requerimientos de procesos tecnológicos.

Matriz de requerimientos de procesos tecnológicos actual	
Identificador	**Descripción del Hallazgo**
H-01	
H-02	
H-03	
H-04	
…	
….	

Apéndice G. Plantilla de revisión documental para los cronogramas de auditoría.

Datos Generales	
Revisión documental #	
Fecha	
Persona encargada	María Jesús Calvo Bolaños
Tema	Hallazgos sobre los cronogramas

Hallazgos generales sobre los cronogramas	
Hallazgo	**Descripción**
H-01	
H-02	
…	
Hallazgos en las duraciones de las etapas de los cronogramas	
Descripción	**Hallazgo de duración aproximada en días**
Kick off	
Requerimientos preliminares:	
Solicitud y recolección de requerimientos preliminares	
Revisión de requerimientos preliminares	
Reuniones de entendimiento según procesos:	
EDM01.Asegurar el establecimiento y el mantenimiento del marco de gobierno	
EDM03.Asegurar la optimización del riesgo	
APO09.Gestionar los acuerdos de servicio	
APO13.Gestionar la seguridad	
BAI06.Gestionar los cambios de TI	
BAI09.Gestionar los activos	
DSS02.Gestionar las peticiones y los incidentes de servicio	
DSS03.Gestionar los problemas	
MEA02.Gestionar el sistema de control interno	
MEA03.Gestionar el cumplimiento de los requisitos externos	

Preparación de entregables por parte del equipo de trabajo:	
Elaboración de productos de auditoría	
Revisión y envío de fichas de auditoría	
Reuniones de discusión	
Ajustes y envío de productos consolidados	
Resultados finales:	
Presentación a Comité de TI	
Presentación a Órgano de Dirección	

Apéndice H. Entrevista semiestructurada de análisis de situación actual para socio del área.

Datos Generales	
Entrevista #	1
Fecha	06 de Abril del 2022
Entrevistado	Socio del área: Luis Gonzalo Rivera
Entrevistador	María Jesús Calvo Bolaños
Tema	Situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de auditoría.

Sección de preguntas:

¿Conoce la matriz de requerimientos preliminares y las herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma, utilizadas en el proceso de auditoría?

Sí, conozco la matriz de requerimientos preliminares y el cronograma. No conozco exactamente cuáles son las herramientas para documentar las reuniones de entendimiento y los riesgos que utiliza actualmente el equipo de TI. Tengo una idea de cuales son porque trabajé con ellas, pero ahora con mi cargo de socio del área no trabajo directamente con estas herramientas.

¿Qué opina de estas herramientas (matriz de requerimientos preliminares, herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma)?

Opino que todas son herramientas necesarias para el proceso de auditoría, las cuales deben ser mejoradas y actualizadas de acuerdo con las necesidades del equipo de TI.

Por ejemplo, voy a hablar de la matriz de requerimientos preliminares que tengo más conocimiento. Esta carece de formalidad frente al cliente porque no contiene una portada o indicaciones de uso. Esto es un punto de mejora porque nosotros como equipo de TI representando a la firma debemos brindar calidad en el servicio y eso incluye entregar herramientas claras, concisas y con buen formato al cliente.

¿Qué expectativas tiene de una propuesta de mejora de estas herramientas (matriz de requerimientos preliminares, herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma)?

Espero que todas herramientas deban ser tan detalladas y fáciles de usar, para que le permita al equipo rapidez y mejor captura de la información, lo cual reduzca el tiempo invertido y aumente la calidad de las auditorías.

También, considero que todas las herramientas se deben ajustar a lo estipulado por entes regulatorios, si fuera el caso (como 14-17), y a lo estipulado por los clientes.

Se debe consultar al equipo de TI sobre las necesidades actuales de estas herramientas. Me gustaría que todos los miembros del equipo conozcan y utilicen las mismas herramientas, para favorecer el entendimiento común y la estandarización de las labores del equipo.

Comentarios

Sin comentarios.

Apéndice I. Entrevista semiestructurada de análisis de situación actual para Gerente de TI y Supervisor de TI.

Datos Generales	
Entrevista #	2
Fecha	06 de abril del 2022
Entrevistados	Gerente de TI: Angélica Chavarría Supervisor de TI: Yeiny Cubero
Entrevistador	María Jesús Calvo Bolaños
Tema	Situación actual de la matriz de requerimientos de procesos tecnológicos y herramientas de gestión de ejecución de auditoría.

Sección de preguntas:

¿Qué opinan de la matriz de requerimientos preliminares, y las herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma?

Matriz de requerimientos:

- Está estructurada de forma general por cada proceso de COBIT 5. Hay muy pocos documentos por cada proceso.
- La documentación o requisitos que se solicitan hacen referencia a cada proceso en general. No están divididas de acuerdo con las actividades de las prácticas de cada proceso.
- Esta matriz la entregamos al cliente. Sin embargo, no tenemos un estándar definido o una guía de usuario para que el cliente nos entregue los documentos solicitados. Esto hace que el cliente utilice sus propios estándares de entrega, lo cual causa confusión en nosotros como equipo a la hora de analizar los documentos.

Reuniones de entendimiento:

- No tenemos un patrón o guía para estructurar las reuniones de entendimiento.
- Las preguntas se plantean por cada proceso, sin embargo, cada miembro plantea las preguntas según su criterio profesional.
- Cada miembro del equipo documenta las respuestas de la reunión como mejor considere y en la herramienta que guste, siempre y cuando las comuniquen a los demás.

- No tenemos una guía de usuario sobre cómo gestionar la reunión, como por ejemplo, establecer una introducción sobre el tema de la reunión, los puntos que se abordarán, espacio para consultas y cierre formal de la reunión. Cada miembro gestiona la reunión a su manera.

Documentación de riesgos dentro de la ficha de auditoría:

- La documentación de los riesgos se estructura con: condición, causa, impacto y recomendación. Esa estructura es fija y no debe cambiarse.
- La descripción del riesgo y la recomendación se hace de acuerdo con el criterio de experto de cada miembro del equipo. No se tiene una estructura o "catálogo" donde puedan tomar riesgos de referencia y quede más estandarizada la sección.
- El impacto de los riesgos se divide en estratégico, operativo, económico y legal, No se tiene definido cada impacto, pero es fácil de identificar e interpretar a cuál impacto hace referencia el riesgo.

Cronograma:

- El cronograma es secuencial y siempre debe realizarse en Project.
- Cada miembro realiza el cronograma, tomando como base cronogramas de proyecto anteriores.
- No se involucran tiempos para validar las reuniones de discusión, realizar ajustes de las fichas de auditoría, aclaración de dudas de la matriz, evaluaciones o resultados. Generalmente no da tiempo incorporarlos.
- Los diferentes tiempos pactados en el cronograma dependen de lo establecido por SUGEF y lo establecido por el cliente. También varían dependiendo de si el cliente tiene o no la documentación o requerimientos del proceso. Por esta razón, nos es difícil establecer tiempos fijos para cada sección.

¿Qué expectativas tienen de una propuesta de mejora de estas herramientas (matriz de requerimientos preliminares, herramientas para documentación de reuniones de entendimiento, documentación de riesgos y cronograma)?

- Con respecto a la matriz de requerimientos, se considera importante incorporar datos de COBIT 2019, para mantener la calidad del servicio. Se prefiere una matriz estructurada de acuerdo con cada práctica del proceso y las actividades que involucra dicha práctica. Asimismo, es importante incorporar una portada junto con una guía de usuario o instrucciones para que el cliente sepa cómo entregar los respectivos documentos. S espera mantener los apartados de fechas de solicitud y entrega de información, para un control por parte del equipo.
- Con respecto a las reuniones de entendimiento, se requiere tener un formato estandarizado de posibles preguntas por cada proceso; entre más detallado mejor. Este formato debe ser comprendido por todos los miembros del equipo para que todos puedan utilizarlo como estándar o base para sus respectivas reuniones

de entendimiento. Se espera una guía sobre cómo gestionar la reunión, para evitar que los miembros del equipo asuman pasos o respuestas.

- Con respecto a los riesgos, se quiere tener estructurados los posibles riesgos por cada proceso, así como sus posibles recomendaciones. Se debe mantener la misma estructura de riesgos. Con respecto al impacto, se espera definir el alcance de cada tipo de impacto: económico, operacional, estratégico o legal.
- Con respecto al cronograma, se debe mantener la herramienta y apartados actuales del cronograma, dado los lineamientos. Se quieren agregar apartados para incorporar tiempos de aclaraciones, ajustes o validaciones. Se puede tener un aproximado de duración por cada proceso, aunque su evaluación vaya a depender de la información que contenga el cliente; eso sí, aclarando que este tiempo puede variar.

¿Considera que las herramientas actuales permiten reducir las cargas laborales del equipo?

No. Las herramientas requieren de mejoras y actualización en general. Actualmente, las cargas laborales pueden aumentar entre cuatro a siete hora aproximadamente, según indican algunos miembros, sin embargo, esto depende de la forma de trabajar de cada uno.

¿Cuál es el costo por hora de las auditorías de TI? ¿Cuál es el rango de costos de una auditoría de este tipo?

El costo por hora de las auditorías de TI ronda entre los $60 y $70. Las horas presupuestadas rondan entre 340 a 350 horas.

Comentarios

Sin comentarios.

Apéndice J. Revisión documental para la matriz de requerimientos de procesos tecnológicos.

Datos Generales	
Revisión documental #	1
Fecha	12 de Abril del 2022
Persona encargada	María Jesús Calvo Bolaños
Tema	Hallazgos de la matriz de requerimientos de procesos tecnológicos.

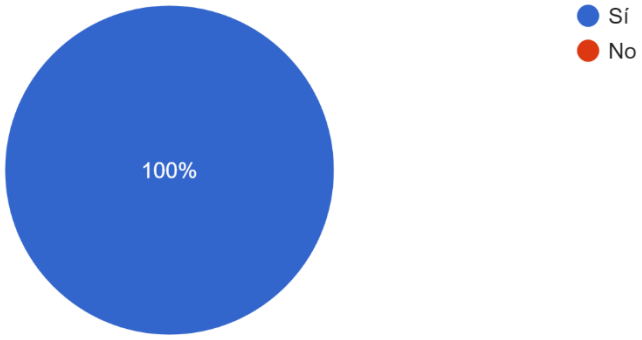
Matriz de requerimientos de procesos tecnológicos actual	
Identificador	**Descripción del Hallazgo**
H-01	La matriz está desarrollada a partir del contenido de COBIT 5.
H-02	La matriz está estructurada por cada proceso de cada dominio de COBIT 5.
H-03	La documentación solicitada hace referencia al proceso en general. Se solicita entre tres a cuatro documentos por proceso. Esto varía de cada auditoría.
H-04	En algunos procesos solicitan documentación sobre el tema del proceso, sin detallar qué tipo y hacen la referencia a que es documentación (ver hallazgo H-10). Por ejemplo, una forma de solicitar es: "Documentación sobre gobernanza de TI".
H-05	La matriz contiene un apartado para especificar el nombre o descripción del documento entregado por el cliente.
H-06	La matriz contiene un apartado para identificar el o los responsables y sus respectivas áreas, de entregar la documentación o requisitos pertinentes.
H-07	La matriz contiene tres apartados para gestionar las fechas de solicitud de la información, así como las fechas de entrega, tanto la esperada como la real.
H-08	La matriz contiene un apartado para comentarios relacionados con la información que se solicita.
H-09	La matriz tiene un apartado para definir el estado de la entrega de la documentación o los requisitos, ya sea en estado "pendiente" o "listo".
H-10	En el encabezado de la matriz se encuentra una aclaración sobre la referencia a la palabra *documentos,* listando los posibles elementos que podrían ser entregados cuando se hable de documentos.
H-11	En el encabezado de la matriz se encuentra una aclaración sobre la referencia a los planes dentro del periodo auditable.
H-12	Cuando se solicitan requerimientos adicionales se genera otro archivo con el nombre "Matriz de requerimientos adicionales", que contiene la misma estructura y solicita la documentación adicional. En otros casos, se coloca en una hoja dentro del Excel original con el mismo nombre.

Apéndice K. Encuesta de situación actual.

Matriz de Requerimientos de Procesos Tecnológicos (Matriz de Requerimientos Preliminares).

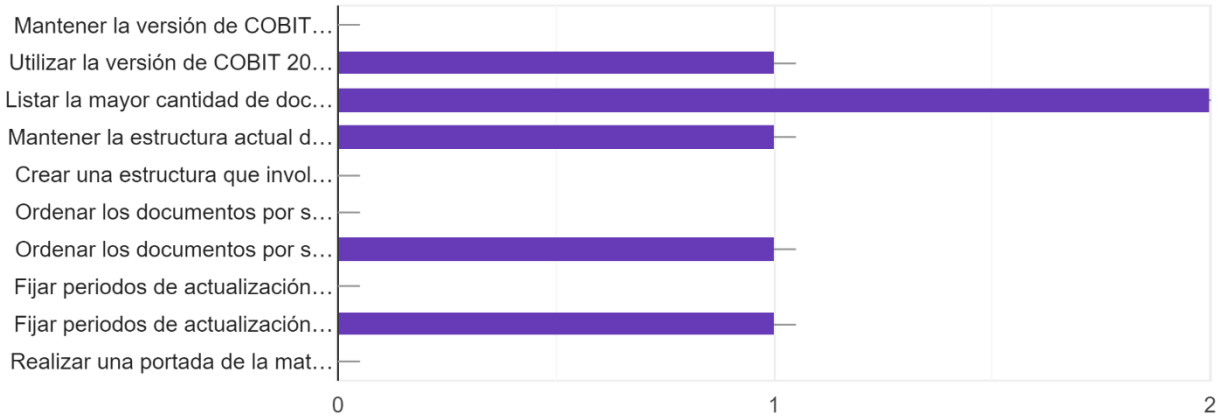
¿Considera necesario realizar una actualización de la matriz de requerimientos ?

3 respuestas



¿Qué aspectos considera pertinentes para realizar una actualización de la matriz de requerimientos ?

3 respuestas

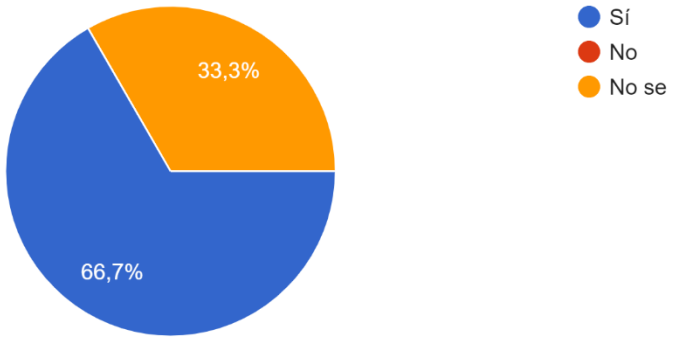


¿En qué rango considera que la matriz de requerimientos es efectiva para la captura de información del cliente?

3 respuestas

¿Considera que una actualización de la matriz de requerimientos puede disminuir sus cargas laborales?

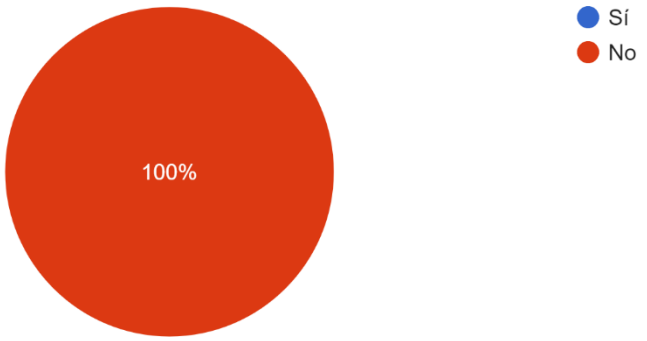
3 respuestas



Herramientas de Gestión de Ejecución de Auditoría

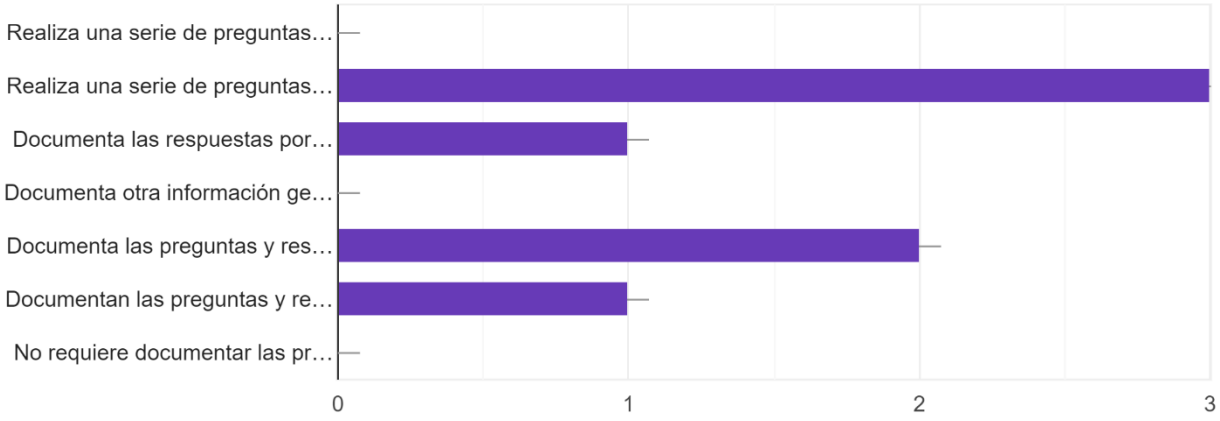
¿Utiliza una guía para el desarrollo y documentación de: las reuniones de entendimiento, los riesgos, y el cronograma?

3 respuestas



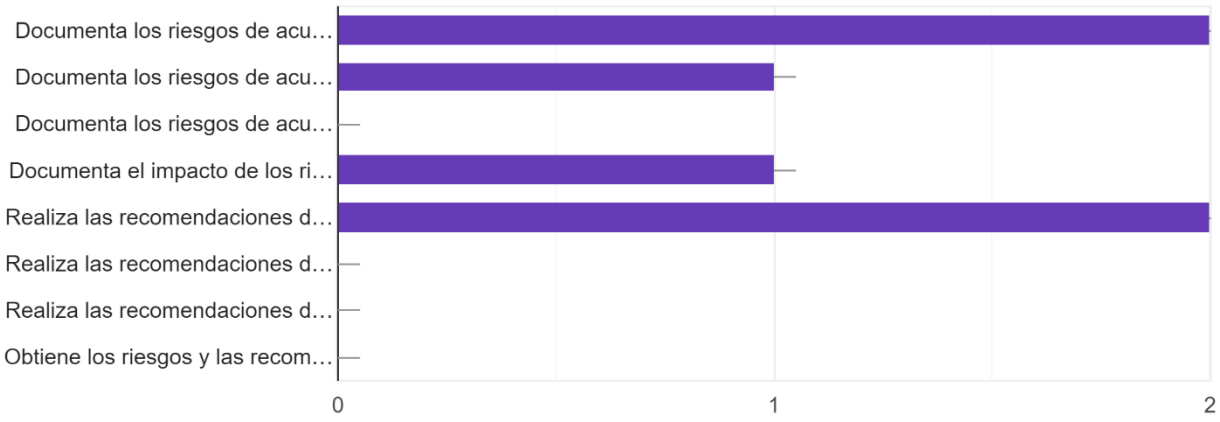
¿Cómo lleva a cabo las reuniones de entendimiento?

3 respuestas



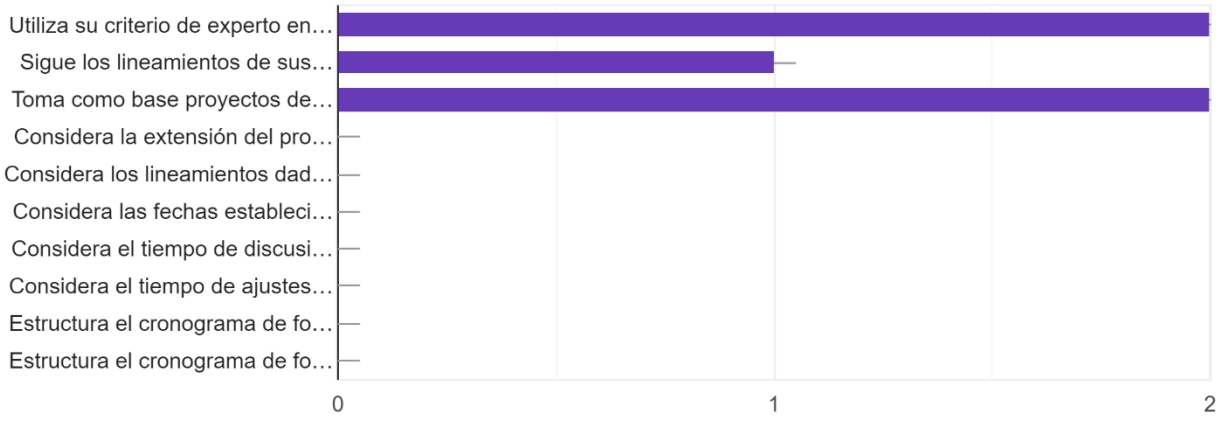
¿Cómo lleva a cabo la documentación de los riesgos de auditoría?

3 respuestas



¿Cómo lleva a cabo el desarrollo del cronograma y sus tiempos?

3 respuestas

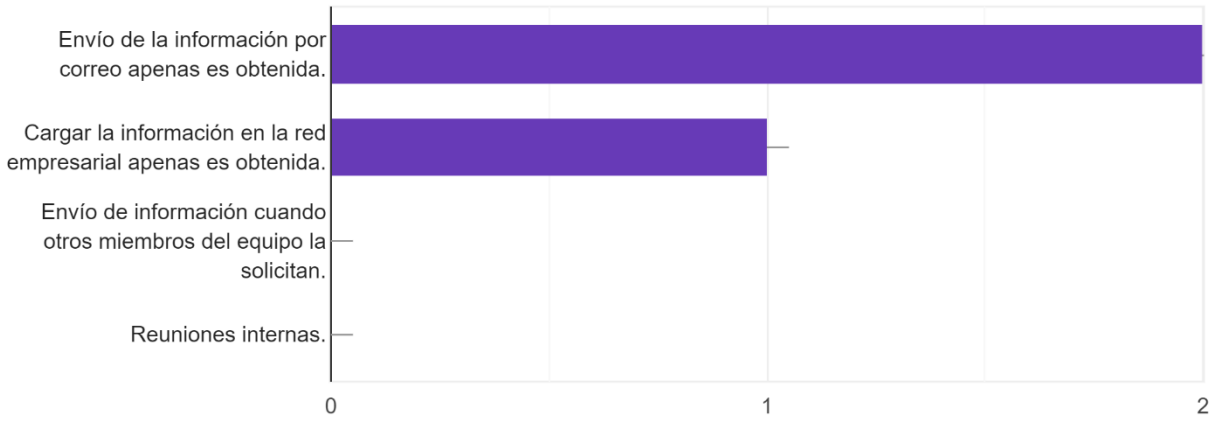


¿En qué rango considera que las herramientas para documentar las reuniones de entendimiento, riesgos y cronograma, son efectivas para la captura de información del cliente?

3 respuestas

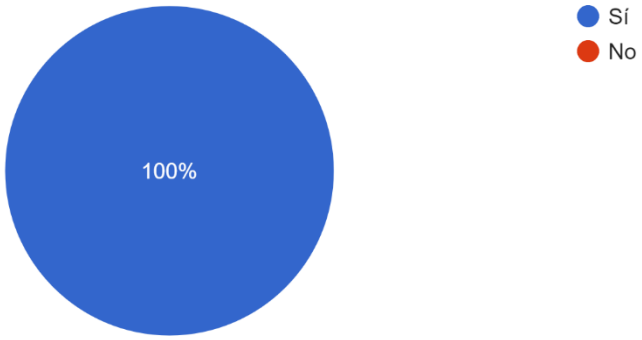
¿Cómo comunica la información que genera a partir de las reuniones de entendimiento, documentación de riesgos y desarrollo de cronograma a los demás integrantes del equipo?

3 respuestas



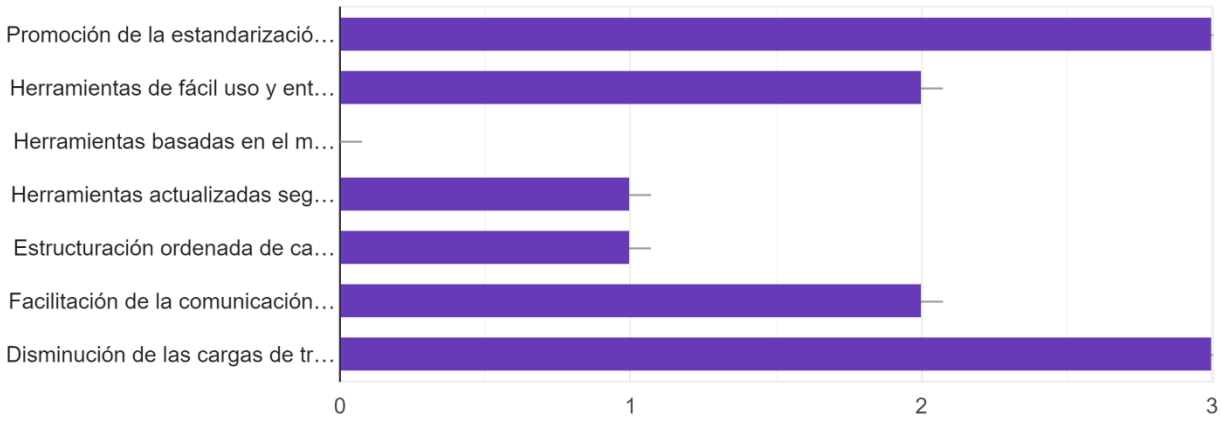
¿Considera necesario estandarizar la documentación de las reuniones de entendimiento, los riesgos y el cronograma en un instructivo de gestión?

2 respuestas



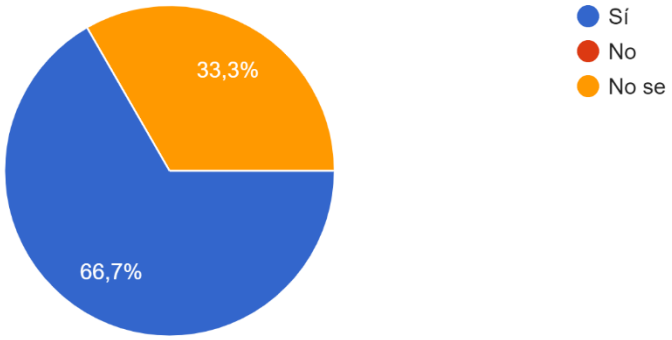
¿Qué expectativas tiene al realizar un instructivo de gestión que detalle las herramientas para documentar las reuniones de entendimiento, riesgos, y cronograma?

3 respuestas



¿Considera que un instructivo de gestión sobre herramientas para las reuniones de entendimiento, riesgos y cronograma, puede disminuir sus cargas laborales?

3 respuestas



Comentarios adicionales

¿Tiene alguna propuesta o comentario?

3 respuestas

- No
- No tengo comentarios
- N/A

Apéndice L. Revisión documental de los cronogramas de auditoría.

Datos Generales	
Revisión documental #	2
Fecha	15 de Abril 2022
Persona encargada	María Jesús Calvo Bolaños
Tema	Hallazgos sobre los cronogramas

Hallazgos generales sobre los cronogramas	
Hallazgo	**Descripción**
H-01	De los cuatro cronogramas revisados se identifica una duración promedio de 70 a 90 días. Esta varía según la auditoría.
H-02	Todos los cronogramas son desarrollados con duración en días, a pesar de que ciertas actividades se realicen en horas, por ejemplo: la reunión de entendimiento dura máximo cuatro horas y la reunión de Kick off dura aproximadamente dos horas.
H-03	Tres de los cronogramas revisados, correspondientes al año 2021, solo especifican como actividad por cada proceso la reunión de entendimiento.
H-04	Únicamente el cronograma del año 2020 desglosa tres actividades por cada proceso, las cuales son la reunión de entendimiento, envío de evidencia adicional y revisión y documentación de la ficha.
H-05	Ninguno de los cronogramas revisados incorpora espacios para consultas o validaciones sobre la matriz de requerimientos.

Hallazgos en las duraciones de las etapas de los cronogramas	
Descripción	**Hallazgo de duración aproximada en días**
Kick off	1 día
Requerimientos preliminares:	
Solicitud y recolección de requerimientos preliminares	Entre 1 a 5 días
Revisión de requerimientos preliminares	Entre 4 a 5 días
Reuniones de entendimiento según procesos:	
EDM01.Asegurar el establecimiento y el mantenimiento del marco de gobierno	Entre 1 a 4 días
EDM03.Asegurar la optimización del riesgo	Entre 1 a 4 días
APO09.Gestionar los acuerdos de servicio	Entre 1 a 3 días

APO13.Gestionar la seguridad	Entre 1 a 4 días
BAI06.Gestionar los cambios de TI	Entre 1 a 4 días
BAI09.Gestionar los activos	1 día
DSS02.Gestionar las peticiones y los incidentes de servicio	1 día
DSS03.Gestionar los problemas	1 día
MEA02.Gestionar el sistema de control interno	Entre 1 a 4 días
MEA03.Gestionar el cumplimiento de los requisitos externos	Entre 1 a 3 días
Preparación de entregables por parte del equipo de trabajo:	
Elaboración de productos de auditoría	Entre 20 a 40 días
Revisión y envío de fichas de auditoría	Entre 2 a 6 días
Reuniones de discusión	Entre 4 a 5 días
Ajustes y envío de productos consolidados	Entre 5 a 6 días
Resultados finales:	
Presentación a Comité de TI	1 día
Presentación a Órgano de Dirección	1 día

Apéndice M. Matriz de requerimientos de procesos tecnológicos inicial.

KPMG

Matriz de Requerimientos de Procesos Tecnológicos

Descripción:

La matriz de requerimientos de procesos tecnológicos o matriz de requerimientos preliminares tiene el objetivo de guiar al auditado en la entrega de documentación relacionada con los procesos por evaluar durante el periodo de auditoría correspondiente.

Esta matriz está desarrollada de acuerdo con lo establecido por COBIT 2019. Para cada dominio, se listan los procesos respectivos, sus prácticas, sus actividades y los requerimientos que se esperan obtener por cada práctica.

Instrucciones de uso:

1. Brindar la documentación existente que cumpla con el (los) requerimiento(s) definidos por cada práctica del proceso. La documentación puede abarcar:
- Planes
- Metodologías
- Políticas
- Reglamentos
- Procedimientos
- Guías, manuales, instructivos
- Protocolos
- Formularios
- Cualquier otro tipo de documentación formal asociado al proceso.

2. Debe completar el apartado de "Documentos proporcionados" con el nombre de los documentos por entregar.

3. En caso de requerir una aclaración, excepción, entre otro aspecto, por favor indicarlo en el apartado de "Comentario".

KPMG

Dominio	Proceso	Práctica	Actividad	Requerimiento	Documentación	Estado de la solicitud	Documentos proporcionados	Área	Responsable	Fecha de solicitud	Fecha entrega	Comentarios
Evaluar, Dirigir y Monitorizar (EDM)	**EDM01.** Asegurar el establecimiento y el mantenimiento del marco de gobierno.	**EDM01.01.** Evaluar el sistema de gobierno	**1.** Analizar e identificar los factores ambientales internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el diseño del gobierno. **2.** Determinar la importancia de TI y su papel con respecto al negocio. **3.** Considerar las regulaciones, leyes, y obligaciones contractuales externas y determinar cómo deberían aplicarse dentro del gobierno de TI de una empresa. **4.** Determinar las implicaciones de todo el entorno de control de la empresa con respecto a TI. **5.** Alinear el uso ético y el procesamiento de la información y su impacto en la sociedad, el entorno natural y los intereses de los interesados internos y externos con la dirección, las metas y los objetivos de la empresa. **6.** Articular los principios que guiarán el diseño del gobierno y la toma de decisiones de TI. **7.** Determinar el modelo óptimo de toma de decisiones para TI. **8.** Determinar los niveles adecuados de delegación de autoridad, incluidas las reglas de limitaciones, para las decisiones de TI.	•Principios rectores del gobierno empresarial. •Modelo de toma de decisiones. •Niveles de autoridad.	•Listado de principios referentes al gobierno de la empresa. •Organigrama de la empresa. •Manual de puestos de la empresa, que especifique la autoridad y responsabilidades de cada parte.						
		EDM01.02 Dirigir el sistema de gobierno	**1.** Comunicar el gobierno de los principios de TI y acordar con la administración ejecutiva la forma de establecer un liderazgo informado y comprometido. **2.** Establecer o delegar el establecimiento de estructuras, procesos y prácticas de gobierno en línea con los principios de diseño acordados. **3.** Establecer un consejo de administración de gobierno de TI. Este consejo de administración debería garantizar que el gobierno de la información y la tecnología, como parte del gobierno de la empresa, se aborda de forma adecuada; aconsejar sobre la dirección estratégica a seguir; y determinar la priorización de los programas de inversión habilitados por TI en línea con la estrategia y prioridades del negocio de la empresa. **4.** Asignar la responsabilidad, autoridad y rendición de cuentas por las decisiones de TI en línea con los principios de diseño de gobierno, de los modelos de toma de decisiones y de delegación acordados. **5.** Asegurar que los mecanismos de comunicación y presentación de informes proporcionan la información adecuada a los responsables de la supervisión y toma de decisiones. **6.** Direccionar al personal para que siga las directrices relevantes en cuanto al comportamiento ético y profesional y asegurar que se conozcan y se apliquen las consecuencias del incumplimiento. **7.** Direccionar el establecimiento de un sistema de recompensas para fomentar el cambio cultural deseado.	•Comunicación del gobierno de la empresa. •Métodos de sistema de recompensa.	•Plan de Comunicación del gobierno de la empresa. •Procedimiento de gestión de recompensas.						
		EDM01.03 Monitorizar el sistema de gobierno	**1.** Evaluar la eficacia y el rendimiento de aquellas partes interesadas a las que se le ha delegado la responsabilidad y autoridad para el gobierno empresarial de TI. **2.** Evaluar de forma periódica si los mecanismos de TI que se han acordado (estructuras, principios, procesos, etc.) se han establecido y operan de forma eficiente. **3.** Evaluar la eficacia del diseño de gobierno e identificar acciones para rectificar cualquier desviación que se encuentre. **4.** Mantener la supervisión de hasta qué punto la TI satisface las obligaciones (regulación, legislación, leyes comunes, contractuales), políticas internas, estándares y guías profesionales. **5.** Proporcionar la supervisión de la eficacia del sistema de control de la empresa y el cumplimiento con el mismo. **6.** Monitorizar los mecanismos regulares y rutinarios para garantizar que el uso de TI cumpla con las obligaciones (regulación, legislación, leyes comunes, contractuales), estándares y guías.	•Retroalimentación sobre el rendimiento y la eficacia del gobierno.	•Plan de aseguramiento del sistema de control interno. •Informes de desempeño del gobierno empresarial. •Informes de auditoria del gobierno empresarial.						
	EDM03. Asegurar la optimización del riesgo	**EDM03.01** Evaluar la gestión de riesgos	**1.** Conocer la organización y su contexto en relación al riesgo de TI. **2.** Determinar el apetito al riesgo de la organización, es decir, el nivel de riesgo relacionado con TI que la empresa está dispuesta a tomar en la búsqueda de sus objetivos empresariales. **3.** Determinar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo. **4.** Determinar el grado de alineamiento de la estrategia de riesgos en TI de la empresa con la estrategia de riesgos de la empresa en su conjunto y garantizar que el apetito al riesgo se sitúe por debajo de la capacidad de riesgo de la organización. **5.** Evaluar los factores de riesgo de TI de forma proactiva antes de tomar decisiones estratégicas a nivel de empresa y garantizar que las consideraciones del riesgo formen parte del proceso de decisión estratégico de la empresa. **6.** Evaluar las actividades de gestión de riesgos para asegurar que se alineen con la capacidad de la empresa para las pérdidas relacionadas con TI y la tolerancia correspondiente por parte de la dirección. **7.** Atraer y conservar las habilidades y el personal necesarios para la gestión de riesgos de las TI.	•Guía de apetito del riesgo. •Evaluación de actividades de gestión de riesgos. •Niveles aprobados de tolerancia al riesgo.	•Procedimiento de la gestión de riesgos. •Guía para la definición del apetito y niveles de tolerancia de la gestión de riesgos.						
		EDM03.02. Dirigir la gestión de riesgos	**1.** Dirigir la traducción e integración de la estrategia de riesgo de TI en las prácticas de gestión de riesgos y las actividades operativas. **2.** Dirigir el desarrollo de planes de comunicación de riesgos (que se extiendan a todos los niveles de la empresa). **3.** Dirigir la implementación de los mecanismo adecuados para responder de forma rápida al cambio de riesgos e informar inmediatamente a los cargos de dirección correspondientes, siguiendo los principios de escalamiento (qué comunicar, cuándo, dónde y cómo). **4.** Ordenar que el riesgo, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento. El riesgo debe gestionarse conforme a las políticas y procedimientos publicados y comunicados a los responsables de la toma de decisiones. **5.** Identificar las metas y métricas claves de los procesos de gobierno y gestión de riesgos que deben monitorizarse, y aprobar las estrategias, métodos, técnicas y procesos para capturar y comunicar la información de las mediciones.	•Proceso aprobado para la medición de la gestión de riesgos. •Objetivos clave a monitorizar para la gestión de riesgos. •Políticas de gestión de riesgos.	•Política de gestión de riesgos. •Métricas para la medición de la gestión de riesgos. •Guía para la medición de la gestión de riesgos.						
		EDM03.03. Monitorizar la gestión de riesgos.	**1.** Comunicar cualquier problema de gestión de riesgos al consejo de administración o comité ejecutivo. **2.** Supervise hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa. **3.** Monitorizar las metas y métricas de los procesos de gobierno y gestión de riesgos contra los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales s para solucionar las causas subyacentes. **4.** Facilitar la revisión por parte de las partes interesadas clave del progreso de la empresa con respecto a las metas identificadas.	•Acciones remediales para solucionar las desviaciones de gestión de riesgos. •Problemas de gestión de riesgos para el consejo de administración.	•Informe ejecutivo de los problemas identificados en la gestión de riesgos, y acciones remediales para solucionarlos.						

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Responsable	Área	Fecha de solicitud	Fecha de entrega	Comentarios
Alinear, Planificar y Organizar (APO)	APO09. Gestionar los acuerdos de servicio	APO09.01. Identificar los servicios de TI	1. Evaluar los servicios y niveles de servicios de TI actuales para identificar las brechas entre los servicios actuales y las actividades empresariales que apoyan. Identificar áreas de mejora de los servicios existentes y opciones de nivel de servicio. 2. Analizar, estudiar y estimar la demanda futura y confirmar la capacidad de servicios actuales habilitados por TI. 3. Analizar actividades del proceso empresarial para identificar la necesidad de servicios de TI nuevos o rediseñados. 4. Comparar los requisitos identificados con los componentes de servicio vigentes del portafolio. Si fuera posible, incluir los componentes de servicio vigentes (servicios de TI, opciones de nivel de servicio y paquetes de servicio) en nuevos paquetes de servicio para satisfacer los requisitos del negocio identificados. 5. Revisar regularmente el portafolio de servicios de TI con la gestión del portafolio y la gestión de relaciones con el negocio para identificar servicios obsoletos. Acordar su retirada y proponer cambios. 6. Cuando sea posible, hacer corresponder las demandas con los paquetes de servicio y crear servicios estandarizados para lograr eficiencias globales.	•Brechas identificadas en los servicios de TI prestados a la empresa. •Definiciones de servicios estándar.	•Formulario de brechas de los servicios de TI.							
		APO09.02. Catalogar los servicios habilitados por TI	1. Publicar en catálogos los servicios activos importantes , paquetes de servicios y opciones de nivel de servicio habilitados por TI desde el portafolio. 2. Asegurar de forma continua que los componentes de servicio en el portafolio y los catálogos de servicios relacionados estén completos y actualizados. 3. Informar a la dirección de gestión de relaciones empresariales acerca de todas las actualizaciones de los catálogos de servicios.	•Catálogos de servicios	•Catálogos de los servicios de TI.							
		APO09.03. Definir y preparar acuerdos de servicio	1. Analizar los requisitos para acuerdos de servicio nuevos o modificados recibidos de la gestión de relaciones con el negocio a fin de asegurar que puedan satisfacerse. Considerar aspectos como los tiempos de servicio, disponibilidad, rendimiento, capacidad, seguridad, privacidad, continuidad, problemas de cumplimiento y regulatorios, usabilidad, limitaciones de la demanda y calidad de los datos. 2. Redactar borradores de acuerdos de servicio al cliente basados en los servicios, paquetes de servicios y opciones de nivel de servicio en los catálogos de servicios relevantes. 3. Finalizar los acuerdos de servicio al cliente con la gestión de relaciones con el negocio. 4. Determinar, acordar y documentar acuerdos operativos internos que sustenten los acuerdos de servicio al cliente, si corresponde. 5. Relacionarse con la gestión de proveedores externos para garantizar que los adecuados contratos comerciales con proveedores de servicios externos sustenten los acuerdos de servicio al cliente, si corresponde.	•Acuerdos a nivel de servicio (SLA) •Acuerdos a nivel operativo (OLA)	•Acuerdos a nivel de servicio (SLA) •Acuerdos a nivel operativo (OLA)							
		APO09.04. Monitorizar y reportar los niveles de servicio	1. Establecer y mantener medidas para monitorizar y recopilar datos de nivel de servicio. 2. Evaluar el rendimiento y proporcionar reportes sobre el rendimiento de los acuerdos de servicio regular y formalmente, incluidas las desviaciones de los valores acordados. Distribuir este informe a la gestión de relaciones con el negocio. 3. Realizar revisiones regulares para pronosticar e identificar las tendencias del rendimiento de nivel de servicio. Incorporar prácticas de gestión de calidad en la monitorización de servicios. 4. Ofrecer la información de gestión apropiada para contribuir a la gestión del rendimiento. 5. Acordar planes de acción y remediaciones para cualquier problema de rendimiento o tendencias negativas.	•Planes de acción de mejora y remediaciones. •Informes de rendimiento del nivel de servicio.	•Plan de mejora y remediación de servicios de TI. •Informes de revisiones o auditoría de los servicios de TI.							
		APO09.05. Revisar los acuerdos y los contratos de servicio	1. Revisar de forma regular los acuerdos de servicio conforme a los términos acordados para garantizar que sean efectivos y estén actualizados. Cuando corresponda, tener en cuenta cambios en requisitos, servicios habilitados por TI, paquetes de servicio y opciones de nivel de servicio. 2. Cuando sea necesario, revisar el acuerdo de servicio vigentes con el proveedor de servicios. Acordar y actualizar los acuerdos operativos internos.	•SLA actualizados	•Informes de revisión o auditoría de los acuerdos a nivel de servicio. •Procedimiento para actualizar los acuerdos a nivel de servicio.							
	APO13. Gestionar la seguridad	APO13.01. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)	1. Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance. 2. Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa. 3. Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad. 4. Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI. 5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI. 6. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información. 7. Comunicar la estrategia de SGSI.	•Declaración del alcance de SGSI. •Política de SGSI.	•Política del Sistema de Gestión de Seguridad de la Información (SGSI), que contenga el alcance del SGSI.							
		APO13.02. Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados. 2. Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad. 3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades. 4. Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información. 5. Implementar programas de formación y concienciación sobre seguridad de la información y privacidad. 6. Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 7. Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	•Plan de tratamiento del riesgo de seguridad de la información. •Casos de negocio de seguridad de la información.	•Plan para el tratamiento de riesgos en seguridad de información. •Documentos de caso de negocio sobre seguridad de la información.							
		APO13.03. Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	1. Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad. 2. Realizar auditorías de SGSI a intervalos planificados. 3. Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI. 4. Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI. 5. Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	•Recomendaciones para la mejora del sistema de gestión de la seguridad de la información (SGSI). •Informes de auditoría del sistema de gestión de seguridad de la información (SGSI).	•Informes de auditoría del SGSI. •Informe ejecutivo sobre recomendaciones hacia el SGSI.							

KPMG

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Responsable	Área	Fecha de solicitud	Fecha de entrega	Comentarios
Construir, Adquirir e Implementar (BAI)	BAI06. Gestionar los cambios de TI	BAI06.01. Evaluar, priorizar y autorizar solicitudes de cambio	1. Usar solicitudes de cambio formales para permitir a los propietarios de los procesos de negocio y a TI solicitar cambios a procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurarse de que todos estos cambios surjan solo a través del proceso de gestión de solicitudes de cambio. 2. Categorizar todos los cambios solicitados (p. ej., proceso de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software de aplicación comprado/empaquetado) y relacionar los elementos de configuración afectados. 3. Priorizar todos los cambios solicitados basándose en los requisitos de negocio y técnicos, recursos requeridos y las razones legales, regulatorias y contractuales para el cambio solicitado. 4. Aprobar formalmente cada cambio por parte de los dueños de los procesos de negocio, gestores de servicios y partes interesadas técnicas de TI, según corresponda. Los cambios que son de bajo riesgo y relativamente frecuentes deben preaprobarse como cambios estándar. 5. Planificar y programar todos los cambios aprobados. 6. Planificar y evaluar todas las solicitudes de una manera estructurada. Incluir un análisis de impacto en los procesos de negocio, la infraestructura, los sistemas y las aplicaciones, los planes de continuidad del negocio (BCP) y los proveedores de servicios para asegurarse de que se hayan identificado todos los componentes afectados. Evaluar la probabilidad de afectar negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, privacidad, legales, contractuales y de cumplimiento del cambio solicitado. Considerar también las interdependencias entre los cambios. Involucrar a los propietarios de los procesos de negocio en el proceso de evaluación, cuando sea conveniente. 7. Considerar el impacto de los proveedores de servicios contratados (p. ej., de procesamiento de negocio , infraestructura, desarrollo de aplicaciones y servicios compartidos externalizados) en el proceso de gestión de cambios. Incluir la integración de los procesos de gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y SLA.	•Plan y cronograma de cambios. •Solicitudes de cambio aprobadas. •Evaluaciones del impacto.	•Procedimiento de gestión de cambios. •Planificación y cronograma para la gestión de cambios. •Listado de solicitudes de cambio aprobadas. •Guía para establecer evaluaciones de impacto en los cambios.							
		BAI06.02. Gestionar cambios de emergencia.	1. Definir lo que constituye un cambio de emergencia. 2. Asegurar que existe un procedimiento documentado para declarar, evaluar, aprobar inicialmente, autorizar después del cambio y registrar un cambio de emergencia. 3. Verificar que todos los acuerdos de acceso de emergencia para los cambios se autoricen, documenten y revoquen adecuadamente después de que el cambio se haya aplicado. 4. Monitorizar todos los cambios de emergencia y realizar las revisiones posteriores a la implementación con la participación de todas las partes interesadas. La revisión debe considerar e iniciar acciones correctivas basadas en las causas raíz, tales como problemas con los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales, e integridad de datos.	•Revisión posterior a la implementación.	•Listado de solicitudes de cambio de emergencia. •Procedimiento para gestionar los cambios de emergencia. •Informes de revisión y monitoreo de los cambios de emergencia.							
		BAI06.03. Hacer seguimiento e informar sobre cambios de estado	1. Categorizar las solicitudes de cambio en el proceso de seguimiento (p. ej., rechazado; aprobado pero no iniciado; aprobado y en proceso; y cerrado). 2. Implementar informes de estado de los cambios con métricas de rendimiento para permitir la gestión de la revisión y la monitorización, tanto del estado detallado de los cambios como del estado general (p. ej., análisis de la antigüedad de las solicitudes de cambio). Asegurarse de que los informes de estado formen una pista de auditoría para que los cambios puedan rastrearse posteriormente, desde su inicio hasta su eventual disposición. 3. Monitorizar los cambios abiertos para asegurarse de que todos los cambios aprobados se cierren de manera oportuna, según su prioridad. 4. Mantener un sistema de seguimiento e informes para todas las solicitudes de cambio.	•Informes de estado de las solicitudes de cambio.	•Guía para documentar el estado de los cambios que incluya la categorización, métricas, revisiones y monitorizaciones efectuadas de las solicitudes de cambio.							
		BAI06.04. Cerrar y documentar los cambios.	1. Incluir los cambios en la documentación en el procedimiento de gestión. Algunos ejemplos de documentación son: procedimientos operativos de negocio y de TI, documentación de continuidad del negocio y recuperación ante desastres, información de configuración, documentación de aplicaciones, pantallas de ayuda y materiales de capacitación. 2. Definir un periodo de retención adecuado para la documentación de los cambios y la documentación del sistema y del usuario antes y después del cambio. 3. Someter la documentación al mismo nivel de revisión que el cambio en sí mismo.	•Cambio en la documentación	•Evidencia (correo, chat, documento, pantallazo, entre otros) del ajuste de los cambios en los procedimientos de la empresa.							
	BAI09. Gestionar los activos	BAI09.01. Identificar y registrar los activos actuales.	1. Identificar todos los activos adquiridos en un registro de activos que recoja el estado actual. Los activos se reportan en la hoja del balance; se compran o crean para aumentar el valor de una compañía o beneficiar las operaciones de la empresa (p. ej., hardware y software). Identificar todos los activos adquiridos y mantener el alineamiento con los procesos de gestión de la configuración y gestión de cambios, el sistema de gestión de la configuración y los datos de contabilidad financiera. 2. Identificar requisitos legales, regulatorios o contractuales que deban abordarse al gestionar el activo. 3. Comprobar que los activos son adecuados para su propósito (es decir, que se puedan usar). 4. Garantizar la contabilidad de todos los activos. 5. Comprobar la existencia de todos los activos adquiridos mediante comprobaciones y conciliación regulares de inventario físico y lógico. Incluir el uso de herramientas de descubrimiento de software. 6. Determinar regularmente si cada activo continúa proporcionando valor. De ser así, estimar la vida útil esperada durante la que proporcionará valor.	•Resultados de revisiones de idoneidad. •Registro de activos. •Resultados de comprobaciones de inventario físicas.	•Procedimiento de revisiones de idoneidad de los activos. •Informe de resultados de revisiones de idoneidad de los activos. •Registro de todos los activos adquiridos actualmente. •Resultados de comprobaciones de inventario físicas.							
		BAI09.02. Gestionar los activos críticos	1. Identificar activos que son críticos para proporcionar la capacidad de servicio mediante la referencia a los requisitos en las definiciones de servicio, los SLA y el sistema de gestión de la configuración. 2. Considerar regularmente el riesgo de fallo o la necesidad de sustitución de cada activo crítico. 3. Comunicar a los clientes y usuarios afectados el impacto esperado (p. ej. restricciones de rendimiento) de las actividades de mantenimiento. 4. Incorporar al calendario global de producción las suspensiones planificadas. Programar actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio. 5. Mantener la resiliencia de los activos críticos aplicando un mantenimiento preventivo regular. Monitorizar el rendimiento y, de ser necesario, proporcionar activos alternativos y/o adicionales para minimizar la probabilidad de fallo. 6. Establecer un plan de mantenimiento preventivo para todo el hardware considerando un análisis de coste beneficio, las recomendaciones de los proveedores, el riesgo de suspensión del servicio, el personal cualificado y otros factores relevantes. 7. Establecer acuerdos de mantenimiento que incluyan el acceso de terceros a las instalaciones de TI de la organización a fin de realizar actividades en el sitio (on-site) o fuera de él (off site) (p. ej. outsourcing). Establecer contratos de servicio formales que contengan o hagan referencia a todas las condiciones de seguridad y privacidad necesarias, incluidos procedimientos de autorización de acceso, para garantizar el cumplimiento con las políticas y estándares de seguridad/privacidad de la organización. 8. Garantizar que los servicios de acceso remoto y los perfiles de usuario (y otros medios usados para el mantenimiento y el diagnóstico) estén activos solo cuando sea necesario. 9. Monitorizar el rendimiento de los activos críticos mediante el examen de tendencias de los incidentes. Cuando sea necesario, realizar acciones de reparación o sustitución.	•Comunicaciones de suspenciones por mantenimiento planificadas. •Contratos de mantenimiento.	•Procedimiento para gestionar los cambios críticos. •Protocolo de comunicación del mantenimiento de activos críticos. •Contratos a acuerdos de mantenimiento de los activos críticos, que especifique condiciones de seguridad, privacidad, accesos, y autorizaciones.							
		BAI09.03. Gestionar el ciclo de vida del activo	1. Proporcionar todos los activos conforme a las solicitudes aprobadas y las políticas y prácticas de adquisición de la empresa. 2. Obtener, recibir, verificar, probar y registrar todos los activos de forma controlada, incluyendo etiquetas físicas, cuando se requiera. 3. Aprobar los pagos y completar el proceso con los proveedores, conforme a las condiciones del contrato acordadas. 4. Implementar los activos siguiendo el ciclo de vida de implementación estándar, incluida la gestión de cambios y las pruebas de aceptación. 5. Asignar los activos a usuarios, con responsabilidades de aceptación y confirmación, como corresponda. 6. Siempre que sea posible, reasignar los activos cuando ya no se necesiten debido a un cambio de rol del usuario, redundancia en un servicio o retirada de un servicio. 7. Planificar, autorizar e implementar actividades relacionadas con la retirada, mientras se conservan los registros correspondientes para satisfacer las necesidades regulatorias y de negocio en curso. 8. Disponer de los activos de forma segura, tras considerar, por ejemplo, el borrado permanente de los datos registrados en los dispositivos y el daño potencial al medio ambiente. 9. Disponer de los activos de forma responsable cuando ya no sean de utilidad debido a la retirada de todos los servicios relacionados, tecnología obsoleta o la falta de usuarios, teniendo en consideración el impacto medioambiental.	•Retiradas autorizadas de activos. •Registro actualizado de activos. •Solicitudes aprobadas de adquisiciones de activos.	•Listado de retiradas autorizadas de activos. •Listado de las solicitudes de adquisiciones de activos aprobadas. •Evidencia (correo, chat, documento, pantallazo, entre otrosde comprobación del registro de activos actualizados.							
		BAI09.04. Optimizar el valor de los activos	1. Revisar regularmente toda la base de activos, considerando si está alineada con las necesidades del negocio. 2. Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor coste. Cuando sea necesario, incluir reemplazos con nuevas alternativas. 3. Revisar las garantías y considerar la relación calidad-precio y las estrategias de reemplazo para determinar las opciones de menor coste. 4. Usar estadísticas de capacidad y uso para identificar activos subutilizados o redundantes que podrían considerarse para su eliminación o sustitución a fin de reducir costes. 5. Revisar la base completa para identificar oportunidades de estandarización, suministro único y otras estrategias que podrían reducir los costes de adquisición, soporte y mantenimiento. 6. Revisar el estado general a fin de identificar oportunidades para aprovechar las tecnologías emergentes o estrategias de suministro alternativas para reducir costes o incrementar la relación calidad-precio.	•Oportunidades para reducir los costes o aumentar el valor de los activos. •Resultados de las revisiones de optimización de costes.	•Metodología / Guía para la revisión de la optimización del valor de los activos. •Informe de resultados sobre revisiones de optimización de los costes de los activos. •Informes de acciones correctivas para reducir los costes o aumentar el valor de los activos.							
		BAI09.05. Gestionar las licencias	1. Mantener un registro de todas las licencias de software adquiridas y los acuerdos de licencias asociados. 2. Realizar regularmente una auditoría para identificar todas las instancias de software con licencia instaladas. 3. Comparar el número de licencias instaladas con el número de licencias adquiridas. Garantizar que el método de medición de cumplimiento de licencias sea conforme a los requisitos de la licencia y del contrato. 4. Cuando las instancias sean inferiores al número de licencias adquiridas, decidir si se deben conservar o poner fin a esas licencias, considerando los posibles ahorros en mantenimiento, capacitación y otros costes innecesarios. 5. Cuando las instancias sean superiores al número de licencias adquiridas, considerar en primer lugar desinstalar las instancias que ya no se requieran o no estén justificadas y comprar entonces, de ser necesario, licencias adicionales para cumplir con el acuerdo de licencias. 6. Considerar de forma regular si puede ser más rentable actualizar los productos y las licencias asociadas.	•Plan de acción para ajustar el número y asignaciones de licencias. •Registro de licencias de software. •Resultados de las auditorías a las licencias instaladas.	•Plan para la gestión de las licencias de software. •Registro de las licencias de software. •Informes de auditoría sobre licencias.							

KPMG

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Área	Responsable	Fecha de solicitud	Fecha de entrega	Comentarios
Entregar, Dar Servicio y Soporte (DSS)	DSS02. Gestionar las peticiones y los incidentes de servicio	DSS02.01. Definir esquemas de clasificación para incidentes y peticiones de servicio	1. Definir esquemas de priorización y clasificación de solicitudes de servicios e incidentes, y los criterios para el registro de problemas. Usar esta información para garantizar estrategias constantes a fin de gestionar e informar a los usuarios sobre los problemas y llevar a cabo análisis de tendencias. 2. Definir modelos de incidentes sobre errores conocidos para permitir una resolución eficiente y eficaz. 3. Definir modelos de solicitud de servicios conforme al tipo de solicitud de servicios para permitir la autoayuda y un servicio eficiente para solicitudes estándar. 4. Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad. 5. Definir las fuentes de conocimiento sobre incidentes y solicitudes y describir cómo usarlas.	•Criterios para el registro de problemas. •Reglas para escalamiento de incidentes. •Esquema y modelos de clasificación de peticiones de servicio e incidentes.	•Guía de criterios para el registro de problemas. •Reglas y procedimientos para el escalamiento de incidentes. •Esquema de priorización y clasificación de peticiones de servicio e incidentes.							
		DSS02.02. Registrar, clasificar y priorizar las peticiones e incidentes	1. Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda gestionarse de forma eficaz y pueda mantenerse un registro histórico completo. 2. Permitir el análisis de tendencias, clasificar las solicitudes e incidentes de servicio, con identificación del tipo y categoría. 3. Priorizar solicitudes e incidentes de servicio basados en la definición del servicio de SLA según el impacto y la urgencia para el negocio.	•Peticiones de servicio e incidentes clasificadas y priorizadas. •Registro de solicitudes de servicio e incidentes.	•Registro de peticiones de servicio e incidentes, clasificadas y priorizadas. •Registro de solicitudes de servicios e incidentes.							
		DSS02.03. Verificar, aprobar y resolver peticiones de servicio	1. Comprobar el derecho a las solicitudes de servicio, utilizando un flujo de proceso predefinido y cambios estándar, cuando sea posible. 2. Obtener la aprobación y confirmación financiera y funcional, si fuera necesario, o las aprobaciones predefinidas para los cambios estándar acordados. 3. Cumplir con las solicitudes realizando el proceso de solicitud seleccionado. Cuando sea posible, usar menús automáticos de autoayuda y modelos de solicitud predefinidas para elementos solicitados con frecuencia.	•Peticiones de servicio aprobadas. •Peticiones de servicio completadas.	•Registro de peticiones de servicio aprobadas. •Registro de peticiones de servicio completadas.							
		DSS02.04. Investigar, diagnosticar y asignar incidentes	1. Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Referenciar los recursos de conocimientos disponibles (incluidos errores y problemas conocido) para identificar posibles resoluciones de incidentes (soluciones temporales y/o permanentes). 2. Si un problema relacionado o error conocido no existe todavía y si el incidente satisface los criterios acordados para el registro de problemas, registrarlo como un problema nuevo. 3. Asignar incidentes a funciones de especialista si se necesita una mayor habilidad. Contar con el nivel directivo adecuado, donde y si se necesita.	•Log de problemas. •Síntomas de incidente.	•Registro de problemas. •Registro de síntomas de incidentes.							
		DSS02.05. Resolver y recuperarse de los incidentes	1. Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución workaround y/o solución permanente). 2. Registrar, si se usaron, workarounds para la resolución de incidentes. 3. Aplicar medidas correctivas, si se requieren. 4. Documentar la resolución de incidentes y evaluar si la resolución puede usarse como una fuente de conocimiento futura.	•Resoluciones de incidentes.	•Informe de resolución de incidentes.							
		DSS02.06. Cerrar las peticiones de servicio y los incidentes	1. Comprobar con los usuarios afectados que la solicitud de servicio se ha cumplido de forma satisfactoria o el incidente se ha resuelto de forma satisfactoria dentro de un plazo de tiempo acordado/aceptable. 2. Cerrar las peticiones e incidentes de servicio.	•Confirmación del usuario del cumplimiento o resolución satisfactoria.	•Evidencia (correo, chat, documento, firma, reunión, entre otros), donde el usuario notifica el cumplimiento y la							
		DSS02.07. Hacer seguimiento al estado y producir informes	1. Supervisar y hacer seguimiento al escalamientos y resoluciones de incidentes y solicitar procedimientos de manejo para progresar hacia la resolución o finalización de los mismos. 2. Identificar las partes interesadas en la información y sus necesidades de datos o informes. Identificar frecuencia y medio de elaboración de los reportes. 3. Producir y distribuir informes en el plazo debido o proporcionar un acceso controlado a los datos en línea. 4. Analizar incidentes y solicitudes de servicio por categoría y tipo. Establecer tendencias e identificar patrones de problemas recurrentes, violaciones o ineficiencias del SLA. 5. Usar la información como un insumo a la planificación de la mejora continua.	•Estado de incidentes e informe de tendencias. •Estado de cumpliminto de peticiones e informe de tendencias.	•Informes de tendencias de problemas recurrentes. •Informes sobre el estado de cumplimiento de las peticiones e incidentes.							
	DSS03. Gestionar los problemas	DSS03.01. Identificar y clasificar los problemas	1. Identificar problemas a través de la correlación de informes de incidentes, registros de errores y otros recursos que permitan la identificación de problemas. 2. Gestionar todos los problemas formalmente con acceso a todos los datos relevantes. Incluir información del sistema de gestión de cambios de TI y de configuración/activo de TI y los detalles del incidente. 3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, análisis de la causa raíz y determinación de soluciones para respaldar la gestión de problemas. Determinar grupos de soporte conforme a las categorías predefinidas, como hardware, red, software, aplicaciones y software de soporte. 4. Definir niveles de prioridad a través de la consulta con el negocio para garantizar que la identificación del problema y el análisis de las causas raíz se gestionan en el plazo debido conforme a los SLA acordados. Basar los niveles de prioridad en el impacto y la urgencia del negocio. 5. Informar del estado de los problemas identificados a la mesa de servicio, para que los clientes y gestores de TI puedan mantenerse informados. 6. Mantener un único catálogo de gestión de problemas para registrar e informar sobre los problemas identificados. Usar el catálogo para establecer pistas de auditoría de los procesos de gestión de problemas incluido el estado de cada problema (es decir, abierto, reabierto, en curso o cerrado).	•Esquema de clasificación de problemas. •Informes de estado del problema. •Registro de problemas.	•Procedimiento de gestión de los problemas. •Catálogo de gestión de problemas. •Esquema de clasificación de los problemas.							
		DSS03.02. Investigar y diagnosticar los problemas	1. Identificar problemas que podrían ser errores conocidos mediante una comparación de los datos de incidentes con la base de datos de errores conocidos y sospechados (p. ej., aquellos comunicados por proveedores externos) Clasificar los problemas como errores conocidos. 2. Asociar los elementos de configuración afectados con el error establecido/conocido. 3. Producir informes para comunicar el progreso a la hora de resolver problemas y gestionar el impacto continuo de los problemas no resueltos. Monitorizar el estado del proceso de manejo de problemas a lo largo de su ciclo de vida, incluyendo los insumos de la gestión de cambios y de la configuración de TI.	•Informes de resolución de problemas. •Causas raíz de problemas	•Registro sobre causas raíz de los problemas. •Informes de resolución de problemas.							
		DSS03.03. Presentar los errores conocidos	1. Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos y desarrollar una solución temporal apropiada. 2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambio de TI) soluciones a los errores conocidos, conforme al costo/ beneficio del caso de negocio, el impacto y la urgencia.	•Soluciones propuestas a errores conocidos. •Registro de errores conocidos.	•Registro de errores conocidos de los problemas. •Registro de acciones correctivas para							
		DSS03.04. Resolver y cerrar los problemas	1. Cerrar los registros de problemas después de la confirmación sobre la eliminación exitosa del error conocido o después del acuerdo con el negocio sobre cómo gestionar el problema de forma alternativa. 2. Informar a la mesa de servicio sobre el calendario de cierre de problemas (p. ej., el calendario para solucionar los errores conocidos, la posible solución temporal o el hecho de que el problema seguirá ahí hasta que se implemente el cambio) y las consecuencias de la estrategia llevada a cabo. Mantener a los usuarios y clientes afectados informados como corresponda. 3. A través del proceso de resolución, obtener informes regulares de gestión de cambios de TI relacionados con el progreso a la hora de resolver problemas y errores. 4. Monitorizar el impacto continuo de los problemas y errores conocidos en los servicios. 5. Revisar y confirmar la resolución satisfactoria de problemas mayores. 6. Asegurar que el conocimiento aprendido de la revisión se incorpore a la reunión de revisión de servicios con el cliente del negocio.	•Comunicación de conocimientos aprendidos. •Registro de problemas cerrados.	•Registro de problemas cerrados. •Procedimiento de comunicación de conocimientos aprendidos con las partes interesadas e involucrados.							
		DSS03.05. Realizar una gestión proactiva de los problemas	1. Captar la información del problema relacionada con cambios e incidentes de TI y comunicarla a las partes interesadas clave. Comunicar a través de informes y reuniones periódicas entre los dueños de los procesos de incidentes, problemas, cambios y gestión de la configuración para considerar los problemas recientes y las posibles acciones correctivas. 2. Garantizar que los dueños y gestores de los procesos de gestión de incidentes, problemas, cambios y configuración se reúnan regularmente para comentar los problemas conocidos y los cambios planificados futuros. 3. Identificar e iniciar soluciones sostenibles (soluciones permanentes) que aborden la causa raíz . Presentar solicitudes de cambio a través de los procesos establecidos de gestión de cambios. 4. Permitir a la empresa supervisar los costes totales de los problemas, captar los esfuerzos de cambios derivados de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar al respecto. 5. Crear informes para supervisar la resolución de problemas en relación con los requisitos del negocio y los SLAs. Asegurar el escalamiento adecuado de los problemas, como comunicarlos al siguiente nivel directivo conforme a los criterios acordados, contactar con proveedores externos o consultar con el consejo asesor de cambios (CAB) para aumentar la prioridad de una solicitud de cambio urgente (RFC) para implementar una solución temporal. 6. Optimizar el uso de recursos y reducir el uso de soluciones temporales; hacer un seguimiento a las tendencias de los problemas.	•Soluciones sostenibles identificadas. •Informes de supervisión de resolución de problemas.	•Informe de soluciones sostenibles para abordar la causa raíz de los problemas. •Informes de supervisión de la resolución de problemas en relación con estalamietos y SLAs.							

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Área	Responsable	Fecha de solicitud	Fecha de entrega	Comentarios
Monitorizar, Evaluar y Valorar (MEA)	MEA02. Gestionar el sistema de control interno	MEA02.01. Supervisar los controles internos	1. Identificar los límites del sistema de control interno. Por ejemplo, considerar cómo los controles internos de la organización, tienen en cuenta las actividades de desarrollo o producción externalizadas y/o ubicadas en otro país (offshore, término en inglés).	•Resultados de benchmarking y otras evaluaciones. •Resultados de la supervisión del control interno y sus revisiones.	•Informe de resultados de benchmarking y evaluaciones relacionadas con el control interno. •Informe de resultados sobre la supervisión del control interno.							
			2. Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicio cumplen con los requisitos legales y regulatorios y con sus obligaciones contractuales.									
			3. Realizar actividades de supervisión y evaluación del control interno basadas en estándares de gobierno de la organización y marcos y prácticas aceptados por la industria. Incluye también la supervisión y evaluación de la eficacia y eficiencia de las actividades de supervisión gerencial.									
			4. Asegurar que las excepciones de control se comuniquen , se sigan y analicen prontamente, y que se prioricen e implementen acciones correctivas apropiadas, conforme al perfil de gestión de riesgos (p. ej., clasificar algunas excepciones como riesgo clave y otras como riesgo no clave).									
			5. Considerar evaluaciones independientes del sistema de control interno (p. ej., por auditoría interna o compañeros).									
			6. Mantener el sistema de control interno, considerando los cambios continuos en el riesgo del negocio y de TI, el entorno de control de la organización y los procesos del negocio y de TI relevantes. Si hay una brecha, evaluar y recomendar cambios.									
			7. Evaluar regularmente el desempeño del marco de control, a través de una comparación con estándares y buenas prácticas aceptadas por la industria. Considerar la adopción formal de una estrategia de mejora continua de la supervisión del control interno.									
		MEA02.02. Revisar la eficacia de los controles del proceso de negocio.	1. Entender y priorizar el riesgo de los objetivos de la organización.	•Evidencia de la efectividad de los controles.	•Informe de resultados de las auditorías del control interno.							
			2. Identificar controles clave y desarrollar una estrategia adecuada para validar los controles.									
			3. Identificar información que indicará si un entorno de control interno está funcionando de forma eficaz.									
			4. Conservar evidencias de la eficacia del control.									
			5. Desarrollar e implementar procedimientos rentables para obtener esta información de acuerdo a los criterios de calidad de la información correspondientes.									
		MEA02.03. Realizar autoevaluaciones de control	1. Definir una estrategia acordada y consistente para realizar autoevaluaciones de control y coordinarse con auditores internos y externos.	•Planes y criterios de autoevaluación. •Resultados de las revisiones de las autoevaluaciones. •Resultados de las autoevaluaciones.	•Plan para la autoevaluación del control interno. •Guía de criterios de autoevaluación del control interno. •Informe de resultados de las autoevaluaciones del control interno.							
			2. Mantener planes de evaluación e identificación de criterios y alcance para llevar a cabo las autoevaluaciones. Planificar la comunicación de los resultados del proceso de autoevaluación al negocio, a TI y a la dirección general y al consejo de administración. Considerar estándares de auditoría interna en el diseño de las autoevaluaciones.									
			3. Determinar la frecuencia de las autoevaluaciones periódicas, considerando globalmente la eficacia y eficiencia de la supervisión continua.									
			4. Asignar las responsabilidades de la autoevaluación a los individuos adecuados para garantizar la objetividad y la competencia.									
			5. Proporcionar revisiones independientes para garantizar la objetividad de la autoevaluación y permitir que se compartan buenas prácticas de control interno de otras empresas.									
			6. Comparar los resultados de las autoevaluaciones con los estándares y buenas prácticas de la industria.									
			7. Resumir e informar de los resultados de las autoevaluaciones y benchmarking para tomar acciones correctivas.									
		MEA02.04. Identificar e informar las deficiencias de control	1. Comunicar procedimientos para el escalamiento de las excepciones de control, análisis de la causa raíz y notificación a los dueños del proceso y a las partes interesadas de TI.	•Acciones correctivas. •Deficiencias del control.	•Registro de deciciencias del control interno y sus acciones correctivas.							
			2. Considerar el riesgo empresarial relacionado para establecer umbrales para el escalamiento de las excepciones de control y fallos.									
			3. Identificar, reportar y registrar las excepciones de control. Asignar responsabilidades para su resolución e informar de su estado.									
			4. Decidir qué excepciones de control deberían comunicarse a la persona responsable de la función y qué excepciones deberían escalarse. Informar a los dueños del proceso y a las partes interesadas.									
			5. Hacer un seguimiento de todas las excepciones para garantizar que se han abordado las acciones acordadas.									
			6. Identificar, iniciar, seguir e implementar acciones correctivas que surjan de las evaluaciones de control y los reportes.									
	MEA03. Gestionar el cumplimiento de los requisitos externos	MEA03.01. Identificar los requisitos externos de cumplimiento	1. Asignar la responsabilidad de identificar y supervisar los cambios en los requisitos legales, regulatorios y otros requisitos contractuales externos, relevantes para el uso de recrsos de TI y el procesamiento de la información dentro de las operaciones empresariales y de TI.	•Log de acciones de cumplimiento requeridas. •Registro de requerimientos de cumplimiento.	•Requerimientos de cumplimiento externo: requisitos legales, regulatorios y contractuales. •Procedimiento de acciones de cumplimiento para los requisitos externos.							
			2. Identificar y evaluar todos los posibles requisitos de cumplimiento y su impacto en las actividades de TI, en áreas como flujo de datos, privacidad, controles internos, informes financieros, regulaciones específicas de la industria, propiedad intelectual, salud y seguridad en el trabajo.									
			3. Evaluar el impacto de los requisitos legales y regulatorios relacionados con TI sobre contratos con terceros relacionados con las operaciones de TI, proveedores de servicio y otros socios comerciales de negocios.									
			4. Definir las consecuencias del incumplimiento.									
			5. Obtener asesoría independiente cuando corresponda, sobre los cambios en la legislación, regulaciones y estándares vigentes.									
			6. Mantener un registro actualizado de todos los requisitos legales, regulatorios y contractuales; de su impacto y las acciones requeridas.									
			7. Mantener un registro global, armonizado e integrado, de los requisitos de cumplimiento externo para la empresa.									
		MEA03.02. Optimizar la respuesta a los requisitos externos	1. Revisar y ajustar continuamente las políticas, principios, estándares, procedimientos y metodologías para que sean eficaces en garantizar el cumplimiento necesario y abordar el riesgo empresarial. Usar expertos internos y externos, cuando sea necesario.	•Comunicaciones de cambios en los requisitos de cumplimiento. •Políticas, principios, procedimientos y	•Procedimiento de comunicación de los cambios en requisitos de cumplimiento. •Listado y registro de principios, estándares,							
			2. Comunicar los requisitos nuevos y modificados a todo el personal relevante.									
		MEA03.03. Confirmar el cumplimiento externo	1. Evaluar regularmente las políticas, estándares, procedimientos y metodologías organizativas en todas las funciones de la empresa, para garantizar el cumplimiento de todos los requisitos legales y regulatorios relevantes relacionados con el procesamiento de la información.	•Confirmaciones de cumplimiento. •Brechas de cumplimiento identificadas.	•Resultados de cumplimiento o incumplimiento de los requisitos externos. •Formulario de brechas de cumplimiento.							
			2. Tratar las brechas de cumplimiento en políticas, estándares y procedimientos con las debida oportunidad.									
			3. Evaluar periódicamente los procesos y actividades del negocio y de TI para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales vigentes.									
			4. Revisar regularmente los patrones recurrentes de fallos de cumplimiento y evaluar las lecciones aprendidas.									
			5. Mejorar las políticas, estándares, procedimientos, metodologías y sus procesos y actividades asociadas con base en la revisión y las lecciones aprendidas.									
		MEA03.04. Obtener aseguramiento de cumplimiento externo	1. Obtener confirmación periódica del cumplimiento con las políticas internas por parte de los dueños de los procesos de negocio y de TI y los jefes de unidades.	•Informes de aseguramiento del cumplimiento. •Informes de los problemas de incumplimiento y sus causa raíz.	•Informes de evaluación del cumplimiento a nivel interno. •Informe de problemas de incumplimiento con su respectiva causa raíz.							
			2. Realizar periódicamente revisiones internas y externas (Independientes, cuando sea posible,) para evaluar los niveles de cumplimiento.									
			3. Si se requiere, obtener declaraciones de los proveedores de servicio externos de TI sobre sus niveles de cumplimiento con las leyes y regulaciones aplicables.									
			4. Si se requiere, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento con leyes y regulaciones aplicables, en la medida en que estén relacionados con las transacciones electrónicas entre empresas.									
			5. Integrar los informes sobre los requisitos legales, regulatorios y contractuales a nivel global de la empresa, involucrando a todas las unidades de negocio.									
			6. Supervisar y comunicar los problemas de incumplimiento y, cuando sea necesario, investigar la causa raíz.									

Apéndice N. Instructivo de gestión inicial

KPMG

Instructivo de Gestión de Ejecución de la auditoría

Introducción

El presente instructivo de gestión proporciona una serie de estructuras básicas y guión que deben ser consideradas en ciertas de las actividades del proceso de auditoría de TI. El objetivo de este documento es estandarizar y brindar conocimiento sobre las herramientas a utilizar y maneras de proceder al momento de ejecutar las actividades correspondiente. A continuación, se mencionan las actividades involucradas en este instructivo:

- **Reuniones de Entendimiento**

  Las reuniones de entendimiento se realizan entre el auditor y el cliente auditado. El auditor de TI se reúne con el cliente auditado para aclarar consultas sobre las evidencias proporcionadas. En el instructivo, se pactan especificaciones generales sobre este tipo de reuniones, y un guión de preguntas que pueden ser adaptadas al contexto de cada cliente y posteriormente utilizadas en la actividad.

- **Documentación de Riesgos**

  La documentación de los riesgos se realiza dentro de las fichas de auditoría. Sigue una estructura formal de condición, causa, impacto y recomendación. En el instructivo, se ejemplifican algunos riesgos por cada proceso, para que el auditor tenga un guión, los adapte al contexto del cliente y posteriormente los documente.

- **Desarrollo del Cronograma de Auditoría**

  El cronograma de auditoría es uno de los primeros entregables durante el proceso de TI. Ayuda a visualizar las actividades, periodos de entrega y duraciones pactadas para la auditoría. En el instructivo, se realiza un guión de cronograma, formalizando las actividades que generalmente son utilizadas, así como periodos aproximados de tiempo.

KPMG

Índice

KPMG

Guión para la documentación de Reuniones de Entendimiento

Este apartado es un guión para ejecutar y documentar las reuniones de entendimiento efectuadas durante el proceso de auditoría de Tecnología de Información.

Especificaciones generales:

- La documentación de las respuestas debe realizarse en un documento digital como Microsoft Word o Excel. Este documento debe ser cargado a la carpeta de trabajo de la auditoría.
- Las preguntas para realizar por cada proceso durante la reunión deben estar alineadas a las actividades de cada práctica del proceso de COBIT 2019. En la sección **Guión de preguntas por cada proceso de COBIT 2019:**, podrán encontrar un guión de preguntas las cuales sirven de base para realizar las preguntas correspondientes por cada proceso que se audite.

Nota: Es importante aclarar que cada organización auditada es diferente, por ende las preguntas deben ser dirigidas de acuerdo con el contexto de cada cliente. Este documento sirve como guión para llevar una misma línea en la gestión de las reuniones de entendimiento, sin embargo, las preguntas e información que se gestione será única para cada cliente auditado.

Estructura de la reunión de entendimiento:

La reunión de entendimiento debe efectuarse bajo la siguiente agenda:

1. Saludo
2. Desglose de los contenidos a abarcar en la reunión.
3. Ejecución de las preguntas necesarias por cada procesos en cuestión.
4. Espacio para consultas por parte del cliente.
5. Despedida y finalización de la reunión.

KPMG

Guión de preguntas por cada proceso de COBIT 2019:

EDM01: Asegurar el establecimiento y el mantenimiento del marco de gobierno	
Práctica	**Guión de preguntas**
EDM01.01. Evaluar el sistema de gobierno	• ¿Tienen identificados los factores internos y externos (leyes, reglamentos, u obligaciones contractuales), y las tendencias que influyen en el gobierno de TI de su empresa ? ¿Cuales son? • ¿Tienen definida la importancia de TI para su negocio y cómo influye en las implicaciones de control? ¿Dónde se evidencia dicha importancia? • ¿Cómo efectúan el alineamiento de la información con el entorno, intereses, metas y objetivos empresariales? ¿Pueden mostrar evidencia del alineamiento? • ¿Tienen definido y documentado los principios de gobierno empresarial, el modelo de toma de decisiones y niveles de autoridad de TI?
EDM01.02. Dirigir el sistema de gobierno	• ¿Cómo comunican el gobierno de TI y las directrices del comportamiento ético y profesional? ¿Cómo evidencian que se comunique la información adecuada? • ¿Tienen identificada y documentada la delegación y asignación de responsabilidades relacionadas con las prácticas de gobierno y directrices de TI? • ¿Tienen definido y documentado el consejo de administración de TI y velan por el cumplimiento de sus funciones? • ¿Cómo establecen su sistema de recompensas? ¿Tienen documentado su sistema de recompensas? ¿Tienen evidencia de su sistema de recompensas?
EDM01.03. Monitorizar el sistema de gobierno	• ¿Cómo evalúan el rendimiento y la eficacia de las partes interesadas que tiene responsabilidades de gobierno de TI? ¿Realizan informes de rendimiento? ¿En dónde se encuentran estos informes? • ¿Cómo monitorean el cumplimiento de estructuras, mecanismos y principios de TI, y las obligaciones debe satisfacer? ¿Tienen evidencias sobre informes de monitoreo? • ¿Cómo evalúan la eficacia del diseño de gobierno de TI y el sistema de control ? ¿Tienen evidencias sobre informes de eficacia?

KPMG

EDM03: Asegurar la optimización del riesgo	
Práctica	**Guión de preguntas**
EDM03.01. Evaluar la gestión de riesgos	• ¿Tienen identificado el apetito y la tolerancia del riesgo de TI de acuerdo con el contexto de la organización? • ¿Cómo aseguran el alineamiento de la estrategia de riesgos de TI con la estrategia de la empresa? ¿Tienen evidencia de este alineamiento? • ¿Cómo evalúan los factores y la gestión de riesgos para que estén alineadas con la tolerancia del riesgo y las capacidades de la empresa para las pérdidas? ¿Tienen evidencia de esta evaluación? • ¿Tienen definido las habilidades y el personal para la gestión de riesgos? ¿Tienen evidencia de esta definición?
EDM03.02. Dirigir la gestión de riesgos	• ¿Tienen un procedimiento que direccionan la estrategia de riesgos, los planes de comunicación de riesgos, y la implementación de mecanismos de respuesta al cambio de riesgos? • ¿Tienen un protocolo de comunicación de riesgos que aseguran que los riesgos, oportunidades o problemas puedan identificarse y comunicarse por cualquier persona de la empresa a la parte correspondiente? • ¿Tienen definido y documentado las metas y métricas para la gestión de riesgos?
EDM03.03. Monitorizar la gestión de riesgos	• ¿Tienen un protocolo o procedimiento para comunicar los problemas de gestión de riesgos a la administración? Si no, ¿Cómo lo comunican? • ¿Cómo supervisan el cumplimiento de la gestión de riesgos, sus metas y métricas de acuerdo con el apetito y tolerancia y los objetivos empresariales? ¿Tienen informes de cumplimiento que puedan evidenciar la supervisión? • ¿Cómo efectúan la revisión del progreso de la empresa de acuerdo con las metas establecidas? ¿Tienen resultados de revisiones que puedan evidenciar la supervisión?

KPMG

APO09: Gestionar los acuerdos de servicio	
Práctica	**Guión de preguntas**
APO09.01. Identificar los servicios de TI	• ¿Cómo identifican las brechas entre los servicios actuales de TI y las actividades que apoyan? ¿Tienen herramientas para la documentación de brecha que evidencie lo anterior? • ¿Cómo analizan las capacidades actuales, las necesidades y la demanda futura relacionadas con los servicios de TI? ¿Tienen evidencia del análisis? • ¿Cada cuánto realizan revisiones periódicas del portafolio de servicios para identificar aquellos obsoletos? ¿Tienen evidencia de dichas supervisiones?
APO09.02. Catalogar los servicios habilitados por TI	• ¿Publican los catálogos de servicio de la empresa? • ¿Cómo aseguran que la información de los catálogos de servicios esté completa y actualizada? ¿Tienen evidencia de la actualización? • ¿Tienen un protocolo de comunicación que gestione la comunicación de los catálogos de servicio a la dirección?
APO09.03. Definir y preparar acuerdos de servicio	• ¿Tienen un procedimiento para realizar acuerdos a nivel de servicio y acuerdos a nivel operativo? (lineamientos, pasos, actividades, comunicaciones, relaciones)
APO09.04. Monitorizar y reportar los niveles de servicio	• ¿Cómo monitorean, evalúan o informan el rendimiento de los acuerdos a nivel de servicio? ¿Tienen informes de rendimiento que evidencie lo anterior? • ¿Cómo realizan revisiones para pronosticar tendencias de rendimiento de nivel de servicio?¿Tienen informes de tendencias que evidencie lo anterior? • ¿Tienen planes de acción y remediación para gestionar los problemas de rendimiento?
APO09.05. Revisar los acuerdos y los contratos de servicio	• ¿Cada cuánto revisan los acuerdos a nivel de servicio vigentes para garantizar su efectividad o actualizarlos para que cumplan con la efectividad pactada? ¿Tienen evidencia que respalde la revisión?

KPMG

APO13: Gestionar la seguridad	
Práctica	**Guión de preguntas**
APO13.01. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)	• ¿Tienen un plan, política o informe que defina el Sistema de Gestión de Seguridad de la Información (SGSI), su alcance (con su declaración de aplicabilidad), limitaciones y alineamiento en torno a las características de la empresa? • ¿Cómo ejecutan las autorizaciones con dirección para la implementación del SGSI? ¿Tienen evidencias de las autorizaciones? • ¿Tienen un protocolo o procedimiento de comunicación de la estrategia de SGSI, sus roles y las responsabilidades?
APO13.02. Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	• ¿Formulan un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos de la empresa, así como componentes de soluciones, tratamientos de riesgos y aportes de diseño y gestión de riesgos de seguridad de la información? • ¿Qué programas o acciones implementan para promover la concienciación de la seguridad y privacidad de la información? ¿Tienen evidencia de estos programas o acciones? • ¿Ejecutan la planificación, diseño, implementación y monitoreo de procedimientos de seguridad para la prevención y detección de eventos de seguridad de forma integrada? ¿Tienen evidencia de dichos procedimientos integrados? • ¿Tienen métricas para medir la eficacia de las prácticas de gestión?
APO13.03. Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	• ¿Cada cuánto llevan a cabo revisiones o auditorías para evaluar el cumplimiento de SGSI para asegurar su eficacia y alcance? ¿Tienen informes de resultados que evidencie las revisiones? • ¿Documentan aquellas acciones o eventos que podrían tener un impacto en el SGSI?

KPMG

BAI06: Gestionar los cambios de TI	
Práctica	**Guion de preguntas**
BAI06.01. Evaluar, priorizar y autorizar solicitudes de cambio	• ¿Poseen solicitudes formales para permitir a los usuarios notificar los cambios.? ¿Cuales son? • ¿Realizan la categorización y priorización de los cambios de acuerdo con los requisitos técnicos y de negocio? • ¿Cómo efectúan las aprobaciones de los cambios aquellos involucrados según corresponda? ¿Tienen evidencia de las aprobaciones? • ¿Tienen documentada la planificación y programación de los cambios de TI, considerando el impacto en los procesos de negocio, infraestructura, sistemas, aplicaciones, proveedores, y demás elementos relacionados con los cambios ?
BAI06.02. Gestionar cambios de emergencia	• ¿Tienen procedimientos documentados para definir, declarar, evaluar, aprobar, autorizar y registrar cambios de emergencia? • ¿Tienen procedimientos para verificar y monitorear que todos los cambios de emergencia se autoricen, documenten y revoquen? • ¿Realizan revisiones posteriores a la implementación de las acciones para el cambio con los interesados ? ¿Tienen informes de revisiones que evidencien lo anterior?
BAI06.03. Hacer seguimiento e informar sobre cambios de estado	• ¿Tienen procedimientos para gestionar la ejecución del monitoreo, categorización (rechazado, aprobado, cerrado, etc.) y evaluaciones del estado de los cambios?
BAI06.04. Cerrar y documentar los cambios.	• ¿Realizan la documentación de los cambios en los procedimientos necesarios? ¿Estos cambios en la documentación son sometidos a revisión? ¿Tienen la documentación y evidencias de revisión respectivas?

8

KPMG

BAI09: Gestiona los activos	
Práctica	**Guión de preguntas**
BAI09.01. Identificar y registrar los activos actuales.	• ¿Llevan un registro de los activos, su estado actual, requisitos legales, regulatorios o contractuales y propósito? ¿Tienen evidencia del registro? • ¿Efectúan revisiones de contabilidad, comprobación y conciliación de los activos? ¿Tienen resultados de revisiones que evidencien lo anterior? • ¿Realizan comprobaciones para verificar la efectividad del valor y propósito de los activos?¿Tienen resultados de comprobaciones que evidencia lo anterior?
BAI09.02. Gestionar los activos críticos	• ¿Tienen documentado los activos críticos y su riesgo de fallo? • ¿Cómo llevan a cabo la comunicación y calendarización de las actividades de mantenimiento para los usuarios afectados? ¿Tienen evidencia de protocolos de comunicación y cronogramas de las actividades de mantenimiento? • ¿Documentan planes de mantenimiento preventivo de los activos de forma regular ? ¿Establecen acuerdos de servicio para el mantenimiento que incluya acceso de terceros a las instalaciones de TI de la empresa? • ¿Cómo garantizan que los accesos remotos y de perfiles de usuarios sean activos únicamente cuando es necesario? ¿Tienen evidencia de revisiones después del tiempo pactado de estos accesos y perfiles? • ¿Cómo llevan a cabo el monitoreo de los activos críticos y las acciones correctivas necesarias? ¿Tienen resultados del monitoreo que evidencie lo anterior?
BAI09.03. Gestionar el ciclo de vida del activo	• ¿Tienen un procedimiento sobre el ciclo de vida de los activos, que documente las acciones para las solicitudes aprobadas de los activos, el registro de los pagos, aprobaciones de los pagos, asignaciones, reasignaciones e implementación de los activos, planificaciones, autorizaciones e implementación de la retirada de los activos, y disponibilidad de los activos?
BAI09.04. Optimizar el valor de los activos	• ¿Efectúan las revisiones de los activos, en términos de costes de mantenimiento, garantías, relación calidad-precio, estado? ¿Tiene informes de revisión de activos que evidencia lo anterior? • ¿Documentan los resultados para identificar oportunidades de mejora y estandarización así como identificar aquellos activos con posibilidad de eliminación o sustitución?
BAI09.05. Gestionar las licencias	• ¿Llevan un registro de las licencias adquiridas con sus acuerdos asociados?

	• ¿Realizan auditorías para evaluar las licencias instaladas? ¿Tienen resultados de auditorías que evidencien lo anterior? • ¿Documentan por medio de planes o procedimiento la gestión de las licencias instaladas de acuerdo con las licencias instaladas versus las licencias adquiridas? • ¿Realizan análisis para evaluar la rentabilidad de la actualización de los productos y licencias asociadas? ¿Tienen los resultados del análisis para evidenciar lo anterior?

KPMG

DSS02:Gestionar las peticiones y los incidentes de servicio	
Práctica	**Guión de preguntas**
DSS02.01. Definir esquemas de clasificación para incidentes y peticiones de servicio	• ¿Tienen esquemas y modelos de clasificación de las peticiones de servicio e incidentes? • ¿Tienen establecidas y definidas las fuentes de conocimiento sobre incidentes y solicitudes, así como las reglas y los procedimientos para la escalación de los incidentes?
DSS02.02. Registrar, clasificar y priorizar las peticiones e incidentes	• ¿Llevan a cabo un registro de las solicitudes e incidentes de servicio, que permita la clasificación y priorización de estos de acuerdo con el impacto y urgencia del negocio?
DSS02.03. Verificar, aprobar y resolver peticiones de servicio	• ¿Tienen definidos el flujo y el proceso para la gestión de las solicitudes de servicio?
DSS02.04. Investigar, diagnosticar y asignar incidentes	• ¿Tiene un procedimiento para diagnosticar y asignar incidentes, considerando sus síntomas, problemas relacionados o errores conocidos, asignación a personal especial, etc.?
DSS02.05. Resolver y recuperarse de los incidentes	• ¿Tienen documentado la resolución de incidentes en términos de medidas correctivas, workarounds, evaluaciones de la resolución ?
DSS02.06. Cerrar las peticiones de servicio y los incidentes	• ¿Cómo realizan la confirmación del usuarios del cumplimiento de su solicitud, y posterior el cierre del incidente? ¿Tienen evidencia de dicha confirmación?
DSS02.07. Hacer seguimiento al estado y producir informes	• ¿Realizan supervisiones y seguimientos sobre los escalamientos y resoluciones de los incidentes, partes interesadas involucradas, tendencias o patrones de problemas? ¿Tienen informes de seguimiento que evidencien lo anterior? • ¿Cómo utilizan la información resultado de las revisiones como insumos para la mejora continua de la empresa? ¿Tienen evidencia sobre lo anterior?

11

KPMG

DSS03: Gestionar los problemas	
Práctica	**Guión de preguntas**
DSS03.01. Identificar y clasificar los problemas	• ¿Tienen un procedimiento o plan sobre la gestión de problemas, el cual identifica los problemas, y define grupos de soporte, clasificaciones, niveles de prioridad, causas raíz, y soluciones para respaldar los problemas? • ¿Cómo comunican el estado de los problemas a los usuarios involucrados? ¿Tienen evidencia de dicha comunicación? • ¿Existe un catálogo de gestión de problemas que informe y registre los problemas identificados?
DSS03.02. Investigar y diagnosticar los problemas	• ¿Cómo identifican y asocian los problemas y sus elementos como errores conocidos? ¿Tienen documentados los errores conocidos? • ¿Realizan y monitorean informes del progreso del problema a lo largo de su ciclo de vida? ¿Tienen el informe del problema que evidencie lo anterior?
DSS03.03. Presentar los errores conocidos	• ¿Documentan las soluciones ante los problemas de errores conocidos conforme a costos, impacto del negocio, urgencia? ¿Tienen evidencia de la documentación requerida?
DSS03.04. Resolver y cerrar los problemas	• ¿Tienen un procedimiento o registro para cerrar los problemas, el cual calendarice el cierre de los problemas y las acciones tomadas en cuenta para la resolución? • ¿Realizan informes de revisión y monitoreo sobre el proceso de resolución de problemas, su impacto, errores conocidos, y resolución satisfactoria? ¿Tienen los resultados de la revisión que evidencie lo anterior? • ¿Tienen un protocolo para comunicar el cierre de problemas a los usuarios afectados y el conocimiento aprendido de la resolución del problema?
DSS03.05. Realizar una gestión proactiva de los problemas	• ¿Documentan y comunican la gestión de los problemas considerando las soluciones sostenibles halladas para estos? ¿Tienen evidencia de dicha documentación y comunicación? • ¿Cómo llevan a cabo las reuniones con los dueños y gestores de los problemas para comentar los problemas y cambios a futuro ? ¿Tienen evidencia de las reuniones mencionadas? • ¿Llevan a cabo informes de supervisión de los costos totales de los problemas, la resolución realizada en términos de requisitos de negocio, SLAs, seguimiento de tendencias de los problemas? ¿Tienen evidencia de los informes de supervisión y sus resultados que evidencia lo anterior?

12

KPMG

MEA02: Gestionar el sistema de control interno	
Práctica	**Guión de preguntas**
MEA02.01. Supervisar los controles internos	• ¿Realizan la supervisión, mantenimiento y evaluación del control interno tomando en cuenta los límites, estado de los proveedores, estándares de gobierno, marcos, prácticas de la industria, evaluaciones independientes como auditorías, cambios continuos del negocio? ¿Tienen evidencia de la supervisión del control interno? • ¿Cómo aseguran que se comunique, priorice, analice e implementen acciones correctivas a las excepciones del control interno? ¿Tienen evidencia del aseguramiento de la comunicación?
MEA02.02. Revisar la eficacia de los controles del proceso de negocio.	• ¿Tienen un procedimiento para revisar la eficacia de los controles de los procesos de negocio, que se identifique los controles clave, estrategias adecuadas de validación de controles, evidencias de eficacia de los controles, formas de obtener información según los criterios de calidad?
MEA02.03. Realizar autoevaluaciones de control	• ¿Tienen un plan que defina la estrategia para realizar autoevaluaciones de control, el cual defina el criterio y alcance para realizar autoevaluaciones, la comunicación, frecuencia, responsabilidades, descripción de las revisiones de la autoevaluación? • ¿Realizan comparaciones de las autoevaluaciones con los estándares y buenas prácticas de la industria, e informan los resultados para tomar acciones correctivas? ¿Tienen evidencia de resultados de las comparaciones?
MEA02.04. Identificar e informar las deficiencias de control	• ¿Tienen un procedimiento para las excepciones de control, el cual defina el escalamiento, el riesgo empresarial relacionado, responsabilidad de la resoluciones, formas de comunicación de las excepciones, estado? • ¿Documentan las acciones correctivas identificadas de las excepciones y deficiencias del control? ¿Tienen los informes que documentan las acciones correctivas que evidencie lo anterior?

13

KPMG

MEA03: Gestionar el cumplimiento de los requisitos externos	
Práctica	**Guión de preguntas**
MEA03.01. Identificar los requisitos externos de cumplimiento	• ¿Mantienen un registro de los requisitos externos de cumplimiento requeridos, tales como los legales, regulatorios, contractuales, con su impacto a nivel de TI, proveedores de servicio y socios comerciales de negocio, consecuencias de su incumplimiento y acciones requeridas ? ¿Tienen evidencia de dicho registro? • ¿Cómo obtienen asesoría para los cambios en la legislación, regulaciones y estándares vigentes? ¿Tienen evidencia de la asesoría brindada?
MEA03.02. Optimizar la respuesta a los requisitos externos	• ¿Actualizan las políticas, principios, estándares, procedimientos y metodologías para garantizar el cumplimiento de los requisitos? ¿Tienen evidencia de dicha actualización ? • ¿Cómo comunican las modificaciones o los nuevos requisitos al personal? ¿Tienen evidencia de dicha comunicación?
MEA03.03. Confirmar el cumplimiento externo	• ¿Cada cuánto realizan evaluaciones sobre las políticas, estándares, procedimiento y metodologías, actividades de negocio y de TI, patrones de fallo de cumplimientos, para garantizar el cumplimiento de los requisitos legales y regulatorios? ¿Tienen evidencia de dicha evaluación? • ¿Documentan las brechas identificadas de la evaluación y mejoran los documentos necesarios tomando como base la revisión y las lecciones aprendidas?
MEA03.04. Obtener aseguramiento de cumplimiento externo	• ¿Cada cuánto realizan las revisiones internas y externas para evaluar los niveles de cumplimiento de las políticas, requisitos legales, regulatorios y contractuales, y las declaraciones de cumplimiento de proveedores y socios? ¿Tienen evidencia sobre el informe documentado? • ¿Documentan los problemas y causa raíz del incumplimiento identificado, y los comunican a los involucrados? ¿Tienen evidencia del informe de problemas y causas ?

14

KPMG

Guión para la documentación de los riesgos de auditoría

Esta sección es un guión para definir los apartados establecidos sobre los riesgos dentro de la documentación de las fichas de auditoría.

Especificaciones generales:

- Los cuadros siguientes contienen los posibles riesgos que pueden materializarse en cada proceso de COBIT 2019. Cada riesgo es documentado de acuerdo con la estructura preestablecida: Condición, Causa, Impacto. Asimismo, para cada riesgo se plantea una recomendación.
- El impacto de los riesgos debe definirse de acuerdo con los siguientes tipos:

Tipo de impacto	Descripción
Estratégico	El impacto estratégico de los riesgos está relacionado con todas aquellas actividades que puedan afectar los objetivos y la estrategias de la organización.
Operativo	El impacto operativo está asociado con aquellas actividades que afectan el curso normal de los procesos de negocio de una organización, imposibilitando una parte o la totalidad de estos.
Económico	El impacto económico referencia a todas aquellas actividades que impactan las operaciones financiera de una organización, tales como créditos, pagos, deudas, cobros, inversiones, gastos, utilidades, entre otros.
Legal	El impacto legal hace referencia a las actividades que afectan las operaciones legales tales como el cumplimiento de políticas externas, reglamentos y relaciones contractuales.

Nota: Es importante aclarar que cada organización auditada es diferente, por ende los riesgos deben definirse de acuerdo con el contexto de cada cliente. Esta serie de riesgos son un guión que oriente al auditor sobre qué tipos de riesgos puede establecer en la documentación correspondiente, alineado a la auditoría propia de este cliente.

15

KPMG

Listado de riesgos por cada proceso de COBIT 2019

EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno.			
Condición	**Causa**	**Impacto**	**Recomendación**
Desconocimiento de los niveles de autoridad	No hay niveles definidos para delegar autoridad y responsabilidades para el gobierno de gestión y las decisiones de TI.	Estratégico	Establecer niveles de autoridad, con sus respectivos límites y responsabilidades para gestionar el sistema de gobierno.
Los principios del gobierno de gestión y la toma de decisiones no están alineados con los factores internos o externos de la empresa	No se identificaron o analizaron los factores internos y externos y su aplicación dentro del gobierno de TI de la empresa antes de definir los principios y toma de decisiones.	Estratégico	Identificar todos los factores internos y externos que tengan implicación en el gobierno de TI. Analizarlos y ajustar los principios para que cumplan con estos.
Problemas de comunicación del gobierno de TI	Canales ambiguos de comunicación del gobierno de TI. Inexistencia de un plan de comunicación.	Operativo	Formular dentro de un plan o procedimiento los canales de comunicación del gobierno de TI, los interesados respectivos y la información a comunicar.

16

KPMG

EDM03. Asegurar la optimización del riesgo			
Condición	**Causa**	**Impacto**	**Recomendación**
La organización no puede soportar las actividades de gestión de riesgos	No se evalúa el apetito y tolerancia al riesgo, así como la capacidad de la organización en el planteamiento de actividades de gestión de riesgos.	Operativo	Analizar el apetito y tolerancia de riesgo, y la capacidad de la empresa, y alinear las actividades de gestión para que cumplan con estos aspectos.
Fallas constantes en la dirección de la gestión de riesgos	Ausencia de una política para la gestión de riesgos	Operativo	Definir una política de gestión de riesgos que involucre la comunicación, el proceso, los objetivos, los mecanismos, metas y métricas para la gestión de riesgos.
Escazas supervisiones o monitoreos de la gestión de riesgos	No hay periodos definidos para supervisar, revisar o monitorear la gestión de riesgos.	Operativo Estratégico	Establecer periodos de monitoreo de la gestión de riesgos con los involucrados que hacen parte de esta.

KPMG

APO09. Gestionar los acuerdos de servicio			
Condición	Causa	Impacto	Recomendación
Estándares de servicios no cumplen con los requerimientos del negocio	Servicios obsoletos. Los servicios actuales no apoyan las actividades empresariales.	Estratégico	Evaluar y estudiar los servicios de acuerdo con la demanda, capacidad y actividades de la empresa
Existencia de servicios obsoletos dentro del catálogo de servicios	Catálogos de servicios no actualizados ni alineados con la estrategia de la organización.	Operativo	Revisar los catálogos de servicios actuales para actualizar sus servicios con respecto al contexto, objetivos y estrategia de la organización.
SLAs no cumplen con las expectativas pactadas sobre el rendimiento, operación y calidad de los servicios	No se realizan evaluaciones o revisiones de los acuerdos de servicio para verificar su actualización y cumplimiento.	Estratégico	Definir periodos de revisión para evaluar el rendimiento de los acuerdos a nivel de servicio.

18

KPMG

APO13. Gestionar la seguridad			
Condición	Causa	Impacto	Recomendación
Desalineamiento del alcance y los límites del SGSI con el negocio	No se define un SGSI de acuerdo a la política empresarial, características, activos, y tecnología de la empresa.	Estratégico	Evaluar las actividades del alcance del SGSI con las características, factores y políticas de la empresa para garantizar su cumplimiento.
Fallos en el tratamiento de los riesgos de la seguridad de la información	-Inexistencia de un plan de tratamiento de riesgos. -Procedimientos, propuestas, o casos de negocio no alineados a los objetivo estratégicos.	Operativo	Definir un plan de tratamiento de riesgos robusto que involucre propuestas, procedimientos, casos de negocio, prácticas y soluciones alineadas a los objetivos de la empresa.
No existe una planificación y documentación sobre el monitoreo y revisión del SGSI	-No existen revisiones regulares para validar el cumplimiento del SGSI. -No se documentan informes de evaluación de los SGSI.	Operativo Estratégico	-Fijar periodos de forma regular para monitorear y revisar el SGSI. -Documentar hallazgos y brindar recomendaciones.

KPMG

BAI06. Gestionar los cambios de TI			
Condición	Causa	Impacto	Recomendación
El proceso de gestión de solicitudes de cambio es desorganizado	No existe un único plan o procedimiento para la gestión de cambios.	Operativo	Definir un plan o procedimiento para la gestión de cambios considerando los requisitos técnicos y de negocio de la empresa.
Manejo inadecuado de los cambios de emergencia	No existe una definición y procedimiento para la gestión de cambios de emergencia.	Operativo	Establecer las actividades respectivas para los cambios de emergencia según los requisitos técnicos y de negocio de la empresa.
Desconocimiento de revisiones y actualizaciones en la documentación relacionada con la gestión de cambios	No hay periodos definidos para revisar el estado de los cambios. La documentación desactualizada.	Operativo Estratégico	-Fijar periodos de revisión de los cambios y de actualización de documentación relacionada a los cambios.

20

KPMG

BAI09. Gestionar los activos			
Condición	**Causa**	**Impacto**	**Recomendación**
Fallas en la organización de los activos	No existe un control de los activos actuales y sus requisitos de acuerdo al negocio	Operativo Económico	Llevar un registro de los activos con sus características y requisitos de acuerdo al negocio.
Los activos no cumplen con los niveles de optimización, o están obsoletos con respecto a la estrategia de la organización	No se efectúan revisiones periódicas de los activos.	Estratégico Económico	Definir revisiones periódicas sobre la base de activos, sus costes de mantenimiento, garantías, capacidades, cumplimiento en el negocio.
Gestión inadecuada de las licencias	No existe un registro de las licencias o un plan de acción para gestionarlas.	Operativo	Registrar las licencias actuales y formular un plan de acción que permita llevar un control y comparación de estas.

KPMG

DSS02. Gestionar las peticiones y los incidentes de servicio			
Condición	Causa	Impacto	Recomendación
Ambigüedad en la gestión de las peticiones y los incidentes de servicio	No hay definición de criterios, priorización, reglas de escalamiento, esquemas o modelos de clasificación de los incidentes.	Operativo	Definir los esquemas de priorización, modelos de clasificación, reglas o procedimientos de los incidentes de acuerdo con el negocio.
Retrasos en la resolución de incidentes	Los incidentes no son registrados, aprobados, soluciones y cerrados apropiadamente.	Operativo	Definir las acciones para registrar, aprobar, solucionar y cerrar apropiadamente los incidentes.
Desconocimiento sobre el estado de cumplimiento de los incidentes	No hay revisiones periódicas para el seguimiento de los estados de los incidentes.	Operativo Estratégico	Fijar periodos de evaluación sobre los estados de los incidentes, y utilizar los resultados como insumos para la mejora continua de la organización.

22

KPMG

DSS03. Gestionar los problemas			
Condición	**Causa**	**Impacto**	**Recomendación**
Ambigüedad en la gestión de problemas.	No existe un esquema para la clasificación de problemas, sus niveles de prioridad, estado, catálogos de gestión.	Operativo	Definir la clasificación de problemas, prioridad, estado, catálogos de gestión, etc.
Retrasos en la resolución de errores conocidos	No existe un registro de los errores conocidos, sus procedimiento, acciones correctivas, canales de comunicación.	Operativo	Llevar un registro de los problemas conocidos con sus procedimientos, acciones correctivas y canales de comunicación.
Fallas en el desarrollo de la retroalimentación de los problemas	No hay reuniones periódicas para comentar y documentar los cambios, soluciones, incidentes, actividades relacionadas con los problemas identificados.	Operativo Estratégico	-Realizar reuniones periódicas con las partes interesadas del problema para identificar sus causas, acciones correctivas, incidencias, cambios en el negocio. -Documentar la retroalimentación de la reunión para favorecer la toma de decisiones.

KPMG

MEA02. Gestionar el sistema de control interno			
Condición	**Causa**	**Impacto**	**Recomendación**
Resultados erróneos en la supervisión de los controles internos	No hay una evaluación de los límites del control interno, su estado, actividades de supervisión y evaluación, excepciones, según las políticas y objetivos del negocio.	Estratégico	Evaluar los límites, estado, actividades, políticas, supervisiones y evaluaciones de los controles internos según los criterios, características y estado del negocio.
Desconocimiento de la efectividad de los controles internos	-No hay revisiones de efectividad o autoevaluaciones de control interno.	Operativo	-Establecer revisiones periódicas para validar la efectividad de los controles. -Definir una estrategia de autoevaluación de los controles que incluya la frecuencia de realización, responsables, y documentación de hallazgos.
Desorganización para identificar y gestionar las deficiencias de los controles	-No se lleva un registro de las deficiencias de los controles, de acuerdo con la estrategia de la organización.	Operativo Estratégico	-Definir procedimientos para la gestión deficiencias del control interno que detalle las excepciones del control, su seguimiento y análisis, responsables involucrados, y documentación relacionada.

KPMG

MEA03. Gestionar el cumplimiento de los requisitos externos			
Condición	**Causa**	**Impacto**	**Recomendación**
Requisitos externos desactualizados	No se lleva un control de todos los posibles requisitos externos así como su impacto, consecuencias de incumplimiento.	Legal	-Establecer responsables que se encarguen de identificar todos los posibles requisitos externos y asigne sus impacto, consecuencias segun las actividades del negocio.
Errores de comunicación de los requisitos externos	No existen canales de comunicación para los requisitos externos.	Operativo	Definir canales de comunicación para informar los requisitos externos al personal.
Incumplimiento de los requisitos externos	-No hay evaluaciones ni revisiones periódicas del cumplimiento de los requisitos externos.	Legal Estratégico	-Establecer evaluaciones o revisiones de los requisitos externos y documentar los hallazgos de cumplimiento.

25

KPMG

Guión para el desarrollo del cronograma

Esta sección es un guión para el desarrollo del cronograma de auditoría.

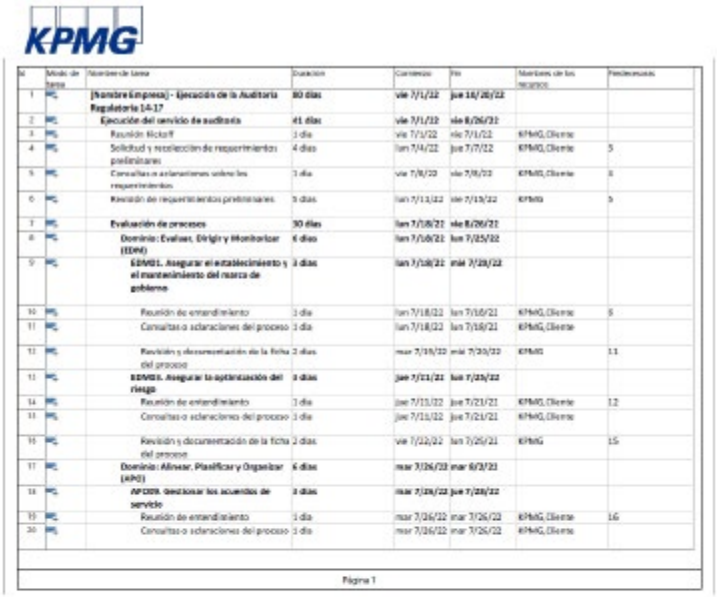
Especificaciones generales:

- El cronograma debe ser realizado en la herramienta Microsoft Project.
- El siguiente cuadro refleja un guión para establecer el cronograma de auditoría, donde se hace un desglose de las actividades mínimas a contener con un aproximado de las duraciones de estas.
- Es importante aclarar que cada cronograma de auditoría debe ser desarrollado de acuerdo al criterio y contexto del cliente auditado. Este cronograma es un guión para establecer aquellas actividades base que deben establecerse, sin embargo, puede estar sujetos a cambios para adaptarse al cliente.

Guión de cronograma:

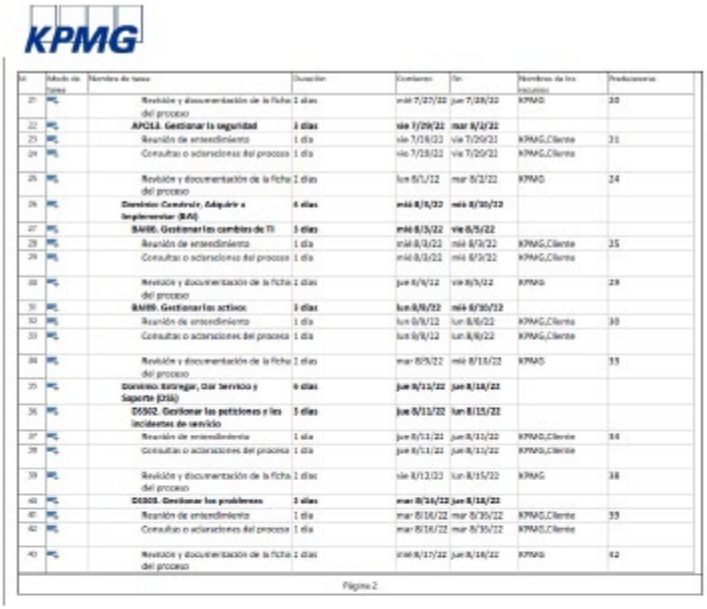
Para el guión del cronograma, se establece un ejemplo para una auditoría que dura aproximadamente 80 días. Se incluyen las actividades más comunes para la ejecución de una auditoría, las cuales van de la mano con lo pactado en el proceso de auditoría.

Las actividades incluyen la reunión de Kickoff, la solicitud de requerimientos con la matriz, la recolección y análisis de estos, la evaluación de cada proceso con sus espacios para la reunión de entendimiento y consultas adicionales, la preparación de los productos de auditoría, y presentaciones finales.



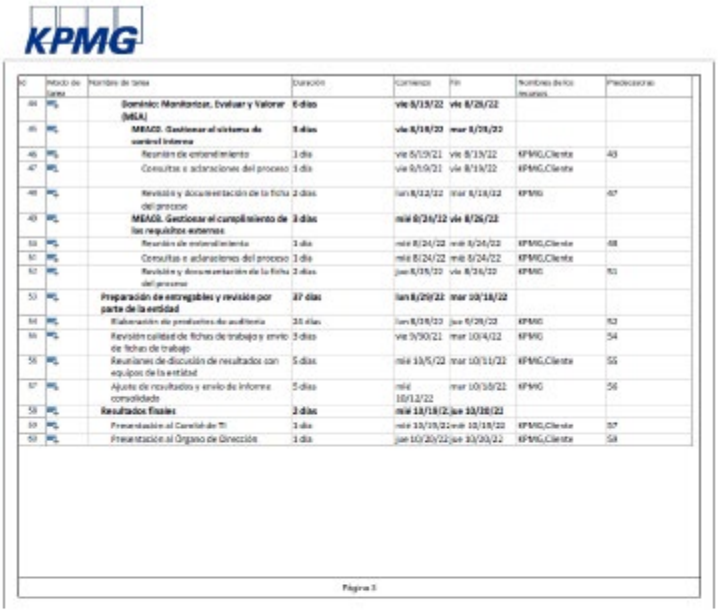
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
1		**[Nombre Empresa] - Ejecución de la Auditoría Regulatoria 14-17**	**80 días**	**vie 7/1/22**	**jue 10/20/22**		
2		**Ejecución del servicio de auditoría**	**41 días**	**vie 7/1/22**	**vie 8/26/22**		
3		Reunión Kickoff	1 día	vie 7/1/22	vie 7/1/22	KPMG,Cliente	
4		Solicitud y recolección de requerimientos preliminares	4 días	lun 7/4/22	jue 7/7/22	KPMG,Cliente	3
5		Consultas o aclaraciones sobre los requerimientos	1 día	vie 7/8/22	vie 7/8/22	KPMG,Cliente	4
6		Revisión de requerimientos preliminares	3 días	lun 7/11/22	vie 7/13/22	KPMG	5
7		**Evaluación de procesos**	**30 días**	**lun 7/18/22**	**vie 8/26/22**		
8		**Dominio: Evaluar, Dirigir y Monitorizar (EDM)**	**6 días**	**lun 7/18/22**	**lun 7/25/22**		
9		**EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno**	**3 días**	**lun 7/18/22**	**mié 7/20/22**		
10		Reunión de entendimiento	1 día	lun 7/18/22	lun 7/18/22	KPMG,Cliente	6
11		Consultas o aclaraciones del proceso	1 día	lun 7/18/22	lun 7/18/22	KPMG,Cliente	
12		Revisión y documentación de la ficha del proceso	2 días	mar 7/19/22	mié 7/20/22	KPMG	11
13		**EDM03. Asegurar la optimización del riesgo**	**3 días**	**jue 7/21/22**	**lun 7/25/22**		
14		Reunión de entendimiento	1 día	jue 7/21/22	jue 7/21/22	KPMG,Cliente	12
15		Consultas o aclaraciones del proceso	1 día	jue 7/21/22	jue 7/21/22	KPMG,Cliente	
16		Revisión y documentación de la ficha del proceso	2 días	vie 7/22/22	lun 7/25/22	KPMG	15
17		**Dominio: Alinear, Planificar y Organizar (APO)**	**6 días**	**mar 7/26/22**	**mar 8/2/22**		
18		**APO09. Gestionar los acuerdos de servicio**	**3 días**	**mar 7/26/22**	**jue 7/28/22**		
19		Reunión de entendimiento	1 día	mar 7/26/22	mar 7/26/22	KPMG,Cliente	16
20		Consultas o aclaraciones del proceso	1 día	mar 7/26/22	mar 7/26/22	KPMG,Cliente	

Página 1



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
21		Revisión y documentación de la ficha del proceso	1 días	mié 7/27/22	jue 7/28/22	KPMG	20
22		**APO13. Gestionar la seguridad**	**3 días**	**vie 7/29/22**	**mar 8/2/22**		
23		Reunión de entendimiento	1 día	vie 7/29/22	vie 7/29/22	KPMG,Cliente	21
24		Consultas o aclaraciones del proceso	1 día	vie 7/29/22	vie 7/29/22	KPMG,Cliente	
25		Revisión y documentación de la ficha del proceso	1 días	lun 8/1/22	mar 8/2/22	KPMG	24
26		**Dominio: Construir, Adquirir e Implementar (BAI)**	**4 días**	**mié 8/3/22**	**mié 8/10/22**		
27		**BAI06. Gestionar los cambios de TI**	**3 días**	**mié 8/3/22**	**vie 8/5/22**		
28		Reunión de entendimiento	1 día	mié 8/3/22	mié 8/3/22	KPMG,Cliente	25
29		Consultas o aclaraciones del proceso	1 día	mié 8/3/22	mié 8/3/22	KPMG,Cliente	
30		Revisión y documentación de la ficha del proceso	1 días	jue 8/4/22	vie 8/5/22	KPMG	29
31		**BAI09. Gestionar los activos**	**3 días**	**lun 8/8/22**	**mié 8/10/22**		
32		Reunión de entendimiento	1 día	lun 8/8/22	lun 8/8/22	KPMG,Cliente	30
33		Consultas o aclaraciones del proceso	1 día	lun 8/8/22	lun 8/8/22	KPMG,Cliente	
34		Revisión y documentación de la ficha del proceso	1 días	mar 8/9/22	mié 8/10/22	KPMG	33
35		**Dominio: Entregar, Dar Servicio y Soporte (DSS)**	**4 días**	**jue 8/11/22**	**jue 8/18/22**		
36		**DSS02. Gestionar las peticiones y los incidentes de servicio**	**3 días**	**jue 8/11/22**	**lun 8/15/22**		
37		Reunión de entendimiento	1 día	jue 8/11/22	jue 8/11/22	KPMG,Cliente	34
38		Consultas o aclaraciones del proceso	1 día	jue 8/11/22	jue 8/11/22	KPMG,Cliente	
39		Revisión y documentación de la ficha del proceso	1 días	vie 8/12/22	lun 8/15/22	KPMG	38
40		**DSS03. Gestionar los problemas**	**3 días**	**mar 8/16/22**	**jue 8/18/22**		
41		Reunión de entendimiento	1 día	mar 8/16/22	mar 8/16/22	KPMG,Cliente	39
42		Consultas o aclaraciones del proceso	1 día	mar 8/16/22	mar 8/16/22	KPMG,Cliente	
43		Revisión y documentación de la ficha del proceso	1 días	mié 8/17/22	jue 8/18/22	KPMG	42

Página 2



ID	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
44		**Dominio: Monitorizar, Evaluar y Valorar (MEA)**	**6 días**	**vie 8/19/22**	**vie 8/26/22**		
45		**MEA03. Gestionar el sistema de control interno**	**5 días**	**vie 8/19/22**	**mar 8/23/22**		
46		Reunión de entendimiento	1 día	vie 8/19/22	vie 8/19/22	KPMG,Cliente	43
47		Consultas o aclaraciones del proceso	1 día	vie 8/19/22	vie 8/19/22	KPMG,Cliente	
48		Revisión y documentación de la ficha del proceso	2 días	lun 8/22/22	mar 8/23/22	KPMG	47
49		**MEA03. Gestionar el cumplimiento de los requisitos externos**	**3 días**	**mié 8/24/22**	**vie 8/26/22**		
50		Reunión de entendimiento	1 día	mié 8/24/22	mié 8/24/22	KPMG,Cliente	48
51		Consultas o aclaraciones del proceso	1 día	mié 8/24/22	mié 8/24/22	KPMG,Cliente	
52		Revisión y documentación de la ficha del proceso	2 días	jue 8/25/22	vie 8/26/22	KPMG	51
53		**Preparación de entregables y revisión por parte de la entidad**	**27 días**	**lun 8/29/22**	**mar 10/18/22**		
54		Elaboración de productos de auditoría	20 días	lun 8/29/22	jue 9/29/22	KPMG	52
55		Revisión calidad de fichas de trabajo y envío de fichas de trabajo	5 días	vie 9/30/21	mar 10/4/22	KPMG	54
56		Reuniones de discusión de resultados con equipos de la entidad	5 días	mié 10/5/22	mar 10/11/22	KPMG,Cliente	55
57		Ajuste de resultados y envío de informe consolidado	5 días	mié 10/12/22	mar 10/18/22	KPMG	56
58		**Resultados finales**	**3 días**	**mié 10/19/22**	**jue 10/20/22**		
59		Presentación al Comité de TI	1 día	mié 10/19/22	mié 10/19/22	KPMG,Cliente	57
60		Presentación al Órgano de Dirección	1 día	jue 10/20/22	jue 10/20/22	KPMG,Cliente	59

Página 3

Visualización del cronograma:

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
1		**[Nombre Empresa] - Ejecución de la Auditoría Regulatoria 14-17**	**80 días**	**vie 7/1/22**	**jue 10/20/22**		
2		**Ejecución del servicio de auditoría**	**41 días**	**vie 7/1/22**	**vie 8/26/22**		
3		Reunión Kickoff	1 día	vie 7/1/22	vie 7/1/22	KPMG,Cliente	
4		Solicitud y recolección de requerimientos preliminares	4 días	lun 7/4/22	jue 7/7/22	KPMG,Cliente	3
5		Consultas o aclaraciones sobre los requerimientos	1 día	vie 7/8/22	vie 7/8/22	KPMG,Cliente	4
6		Revisión de requerimientos preliminares	5 días	lun 7/11/22	vie 7/15/22	KPMG	5
7		**Evaluación de procesos**	**30 días**	**lun 7/18/22**	**vie 8/26/22**		
8		**Dominio: Evaluar, Dirigir y Monitorizar (EDM)**	**6 días**	**lun 7/18/22**	**lun 7/25/22**		
9		**EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno**	**3 días**	**lun 7/18/22**	**mié 7/20/22**		
10		Reunión de entendimiento	1 día	lun 7/18/22	lun 7/18/22	KPMG,Cliente	6
11		Consultas o aclaraciones del proceso	1 día	lun 7/18/22	lun 7/18/22	KPMG,Cliente	
12		Revisión y documentación de la ficha del proceso	2 días	mar 7/19/22	mié 7/20/22	KPMG	11
13		**EDM03. Asegurar la optimización del riesgo**	**3 días**	**jue 7/21/22**	**lun 7/25/22**		
14		Reunión de entendimiento	1 día	jue 7/21/22	jue 7/21/22	KPMG,Cliente	12
15		Consultas o aclaraciones del proceso	1 día	jue 7/21/22	jue 7/21/22	KPMG,Cliente	
16		Revisión y documentación de la ficha del proceso	2 días	vie 7/22/22	lun 7/25/22	KPMG	15
17		**Dominio: Alinear, Planificar y Organizar (APO)**	**6 días**	**mar 7/26/22**	**mar 8/2/22**		
18		**APO09. Gestionar los acuerdos de servicio**	**3 días**	**mar 7/26/22**	**jue 7/28/22**		
19		Reunión de entendimiento	1 día	mar 7/26/22	mar 7/26/22	KPMG,Cliente	16
20		Consultas o aclaraciones del proceso	1 día	mar 7/26/22	mar 7/26/22	KPMG,Cliente	

Página 1

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
21		Revisión y documentación de la ficha del proceso	2 días	mié 7/27/22	jue 7/28/22	KPMG	20
22		**APO13. Gestionar la seguridad**	**3 días**	**vie 7/29/22**	**mar 8/2/22**		
23		Reunión de entendimiento	1 día	vie 7/29/22	vie 7/29/22	KPMG,Cliente	21
24		Consultas o aclaraciones del proceso	1 día	vie 7/29/22	vie 7/29/22	KPMG,Cliente	
25		Revisión y documentación de la ficha del proceso	2 días	lun 8/1/22	mar 8/2/22	KPMG	24
26		**Dominio: Construir, Adquirir e Implementar (BAI)**	**6 días**	**mié 8/3/22**	**mié 8/10/22**		
27		**BAI06. Gestionar los cambios de TI**	**3 días**	**mié 8/3/22**	**vie 8/5/22**		
28		Reunión de entendimiento	1 día	mié 8/3/22	mié 8/3/22	KPMG,Cliente	25
29		Consultas o aclaraciones del proceso	1 día	mié 8/3/22	mié 8/3/22	KPMG,Cliente	
30		Revisión y documentación de la ficha del proceso	2 días	jue 8/4/22	vie 8/5/22	KPMG	29
31		**BAI09. Gestionar los activos**	**3 días**	**lun 8/8/22**	**mié 8/10/22**		
32		Reunión de entendimiento	1 día	lun 8/8/22	lun 8/8/22	KPMG,Cliente	30
33		Consultas o aclaraciones del proceso	1 día	lun 8/8/22	lun 8/8/22	KPMG,Cliente	
34		Revisión y documentación de la ficha del proceso	2 días	mar 8/9/22	mié 8/10/22	KPMG	33
35		**Dominio: Entregar, Dar Servicio y Soporte (DSS)**	**6 días**	**jue 8/11/22**	**jue 8/18/22**		
36		**DSS02. Gestionar las peticiones y los incidentes de servicio**	**3 días**	**jue 8/11/22**	**lun 8/15/22**		
37		Reunión de entendimiento	1 día	jue 8/11/22	jue 8/11/22	KPMG,Cliente	34
38		Consultas o aclaraciones del proceso	1 día	jue 8/11/22	jue 8/11/22	KPMG,Cliente	
39		Revisión y documentación de la ficha del proceso	2 días	vie 8/12/22	lun 8/15/22	KPMG	38
40		**DSS03. Gestionar los problemas**	**3 días**	**mar 8/16/22**	**jue 8/18/22**		
41		Reunión de entendimiento	1 día	mar 8/16/22	mar 8/16/22	KPMG,Cliente	39
42		Consultas o aclaraciones del proceso	1 día	mar 8/16/22	mar 8/16/22	KPMG,Cliente	
43		Revisión y documentación de la ficha del proceso	2 días	mié 8/17/22	jue 8/18/22	KPMG	42

Página 2

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
44		**Dominio: Monitorizar, Evaluar y Valorar (MEA)**	**6 días**	**vie 8/19/22**	**vie 8/26/22**		
45		**MEA02. Gestionar el sistema de control interno**	**3 días**	**vie 8/19/22**	**mar 8/23/22**		
46		Reunión de entendimiento	1 día	vie 8/19/22	vie 8/19/22	KPMG,Cliente	43
47		Consultas o aclaraciones del proceso	1 día	vie 8/19/22	vie 8/19/22	KPMG,Cliente	
48		Revisión y documentación de la ficha del proceso	2 días	lun 8/22/22	mar 8/23/22	KPMG	47
49		**MEA03. Gestionar el cumplimiento de los requisitos externos**	**3 días**	**mié 8/24/22**	**vie 8/26/22**		
50		Reunión de entendimiento	1 día	mié 8/24/22	mié 8/24/22	KPMG,Cliente	48
51		Consultas o aclaraciones del proceso	1 día	mié 8/24/22	mié 8/24/22	KPMG,Cliente	
52		Revisión y documentación de la ficha del proceso	2 días	jue 8/25/22	vie 8/26/22	KPMG	51
53		**Preparación de entregables y revisión por parte de la entidad**	**37 días**	**lun 8/29/22**	**mar 10/18/22**		
54		Elaboración de productos de auditoría	24 días	lun 8/29/22	jue 9/29/22	KPMG	52
55		Revisión calidad de fichas de trabajo y envío de fichas de trabajo	3 días	vie 9/30/22	mar 10/4/22	KPMG	54
56		Reuniones de discusión de resultados con equipos de la entidad	5 días	mié 10/5/22	mar 10/11/22	KPMG,Cliente	55
57		Ajuste de resultados y envío de informe consolidado	5 días	mié 10/12/22	mar 10/18/22	KPMG	56
58		**Resultados finales**	**2 días**	**mié 10/19/2**	**jue 10/20/22**		
59		Presentación al Comité de TI	1 día	mié 10/19/2	mié 10/19/22	KPMG,Cliente	57
60		Presentación al Órgano de Dirección	1 día	jue 10/20/22	jue 10/20/22	KPMG,Cliente	59

Página 3

Apéndice Ñ. Pruebas para evaluación de la propuesta de solución.

Prueba de evaluación de la matriz de requerimientos de procesos tecnológicos	
Indicaciones de las pruebas	• Revisar la descripción de la prueba cuando corresponda. • Participar en el grupo focal de cada prueba, donde debe brindar su opinión, así como recomendaciones o ajustes de la herramienta en cuestión. • Una vez finalizado el grupo focal para todas las pruebas, debe llenar la siguiente encuesta: https://forms.gle/sRF6ZgNpMTCBw6qs8, para indicar la calificación de las herramientas con respecto a su nivel de cumplimiento. Debe calificar con la numeración del 1 al 3. Corresponde 1 a una calificación baja y 3 a una calificación alta.
Descripción de las pruebas	
Prueba #1	Bajo el supuesto de que se está realizando una auditoría de TI en una entidad financiera, la cual ya ha sido auditada por el equipo durante el año 2021, deben tomar la matriz de requerimientos tecnológicos propuesta y validar su información para verificar si es de utilidad y fácil comprensión tanto para el equipo como para el cliente.
Prueba #2	Bajo el supuesto de que se está realizando una auditoría de TI en una entidad financiera, la cual ya ha sido auditada por el equipo durante el año 2021, deben tomar el guion de la documentación de reuniones de entendimiento para formular preguntas, llevar a cabo la reunión, documentar las respuestas y validar que la información propuesta sea de utilidad y comprensión tanto para el equipo como para el cliente.
Prueba #3	Bajo el supuesto de que se está realizando una auditoría de TI en una entidad financiera, la cual ya ha sido auditada por el equipo durante el año 2021, deben tomar el guion de la documentación de riesgos para definir la condición, causa, impacto y recomendación y validar que la información propuesta sea de utilidad y comprensión tanto para el equipo como para el cliente.
Prueba #4	Bajo el supuesto de que se está realizando una auditoría de TI en una entidad financiera, la cual ya ha sido auditada por el equipo durante el año 2021, deben tomar el guion del cronograma para definir uno en términos del contexto de la entidad y validar que la información propuesta sea de utilidad y comprensión tanto para el equipo como para el cliente.

Apéndice O. Grupo focal para la evaluación de la matriz de requerimientos de procesos tecnológicos.

Datos Generales	
Grupo focal #	1
Fecha	17 Mayo 2022
Participantes	Gerente de TI Supervisor de TI Asesores
Entrevistador	María Jesús Calvo Bolaños
Objetivo	Evaluar la prueba para validar el cumplimiento de la matriz de requerimientos de procesos tecnológicos.

Temas por abarcar:

- **Nivel de detalle, estructuración y estandarización**

En general, la matriz tiene un nivel de detalle y estructura aceptable. Contiene los apartados esperados de las prácticas y sus actividades lo cual respalda el origen del requerimiento y está actualizada con la última versión de COBIT como se indicó.

La sección de inicio está bien, general pero entendible para cliente.

- **Comprensión de la herramienta para el equipo y para el cliente (cuando corresponda)**

En general sí se ve comprensible para el cliente y para el equipo.

- **Recomendaciones o ajustes**

En la sección de inicio se pueden definir los tipos de documentos, pues algunos clientes usan términos diferentes para un plan, procedimiento, metodología, otro. Así se ahorra la aclaración y la solicitud de un nuevo documento.

Se puede hacer otra hoja que contenga los apartados de la matriz para especificar qué es cada uno y quién debe completarlos, ya sea el cliente o nosotros.

- **Disminución de horas extras**

La matriz propuesta brinda más opciones de requerimientos al cliente, lo cual podría disminuir el tiempo de consultas y reenvío de información, pero no lo suficiente para disminuir las horas extra de forma considerada dado que hay pendientes muchos factores como el tiempo de respuesta del cliente que no depende de nosotros; tal vez una o dos horas se puedan disminuir.

Se considera que la matriz, con su inicio, detalle de los procesos y una vez aplicadas las recomendaciones, es un insumo apropiado para comprender el funcionamiento de la actividad como tal y tener una guía sobre cómo gestionarla, sobre todo para los miembros que no se involucran constantemente en estas auditorías o aquellos nuevos integrantes del equipo.

Apéndice P. Grupo focal para la evaluación del instructivo de gestión: documentación de reuniones de entendimiento.

Datos Generales	
Grupo focal #	2
Fecha	18 Mayo 2022
Participantes	Gerente de TI Supervisor de TI Asesores
Entrevistador	María Jesús Calvo Bolaños
Objetivo	Evaluar la prueba para validar el cumplimiento de la documentación de reuniones de entendimiento del instructivo de gestión.

Sección de preguntas.

- **Nivel de detalle, estructuración y estandarización**

La estructuración de la reunión y las indicaciones iniciales están bastante detalladas y claras. Son puntuales, lo cual hace la lectura fácil y rápida.

En términos de nivel de detalle, algunas preguntas del guion no contienen la pregunta formal de solicitud del nombre de documento o brindar evidencia. Pero en general, reflejan la actividad y sí funcionan para establecer preguntas especializadas para cada cliente.

- **Comprensión de la herramienta para el equipo y para el cliente (cuando corresponda)**

La estructuras, las indicaciones y el guion de preguntas son comprensibles para todos.

- **Recomendaciones o ajustes**

Para aquellas preguntas que hablan de tener un procedimiento, o tener un plan, se debe especificar cuál es nombre, dónde se localiza para dar más detalle al cliente, o consulta de evidencia. De esta forma se ahorra la respuesta de solamente un “sí” que en estos casos no aplica.

- **Disminución de horas extras**

Con esto, las horas se podrían disminuir una hora máximo, o mantenerse de 4 a 7, porque para las reuniones depende el tiempo que dure el cliente aclarando el proceso. Se considera esta herramienta como insumo para mantener la línea base de trabajo estandarizada y que todos sigan las mismas bases de trabajo.

Apéndice Q. Grupo focal para la evaluación del instructivo de gestión: documentación de riesgos de auditoría.

Datos Generales	
Grupo focal #	2
Fecha	18 Mayo 2022
Participantes	Gerente de TI Supervisor de TI Asesores
Entrevistador	María Jesús Calvo Bolaños
Objetivo	Evaluar la prueba para validar el cumplimiento de la documentación de riesgos de auditoría del instructivo de gestión.

Sección de preguntas.

- **Nivel de detalle, estructuración y estandarización**

Está muy bien, se pacta la estructura utilizada por el equipo, se definen correctamente los impactos más utilizados, y los ejemplos de riesgos son concisos y claros con respecto a los riesgos que se definen en las fichas.

- **Comprensión de la herramienta para el equipo y para el cliente (cuando corresponda)**

Es comprensible para todo el equipo.

- **Recomendaciones o ajustes**

De momento, ninguna está bien establecida. A futuro se podrían seguir incorporando riesgos para actualizar la herramienta.

- **Disminución de horas extras**

Los riesgos así definidos y estructurados permiten que el equipo siga la misma línea de redacción, además de que ya todos tienen un lugar dónde buscar riesgos en caso de dudas en la definición. Sin embargo, se considera, por las mismas razones anteriores, que las cargas se mantienen o disminuirían una hora.

Apéndice R. Grupo focal para la evaluación del instructivo de gestión: desarrollo del cronograma.

Datos Generales	
Grupo focal #	2
Fecha	18 Mayo 2022
Participantes	Gerente de TI Supervisor de TI Asesores
Entrevistador	María Jesús Calvo Bolaños
Objetivo	Evaluar la prueba para validar el cumplimiento del cronograma de auditoría del instructivo de gestión.

Sección de preguntas.

- **Nivel de detalle, estructuración y estandarización**

En general las actividades del cronograma están bien. El establecimiento de promedios en general es adecuado, sin embargo, sí se debe recalcar que van a variar en cada auditoría.

- **Comprensión de la herramienta para el equipo y para el cliente (cuando corresponda)**

Sí se comprende bien la definición de actividades y tiempos.

- **Recomendaciones o ajustes**

Se puede disminuir la cantidad de tiempo en el Kickoff a medio día o menos. Estas reuniones duran máximo 2 horas. Las presentaciones de resultados pueden abarcar medio día cada una, ya que el tiempo utilizado son dos horas máximo.

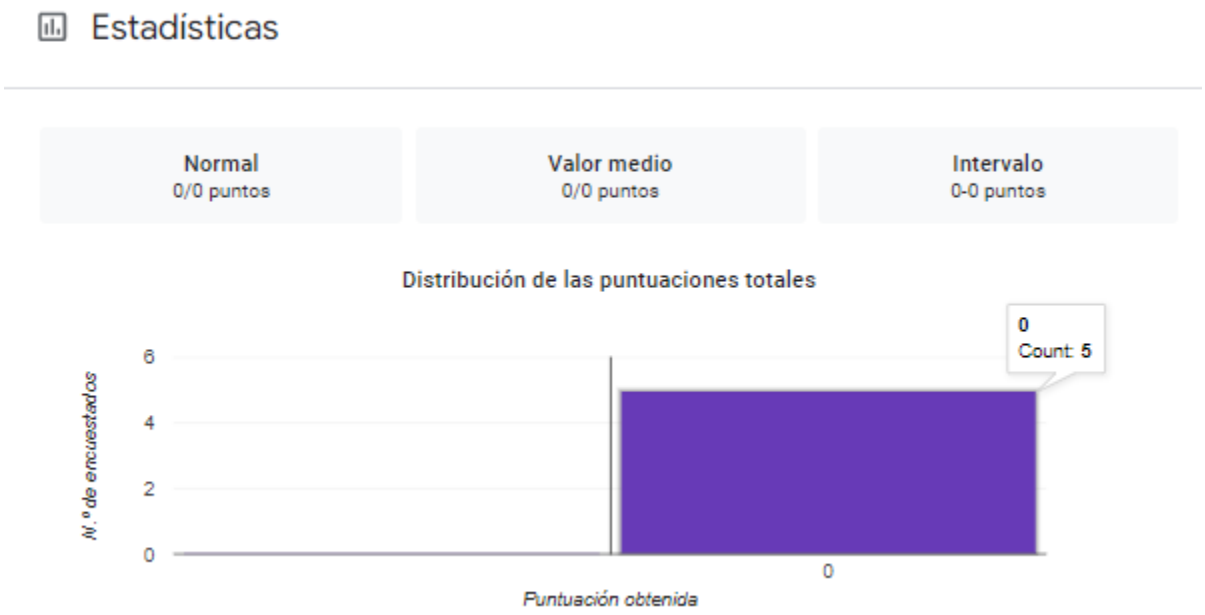
Por lo general, los procesos APO suelen ser más complejos, entonces se podría agregar un día más.

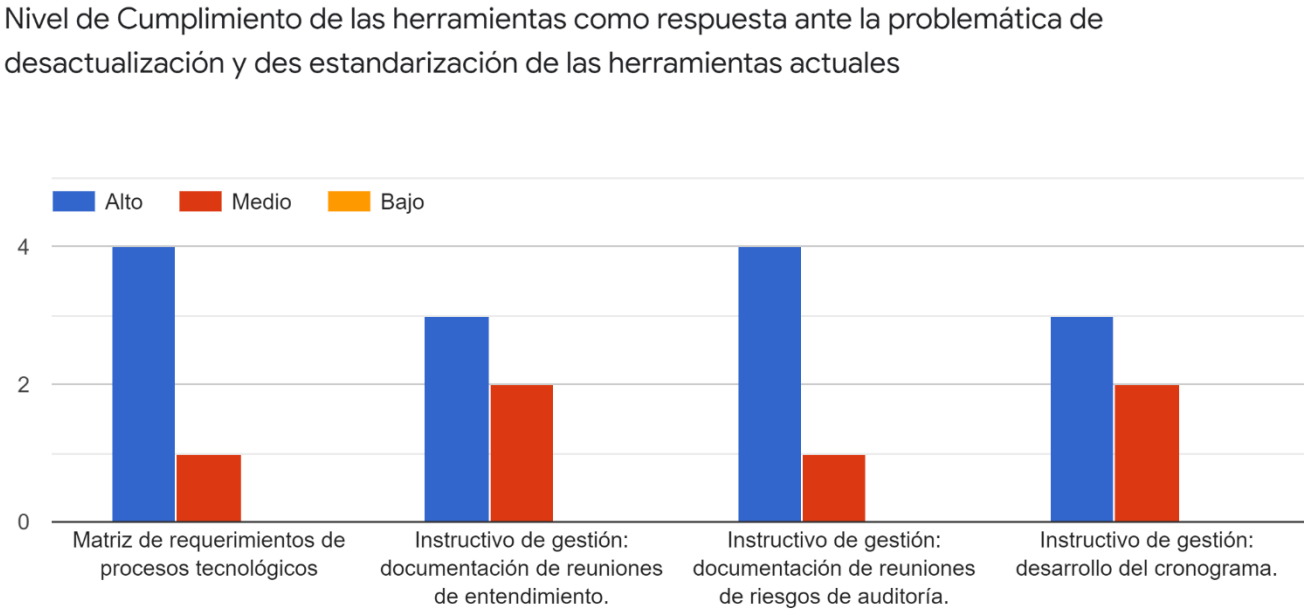
En términos de formato, se pueden separar algunas actividades como revisión y envío de fichas, o ajuste de resultados y envío de informe, ya que son actividades independientes. Las entregas pueden ser definidas como hitos.

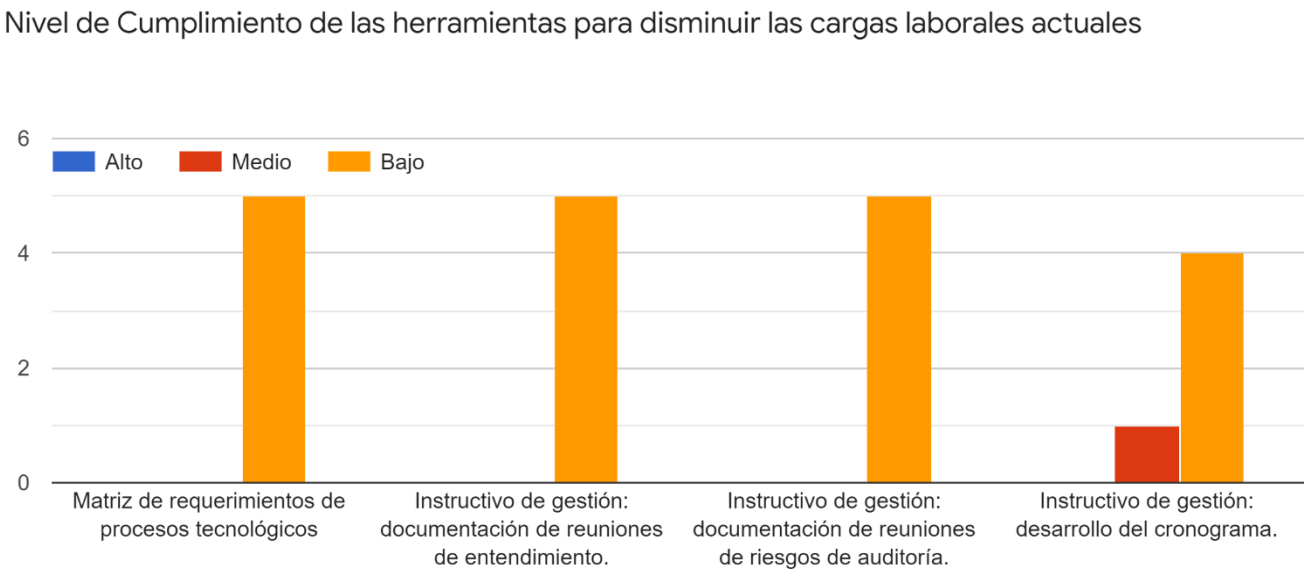
¿Consideran que este guion reduce los tiempos de trabajo con respecto a la actividad y por tanto reduce sus cargas laborales extra? Si consideran que reducen sus cargas, especificar un aproximado.

Lo mismo que lo mencionado en las otras pruebas. Este cronograma es de utilidad para promover el conocimiento sobre cómo es, qué actividades involucra y dar ejemplos de duraciones, lo cual sirve para explicar y dar a conocer la actividad. Sin embargo, las horas extra pueden disminuir muy poco, 1 o 2 horas, dado que no depende solo del equipo.

Apéndice S. Encuesta de calificación de la evaluación de la propuesta de solución.






Nivel de Cumplimiento de las herramientas para disminuir las cargas laborales actuales
6
4
2
0
Alto
Medio
Bajo
Matriz de requerimientos de procesos tecnológicos
Instructivo de gestión: documentación de reuniones de entendimiento.
Instructivo de gestión: documentación de reuniones de riesgos de auditoría.
Instructivo de gestión: desarrollo del cronograma.

Apéndice T. Matriz de requerimientos de procesos tecnológicos final

Matriz de Requerimientos de Procesos Tecnológicos

Descripción:

La matriz de requerimientos de procesos tecnológicos o matriz de requerimientos preliminares tiene el objetivo de guiar al auditado en la entrega de documentación relacionada con los procesos por evaluar durante el periodo de auditoría correspondiente.

Esta matriz está desarrollada de acuerdo con lo establecido por COBIT 2019. Para cada dominio, se listan los procesos respectivos, sus prácticas, sus actividades y los requerimientos que se esperan obtener por cada práctica.

Instrucciones de uso:

1. Brindar la documentación existente que cumpla con el (los) requerimiento(s) definidos por cada práctica del proceso. La documentación puede abarcar:

•**Planes:** Documento que precisa los detalles para realizar un proyecto, actividad, acción, proceso. Establece la definición sobre qué se va a hacer, indicando políticas, objetivos, alcance, programas, métodos, procedimientos, y cualquier aspecto que la organización considere oportuno.
•**Metodologías:** Corresponde a un conjunto de métodos y actividades que deben ser seguidas para cumplir con el desarrollo de actividades.
•**Políticas:** Es una declaración de alto nivel que describe lo que la organización está tratando de lograr así como los diferentes compromisos para conseguirlo.
•**Reglamentos:** Colección de reglas dadas por una autoridad, las cuales deben ser acatadas para la ejecución de procedimientos, actividades, planes, entre otros.
•**Procedimientos:** Es una forma específica de llevar a cabo un proceso o una actividad. Establece la forma de hacer el proceso o la actividad.
• Guías, manuales, instructivos: Documentos de fácil entendimiento que establece el paso a paso sobre como ejecutar, procesar o analizar actividades, procedimientos, procesos, etc.
•**Protocolos:** Conjunto de reglas establecidas por norma o costumbre de la organización para ejecutar actividades.
•**Formularios:** Documentos que contienen espacios predeterminados para completar información de temas específicos, a nivel interno o externo de la organización.
•**Cualquier otro tipo de documentación formal asociado al proceso:** Corresponde a cualquier tipo de informe, documentación, resultados, o respuestas que sirvan como evidencia para responder a los requerimientos solicitados.

2. Debe completar el apartado de "Documentos proporcionados" con el nombre de los documentos por entregar.

3. En caso de requerir una aclaración, excepción, entre otro aspecto, por favor indicarlo en el apartado de "Comentario".

Matriz de Requerimientos de Procesos Tecnológicos

Guía de usuario:

Como parte de la guía de usuario, a continuación se establece cada apartado de la matriz de requerimientos, indicando una descripción general y el usuario correspondiente que debe completarlo.

Apartado	Descripción general	Usuario responsable
Dominio	Indica el dominio de COBIT: EDM, APO, BAI, DSS, MEA.	KPMG
Proceso	Listado de los procesos del dominio respectivo.	KPMG
Práctica	Listado de todas las prácticas de cada proceso.	KPMG
Actividad	Listado de todas las actividades de las prácticas de cada proceso.	KPMG
Requerimientos	Listados de los requerimientos requeridos por cada práctica de los procesos, según lo indicado en COBIT 2019.	KPMG
Ejemplos de documentos	Listado de ejemplos de documentos que pueden ser entregados para responder a los requerimientos de las prácticas definidos.	KPMG
Estado de la solicitud	El estado de la solicitud sirve de control para la gestión de la solicitud y entrega de requerimientos. Se divide en tres elementos, los cuales deben ser colocados por el auditor de KPMG: •No iniciado: El requerimiento aún no ha sido solicitado. •En proceso: El requerimiento fue solicitado y se está en espera de entrega. •Finalizado: El requerimiento ya ha sido entregado. **Nota:** El estado de la solicitud se realiza por cada evidencia de documentación entregada para responder al requerimiento.	KPMG
Documentos proporcionados	En este apartado el cliente debe indicar el nombre de los documentos o evidencias que adjuntó para responder a los requerimientos. Dicho nombre debe coincidir con el nombre de la evidencia para evitar consecuencias de ambigüedad.	Cliente
Área	Se especifica el área responsable de la entrega de requerimientos.	KPMG
Responsable	Se indica de la persona dentro del área de brindar los requerimientos solicitados.	KPMG
Fecha de solicitud	El auditor de KPMG indica la fecha en que realizó la solicitud de los requerimientos.	KPMG
Fecha de entrega	El cliente indica la fecha en que está entregando los requerimientos solicitados.	Cliente
Comentarios	Este apartado es un espacio para que el auditor o el cliente indiquen comentarios, aclaraciones o excepciones a los requerimientos solicitados.	KPMG, Cliente

KPMG

Dominio	Proceso	Práctica	Actividad	Requerimiento	Documentación	Estado de la solicitud	Documentos proporcionados	Área	Responsable	Fecha de solicitud	Fecha entrega	Comentarios
Evaluar, Dirigir y Monitorizar (EDM)	**EDM01.** Asegurar el establecimiento y el mantenimiento del marco de gobierno.	**EDM01.01.** Evaluar el sistema de gobierno	**1.** Analizar e identificar los factores ambientales internos y externos (obligaciones legales, regulatorias y contractuales), así como las tendencias en el entorno de negocio que pueden influir en el diseño del gobierno. **2.** Determinar la importancia de TI y su papel con respecto al negocio. **3.** Considerar las regulaciones, leyes, y obligaciones contractuales externas y determinar cómo deberían aplicarse dentro del gobierno de TI de una empresa. **4.** Determinar las implicaciones de todo el entorno de control de la empresa con respecto a TI. **5.** Alinear el uso ético y el procesamiento de la información y su impacto en la sociedad, el entorno natural y los intereses de los interesados internos y externos con la dirección, las metas y los objetivos de la empresa. **6.** Articular los principios que guiarán el diseño del gobierno y la toma de decisiones de TI. **7.** Determinar el modelo óptimo de toma de decisiones para TI. **8.** Determinar los niveles adecuados de delegación de autoridad, incluidas las reglas de limitaciones, para las decisiones de TI.	•Principios rectores del gobierno empresarial. •Modelo de toma de decisiones. •Niveles de autoridad.	•Listado de principios referentes al gobierno de la empresa. •Organigrama de la empresa. •Manual de puestos de la empresa, que especifique la autoridad y responsabilidades de cada parte.						
		EDM01.02 Dirigir el sistema de gobierno	**1.** Comunicar el gobierno de los principios de TI y acordar con la administración ejecutiva la forma de establecer un liderazgo informado y comprometido. **2.** Establecer o delegar el establecimiento de estructuras, procesos y prácticas de gobierno en línea con los principios de diseño acordados. **3.** Establecer un consejo de administración de gobierno de TI. Este consejo de administración debería garantizar que el gobierno de la información y la tecnología, como parte del gobierno de la empresa, se aborda de forma adecuada; aconsejar sobre la dirección estratégica a seguir; y determinar la priorización de los programas de inversión habilitados por TI en línea con la estrategia y prioridades del negocio de la empresa. **4.** Asignar la responsabilidad, autoridad y rendición de cuentas por las decisiones de TI en línea con los principios de diseño de gobierno, de los modelos de toma de decisiones y de delegación acordados. **5.** Asegurar que los mecanismos de comunicación y presentación de informes proporcionan la información adecuada a los responsables de la supervisión y toma de decisiones. **6.** Direccionar al personal para que siga las directrices relevantes en cuanto al comportamiento ético y profesional y asegurar que se conozcan y se apliquen las consecuencias del incumplimiento. **7.** Direccionar el establecimiento de un sistema de recompensas para fomentar el cambio cultural deseado.	•Comunicación del gobierno de la empresa. •Métodos de sistema de recompensa.	•Plan de Comunicación del gobierno de la empresa. •Procedimiento de gestión de recompensas.						
		EDM01.03 Monitorizar el sistema de gobierno	**1.** Evaluar la eficacia y el rendimiento de aquellas partes interesadas a las que se le ha delegado la responsabilidad y autoridad para el gobierno empresarial de TI. **2.** Evaluar de forma periódica si los mecanismos de TI que se han acordado (estructuras, principios, procesos, etc.) se han establecido y operan de forma eficiente. **3.** Evaluar la eficacia del diseño de gobierno e identificar acciones para rectificar cualquier desviación que se encuentre. **4.** Mantener la supervisión de hasta qué punto la TI satisface las obligaciones (regulación, legislación, leyes comunes, contractuales), políticas internas, estándares y guías profesionales. **5.** Proporcionar la supervisión de la eficacia del sistema de control de la empresa y el cumplimiento con el mismo. **6.** Monitorizar los mecanismos regulares y rutinarios para garantizar que el uso de TI cumpla con las obligaciones (regulación, legislación, leyes comunes, contractuales), estándares y guías.	•Retroalimentación sobre el rendimiento y la eficacia del gobierno.	•Plan de aseguramiento del sistema de control interno. •Informes de desempeño del gobierno empresarial. •Informes de auditoria del gobierno empresarial.						
	EDM03. Asegurar la optimización del riesgo	**EDM03.01** Evaluar la gestión de riesgos	**1.** Conocer la organización y su contexto en relación al riesgo de TI. **2.** Determinar el apetito al riesgo de la organización, es decir, el nivel de riesgo relacionado con TI que la empresa está dispuesta a tomar en la búsqueda de sus objetivos empresariales. **3.** Determinar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo. **4.** Determinar el grado de alineamiento de la estrategia de riesgos en TI de la empresa con la estrategia de riesgos de la empresa en su conjunto y garantizar que el apetito al riesgo se sitúe por debajo de la capacidad de riesgo de la organización. **5.** Evaluar los factores de riesgo de TI de forma proactiva antes de tomar decisiones estratégicas a nivel de empresa y garantizar que las consideraciones del riesgo formen parte del proceso de decisión estratégico de la empresa. **6.** Evaluar las actividades de gestión de riesgos para asegurar que se alineen con la capacidad de la empresa para las pérdidas relacionadas con TI y la tolerancia correspondiente por parte de la dirección. **7.** Atraer y conservar las habilidades y el personal necesarios para la gestión de riesgos de las TI.	•Guía de apetito del riesgo. •Evaluación de actividades de gestión de riesgos. •Niveles aprobados de tolerancia al riesgo.	•Procedimiento de la gestión de riesgos. •Guía para la definición del apetito y niveles de tolerancia de la gestión de riesgos.						
		EDM03.02. Dirigir la gestión de riesgos	**1.** Dirigir la traducción e integración de la estrategia de riesgo de TI en las prácticas de gestión de riesgos y las actividades operativas. **2.** Dirigir el desarrollo de planes de comunicación de riesgos (que se extiendan a todos los niveles de la empresa). **3.** Dirigir la implementación de los mecanismo adecuados para responder de forma rápida al cambio de riesgos e informar inmediatamente a los cargos de dirección correspondientes, siguiendo los principios de escalamiento (qué comunicar, cuándo, dónde y cómo). **4.** Ordenar que el riesgo, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento. El riesgo debe gestionarse conforme a las políticas y procedimientos publicados y comunicados a los responsables de la toma de decisiones. **5.** Identificar las metas y métricas claves de los procesos de gobierno y gestión de riesgos que deben monitorizarse, y aprobar las estrategias, métodos, técnicas y procesos para capturar y comunicar la información de las mediciones.	•Proceso aprobado para la medición de la gestión de riesgos. •Objetivos clave a monitorizar para la gestión de riesgos. •Políticas de gestión de riesgos.	•Política de gestión de riesgos. •Métricas para la medición de la gestión de riesgos. •Guía para la medición de la gestión de riesgos.						
		EDM03.03. Monitorizar la gestión de riesgos.	**1.** Comunicar cualquier problema de gestión de riesgos al consejo de administración o comité ejecutivo. **2.** Supervise hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa. **3.** Monitorizar las metas y métricas de los procesos de gobierno y gestión de riesgos contra los objetivos, analizar la causa de las posibles desviaciones, y poner en marcha las acciones remediales s para solucionar las causas subyacentes. **4.** Facilitar la revisión por parte de las partes interesadas clave del progreso de la empresa con respecto a las metas identificadas.	•Acciones remediales para solucionar las desviaciones de gestión de riesgos. •Problemas de gestión de riesgos para el consejo de administración.	•Informe ejecutivo de los problemas identificados en la gestión de riesgos, y acciones remediales para solucionarlos.						

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Responsable	Área	Fecha de solicitud	Fecha de entrega	Comentarios
Alinear, Planificar y Organizar (APO)	APO09. Gestionar los acuerdos de servicio	APO09.01. Identificar los servicios de TI	1. Evaluar los servicios y niveles de servicios de TI actuales para identificar las brechas entre los servicios actuales y las actividades empresariales que apoyan. Identificar áreas de mejora de los servicios existentes y opciones de nivel de servicio. 2. Analizar, estudiar y estimar la demanda futura y confirmar la capacidad de servicios actuales habilitados por TI. 3. Analizar actividades del proceso empresarial para identificar la necesidad de servicios de TI nuevos o rediseñados. 4. Comparar los requisitos identificados con los componentes de servicio vigentes del portafolio. Si fuera posible, incluir los componentes de servicio vigentes (servicios de TI, opciones de nivel de servicio y paquetes de servicio) en nuevos paquetes de servicio para satisfacer los requisitos del negocio identificados. 5. Revisar regularmente el portafolio de servicios de TI con la gestión del portafolio y la gestión de relaciones con el negocio para identificar servicios obsoletos. Acordar su retirada y proponer cambios. 6. Cuando sea posible, hacer corresponder las demandas con los paquetes de servicio y crear servicios estandarizados para lograr eficiencias globales.	•Brechas identificadas en los servicios de TI prestados a la empresa. •Definiciones de servicios estándar.	•Formulario de brechas de los servicios de TI.							
		APO09.02. Catalogar los servicios habilitados por TI	1. Publicar en catálogos los servicios activos importantes , paquetes de servicios y opciones de nivel de servicio habilitados por TI desde el portafolio. 2. Asegurar de forma continua que los componentes de servicio en el portafolio y los catálogos de servicios relacionados estén completos y actualizados. 3. Informar a la dirección de gestión de relaciones empresariales acerca de todas las actualizaciones de los catálogos de servicios.	•Catálogos de servicios	•Catálogos de los servicios de TI.							
		APO09.03. Definir y preparar acuerdos de servicio	1. Analizar los requisitos para acuerdos de servicio nuevos o modificados recibidos de la gestión de relaciones con el negocio a fin de asegurar que puedan satisfacerse. Considerar aspectos como los tiempos de servicio, disponibilidad, rendimiento, capacidad, seguridad, privacidad, continuidad, problemas de cumplimiento y regulatorios, usabilidad, limitaciones de la demanda y calidad de los datos. 2. Redactar borradores de acuerdos de servicio al cliente basados en los servicios, paquetes de servicios y opciones de nivel de servicio en los catálogos de servicios relevantes. 3. Finalizar los acuerdos de servicio al cliente con la gestión de relaciones con el negocio. 4. Determinar, acordar y documentar acuerdos operativos internos que sustenten los acuerdos de servicio al cliente, si corresponde. 5. Relacionarse con la gestión de proveedores externos para garantizar que los adecuados contratos comerciales con proveedores de servicios externos sustenten los acuerdos de servicio al cliente, si corresponde.	•Acuerdos a nivel de servicio (SLA) •Acuerdos a nivel operativo (OLA)	•Acuerdos a nivel de servicio (SLA) •Acuerdos a nivel operativo (OLA)							
		APO09.04. Monitorizar y reportar los niveles de servicio	1. Establecer y mantener medidas para monitorizar y recopilar datos de nivel de servicio. 2. Evaluar el rendimiento y proporcionar reportes sobre el rendimiento de los acuerdos de servicio regular y formalmente, incluidas las desviaciones de los valores acordados. Distribuir este informe a la gestión de relaciones con el negocio. 3. Realizar revisiones regulares para pronosticar e identificar las tendencias del rendimiento de nivel de servicio. Incorporar prácticas de gestión de calidad en la monitorización de servicios. 4. Ofrecer la información de gestión apropiada para contribuir a la gestión del rendimiento. 5. Acordar planes de acción y remediaciones para cualquier problema de rendimiento o tendencias negativas.	•Planes de acción de mejora y remediaciones. •Informes de rendimiento del nivel de servicio.	•Plan de mejora y remediación de servicios de TI. •Informes de revisiones o auditoría de los servicios de TI.							
		APO09.05. Revisar los acuerdos y los contratos de servicio	1. Revisar de forma regular los acuerdos de servicio conforme a los términos acordados para garantizar que sean efectivos y estén actualizados. Cuando corresponda, tener en cuenta cambios en requisitos, servicios habilitados por TI, paquetes de servicio y opciones de nivel de servicio. 2. Cuando sea necesario, revisar el acuerdo de servicio vigentes con el proveedor de servicios. Acordar y actualizar los acuerdos operativos internos.	•SLA actualizados	•Informes de revisión o auditoría de los acuerdos a nivel de servicio. •Procedimiento para actualizar los acuerdos a nivel de servicio.							
	APO13. Gestionar la seguridad	APO13.01. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)	1. Definir el alcance y los límites del sistema de gestión de seguridad de la información (SGSI) en términos de las características de la empresa, organización, ubicación, activos y tecnología. Incluir detalles y justificación de las exclusiones del alcance. 2. Definir un SGSI conforme a la política empresarial y el contexto en el que opera la empresa. 3. Alinear el SGSI con el enfoque global de la empresa hacia la gestión de la seguridad. 4. Obtener la autorización de la dirección para implementar y operar o cambiar el SGSI. 5. Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI. 6. Definir y comunicar los roles y responsabilidades de la gestión de seguridad de la información. 7. Comunicar la estrategia de SGSI.	•Declaración del alcance de SGSI. •Política de SGSI.	•Política del Sistema de Gestión de Seguridad de la Información (SGSI), que contenga el alcance del SGSI.							
		APO13.02. Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	1. Formular y mantener un plan de tratamiento de riesgos de seguridad de la información alineado con objetivos estratégicos y la arquitectura empresarial. Asegurar que el plan identifique las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con los recursos, responsabilidades y prioridades asociados para la gestión de los riesgos de seguridad de la información identificados. 2. Mantener, como parte de la arquitectura de la empresa, un inventario de los componentes de la solución establecida para gestionar los riesgos relacionados con la seguridad. 3. Desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad, apoyadas por casos de negocio apropiados que incluyan consideraciones de financiación y asignación de roles y responsabilidades. 4. Proporcionar aportes para el diseño y desarrollo de prácticas y soluciones de gestión, seleccionadas en el plan de tratamiento de riesgos de seguridad de la información. 5. Implementar programas de formación y concienciación sobre seguridad de la información y privacidad. 6. Integrar la planificación, diseño, implementación y monitorización de procedimientos de seguridad de la información y privacidad y otros controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 7. Definir cómo medir la eficacia de las prácticas de gestión seleccionadas. Especificar cómo deben usarse estas medidas para evaluar la eficacia para producir resultados comparables y reproducibles.	•Plan de tratamiento del riesgo de seguridad de la información. •Casos de negocio de seguridad de la información.	•Plan para el tratamiento de riesgos en seguridad de información. •Documentos de caso de negocio sobre seguridad de la información.							
		APO13.03. Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	1. Llevar a cabo revisiones regulares de la eficacia del SGSI. Incluir el cumplimiento de la política y los objetivos del SGSI y revisar las prácticas de seguridad y privacidad. 2. Realizar auditorías de SGSI a intervalos planificados. 3. Realizar periódicamente una revisión de la gestión del SGSI para asegurar que el alcance sigue siendo adecuado y que se identifican mejoras en el proceso del SGSI. 4. Registrar acciones y eventos que podrían tener un impacto en la eficacia o el rendimiento del SGSI. 5. Hacer aportes para el mantenimiento de los planes de seguridad para tener en cuenta los hallazgos de las actividades de monitorización y revisión.	•Recomendaciones para la mejora del sistema de gestión de la seguridad de la información (SGSI). •Informes de auditoría del sistema de gestión de seguridad de la información (SGSI).	•Informes de auditoría del SGSI. •Informe ejecutivo sobre recomendaciones hacia el SGSI.							

KPMG

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Responsable	Área	Fecha de solicitud	Fecha de entrega	Comentarios
Construir, Adquirir e Implementar (BAI)	BAI06. Gestionar los cambios de TI	**BAI06.01.** Evaluar, priorizar y autorizar solicitudes de cambio	**1.** Usar solicitudes de cambio formales para permitir a los propietarios de los procesos de negocio y a TI solicitar cambios a procesos de negocio, infraestructura, sistemas o aplicaciones. Asegurarse de que todos estos cambios surjan solo a través del proceso de gestión de solicitudes de cambio. **2.** Categorizar todos los cambios solicitados (p. ej., procesos de negocio, infraestructura, sistemas operativos, redes, sistemas de aplicación, software de aplicación comprado/empaquetado) y relacionar los elementos de configuración afectados. **3.** Priorizar todos los cambios solicitados basándose en los requisitos de negocio y técnicos, recursos requeridos y las razones legales, regulatorias y contractuales para el cambio solicitado. **4.** Aprobar formalmente cada cambio por parte de los dueños de los procesos de negocio, gestores de servicios y partes interesadas técnicas de TI, según corresponda. Los cambios que son de bajo riesgo y relativamente frecuentes deben preaprobarse como cambios estándar. **5.** Planificar y programar todos los cambios aprobados. **6.** Planificar y evaluar todas las solicitudes de una manera estructurada. Incluir un análisis de impacto en los procesos de negocio, la infraestructura, los sistemas y las aplicaciones, los planes de continuidad del negocio (BCP) y los proveedores de servicios para asegurarse de que se hayan identificado todos los componentes afectados. Evaluar la probabilidad de afectar negativamente el entorno operativo y el riesgo de implementar el cambio. Considerar las implicaciones de seguridad, privacidad, legales, contractuales y de cumplimiento del cambio solicitado. Considerar también las interdependencias entre los cambios. Involucrar a los propietarios de los procesos de negocio en el proceso de evaluación, cuando sea conveniente. **7.** Considerar el impacto de los proveedores de servicios contratados (p. ej., de procesamiento de negocio , infraestructura, desarrollo de aplicaciones y servicios compartidos externalizados) en el proceso de gestión de cambios. Incluir la integración de los procesos de gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y SLA.	•Plan y cronograma de cambios. •Solicitudes de cambio aprobadas. •Evaluaciones del impacto.	•Procedimiento de gestión de cambios. •Planificación y cronograma para la gestión de cambios. •Listado de solicitudes de cambio aprobadas. •Guía para establecer evaluaciones de impacto en los cambios.							
		BAI06.02. Gestionar cambios de emergencia.	**1.** Definir lo que constituye un cambio de emergencia. **2.** Asegurar que existe un procedimiento documentado para declarar, evaluar, aprobar inicialmente, autorizar después del cambio y registrar un cambio de emergencia. **3.** Verificar que todos los acuerdos de acceso de emergencia para los cambios se autoricen, documenten y revoquen adecuadamente después de que el cambio se haya aplicado. **4.** Monitorizar todos los cambios de emergencia y realizar las revisiones posteriores a la implementación con la participación de todas las partes interesadas. La revisión debe considerar e iniciar acciones correctivas basadas en las causas raíz, tales como problemas con los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales, e integridad de datos.	•Revisión posterior a la implementación.	•Listado de solicitudes de cambio de emergencia. •Procedimiento para gestionar los cambios de emergencia. •Informes de revisión y monitoreo de los cambios de emergencia.							
		BAI06.03. Hacer seguimiento e informar sobre cambios de estado	**1.** Categorizar las solicitudes de cambio en el proceso de seguimiento (p. ej., rechazado; aprobado pero no iniciado; aprobado y en proceso; y cerrado). **2.** Implementar informes de estado de los cambios con métricas de rendimiento para permitir la gestión de la revisión y la monitorización, tanto del estado detallado de los cambios como del estado general (p. ej., análisis de la antigüedad de las solicitudes de cambio). Asegurarse de que los informes de estado formen una pista de auditoría para que los cambios puedan rastrearse posteriormente, desde su inicio hasta su eventual disposición. **3.** Monitorizar los cambios abiertos para asegurarse de que todos los cambios aprobados se cierren de manera oportuna, según su prioridad. **4.** Mantener un sistema de seguimiento e informes para todas las solicitudes de cambio.	•Informes de estado de las solicitudes de cambio.	•Guía para documentar el estado de los cambios que incluya la categorización, métricas, revisiones y monitorizaciones efectuadas de las solicitudes de cambio.							
		BAI06.04. Cerrar y documentar los cambios.	**1.** Incluir los cambios en la documentación en el procedimiento de gestión. Algunos ejemplos de documentación son: procedimientos operativos de negocio y de TI, documentación de continuidad del negocio y recuperación ante desastres, información de configuración, documentación de aplicaciones, pantallas de ayuda y materiales de capacitación. **2.** Definir un periodo de retención adecuado para la documentación de los cambios y la documentación del sistema y del usuario antes y después del cambio. **3.** Someter la documentación al mismo nivel de revisión que el cambio en sí mismo.	•Cambio en la documentación	•Evidencia (correo, chat, documento, pantallazo, entre otros) del ajuste de los cambios en los procedimientos de la empresa.							
	BAI09. Gestionar los activos	**BAI09.01.** Identificar y registrar los activos actuales.	**1.** Identificar todos los activos adquiridos en un registro de activos que recoja el estado actual. Los activos se reportan en la hoja del balance; se compran o crean para aumentar el valor de una compañía o beneficiar las operaciones de la empresa (p. ej., hardware y software). Identificar todos los activos adquiridos y mantener el alineamiento con los procesos de gestión de la configuración y gestión de cambios, el sistema de gestión de la configuración y los datos de contabilidad financiera. **2.** Identificar requisitos legales, regulatorios o contractuales que deban abordarse al gestionar el activo. **3.** Comprobar que los activos son adecuados para su propósito (es decir, que se puedan usar). **4.** Garantizar la contabilidad de todos los activos. **5.** Comprobar la existencia de todos los activos adquiridos mediante comprobaciones y conciliación regulares de inventario físico y lógico. Incluir el uso de herramientas de descubrimiento de software. **6.** Determinar regularmente si cada activo continúa proporcionando valor. De ser así, estimar la vida útil esperada durante la que proporcionará valor.	•Resultados de revisiones de idoneidad. •Registro de activos. •Resultados de comprobaciones de inventario físicas.	•Procedimiento de revisiones de idoneidad de los activos. •Informe de resultados de revisiones de idoneidad de los activos. •Registro de todos los activos adquiridos actualmente. •Resultados de comprobaciones de inventario físicas.							
		BAI09.02. Gestionar los activos críticos	**1.** Identificar activos que son críticos para proporcionar la capacidad de servicio mediante la referencia a los requisitos en las definiciones de servicio, los SLA y el sistema de gestión de la configuración. **2.** Considerar regularmente el riesgo de fallo o la necesidad de sustitución de cada activo crítico. **3.** Comunicar a los clientes y usuarios afectados el impacto esperado (p. ej. restricciones de rendimiento) de las actividades de mantenimiento. **4.** Incorporar al calendario global de producción las suspensiones planificadas. Programar actividades de mantenimiento para minimizar el impacto adverso en los procesos de negocio. **5.** Mantener la resiliencia de los activos críticos aplicando un mantenimiento preventivo regular. Monitorizar el rendimiento y, de ser necesario, proporcionar activos alternativos y/o adicionales para minimizar la probabilidad de fallo. **6.** Establecer un plan de mantenimiento preventivo para todo el hardware considerando un análisis de coste beneficio, las recomendaciones de los proveedores, el riesgo de suspensión del servicio, el personal calificado y otros factores relevantes. **7.** Establecer acuerdos de mantenimiento que incluyan el acceso de terceros a las instalaciones de TI de la organización a fin de realizar actividades en el sitio (on-site) o fuera de él (off site) (p. ej. outsourcing). Establecer contratos de servicio formales que contengan o hagan referencia a todas las condiciones de seguridad y privacidad necesarias, incluidos procedimientos de autorización de acceso, para garantizar el cumplimiento con las políticas y estándares de seguridad/privacidad de la organización. **8.** Garantizar que los servicios de acceso remoto y los perfiles de usuario (y otros medios usados para el mantenimiento y el diagnóstico) estén activos solo cuando sea necesario. **9.** Monitorizar el rendimiento de los activos críticos mediante el examen de tendencias de los incidentes. Cuando sea necesario, realizar acciones de reparación o sustitución.	•Comunicaciones de suspenciones por mantenimiento planificadas. •Contratos de mantenimiento.	•Procedimiento para gestionar los cambios críticos. •Protocolo de comunicación del mantenimiento de activos críticos. •Contratos a acuerdos de mantenimiento de los activos críticos, que especifique condiciones de seguridad, privacidad, acceso, y autorizaciones.							
		BAI09.03. Gestionar el ciclo de vida del activo	**1.** Proporcionar todos los activos conforme a las solicitudes aprobadas y las políticas y prácticas de adquisición de la empresa. **2.** Obtener, recibir, verificar, probar y registrar todos los activos de forma controlada, incluyendo etiquetas físicas, cuando se requiera. **3.** Aprobar los pagos y completar el proceso con los proveedores, conforme a las condiciones del contrato acordadas. **4.** Implementar los activos siguiendo el ciclo de vida de implementación estándar, incluida la gestión de cambios y las pruebas de aceptación. **5.** Asignar los activos a usuarios, con responsabilidades de aceptación y confirmación, como corresponda. **6.** Siempre que sea posible, reasignar los activos cuando ya no se necesiten debido a un cambio de rol del usuario, redundancia o un servicio o retirada de un servicio. **7.** Planificar, autorizar e implementar actividades relacionadas con la retirada, mientras se conservan los registros correspondientes para satisfacer las necesidades regulatorias y de negocio en curso. **8.** Disponer de los activos de forma segura, tras considerar, por ejemplo, el borrado permanente de los datos registrados en los dispositivos y el daño potencial al medio ambiente. **9.** Disponer de los activos de forma responsable cuando ya no sean de utilidad debido a la retirada de todos los servicios relacionados, tecnología obsoleta o la falta de usuarios, teniendo en consideración el impacto medioambiental.	•Retiradas autorizadas de activos. •Registro actualizado de activos. •Solicitudes aprobadas de adquisiciones de activos.	•Listado de retiradas autorizadas de activos. •Listado de las solicitudes de adquisiciones de activos aprobadas. •Evidencia (correo, chat, documento, pantallazo, entre otroside comprobación del registro de activos actualizados.							
		BAI09.04. Optimizar el valor de los activos	**1.** Revisar regularmente toda la base de activos, considerando si está alineada con las necesidades del negocio. **2.** Evaluar los costes de mantenimiento, considerar si son razonables e identificar opciones de menor coste. Cuando sea necesario, incluir reemplazos con nuevas alternativas. **3.** Revisar las garantías y considerar la relación calidad-precio y las estrategias de reemplazo para determinar las opciones de menor coste. **4.** Usar estadísticas de capacidad y uso para identificar activos subutilizados o redundantes que podrían considerarse para su eliminación o sustitución a fin de reducir costes. **5.** Revisar la base completa para identificar oportunidades de estandarización, suministro único y otras estrategias que podrían reducir los costes de adquisición, soporte y mantenimiento. **6.** Revisar el estado general a fin de identificar oportunidades para aprovechar las tecnologías emergentes o estrategias de suministro alternativas para reducir costes o incrementar la relación calidad-precio.	•Oportunidades para reducir los costes o aumentar el valor de los activos. •Resultados de las revisiones de optimización de costes.	•Metodología / Guía para la revisión de la optimización del valor de los activos. •Informe de resultados sobre revisiones de optimización de los costes de los activos. •Informes de acciones correctivas para reducir los costes o aumentar el valor de los activos.							
		BAI09.05. Gestionar las licencias	**1.** Mantener un registro de todas las licencias de software adquiridas y los acuerdos de licencias asociados. **2.** Realizar regularmente una auditoría para identificar todas las instancias de software con licencia instaladas. **3.** Comparar el número de licencias instaladas con el número de licencias adquiridas. Garantizar que el método de medición de cumplimiento de licencias sea conforme a los requisitos de la licencia y del contrato. **4.** Cuando las instancias sean inferiores al número de licencias adquiridas, decidir si se deben conservar o poner fin a esas licencias, considerando los posibles ahorros en mantenimiento, capacitación y otros costes innecesarios. **5.** Cuando las instancias sean superiores al número de licencias adquiridas, considerar en primer lugar desinstalar las instancias que ya no se requieran o no estén justificadas y comprar entonces, de ser necesario, licencias adicionales para cumplir con el acuerdo de licencias. **6.** Considerar de forma regular si puede ser más rentable actualizar los productos y las licencias asociadas.	•Plan de acción para ajustar el número y asignaciones de licencias. •Registro de licencias de software. •Resultados de las auditorías a las licencias instaladas.	•Plan para la gestión de las licencias de software. •Registro de las licencias de software. •Informes de auditoría sobre licencias.							

KPMG

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Área	Responsable	Fecha de solicitud	Fecha de entrega	Comentarios
Entregar, Dar Servicio y Soporte (DSS)	DSS02. Gestionar las peticiones y los incidentes de servicio	DSS02.01. Definir esquemas de clasificación para incidentes y peticiones de servicio	1. Definir esquemas de priorización y clasificación de solicitudes de servicios e incidentes, y los criterios para el registro de problemas. Usar esta información para garantizar estrategias constantes a fin de gestionar e informar a los usuarios sobre los problemas y llevar a cabo análisis de tendencias. 2. Definir modelos de incidentes sobre errores conocidos para permitir una resolución eficiente y eficaz. 3. Definir modelos de solicitud de servicios conforme al tipo de solicitud de servicios para permitir la autoayuda y un servicio eficiente para solicitudes estándar. 4. Definir las reglas y procedimientos de escalamiento de incidentes, sobre todo para incidentes importantes e incidentes de seguridad. 5. Definir las fuentes de conocimiento sobre incidentes y solicitudes y describir cómo usarlas.	•Criterios para el registro de problemas. •Reglas para escalamiento de incidentes. •Esquema y modelos de clasificación de peticiones de servicio e incidentes.	•Guía de criterios para el registro de problemas. •Reglas y procedimientos para el escalamiento de incidentes. •Esquema de priorización y clasificación de peticiones de servicio e incidentes.							
		DSS02.02. Registrar, clasificar y priorizar las peticiones e incidentes	1. Registrar todas las solicitudes e incidentes de servicio, mediante el registro de toda la información relevante, para que pueda gestionarse de forma eficaz y pueda mantenerse un registro histórico completo. 2. Permitir el análisis de tendencias, clasificar las solicitudes e incidentes de servicio, con identificación del tipo y categoría. 3. Priorizar solicitudes e incidentes de servicio basados en la definición del servicio de SLA según el impacto y la urgencia para el negocio.	•Peticiones de servicio e incidentes clasificadas y priorizadas. •Registro de solicitudes de servicio e incidentes.	•Registro de peticiones de servicio e incidentes, clasificadas y priorizadas. •Registro de solicitudes de servicios e incidentes.							
		DSS02.03. Verificar, aprobar y resolver peticiones de servicio	1. Comprobar el derecho a las solicitudes de servicio, utilizando un flujo de proceso predefinido y cambios estándar, cuando sea posible. 2. Obtener la aprobación y confirmación financiera y funcional, si fuera necesario, o las aprobaciones predefinidas para los cambios estándar acordados. 3. Cumplir con las solicitudes realizando el proceso de solicitud seleccionado. Cuando sea posible, usar menús automáticos de autoayuda y modelos de solicitud predefinidas para elementos solicitados con frecuencia.	•Peticiones de servicio aprobadas. •Peticiones de servicio completadas.	•Registro de peticiones de servicio aprobadas. •Registro de peticiones de servicio completadas.							
		DSS02.04. Investigar, diagnosticar y asignar incidentes	1. Identificar y describir síntomas relevantes para establecer las causas más probables de los incidentes. Referenciar los recursos de conocimientos disponibles (incluidos errores y problemas conocidos) para identificar posibles resoluciones de incidentes (soluciones temporales y/o permanentes). 2. Si un problema relacionado o error conocido no existe todavía y si el incidente satisface los criterios acordados para el registro de problemas, registrarlo como un problema nuevo. 3. Asignar incidentes a funciones de especialista si se necesita una mayor habilidad. Contar con el nivel directivo adecuado, donde y si se necesita.	•Log de problemas. •Síntomas de incidente.	•Registro de problemas. •Registro de síntomas de incidentes.							
		DSS02.05. Resolver y recuperarse de los incidentes	1. Seleccionar y aplicar las resoluciones de incidentes más adecuadas (solución workaround y/o solución permanente). 2. Registrar, si se usaron, workarounds para la resolución de incidentes. 3. Aplicar medidas correctivas, si se requieren. 4. Documentar la resolución de incidentes y evaluar si la resolución puede usarse como una fuente de conocimiento futura.	•Resoluciones de incidentes.	•Informe de resolución de incidentes.							
		DSS02.06. Cerrar las peticiones de servicio y los incidentes	1. Comprobar con los usuarios afectados que la solicitud de servicio se ha cumplido de forma satisfactoria o el incidente se ha resuelto de forma satisfactoria dentro de un plazo de tiempo acordado/aceptable. 2. Cerrar las peticiones e incidentes de servicio.	•Confirmación del usuario del cumplimiento o resolución satisfactoria.	•Evidencia (correo, chat, documento, firma, reunión, entre otros), donde el usuario notifica el cumplimiento y la							
		DSS02.07. Hacer seguimiento al estado y producir informes	1. Supervisar y hacer seguimiento al escalamientos y resoluciones de incidentes y solicitar procedimientos de manejo para progresar hacia la resolución o finalización de los mismos. 2. Identificar las partes interesadas en la información y sus necesidades de datos o informes. Identificar frecuencia y medio de elaboración de los reportes. 3. Producir y distribuir informes en el plazo debido o proporcionar un acceso controlado a los datos en línea. 4. Analizar incidentes y solicitudes de servicio por categoría y tipo. Establecer tendencias e identificar patrones de problemas recurrentes, violaciones o ineficiencias del SLA. 5. Usar la información como un insumo a la planificación de la mejora continua.	•Estado de incidentes e informe de tendencias. •Estado de cumpliminto de peticiones e informe de tendencias.	•Informes de tendencias de problemas recurrentes. •Informes sobre el estado de cumplimiento de las peticiones e incidentes.							
	DSS03. Gestionar los problemas	DSS03.01. Identificar y clasificar los problemas	1. Identificar problemas a través de la correlación de informes de incidentes, registros de errores y otros recursos que permitan la identificación de problemas. 2. Gestionar todos los problemas formalmente con acceso a todos los datos relevantes. Incluir información del sistema de gestión de cambios de TI y de configuración/activo de TI y los detalles del incidente. 3. Definir grupos de soporte adecuados para ayudar en la identificación de problemas, análisis de la causa raíz y determinación de soluciones para respaldar la gestión de problemas. Determinar grupos de soporte conforme a las categorías predefinidas, como hardware, red, software, aplicaciones y software de soporte. 4. Definir niveles de prioridad a través de la consulta con el negocio para garantizar que la identificación del problema y el análisis de las causas raíz se gestionan en el plazo debido conforme a los SLA acordados. Basar los niveles de prioridad en el impacto y la urgencia del negocio. 5. Informar del estado de los problemas identificados a la mesa de servicio, para que los clientes y gestores de TI puedan mantenerse informados. 6. Mantener un único catálogo de gestión de problemas para registrar e informar sobre los problemas identificados. Usar el catálogo para establecer pistas de auditoría de los procesos de gestión de problemas incluido el estado de cada problema (es decir, abierto, reabierto, en curso o cerrado).	•Esquema de clasificación de problemas. •Informes de estado del problema. •Registro de problemas.	•Procedimiento de gestión de los problemas. •Catálogo de gestión de problemas. •Esquema de clasificación de los problemas.							
		DSS03.02. Investigar y diagnosticar los problemas	1. Identificar problemas que podrían ser errores conocidos mediante una comparación de los datos de incidentes con la base de datos de errores conocidos y sospechados (p. ej., aquellos comunicados por proveedores externos) Clasificar los problemas como errores conocidos. 2. Asociar los elementos de configuración afectados con el error establecido/conocido. 3. Producir informes para comunicar el progreso a la hora de resolver problemas y gestionar el impacto continuo de los problemas no resueltos. Monitorizar el estado del proceso de manejo de problemas a lo largo de su ciclo de vida, incluyendo los insumos de la gestión de cambios y de la configuración de TI.	•Informes de resolución de problemas. •Causas raíz de problemas	•Registro sobre causas raíz de los problemas. •Informes de resolución de problemas.							
		DSS03.03. Presentar los errores conocidos	1. Tan pronto como se identifiquen las causas raíz de los problemas, crear registros de los errores conocidos y desarrollar una solución temporal apropiada. 2. Identificar, evaluar, priorizar y procesar (a través de la gestión de cambio de TI) soluciones a los errores conocidos, conforme al coste/ beneficio del caso de negocio, el impacto y la urgencia.	•Soluciones propuestas a errores conocidos. •Registro de errores conocidos.	•Registro de errores conocidos de los problemas. •Registro de acciones correctivas para							
		DSS03.04. Resolver y cerrar los problemas	1. Cerrar los registros de problemas después de la confirmación sobre la eliminación exitosa del error conocido o después del acuerdo con el negocio sobre cómo gestionar el problema de forma alternativa. 2. Informar a la mesa de servicio sobre el calendario de cierre de problemas (p. ej., el calendario para solucionar los errores conocidos, la posible solución temporal o el hecho de que el problema seguirá ahí hasta que se implemente el cambio) y las consecuencias de la estrategia llevada a cabo. Mantener a los usuarios y clientes afectados informados como corresponda. 3. A través del proceso de resolución, obtener informes regulares de gestión de cambios de TI relacionados con el progreso a la hora de resolver problemas y errores. 4. Monitorizar el impacto continuo de los problemas y errores conocidos en los servicios. 5. Revisar y confirmar la resolución satisfactoria de problemas mayores. 6. Asegurar que el conocimiento aprendido de la revisión se incorpore a la reunión de revisión de servicios con el cliente del negocio.	•Comunicación de conocimientos aprendidos. •Registro de problemas cerrados.	•Registro de problemas cerrados. •Procedimiento de comunicación de conocimientos aprendidos con las partes interesadas e involucrados.							
		DSS03.05. Realizar una gestión proactiva de los problemas	1. Captar la información del problema relacionada con cambios e incidentes de TI y comunicarla a las partes interesadas clave. Comunicar a través de informes y reuniones periódicas entre los dueños de los procesos de incidentes, problemas, cambios y gestión de la configuración para considerar los problemas recientes y las posibles acciones correctivas. 2. Garantizar que los dueños y gestores de los procesos de gestión de incidentes, problemas, cambios y configuración se reúnan regularmente para comentar los problemas conocidos y los cambios planificados futuros. 3. Identificar e iniciar soluciones sostenibles (soluciones permanentes) que aborden la causa raíz . Presentar solicitudes de cambio a través de los procesos establecidos de gestión de cambios. 4. Permitir a la empresa supervisar los costes totales de los problemas, captar los esfuerzos de cambios derivados de las actividades del proceso de gestión de problemas (p. ej., soluciones a problemas y errores conocidos) e informar al respecto. 5. Crear informes para supervisar la resolución de problemas en relación con los requisitos del negocio y los SLAs. Asegurar el escalamiento adecuado de los problemas, como comunicarlos al siguiente nivel directivo conforme a los criterios acordados, contactar con proveedores externos o consultar con el consejo asesor de cambios (CAB) para aumentar la prioridad de una solicitud de cambio urgente (RFC) para implementar una solución temporal. 6. Optimizar el uso de recursos y reducir el uso de soluciones temporales; hacer un seguimiento a las tendencias de los problemas.	•Soluciones sostenibles identificadas. •Informes de supervisión de resolución de problemas.	•Informe de soluciones sostenibles para abordar la causa raíz de los problemas. •Informes de supervisión de la resolución de problemas en relación con estalamietos y SLAs.							

Dominio	Proceso	Práctica	Actividad	Requerimientos	Documentación	Estado de la solicitud	Documentos proporcionados	Área	Responsable	Fecha de solicitud	Fecha de entrega	Comentarios
Monitorizar, Evaluar y Valorar (MEA)	MEA02. Gestionar el sistema de control interno	MEA02.01. Supervisar los controles internos	1. Identificar los límites del sistema de control interno. Por ejemplo, considerar cómo los controles internos de la organización, tienen en cuenta las actividades de desarrollo o producción externalizadas y/o ubicadas en otro país (offshore, término en inglés).	•Resultados de benchmarking y otras evaluaciones. •Resultados de la supervisión del control interno y sus revisiones.	•Informe de resultados de benchmarking y evaluaciones relacionadas con el control interno. •Informe de resultados sobre la supervisión del control interno.							
			2. Evaluar el estado de los controles internos de los proveedores de servicios externos. Confirmar que los proveedores de servicio cumplen con los requisitos legales y regulatorios y con sus obligaciones contractuales.									
			3. Realizar actividades de supervisión y evaluación del control interno basadas en estándares de gobierno de la organización y marcos y prácticas aceptados por la industria. Incluye también la supervisión y evaluación de la eficacia y eficiencia de las actividades de supervisión gerencial.									
			4. Asegurar que las excepciones de control se comuniquen , se sigan y analicen prontamente, y que se prioricen e implementen acciones correctivas apropiadas, conforme al perfil de gestión de riesgos (p. ej., clasificar algunas excepciones como riesgo clave y otras como riesgo no clave).									
			5. Considerar evaluaciones independientes del sistema de control interno (p. ej., por auditoría interna o compañeros).									
			6. Mantener el sistema de control interno, considerando los cambios continuos en el riesgo del negocio y de TI, el entorno de control de la organización y los procesos del negocio y de TI relevantes. Si hay una brecha, evaluar y recomendar cambios.									
			7. Evaluar regularmente el desempeño del marco de control, a través de una comparación con estándares y buenas prácticas aceptadas por la industria. Considerar la adopción formal de una estrategia de mejora continua de la supervisión del control interno.									
		MEA02.02. Revisar la eficacia de los controles del proceso de negocio.	1. Entender y priorizar el riesgo de los objetivos de la organización.	•Evidencia de la efectividad de los controles.	•Informe de resultados de las auditorías del control interno.							
			2. Identificar controles clave y desarrollar una estrategia adecuada para validar los controles.									
			3. Identificar información que indicará si un entorno de control interno está funcionando de forma eficaz.									
			4. Conservar evidencias de la eficacia del control.									
			5. Desarrollar e implementar procedimientos rentables para obtener esta información de acuerdo a los criterios de calidad de la información correspondientes.									
		MEA02.03. Realizar autoevaluaciones de control	1. Definir una estrategia acordada y consistente para realizar autoevaluaciones de control y coordinarse con auditores internos y externos.	•Planes y criterios de autoevaluación. •Resultados de las revisiones de las autoevaluaciones. •Resultados de las autoevaluaciones.	•Plan para la autoevaluación del control interno. •Guía de criterios de autoevaluación del control interno. •Informe de resultados de las autoevaluaciones del control interno.							
			2. Mantener planes de evaluación e identificación de criterios y alcance para llevar a cabo las autoevaluaciones. Planificar la comunicación de los resultados del proceso de autoevaluación al negocio, a TI y a la dirección general y al consejo de administración. Considerar estándares de auditoría interna en el diseño de las autoevaluaciones.									
			3. Determinar la frecuencia de las autoevaluaciones periódicas, considerando globalmente la eficacia y eficiencia de la supervisión continua.									
			4. Asignar las responsabilidades de la autoevaluación a los individuos adecuados para garantizar la objetividad y la competencia.									
			5. Proporcionar revisiones independientes para garantizar la objetividad de la autoevaluación y permitir que se compartan buenas prácticas de control interno de otras empresas.									
			6. Comparar los resultados de las autoevaluaciones con los estándares y buenas prácticas de la industria.									
			7. Resumir e informar de los resultados de las autoevaluaciones y benchmarking para tomar acciones correctivas.									
		MEA02.04. Identificar e informar las deficiencias de control	1. Comunicar procedimientos para el escalamiento de las excepciones de control, análisis de la causa raíz y notificación a los dueños del proceso y a las partes interesadas de TI.	•Acciones correctivas. •Deficiencias del control.	•Registro de deciciencias del control interno y sus acciones correctivas.							
			2. Considerar el riesgo empresarial relacionado para establecer umbrales para el escalamiento de las excepciones de control y fallos.									
			3. Identificar, reportar y registrar las excepciones de control. Asignar responsabilidades para su resolución e informar de su estado.									
			4. Decidir qué excepciones de control deberían comunicarse a la persona responsable de la función y qué excepciones deberían escalarse. Informar a los dueños del proceso y a las partes interesadas.									
			5. Hacer un seguimiento de todas las excepciones para garantizar que se han abordado las acciones acordadas.									
			6. Identificar, iniciar, seguir e implementar acciones correctivas que surjan de las evaluaciones de control y los reportes.									
	MEA03. Gestionar el cumplimiento de los requisitos externos	MEA03.01. Identificar los requisitos externos de cumplimiento	1. Asignar la responsabilidad de identificar y supervisar los cambios en los requisitos legales, regulatorios y otros requisitos contractuales externos, relevantes para el uso de recrsos de TI y el procesamiento de la información dentro de las operaciones empresariales y de TI.	•Log de acciones de cumplimiento requeridas. •Registro de requerimientos de cumplimiento.	•Requerimientos de cumplimiento externo: requisitos legales, regulatorios y contractuales. •Procedimiento de acciones de cumplimiento para los requisitos externos.							
			2. Identificar y evaluar todos los posibles requisitos de cumplimiento y su impacto en las actividades de TI, en áreas como flujo de datos, privacidad, controles internos, informes financieros, regulaciones específicas de la industria, propiedad intelectual, salud y seguridad en el trabajo.									
			3. Evaluar el impacto de los requisitos legales y regulatorios relacionados con TI sobre contratos con terceros relacionados con las operaciones de TI, proveedores de servicio y otros socios comerciales de negocios.									
			4. Definir las consecuencias del incumplimiento.									
			5. Obtener asesoría independiente cuando corresponda, sobre los cambios en la legislación, regulaciones y estándares vigentes.									
			6. Mantener un registro actualizado de todos los requisitos legales, regulatorios y contractuales; de su impacto y las acciones requeridas.									
			7. Mantener un registro global, armonizado e integrado, de los requisitos de cumplimiento externo para la empresa.									
		MEA03.02. Optimizar la respuesta a los requisitos externos	1. Revisar y ajustar continuamente las políticas, principios, estándares, procedimientos y metodologías para que sean eficaces en garantizar el cumplimiento necesario y abordar el riesgo empresarial. Usar expertos internos y externos, cuando sea necesario.	•Comunicaciones de cambios en los requisitos de cumplimiento. •Políticas, principios, procedimientos y	•Procedimiento de comunicación de los cambios en requisitos de cumplimiento. •Listado y registro de principios, estándares,							
			2. Comunicar los requisitos nuevos y modificados a todo el personal relevante.									
		MEA03.03. Confirmar el cumplimiento externo	1. Evaluar regularmente las políticas, estándares, procedimientos y metodologías organizativas en todas las funciones de la empresa, para garantizar el cumplimiento de todos los requisitos legales y regulatorios relevantes relacionados con el procesamiento de la información.	•Confirmaciones de cumplimiento. •Brechas de cumplimiento identificadas.	•Resultados de cumplimiento o incumplimiento de los requisitos externos. •Formulario de brechas de cumplimiento.							
			2. Tratar las brechas de cumplimiento en políticas, estándares y procedimientos con las debida oportunidad.									
			3. Evaluar periódicamente los procesos y actividades del negocio y de TI para asegurar el cumplimiento de los requisitos legales, regulatorios y contractuales vigentes.									
			4. Revisar regularmente los patrones recurrentes de fallos de cumplimiento y evaluar las lecciones aprendidas.									
			5. Mejorar las políticas, estándares, procedimientos, metodologías y sus procesos y actividades asociadas con base en la revisión y las lecciones aprendidas.									
		MEA03.04. Obtener aseguramiento de cumplimiento externo	1. Obtener confirmación periódica del cumplimiento con las políticas internas por parte de los dueños de los procesos de negocio y de TI y los jefes de unidades.	•Informes de aseguramiento del cumplimiento. •Informes de los problemas de incumplimiento y sus causa raíz.	•Informes de evaluación del cumplimiento a nivel interno. •Informe de problemas de incumplimiento con su respectiva causa raíz.							
			2. Realizar periódicamente revisiones internas y externas (Independientes, cuando sea posible,) para evaluar los niveles de cumplimiento.									
			3. Si se requiere, obtener declaraciones de los proveedores de servicio externos de TI sobre sus niveles de cumplimiento con las leyes y regulaciones aplicables.									
			4. Si se requiere, obtener declaraciones de los socios de negocio sobre sus niveles de cumplimiento con leyes y regulaciones aplicables, en la medida en que estén relacionados con las transacciones electrónicas entre empresas.									
			5. Integrar los informes sobre los requisitos legales, regulatorios y contractuales a nivel global de la empresa, involucrando a todas las unidades de negocio.									
			6. Supervisar y comunicar los problemas de incumplimiento y, cuando sea necesario, investigar la causa raíz.									

Apéndice U. Instructivo de gestión final

KPMG

Instructivo de Gestión de Ejecución de la auditoría

Introducción

El presente instructivo de gestión proporciona una serie de estructuras básicas y guión que deben ser consideradas en ciertas de las actividades del proceso de auditoría de TI. El objetivo de este documento es estandarizar y brindar conocimiento sobre las herramientas a utilizar y maneras de proceder al momento de ejecutar las actividades correspondiente. A continuación, se mencionan las actividades involucradas en este instructivo:

- **Reuniones de Entendimiento**

  Las reuniones de entendimiento se realizan entre el auditor y el cliente auditado. El auditor de TI se reúne con el cliente auditado para aclarar consultas sobre las evidencias proporcionadas. En el instructivo, se pactan especificaciones generales sobre este tipo de reuniones, y un guión de preguntas que pueden ser adaptadas al contexto de cada cliente y posteriormente utilizadas en la actividad.

- **Documentación de Riesgos**

  La documentación de los riesgos se realiza dentro de las fichas de auditoría. Sigue una estructura formal de condición, causa, impacto y recomendación. En el instructivo, se ejemplifican algunos riesgos por cada proceso, para que el auditor tenga un guión, los adapte al contexto del cliente y posteriormente los documente.

- **Desarrollo del Cronograma de Auditoría**

  El cronograma de auditoría es uno de los primeros entregables durante el proceso de TI. Ayuda a visualizar las actividades, periodos de entrega y duraciones pactadas para la auditoría. En el instructivo, se realiza un guión de cronograma, formalizando las actividades que generalmente son utilizadas, así como periodos aproximados de tiempo.

Índice

KPMG

Guión para la documentación de Reuniones de Entendimiento

Este apartado es un guión para ejecutar y documentar las reuniones de entendimiento efectuadas durante el proceso de auditoría de Tecnología de Información.

Especificaciones generales:

- La documentación de las respuestas debe realizarse en un documento digital como Microsoft Word o Excel. Este documento debe ser cargado a la carpeta de trabajo de la auditoría.
- Las preguntas para realizar por cada proceso durante la reunión deben estar alineadas a las actividades de cada práctica del proceso de COBIT 2019. En la sección **Guión de preguntas por cada proceso de COBIT 2019:**, podrán encontrar un guión de preguntas las cuales sirven de base para realizar las preguntas correspondientes por cada proceso que se audite.

Nota: Es importante aclarar que cada organización auditada es diferente, por ende las preguntas deben ser dirigidas de acuerdo con el contexto de cada cliente. Este documento sirve como guión para llevar una misma línea en la gestión de las reuniones de entendimiento, sin embargo, las preguntas e información que se gestione será única para cada cliente auditado.

Estructura de la reunión de entendimiento:

La reunión de entendimiento debe efectuarse bajo la siguiente agenda:

1. Saludo
2. Desglose de los contenidos a abarcar en la reunión.
3. Ejecución de las preguntas necesarias por cada procesos en cuestión.
4. Espacio para consultas por parte del cliente.
5. Despedida y finalización de la reunión.

KPMG

Guión de preguntas por cada proceso de COBIT 2019:

EDM01: Asegurar el establecimiento y el mantenimiento del marco de gobierno	
Practica	**Guión de preguntas**
EDM01.01. Evaluar el sistema de gobierno	• ¿Tienen identificados los factores internos y externos (leyes, reglamentos, u obligaciones contractuales), y las tendencias que influyen en el gobierno de TI de su empresa ? ¿Cuales son? ¿Puede mostrar evidencia de lo anterior? • ¿Tienen definida la importancia de TI para su negocio y cómo influye en las implicaciones de control? ¿Dónde se evidencia dicha importancia? • ¿Cómo efectúan el alineamiento de la información con el entorno, intereses, metas y objetivos empresariales? ¿Pueden mostrar evidencia del alineamiento? • ¿Tienen definido y documentado los principios de gobierno empresarial, el modelo de toma de decisiones y niveles de autoridad de TI? ¿En cuál documento? ¿Pueden mostrarlo como evidencia?
EDM01.02. Dirigir el sistema de gobierno	• ¿Cómo comunican el gobierno de TI y las directrices del comportamiento ético y profesional? ¿Cómo evidencian que se comunique la información adecuada? • ¿Tienen identificada y documentada la delegación y asignación de responsabilidades relacionadas con las prácticas de gobierno y directrices de TI? ¿En cuál documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Tienen definido y documentado el consejo de administración de TI y velan por el cumplimiento de sus funciones? ¿En cuál documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Cómo establecen su sistema de recompensas? ¿Tienen documentado su sistema de recompensas? ¿Tienen evidencia de su sistema de recompensas?
EDM01.03. Monitorizar el sistema de gobierno	• ¿Cómo evalúan el rendimiento y la eficacia de las partes interesadas que tiene responsabilidades de gobierno de TI? ¿Realizan informes de rendimiento? ¿En dónde se encuentran estos informes? • ¿Cómo monitorean el cumplimiento de estructuras, mecanismos y principios de TI, y las obligaciones debe satisfacer? ¿Tienen evidencias sobre informes de monitoreo? • ¿Cómo evalúan la eficacia del diseño de gobierno de TI y el sistema de control ? ¿Tienen evidencias sobre informes de eficacia?

KPMG

EDM03: Asegurar la optimización del riesgo	
Práctica	**Guión de preguntas**
EDM03.01. Evaluar la gestión de riesgos	• ¿Tienen identificado el apetito y la tolerancia del riesgo de TI de acuerdo con el contexto de la organización? ¿En cuál documento? ¿Pueden mostrarlo como evidencia? • ¿Cómo aseguran el alineamiento de la estrategia de riesgos de TI con la estrategia de la empresa? ¿Tienen evidencia de este alineamiento? • ¿Cómo evalúan los factores y la gestión de riesgos para que estén alineadas con la tolerancia del riesgo y las capacidades de la empresa para las pérdidas? ¿Tienen evidencia de esta evaluación? • ¿Tienen definido las habilidades y el personal para la gestión de riesgos? ¿Tienen evidencia de esta definición? ¿En cuál documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
EDM03.02. Dirigir la gestión de riesgos	• ¿Tienen un procedimiento que direccionan la estrategia de riesgos, los planes de comunicación de riesgos, y la implementación de mecanismos de respuesta al cambio de riesgos? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Tienen un protocolo de comunicación de riesgos que aseguran que los riesgos, oportunidades o problemas puedan identificarse y comunicarse por cualquier persona de la empresa a la parte correspondiente? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Tienen definido y documentado las metas y métricas para la gestión de riesgos? ¿En cuál documento? ¿Pueden mostrarlo como evidencia?
EDM03.03. Monitorizar la gestión de riesgos	• ¿Tienen un protocolo o procedimiento para comunicar los problemas de gestión de riesgos a la administración? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? Si no, ¿Cómo lo comunican? ¿Pueden mostrar evidencia de lo anterior? • ¿Cómo supervisan el cumplimiento de la gestión de riesgos, sus metas y métricas de acuerdo con el apetito y tolerancia y los objetivos empresariales? ¿Tienen informes de cumplimiento que puedan evidenciar la supervisión? • ¿Cómo efectúan la revisión del progreso de la empresa de acuerdo con las metas establecidas? ¿Tienen resultados de revisiones que puedan evidenciar la supervisión?

KPMG

APO09: Gestionar los acuerdos de servicio	
Práctica	**Guión de preguntas**
APO09.01. Identificar los servicios de TI	• ¿Cómo identifican las brechas entre los servicios actuales de TI y las actividades que apoyan? ¿Tienen herramientas para la documentación de brecha que evidencie lo anterior? • ¿Cómo analizan las capacidades actuales, las necesidades y la demanda futura relacionadas con los servicios de TI? ¿Tienen evidencia del análisis? • ¿Cada cuánto realizan revisiones periódicas del portafolio de servicios para identificar aquellos obsoletos? ¿Tienen evidencia de dichas supervisiones?
APO09.02. Catalogar los servicios habilitados por TI	• ¿Tienen catálogos de servicios?¿Los tienen publicados? ¿Dónde los publican? • ¿Cómo aseguran que la información de los catálogos de servicios esté completa y actualizada? ¿Tienen evidencia de la actualización? • ¿Tienen un protocolo de comunicación que gestione la comunicación de los catálogos de servicio a la dirección? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
APO09.03. Definir y preparar acuerdos de servicio	• ¿Tienen un procedimiento para realizar acuerdos a nivel de servicio y acuerdos a nivel operativo? (lineamientos, pasos, actividades, comunicaciones, relaciones) ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
APO09.04. Monitorizar y reportar los niveles de servicio	• ¿Cómo monitorean, evalúan e informan el rendimiento de los acuerdos a nivel de servicio? ¿Tienen informes de rendimiento que evidencie lo anterior? • ¿Cómo realizan revisiones para pronosticar tendencias de rendimiento de nivel de servicio?¿Tienen informes de tendencias que evidencie lo anterior? • ¿Tienen planes de acción y remediación para gestionar los problemas de rendimiento? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
APO09.05. Revisar los acuerdos y los contratos de servicio	• ¿Cada cuanto revisan los acuerdos a nivel de servicio vigentes para garantizar su efectividad o actualizarlos para que cumplan con la efectividad pactada? ¿Tienen evidencia que respalde la revisión?

6

KPMG

APO13: Gestionar la seguridad	
Práctica	**Guión de preguntas**
APO13.01. Establecer y mantener un sistema de gestión de seguridad de la información (SGSI)	• ¿Tienen un plan, política o informe que defina el Sistema de Gestión de Seguridad de la Información (SGSI), su alcance (con su declaración de aplicabilidad), limitaciones y alineamiento en torno a las características de la empresa? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Cómo ejecutan las autorizaciones con dirección para la implementación del SGSI? ¿Tienen evidencias de las autorizaciones? • ¿Tienen un protocolo o procedimiento de comunicación de la estrategia de SGSI, sus roles y las responsabilidades? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
APO13.02. Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad	• ¿Formulan un plan de tratamiento de riesgos de seguridad de la información alineado con los objetivos estratégicos de la empresa, así como componentes de soluciones, tratamientos de riesgos y aportes de diseño y gestión de riesgos de seguridad de la información? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Qué programas o acciones implementan para promover la concienciación de la seguridad y privacidad de la información? ¿Tienen evidencia de estos programas o acciones? • ¿Ejecutan la planificación, diseño, implementación y monitoreo de procedimientos de seguridad para la prevención y detección de eventos de seguridad de forma integrada? ¿Tienen evidencia de dichos procedimientos integrados? • ¿Tienen métricas para medir la eficacia de las prácticas de gestión? ¿Cuáles son las métricas? ¿Dónde se encuentran documentadas? ¿Puede mostrar evidencia de las métricas?
APO13.03. Monitorizar y revisar el sistema de gestión de seguridad de la información (SGSI)	• ¿Cada cuánto llevan a cabo revisiones o auditorías para evaluar el cumplimiento de SGSI para asegurar su eficacia y alcance? ¿Tienen informes de resultados que evidencie las revisiones? • ¿Documentan aquellas acciones o eventos que podrían tener un impacto en el SGSI? ¿En cuál documento?¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?

KPMG

BAI06: Gestionar los cambios de TI	
Práctica	**Guión de preguntas**
BAI06.01. Evaluar, priorizar y autorizar solicitudes de cambio	• ¿Qué utilizan para realizar solicitudes formales para permitir a los usuarios notificar los cambios.? ¿Dónde se encuentra? ¿Puede mostrar evidencia? • ¿Realizan la categorización y priorización de los cambios de acuerdo con los requisitos técnicos y de negocio? ¿Dónde lo documentan? ¿Pueden mostrarlo como evidencia? • ¿Cómo efectúan las aprobaciones de los cambios aquellos involucrados según corresponda? ¿Tienen evidencia de las aprobaciones? • ¿Tienen documentada la planificación y programación de los cambios de TI, considerando el impacto en los procesos de negocio, infraestructura, sistemas, aplicaciones, proveedores, y demás elementos relacionados con los cambios ? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
BAI06.02. Gestionar cambios de emergencia	• ¿Tienen procedimientos documentados para definir, declarar, evaluar, aprobar, autorizar y registrar cambios de emergencia? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Tienen procedimientos para verificar y monitorear que todos los cambios de emergencia se autoricen, documenten y revoquen? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Realizan revisiones posteriores a la implementación de las acciones para el cambio con los interesados ? ¿Tienen informes de revisiones que evidencien lo anterior?
BAI06.03. Hacer seguimiento e informar sobre cambios de estado	• ¿Tienen procedimientos para gestionar la ejecución del monitoreo, categorización (rechazado, aprobado, cerrado, etc.) y evaluaciones del estado de los cambios? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
BAI06.04. Cerrar y documentar los cambios.	• ¿Realizan la documentación de los cambios en los procedimientos necesarios? ¿Estos cambios en la documentación son sometidos a revisión? ¿Cual es el documento? ¿Dónde se encuentra? ¿Tienen la documentación y evidencias de revisión respectivas?

8

KPMG

BAI09: Gestiona los activos	
Práctica	**Guión de preguntas**
BAI09.01. Identificar y registrar los activos actuales.	• ¿Llevan un registro de los activos, su estado actual, requisitos legales, regulatorios o contractuales y propósito? ¿Tienen evidencia del registro? • ¿Efectúan revisiones de contabilidad, comprobación y conciliación de los activos? ¿Tienen resultados de revisiones que evidencien lo anterior? • ¿Realizan comprobaciones para verificar la efectividad del valor y propósito de los activos?¿Tienen resultados de comprobaciones que evidencia lo anterior?
BAI09.02. Gestionar los activos críticos	• ¿Tienen documentado los activos críticos y su riesgo de fallo? ¿Dónde los documentos? ¿Cual es el nombre del documento?¿Pueden mostrar evidencia de lo anterior? • ¿Cómo llevan a cabo la comunicación y calendarización de las actividades de mantenimiento para los usuarios afectados? ¿Tienen evidencia de protocolos de comunicación y cronogramas de las actividades de mantenimiento? • ¿Documentan planes de mantenimiento preventivo de los activos de forma regular? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Establecen acuerdos de servicio para el mantenimiento que incluya acceso de terceros a las instalaciones de TI de la empresa? ¿Pueden mostrar evidencia del acceso a terceros dentro de los acuerdos de servicio? • ¿Cómo garantizan que los accesos remotos y de perfiles de usuarios sean activos únicamente cuando es necesario? ¿Tienen evidencia de revisiones después del tiempo pactado de estos accesos y perfiles? • ¿Cómo llevan a cabo el monitoreo de los activos críticos y las acciones correctivas necesarias? ¿Tienen resultados del monitoreo que evidencie lo anterior?
BAI09.03. Gestionar el ciclo de vida del activo	• ¿Tienen un procedimiento sobre el ciclo de vida de los activos, que documente las acciones para las solicitudes aprobadas de los activos, el registro de los pagos, aprobaciones de los pagos, asignaciones, reasignaciones e implementación de los activos, planificaciones, autorizaciones e implementación de la retirada de los activos, y disponibilidad de los activos? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
BAI09.04. Optimizar el valor de los activos	• ¿Efectúan las revisiones de los activos, en términos de costes de mantenimiento, garantías, relación calidad-precio, estado? ¿Tiene informes de revisión de activos que evidencia lo anterior?

9

KPMG

	• ¿Documentan los resultados para identificar oportunidades de mejora y estandarización así como identificar aquellos activos con posibilidad de eliminación o sustitución? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
BAI09.05. Gestionar las licencias	• ¿Llevan un registro de las licencias adquiridas con sus acuerdos asociados? ¿Cuál es el nombre del registro? ¿Dónde se encuentra? ¿Pueden mostrarlo comoevidencia? • ¿Realizan auditorías para evaluar las licencias instaladas? ¿Tienen resultados de auditorías que evidencien lo anterior? • ¿Documentan por medio de planes o procedimiento la gestión de las licencias instaladas de acuerdo con las licencias instaladas versus las licencias adquiridas? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Realizan análisis para evaluar la rentabilidad de la actualización de los productos y licencias asociadas? ¿Tienen los resultados del análisis para evidenciar lo anterior?

KPMG

DSS02:Gestionar las peticiones y los incidentes de servicio	
Práctica	**Guión de preguntas**
DSS02.01. Definir esquemas de clasificación para incidentes y peticiones de servicio	• ¿Tienen esquemas y modelos de clasificación de las peticiones de servicio e incidentes? ¿Cuál es el nombre? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Tienen establecidas y definidas las fuentes de conocimiento sobre incidentes y solicitudes, así como las reglas y los procedimientos para la escalación de los incidentes? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
DSS02.02. Registrar, clasificar y priorizar las peticiones e incidentes	• ¿Llevan a cabo un registro de las solicitudes e incidentes de servicio, que permita la clasificación y priorización de estos de acuerdo con el impacto y urgencia del negocio? ¿Dónde las registras? ¿Cuál es el nombre del registro? ¿Pueden mostrarlo como evidencia?
DSS02.03. Verificar, aprobar y resolver peticiones de servicio	• ¿Tienen definidos el flujo y el proceso para la gestión de las solicitudes de servicio? ¿Dónde los documentas? ¿Cuál es nombre del documento? ¿Pueden mostrarlo como evidencia?
DSS02.04. Investigar, diagnosticar y asignar incidentes	• ¿Tiene un procedimiento para diagnosticar y asignar incidentes, considerando sus síntomas, problemas relacionados o errores conocidos, asignación a personal especial, etc.? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
DSS02.05. Resolver y recuperarse de los incidentes	• ¿Tienen documentado la resolución de incidentes en términos de medidas correctivas, workarounds, evaluaciones de la resolución ? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
DSS02.06. Cerrar las peticiones de servicio y los incidentes	• ¿Cómo realizan la confirmación del usuarios del cumplimiento de su solicitud, y posterior el cierre del incidente? ¿Tienen evidencia de dicha confirmación?
DSS02.07. Hacer seguimiento al estado y producir informes	• ¿Realizan supervisiones y seguimientos sobre los escalamientos y resoluciones de los incidentes, partes interesadas involucradas, tendencias o patrones de problemas? ¿Tienen informes de seguimiento que evidencien lo anterior? • ¿Cómo utilizan la información resultado de las revisiones como insumos para la mejora continua de la empresa? ¿Tienen evidencia sobre lo anterior?

11

KPMG

DSS03: Gestionar los problemas	
Práctica	**Guión de preguntas**
DSS03.01. Identificar y clasificar los problemas	• ¿Tienen un procedimiento o plan sobre la gestión de problemas, el cual identifica los problemas, y define grupos de soporte, clasificaciones, niveles de prioridad, causas raíz, y soluciones para respaldar los problemas? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Cómo comunican el estado de los problemas a los usuarios involucrados? ¿Tienen evidencia de dicha comunicación? • ¿Existe un catálogo de gestión de problemas que informe y registre los problemas identificados? ¿Cual es el nombre del catálogo? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
DSS03.02. Investigar y diagnosticar los problemas	• ¿Cómo identifican y asocian los problemas y sus elementos como errores conocidos? ¿Tienen documentados los errores conocidos? • ¿Realizan y monitorean informes del progreso del problema a lo largo de su ciclo de vida? ¿Tienen el informe del problema que evidencie lo anterior?
DSS03.03. Presentar los errores conocidos	• ¿Documentan las soluciones ante los problemas de errores conocidos conforme a costos, impacto del negocio, urgencia? ¿Tienen evidencia de la documentación requerida?
DSS03.04. Resolver y cerrar los problemas	• ¿Tienen un procedimiento o registro para cerrar los problemas, el cual calendarice el cierre de los problemas y las acciones tomadas en cuenta para la resolución? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Realizan informes de revisión y monitoreo sobre el proceso de resolución de problemas, su impacto, errores conocidos, y resolución satisfactoria? ¿Tienen los resultados de la revisión que evidencie lo anterior? • ¿Tienen un protocolo para comunicar el cierre de problemas a los usuarios afectados y el conocimiento aprendido de la resolución del problema? ¿Cual es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
DSS03.05. Realizar una gestión proactiva de los problemas	• ¿Documentan y comunican la gestión de los problemas considerando las soluciones sostenibles halladas para estos? ¿Tienen evidencia de dicha documentación y comunicación? • ¿Cómo llevan a cabo las reuniones con los dueños y gestores de los problemas para comentar los problemas y cambios a futuro ? ¿Tienen evidencia de las reuniones mencionadas? • ¿Llevan a cabo informes de supervisión de costos totales de problemas, la resolución realizada en términos de requisitos de negocio, SLAs, seguimiento de tendencias de los problemas?

12

KPMG

	¿Tienen evidencia de los informes de supervisión y sus resultados que evidencia lo anterior?

MEA02: Gestionar el sistema de control interno	
Práctica	**Guion de preguntas**
MEA02.01. Supervisar los controles internos	• ¿Realizan la supervisión, mantenimiento y evaluación del control interno tomando en cuenta los límites, estado de los proveedores, estándares de gobierno, marcos, prácticas de la industria, evaluaciones independientes como auditorías, cambios continuos del negocio? ¿Tienen evidencia de la supervisión del control interno? • ¿Cómo aseguran que se comunique, priorice, analice e implementen acciones correctivas a las excepciones del control interno? ¿Tienen evidencia del aseguramiento de la comunicación?
MEA02.02. Revisar la eficacia de los controles del proceso de negocio.	• ¿Tienen un procedimiento para revisar la eficacia de los controles de los procesos de negocio, que se identifique los controles clave, estrategias adecuadas de validación de controles, evidencias de eficacia de los controles, formas de obtener información según los criterios de calidad? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia?
MEA02.03. Realizar autoevaluaciones de control	• ¿Tienen un plan que defina la estrategia para realizar autoevaluaciones de control, el cual defina el criterio y alcance para realizar autoevaluaciones, la comunicación, frecuencia, responsabilidades, descripción de las revisiones de la autoevaluación? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Realizan comparaciones de las autoevaluaciones con los estándares y buenas prácticas de la industria, e informan los resultados para tomar acciones correctivas? ¿Tienen evidencia de resultados de las comparaciones?
MEA02.04. Identificar e informar las deficiencias de control	• ¿Tienen un procedimiento para las excepciones de control, el cual defina el escalamiento, el riesgo empresarial relacionado, responsabilidad de la resoluciones, formas de comunicación de las excepciones, estado? ¿Cuál es el documento? ¿Dónde se encuentra? ¿Pueden mostrarlo como evidencia? • ¿Documentan las acciones correctivas identificadas de las excepciones y deficiencias del control? ¿Tienen los informes que documentan las acciones correctivas que evidencie lo anterior?

KPMG

MEA03: Gestionar el cumplimiento de los requisitos externos	
Práctica	**Guión de preguntas**
MEA03.01. Identificar los requisitos externos de cumplimiento	• ¿Mantienen un registro de los requisitos externos de cumplimiento requeridos, tales como los legales, regulatorios, contractuales, con su impacto a nivel de TI, proveedores de servicio y socios comerciales de negocio, consecuencias de su incumplimiento y acciones requeridas ? ¿Tienen evidencia de dicho registro? • ¿Cómo obtienen asesoría para los cambios en la legislación, regulaciones y estándares vigentes? ¿Tienen evidencia de la asesoría brindada?
MEA03.02. Optimizar la respuesta a los requisitos externos	• ¿Actualizan las políticas, principios, estándares, procedimientos y metodologías para garantizar el cumplimiento de los requisitos? ¿Tienen evidencia de dicha actualización ? • ¿Cómo comunican las modificaciones o los nuevos requisitos al personal? ¿Tienen evidencia de dicha comunicación?
MEA03.03. Confirmar el cumplimiento externo	• ¿Cada cuánto realizan evaluaciones sobre las políticas, estándares, procedimiento y metodologías, actividades de negocio y de TI, patrones de fallo de cumplimientos, para garantizar el cumplimiento de los requisitos legales y regulatorios? ¿Tienen evidencia de dicha evaluación? • ¿Documentan las brechas identificadas de la evaluación y mejoran los documentos necesarios tomando como base la revisión y las lecciones aprendidas? ¿Dónde lo documentan?¿Cuál es nombre del documento? ¿Pueden mostrarlo como evidencia?
MEA03.04. Obtener aseguramiento de cumplimiento externo	• ¿Cada cuánto realizan las revisiones internas y externas para evaluar los niveles de cumplimiento de las políticas, requisitos legales, regulatorios y contractuales, y las declaraciones de cumplimiento de proveedores y socios? ¿Tienen evidencia sobre el informe documentado? • ¿Documentan los problemas y causa raíz del incumplimiento identificado, y los comunican a los involucrados? ¿Tienen evidencia del informe de problemas y causas ?

14

KPMG

Guión para la documentación de los riesgos de auditoría

Esta sección es un guión para definir los apartados establecidos sobre los riesgos dentro de la documentación de las fichas de auditoría.

Especificaciones generales:

- Los cuadros siguientes contienen los posibles riesgos que pueden materializarse en cada proceso de COBIT 2019. Cada riesgo es documentado de acuerdo con la estructura preestablecida: Condición, Causa, Impacto. Asimismo, para cada riesgo se plantea una recomendación.
- El impacto de los riesgos debe definirse de acuerdo con los siguientes tipos:

Tipo de impacto	Descripción
Estratégico	El impacto estratégico de los riesgos está relacionado con todas aquellas actividades que puedan afectar los objetivos y la estrategias de la organización.
Operativo	El impacto operativo está asociado con aquellas actividades que afectan el curso normal de los procesos de negocio de una organización, imposibilitando una parte o la totalidad de estos.
Económico	El impacto económico referencia a todas aquellas actividades que impactan las operaciones financiera de una organización, tales como créditos, pagos, deudas, cobros, inversiones, gastos, utilidades, entre otros.
Legal	El impacto legal hace referencia a las actividades que afectan las operaciones legales tales como el cumplimiento de políticas externas, reglamentos y relaciones contractuales.

Nota: Es importante aclarar que cada organización auditada es diferente, por ende los riesgos deben definirse de acuerdo con el contexto de cada cliente. Esta serie de riesgos son un guión que oriente al auditor sobre qué tipos de riesgos puede establecer en la documentación correspondiente, alineado a la auditoria propia de este cliente.

15

KPMG

Listado de riesgos por cada proceso de COBIT 2019

EDM01. Asegurar el establecimiento y el mantenimiento del marco de gobierno.			
Condición	**Causa**	**Impacto**	**Recomendación**
Desconocimiento de los niveles de autoridad	No hay niveles definidos para delegar autoridad y responsabilidades para el gobierno de gestión y las decisiones de TI.	Estratégico	Establecer niveles de autoridad, con sus respectivos límites y responsabilidades para gestionar el sistema de gobierno.
Los principios del gobierno de gestión y la toma de decisiones no están alineados con los factores internos o externos de la empresa	No se identificaron o analizaron los factores internos y externos y su aplicación dentro del gobierno de TI de la empresa antes de definir los principios y toma de decisiones.	Estratégico	Identificar todos los factores internos y externos que tengan implicación en el gobierno de TI. Analizarlos y ajustar los principios para que cumplan con estos.
Problemas de comunicación del gobierno de TI	Canales ambiguos de comunicación del gobierno de TI. Inexistencia de un plan de comunicación.	Operativo	Formular dentro de un plan o procedimiento los canales de comunicación del gobierno de TI, los interesados respectivos y la información a comunicar.

KPMG

EDM03. Asegurar la optimización del riesgo			
Condición	**Causa**	**Impacto**	**Recomendación**
La organización no puede soportar las actividades de gestión de riesgos	No se evalúa el apetito y tolerancia al riesgo, así como la capacidad de la organización en el planteamiento de actividades de gestión de riesgos.	Operativo	Analizar el apetito y tolerancia de riesgo, y la capacidad de la empresa, y alinear las actividades de gestión para que cumplan con estos aspectos.
Fallas constantes en la dirección de la gestión de riesgos	Ausencia de una política para la gestión de riesgos	Operativo	Definir una política de gestión de riesgos que involucre la comunicación, el proceso, los objetivos, los mecanismos, metas y métricas para la gestión de riesgos.
Escazas supervisiones o monitoreos de la gestión de riesgos	No hay periodos definidos para supervisar, revisar o monitorear la gestión de riesgos.	Operativo Estratégico	Establecer periodos de monitoreo de la gestión de riesgos con los involucrados que hacen parte de esta.

KPMG

APO09. Gestionar los acuerdos de servicio			
Condición	Causa	Impacto	Recomendación
Estándares de servicios no cumplen con los requerimientos del negocio	Servicios obsoletos. Los servicios actuales no apoyan las actividades empresariales.	Estratégico	Evaluar y estudiar los servicios de acuerdo con la demanda, capacidad y actividades de la empresa
Existencia de servicios obsoletos dentro del catálogo de servicios	Catálogos de servicios no actualizados ni alineados con la estrategia de la organización.	Operativo	Revisar los catálogos de servicios actuales para actualizar sus servicios con respecto al contexto, objetivos y estrategia de la organización.
SLAs no cumplen con las expectativas pactadas sobre el rendimiento, operación y calidad de los servicios	No se realizan evaluaciones o revisiones de los acuerdos de servicio para verificar su actualización y cumplimiento.	Estratégico	Definir periodos de revisión para evaluar el rendimiento de los acuerdos a nivel de servicio.

18

KPMG

APO13. Gestionar la seguridad			
Condición	**Causa**	**Impacto**	**Recomendación**
Desalineamiento del alcance y los límites del SGSI con el negocio	No se define un SGSI de acuerdo a la política empresarial, características, activos, y tecnología de la empresa.	Estratégico	Evaluar las actividades del alcance del SGSI con las características, factores y políticas de la empresa para garantizar su cumplimiento.
Fallos en el tratamiento de los riesgos de la seguridad de la información	-Inexistencia de un plan de tratamiento de riesgos. -Procedimientos, propuestas, o casos de negocio no alineados a los objetivo estratégicos.	Operativo	Definir un plan de tratamiento de riesgos robusto que involucre propuestas, procedimientos, casos de negocio, prácticas y soluciones alineadas a los objetivos de la empresa.
No existe una planificación y documentación sobre el monitoreo y revisión del SGSI	-No existen revisiones regulares para validar el cumplimiento del SGSI. -No se documentan informes de evaluación de los SGSI.	Operativo Estratégico	-Fijar periodos de forma regular para monitorear y revisar el SGSI. -Documentar hallazgos y brindar recomendaciones.

KPMG

BAI06. Gestionar los cambios de TI			
Condición	**Causa**	**Impacto**	**Recomendación**
El proceso de gestión de solicitudes de cambio es desorganizado	No existe un único plan o procedimiento para la gestión de cambios.	Operativo	Definir un plan o procedimiento para la gestión de cambios considerando los requisitos técnicos y de negocio de la empresa.
Manejo inadecuado de los cambios de emergencia	No existe una definición y procedimiento para la gestión de cambios de emergencia.	Operativo	Establecer las actividades respectivas para los cambios de emergencia según los requisitos técnicos y de negocio de la empresa.
Desconocimiento de revisiones y actualizaciones en la documentación relacionada con la gestión de cambios	No hay periodos definidos para revisar el estado de los cambios. La documentación desactualizada.	Operativo Estratégico	-Fijar periodos de revisión de los cambios y de actualización de documentación relacionada a los cambios.

KPMG

BAI09. Gestionar los activos			
Condición	**Causa**	**Impacto**	**Recomendación**
Fallas en la organización de los activos	No existe un control de los activos actuales y sus requisitos de acuerdo al negocio	Operativo Económico	Llevar un registro de los activos con sus características y requisitos de acuerdo al negocio.
Los activos no cumplen con los niveles de optimización, o están obsoletos con respecto a la estrategia de la organización	No se efectúan revisiones periódicas de los activos.	Estratégico Económico	Definir revisiones periódicas sobre la base de activos, sus costes de mantenimiento, garantías, capacidades, cumplimiento en el negocio.
Gestión inadecuada de las licencias	No existe un registro de las licencias o un plan de acción para gestionarlas.	Operativo	Registrar las licencias actuales y formular un plan de acción que permita llevar un control y comparación de estas.

KPMG

DSS02. Gestionar las peticiones y los incidentes de servicio			
Condición	Causa	Impacto	Recomendación
Ambigüedad en la gestión de las peticiones y los incidentes de servicio	No hay definición de criterios, priorización, reglas de escalamiento, esquemas o modelos de clasificación de los incidentes.	Operativo	Definir los esquemas de priorización, modelos de clasificación, reglas o procedimientos de los incidentes de acuerdo con el negocio.
Retrasos en la resolución de incidentes	Los incidentes no son registrados, aprobados, soluciones y cerrados apropiadamente.	Operativo	Definir las acciones para registrar, aprobar, solucionar y cerrar apropiadamente los incidentes.
Desconocimiento sobre el estado de cumplimiento de los incidentes	No hay revisiones periódicas para el seguimiento de los estados de los incidentes.	Operativo Estratégico	Fijar periodos de evaluación sobre los estados de los incidentes, y utilizar los resultados como insumos para la mejora continua de la organización.

KPMG

DSS03. Gestionar los problemas			
Condición	Causa	Impacto	Recomendación
Ambigüedad en la gestión de problemas.	No existe un esquema para la clasificación de problemas, sus niveles de prioridad, estado, catalogos de gestión.	Operativo	Definir la clasificación de problemas, prioridad, estado, catalogos de gestión, etc.
Retrasos en la resolución de errores conocidos	No existe un registro de los errores conocidos, sus procedimiento, acciones correctivas, canales de comunicación.	Operativo	Llevar un registro de los problemas conocidos con sus procedimientos, acciones correctivas y canales de comunicación.
Fallas en el desarrollo de la retroalimentación de los problemas	No hay reuniones periódicas para comentar y documentar los cambios, soluciones, incidentes, actividades relacionadas con los problemas identificados.	Operativo Estratégico	-Realizar reuniones periódicas con las partes interesadas del problema para identificar sus causas, acciones correctivas, incidencias, cambios en el negocio. -Documentar la retroalimentación de la reunión para favorecer la toma de decisiones.

KPMG

MEA02. Gestionar el sistema de control interno			
Condición	Causa	Impacto	Recomendación
Resultados erróneos en la supervisión de los controles internos	No hay una evaluación de los límites del control interno, su estado, actividades de supervisión y evaluación, excepciones, según las políticas y objetivos del negocio.	Estratégico	Evaluar los límites, estado, actividades, políticas, supervisiones y evaluaciones de los controles internos según los criterios, características y estado del negocio.
Desconocimiento de la efectividad de los controles internos	-No hay revisiones de efectividad o autoevaluaciones de control interno.	Operativo	-Establecer revisiones periódicas para validar la efectividad de los controles. -Definir una estrategia de autoevaluación de los controles que incluya la frecuencia de realización, responsables, y documentación de hallazgos.
Desorganización para identificar y gestionar las deficiencias de los controles	-No se lleva un registro de las deficiencias de los controles, de acuerdo con la estrategia de la organización.	Operativo Estratégico	-Definir procedimientos para la gestión deficiencias del control interno que detalle las excepciones del control, su seguimiento y analisis, responsables involucrados, y documentación relacionada.

KPMG

MEA03. Gestionar el cumplimiento de los requisitos externos			
Condición	**Causa**	**Impacto**	**Recomendación**
Requisitos externos desactualizados	No se lleva un control de todos los posibles requisitos externos así como su impacto, consecuencias de incumplimiento.	Legal	-Establecer responsables que se encarguen de identificar todos los posibles requisitos externos y asigne sus impacto, consecuencias según las actividades del negocio.
Errores de comunicación de los requisitos externos	No existen canales de comunicación para los requisitos externos.	Operativo	Definir canales de comunicación para informar los requisitos externos al personal.
Incumplimiento de los requisitos externos	-No hay evaluaciones ni revisiones periódicas del cumplimiento de los requisitos externos.	Legal Estratégico	-Establecer evaluaciones o revisiones de los requisitos externos y documentar los hallazgos de cumplimiento.

25

KPMG

Guión para el desarrollo del cronograma

Esta sección es un guión para el desarrollo del cronograma de auditoría.

Especificaciones generales:

- El cronograma debe ser realizado en la herramienta Microsoft Project.
- El siguiente cuadro refleja un guión para establecer el cronograma de auditoría, donde se hace un desglose de las actividades mínimas a contener con un aproximado de las duraciones de estas.
- Es importante aclarar que cada cronograma de auditoría debe ser desarrollado de acuerdo al criterio y contexto del cliente auditado. Este cronograma es un guión para establecer aquellas actividades base que deben establecerse, sin embargo, puede estar sujetos a cambios para adaptarse al cliente.

Guión de cronograma:

Para el guión del cronograma, se establece un ejemplo para una auditoría que dura aproximadamente 80 días. Se incluyen las actividades más comunes para la ejecución de una auditoría, las cuales van de la mano con lo pactado en el proceso de auditoría.

Las actividades incluyen la reunión de Kickoff, la solicitud de requerimientos con la matriz, la recolección y análisis de estos, la evaluación de cada proceso con sus espacios para la reunión de entendimiento y consultas adicionales, la preparación de los productos de auditoría, y presentaciones finales.

KPMG

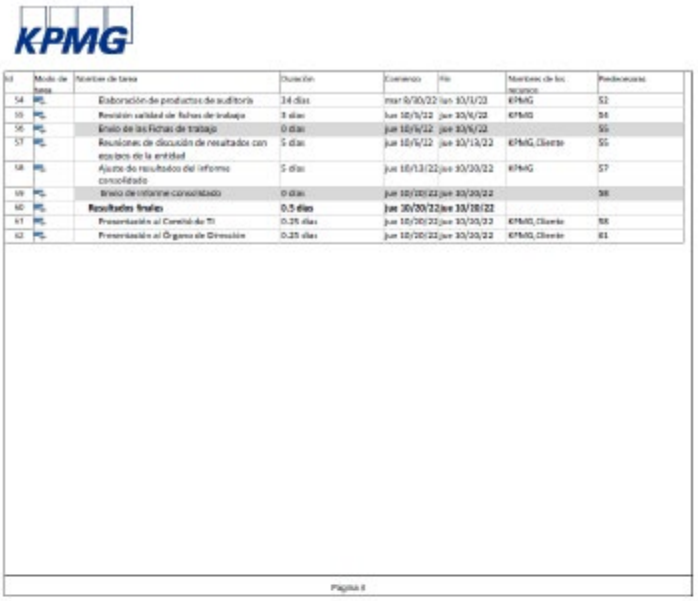
Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
1		**(Nombre Empresa) - Ejecución de la Auditoría Regulatoria 14-17**	**30 días**	**vie 7/1/22**	**jue 10/30/22**		
2		**Ejecución del servicio de auditoría**	**82.5 días**	**vie 7/1/22**	**mar 8/30/22**		
3		Reunión Kickoff	0.5 días	vie 7/1/22	vie 7/1/22	KPMG,Cliente	
4		Solicitud y recolección de requerimientos preliminares	4 días	vie 7/1/22	jue 7/7/22	KPMG,Cliente	3
5		Consultas o aclaraciones sobre los requerimientos	1 día	jue 7/7/22	vie 7/8/22	KPMG,Cliente	4
6		Revisión de requerimientos preliminares	5 días	vie 7/8/22	vie 7/15/22	KPMG	5
7		**Evaluación de procesos**	**32 días**	**vie 7/15/22**	**mar 8/30/22**		
8		**Dominio: Evaluar, Dirigir y Monitorizar (EDM)**	**6 días**	**vie 7/15/22**	**lun 7/25/22**		
9		**EDM01. Asegurar el establecimiento y el mantenimiento del marco de**	**3 días**	**vie 7/15/22**	**mié 7/20/22**		
10		Reunión de entendimiento	0.5 días	vie 7/15/22	vie 7/15/22	KPMG,Cliente	6
11		Consultas o aclaraciones del proceso	0.5 días	lun 7/18/22	lun 7/18/22	KPMG,Cliente	10
12		Revisión y documentación de la ficha del proceso	2 días	lun 7/18/22	mié 7/20/22	KPMG	11
13		**EDM02. Asegurar la optimización del v**	**3 días**	**mié 7/20/22**	**lun 7/25/22**		
14		Reunión de entendimiento	0.5 días	mié 7/20/22	mié 7/20/22	KPMG,Cliente	12
15		Consultas o aclaraciones del proceso	0.5 días	jue 7/21/22	jue 7/21/22	KPMG,Cliente	14
16		Revisión y documentación de la ficha del proceso	2 días	jue 7/21/22	lun 7/25/22	KPMG	15
17		**Dominio: Alinear, Planificar y Organizar (APO)**	**18 días**	**lun 7/25/22**	**jue 8/18/22**		
18		**APO09. Gestionar los acuerdos de servic**	**4 días**	**lun 7/25/22**	**vie 7/29/22**		
19		Reunión de entendimiento	0.5 días	lun 7/25/22	lun 7/25/22	KPMG,Cliente	16
20		Consultas o aclaraciones del proceso	0.5 días	mar 7/26/22	mar 7/26/22	KPMG,Cliente	19
21		Revisión y documentación de la ficha del proceso	3 días	mar 7/26/22	vie 7/29/22	KPMG	20
22		**APO13. Gestionar la seguridad**	**4 días**	**vie 7/29/22**	**jue 8/4/22**		
23		Reunión de entendimiento	0.5 días	vie 7/29/22	vie 7/29/22	KPMG,Cliente	21
24		Consultas o aclaraciones del proceso	0.5 días	lun 8/1/22	lun 8/1/22	KPMG,Cliente	23
25		Revisión y documentación de la ficha del proceso	5 días	lun 8/1/22	jue 8/4/22	KPMG	24
26		**Dominio: Construir, Adquirir e Implementar (BAI)**	**6 días**	**jue 8/4/22**	**vie 8/12/22**		
27		**BAI06. Gestionar los cambios de TI**	**3 días**	**jue 8/4/22**	**mar 8/9/22**		

Página 1

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
28		Reunión de entendimiento	3.5 días	jue 8/4/22	jue 8/4/22	KPMG,Cliente	25
29		Consultas o aclaraciones del proceso	3.5 días	vie 8/5/22	vie 8/5/22	KPMG,Cliente	28
30		Revisión y documentación de la ficha del proceso	2 días	vie 8/5/22	mar 8/9/22	KPMG	29
31		**BAI09. Gestionar los activos**	**3 días**	**mar 8/9/22**	**vie 8/12/22**		
32		Reunión de entendimiento	3.5 días	mar 8/9/22	mar 8/9/22	KPMG,Cliente	30
33		Consultas o aclaraciones del proceso	3.5 días	mié 8/10/22	mié 8/10/22	KPMG,Cliente	32
34		Revisión y documentación de la ficha del proceso	2 días	mié 8/10/22	vie 8/12/22	KPMG	33
35		**Dominio: Entregar, Dar Servicio y Soporte**	**5 días**	**vie 8/12/22**	**lun 8/22/22**		
36		**DSS02. Gestionar las peticiones y los incidentes de servicio**	**3 días**	**vie 8/12/22**	**mié 8/17/22**		
37		Reunión de entendimiento	3.5 días	vie 8/12/22	vie 8/12/22	KPMG,Cliente	34
38		Consultas o aclaraciones del proceso	3.5 días	lun 8/15/22	lun 8/15/22	KPMG,Cliente	37
39		Revisión y documentación de la ficha del proceso	2 días	lun 8/15/22	mié 8/17/22	KPMG	38
40		**DSS03. Gestionar los problemas**	**3 días**	**mié 8/17/22**	**lun 8/22/22**		
41		Reunión de entendimiento	3.5 días	mié 8/17/22	mié 8/17/22	KPMG,Cliente	39
42		Consultas o aclaraciones del proceso	3.5 días	jue 8/18/22	jue 8/18/22	KPMG,Cliente	41
43		Revisión y documentación de la ficha del proceso	2 días	jue 8/18/22	lun 8/22/22	KPMG	42
44		**Dominio: Monitorizar, Evaluar y Valorar**	**5 días**	**lun 8/12/22**	**mar 8/30/22**		
45		**MEA02. Gestionar el sistema de control interno**	**3 días**	**lun 8/12/22**	**jue 8/25/22**		
46		Reunión de entendimiento	3.5 días	lun 8/22/22	lun 8/22/22	KPMG,Cliente	43
47		Consultas o aclaraciones del proceso	3.5 días	mar 8/23/22	mar 8/23/22	KPMG,Cliente	46
48		Revisión y documentación de la ficha del proceso	2 días	mar 8/23/22	jue 8/25/22	KPMG	47
49		**MEA03. Gestionar el cumplimiento de los requisitos externos**	**3 días**	**jue 8/25/22**	**mar 8/30/22**		
50		Reunión de entendimiento	3.5 días	jue 8/25/22	jue 8/25/22	KPMG,Cliente	48
51		Consultas o aclaraciones del proceso	3.5 días	vie 8/26/22	vie 8/26/22	KPMG,Cliente	50
52		Revisión y documentación de la ficha del proceso	2 días	vie 8/26/22	mar 8/30/22	KPMG	51
53		**Preparación de entregables y revisión por parte de la entidad**	**37 días**	**mar 6/28/22**	**jue 10/20/22**		

Página 2

28



Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
54		Elaboración de productos de auditoría	14 días	mar 9/30/22	lun 10/17/22	KPMG	52
55		Revisión calidad de fichas de trabajo	3 días	lun 10/3/22	jue 10/6/22	KPMG	54
56		Envío de las Fichas de trabajo	0 días	jue 10/6/22	jue 10/6/22		55
57		Reuniones de discusión de resultados con equipo de la entidad	5 días	jue 10/6/22	jue 10/13/22	KPMG,Cliente	55
58		Ajuste de resultados del informe consolidado	5 días	jue 10/13/22	jue 10/20/22	KPMG	57
59		Envío de informe consolidado	0 días	jue 10/20/22	jue 10/20/22		58
60		**Resultados finales**	**0.5 días**	**jue 10/20/22**	**jue 10/20/22**		
61		Presentación al Comité de TI	0.25 días	jue 10/20/22	jue 10/20/22	KPMG,Cliente	58
62		Presentación al Órgano de Dirección	0.25 días	jue 10/20/22	jue 10/20/22	KPMG,Cliente	61

Página 8

29

Visualización del cronograma:

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
1		**[Nombre Empresa] - Ejecución de la Auditoría Regulatoria 14-17**	**80 días**	**vie 7/1/22**	**jue 10/20/22**		
2		**Ejecución del servicio de auditoría**	**42.5 días**	**vie 7/1/22**	**mar 8/30/22**		
3		Reunión Kickoff	0.5 días	vie 7/1/22	vie 7/1/22	KPMG,Cliente	
4		Solicitud y recolección de requerimientos preliminares	4 días	vie 7/1/22	jue 7/7/22	KPMG,Cliente	3
5		Consultas o aclaraciones sobre los requerimientos	1 día	jue 7/7/22	vie 7/8/22	KPMG,Cliente	4
6		Revisión de requerimientos preliminares	5 días	vie 7/8/22	vie 7/15/22	KPMG	5
7		**Evaluación de procesos**	**32 días**	**vie 7/15/22**	**mar 8/30/22**		
8		**Dominio: Evaluar, Dirigir y Monitorizar (E**	**6 días**	**vie 7/15/22**	**lun 7/25/22**		
9		**EDM01. Asegurar el establecimiento y el mantenimiento del marco de**	**3 días**	**vie 7/15/22**	**mié 7/20/22**		
10		Reunión de entendimiento	0.5 días	vie 7/15/22	vie 7/15/22	KPMG,Cliente	6
11		Consultas o aclaraciones del proceso	0.5 días	lun 7/18/22	lun 7/18/22	KPMG,Cliente	10
12		Revisión y documentación de la ficha del proceso	2 días	lun 7/18/22	mié 7/20/22	KPMG	11
13		**EDM03. Asegurar la optimización del ri**	**3 días**	**mié 7/20/22**	**lun 7/25/22**		
14		Reunión de entendimiento	0.5 días	mié 7/20/22	mié 7/20/22	KPMG,Cliente	12
15		Consultas o aclaraciones del proceso	0.5 días	jue 7/21/22	jue 7/21/22	KPMG,Cliente	14
16		Revisión y documentación de la ficha del proceso	2 días	jue 7/21/22	lun 7/25/22	KPMG	15
17		**Dominio: Alinear, Planificar y Organizar (A**	**8 días**	**lun 7/25/22**	**jue 8/4/22**		
18		**APO09. Gestionar los acuerdos de servi**	**4 días**	**lun 7/25/22**	**vie 7/29/22**		
19		Reunión de entendimiento	0.5 días	lun 7/25/22	lun 7/25/22	KPMG,Cliente	16
20		Consultas o aclaraciones del proceso	0.5 días	mar 7/26/22	mar 7/26/22	KPMG,Cliente	19
21		Revisión y documentación de la ficha del proceso	3 días	mar 7/26/22	vie 7/29/22	KPMG	20
22		**APO13. Gestionar la seguridad**	**4 días**	**vie 7/29/22**	**jue 8/4/22**		
23		Reunión de entendimiento	0.5 días	vie 7/29/22	vie 7/29/22	KPMG,Cliente	21
24		Consultas o aclaraciones del proceso	0.5 días	lun 8/1/22	lun 8/1/22	KPMG,Cliente	23
25		Revisión y documentación de la ficha del proceso	3 días	lun 8/1/22	jue 8/4/22	KPMG	24
26		**Dominio: Construir, Adquirir e Implementar (BAI)**	**6 días**	**jue 8/4/22**	**vie 8/12/22**		
27		**BAI06. Gestionar los cambios de TI**	**3 días**	**jue 8/4/22**	**mar 8/9/22**		

Página 1

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
28		Reunión de entendimiento	0.5 días	jue 8/4/22	jue 8/4/22	KPMG,Cliente	25
29		Consultas o aclaraciones del proceso	0.5 días	vie 8/5/22	vie 8/5/22	KPMG,Cliente	28
30		Revisión y documentación de la ficha del proceso	2 días	vie 8/5/22	mar 8/9/22	KPMG	29
31		**BAI09. Gestionar los activos**	**3 días**	**mar 8/9/22**	**vie 8/12/22**		
32		Reunión de entendimiento	0.5 días	mar 8/9/22	mar 8/9/22	KPMG,Cliente	30
33		Consultas o aclaraciones del proceso	0.5 días	mié 8/10/22	mié 8/10/22	KPMG,Cliente	32
34		Revisión y documentación de la ficha del proceso	2 días	mié 8/10/22	vie 8/12/22	KPMG	33
35		**Dominio: Entregar, Dar Servicio y Soporte**	**6 días**	**vie 8/12/22**	**lun 8/22/22**		
36		**DSS02. Gestionar las peticiones y los incidentes de servicio**	**3 días**	**vie 8/12/22**	**mié 8/17/22**		
37		Reunión de entendimiento	0.5 días	vie 8/12/22	vie 8/12/22	KPMG,Cliente	34
38		Consultas o aclaraciones del proceso	0.5 días	lun 8/15/22	lun 8/15/22	KPMG,Cliente	37
39		Revisión y documentación de la ficha del proceso	2 días	lun 8/15/22	mié 8/17/22	KPMG	38
40		**DSS03. Gestionar los problemas**	**3 días**	**mié 8/17/22**	**lun 8/22/22**		
41		Reunión de entendimiento	0.5 días	mié 8/17/22	mié 8/17/22	KPMG,Cliente	39
42		Consultas o aclaraciones del proceso	0.5 días	jue 8/18/22	jue 8/18/22	KPMG,Cliente	41
43		Revisión y documentación de la ficha del proceso	2 días	jue 8/18/22	lun 8/22/22	KPMG	42
44		**Dominio: Monitorizar, Evaluar y Valorar (**	**6 días**	**lun 8/22/22**	**mar 8/30/22**		
45		**MEA02. Gestionar el sistema de control interno**	**3 días**	**lun 8/22/22**	**jue 8/25/22**		
46		Reunión de entendimiento	0.5 días	lun 8/22/22	lun 8/22/22	KPMG,Cliente	43
47		Consultas o aclaraciones del proceso	0.5 días	mar 8/23/22	mar 8/23/22	KPMG,Cliente	46
48		Revisión y documentación de la ficha del proceso	2 días	mar 8/23/22	jue 8/25/22	KPMG	47
49		**MEA03. Gestionar el cumplimiento de los requisitos externos**	**3 días**	**jue 8/25/22**	**mar 8/30/22**		
50		Reunión de entendimiento	0.5 días	jue 8/25/22	jue 8/25/22	KPMG,Cliente	48
51		Consultas o aclaraciones del proceso	0.5 días	vie 8/26/22	vie 8/26/22	KPMG,Cliente	50
52		Revisión y documentación de la ficha del proceso	2 días	vie 8/26/22	mar 8/30/22	KPMG	51
53		**Preparación de entregables y revisión por parte de la entidad**	**37 días**	**mar 8/30/22**	**jue 10/20/22**		

Página 2

Id	Modo de tarea	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos	Predecesoras
54		Elaboración de productos de auditoría	24 días	mar 8/30/22	lun 10/3/22	KPMG	52
55		Revisión calidad de fichas de trabajo	3 días	lun 10/3/22	jue 10/6/22	KPMG	54
56		Envio de las Fichas de trabajo	0 días	jue 10/6/22	jue 10/6/22		55
57		Reuniones de discusión de resultados con equipos de la entidad	5 días	jue 10/6/22	jue 10/13/22	KPMG,Cliente	55
58		Ajuste de resultados del informe consolidado	5 días	jue 10/13/22	jue 10/20/22	KPMG	57
59		Envío de informe consolidado	0 días	jue 10/20/22	jue 10/20/22		58
60		**Resultados finales**	**0.5 días**	**jue 10/20/22**	**jue 10/20/22**		
61		Presentación al Comité de TI	0.25 días	jue 10/20/22	jue 10/20/22	KPMG,Cliente	58
62		Presentación al Órgano de Dirección	0.25 días	jue 10/20/22	jue 10/20/22	KPMG,Cliente	61

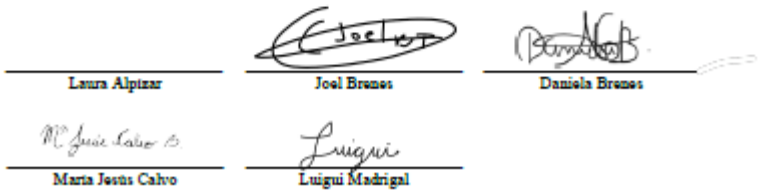
Página 3

Apéndice V. Minutas

Minuta 1

Minuta de Reunión			
Información general			
Reunión N°:	1	**Fecha:**	15-feb-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	De 3:30 pm a 4:30 pm
Objetivo de la reunión:	Bienvenida y organización del curso.		
Participantes	**Presentes:**	• Laura Alpízar • Joel Brenes • Daniela Brenes • María Jesús Calvo • Luigui Madrigal	
	Ausentes:		
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Coordinación de reunión con empresa.	-El estudiante debe agenda la primera reunión con la empresa. -La profesora explica la metodología de las reuniones con la empresa.	Cada estudiante le comunica a la profesora la fecha y hora de la reunión.
02	Elaboración de plantilla del documento	-Realizar una plantilla para el nuevo proyecto.	Queda a criterio del estudiante enviar la plantilla a la profesora para su revisión.
03	Elaboración del Capítulo 1	-Transcribir el anteproyecto según corresponda.	Capítulo 1 debe entregarse según cronograma (semana 4)
Próxima reunión			
Temas a tratar		**Fecha**	**Convocados:**
-		-	-

Firmas:



Laura Alpízar | Joel Brenes | Daniela Brenes

María Jesús Calvo | Luigui Madrigal

Minuta 2

Minuta de Reunión			
Información general			
Reunión N°:	2	**Fecha:**	17-feb-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	1:00 pm a 1:30 pm
Objetivo de la reunión:	Primera reunión entre empresa y profesora tutora		
Participantes	Presentes:	Angélica Chavarría Yeiny Cubero Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Presentación de responsabilidades	Presentación de responsabilidades de la estudiante y la contraparte.	-
02	Presentación del cronograma y evaluación del curso	Visualización del cronograma y los porcentajes de evaluación del TFG.	La estudiante debe agendar las próximas reuniones según cronograma.
03	Evaluaciones por parte de la organización	Especificación y visualización de fechas de las evaluaciones que debe hacer la contraparte.	Yeiny Cubero será la encargada de la firma de las evaluaciones.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
Segunda reunión entre empresa y profesora tutora		Semana del 28/03/2022 al 02/04/2022	Laura Alpízar María Jesús Calvo Angélica Chavarría o Yeiny Cubero

Firmas:

Laura Alpízar Chaves (Tutora)

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 3

Minuta de Reunión			
Información general			
Reunión N°:	3	**Fecha:**	21-feb-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	1:30 pm a 2:00 pm
Objetivo de la reunión:	Delimitación del problema y objetivos del TFG.		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Aclaración del problema y objetivos del TFG.	Se ajusta el problema orientado a las herramientas utilizadas en el proceso de auditoría. Se agrega el objetivo relacionado con tema financiero.	La estudiante realizará los ajustes conversados en el Capítulo 1. La estudiante entregará el capítulo antes del 05 de marzo.
02	Mapa de conceptos del TFG	Después de realizar el capítulo 1, iniciar el mapa de conceptos para el marco teórico.	La estudiante se compromete a enviar el mapa de conceptos ante el 05 de marzo, junto con el capítulo 1.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Minuta 4

Minuta de Reunión			
Información general			
Reunión N°:	4	**Fecha:**	22-feb-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	10:00 am a 10:30 am
Objetivo de la reunión:	Problema y tema oficial del Trabajo Final de Graduación (Capítulo 1)		
Participantes	Presentes:	Angélica Chavarría Yeiny Cubero María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Definición del problema y tema de TFG.	La estudiante le presenta a la empresa, por medio del Capítulo 1, la problemática y el tema delimitado para trabajar el TFG.	La estudiante realizará una actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría, basados en el marco de referencia COBIT 2019.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
Avance del proyecto el cual será presentado en la segunda reunión entre empresa y tutora.		Semana del 28/03/2022 al 02/04/2022	Laura Alpízar María Jesús Calvo Angélica Chavarría o Yeiny Cubero

Firmas:

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 5

Minuta de Reunión			
Información general			
Reunión N°:	5	**Fecha:**	05-mar-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	11:00 am a 11:30 am
Objetivo de la reunión:	Correcciones del Capítulo 1 e instrucciones para el Capítulo 2		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Correcciones del Capítulo 1	Ajuste del organigrama del equipo para involucrar al socio del área.	Corregir el diagrama
02	Corrección del mapa de conceptos	Revisión del mapa de conceptos. La tutora indica el alcance por abarcar en cada concepto.	Iniciar con el marco teórico a partir del mapa de conceptos y entregarlo antes del 19 de marzo.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Minuta 6

Minuta de Reunión			
Información general			
Reunión N°:	6	**Fecha:**	22-mar-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	2:30 pm a 3:00 pm
Objetivo de la reunión:	Revisión del Capítulo 3		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Apartados de la metodología	La estudiante muestra el trabajo realizado de los apartados de la metodología.	La estudiante aplica los ajustes dados por la profesora en la metodología. Lo entregará antes del 02 de abril.
02	Resolución de consultas	La estudiante aclara consultas de los apartados de la metodología con la profesora.	
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Minuta 7

Minuta de Reunión			
Información general			
Reunión N°:	7	**Fecha:**	24-mar-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	2:00 pm a 2:30 pm
Objetivo de la reunión:	Metodología del TFG		
Participantes	Presentes:	Laura Alpízar Joel Brenes Daniela Brenes María Jesús Calvo Luigui Madrigal	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Ejemplo de marco metodológico	Se estudia un TFG para comprender los elementos necesarios del marco metodológico.	La profesora compartirá el ejemplo a los estudiantes por medio de Microsoft Teams.
02	Progreso del TFG	Se comentan las situaciones de los estudiantes (avance para cada estudiante)	Notificar a la profesora si se tienen problemas con la empresa.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Minuta 8

Minuta de Reunión			
Información general			
Reunión N°:	8	**Fecha:**	30-mar-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	12:00 pm a 12:30 pm
Objetivo de la reunión:	Evaluación de presentación para empresa		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Presentación para segunda reunión con organización	La estudiante muestra la presentación para la segunda reunión y la tutora realiza la realimentación necesaria.	La estudiante aplica la realimentación brindada para la reunión del 31 de marzo.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Minuta 9

Minuta de Reunión			
Información general			
Reunión N°:	9	**Fecha:**	31-mar-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	1:00 pm a 1:30 pm
Objetivo de la reunión:	Segunda reunión entre empresa y profesora tutora.		
Participantes	Presentes:	Yeiny Cubero Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Presentación de avance de TFG	La estudiante presenta el avance realizado con respecto a la introducción, marco teórico y metodología.	-
02	Indicación de actividades por realizar	La estudiante indica las técnicas e instrumentos a utilizar para las fases siguientes del TFG.	La estudiante debe organizar las sesiones respectivas para las entrevistas pactadas. La contraparte se compromete a participar en las actividades pactadas por la estudiante.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
Tercera reunión entre empresa y profesora tutora.		Semana del 16/05/2022 al 21/05/2022	Laura Alpízar María Jesús Calvo Angélica Chavarría o Yeiny Cubero

Firmas:

Laura Alpízar Chaves (Tutora)

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 10

Minuta de Reunión			
Información general			
Reunión N°:	10	**Fecha:**	06-abr-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	4:00 pm a 5:00 pm
Objetivo de la reunión:	Entrevistas de Situación Actual		
Participantes	Presentes:	Luis Rivera Angélica Chavarría Yeiny Cubero María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Entrevista situación actual socio	Se aplica la entrevista al socio del área.	La estudiante se compromete a recopilar las respuestas y documentarlas en la sección correspondiente.
02	Entrevista situación actual gerente y supervisor de TI	Se aplica entrevista al gerente y supervisor de TI	
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 11

Minuta de Reunión			
Información general			
Reunión N°:	11	**Fecha:**	29-abr-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	6:00 pm a 6:30 pm
Objetivo de la reunión:	Revisión del Capítulo 4 y consultas del Capítulo 5		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Revisión del capítulo 4	La estudiante muestra el capítulo 4 realizado y la tutora hace la realimentación correspondiente.	La estudiante debe corregir el análisis de brecha.
02	Consultas de la propuesta de solución	La estudiante explica la idea para la propuesta de solución a la profesora.	La estudiante debe realizar la propuesta de acuerdo con las recomendaciones dadas por la tutora.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Minuta 12

Minuta de Reunión			
Información general			
Reunión N°:	12	**Fecha:**	04-may-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	4:00 pm a 4:30 pm
Objetivo de la reunión:	Resultados de Situación Actual		
Participantes	Presentes:	Angélica Chavarría Yeiny Cubero María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Resultados de la situación actual	La estudiante expone la situación actual producto de las técnicas aplicadas a la empresa.	-
02	Siguientes fases de TFG	La estudiante recuerda a la empresa las fases finales del TFG: la formación de la propuesta de solución y su evaluación.	La estudiante debe agendar las reuniones pertinentes para cumplir con las fases siguientes.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 13

Minuta de Reunión			
Información general			
Reunión N°:	13	**Fecha:**	11-may-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	1:00 pm a 1:30 pm
Objetivo de la reunión:	Revisión de avance del Capítulo 5		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Revisión de la propuesta	La estudiante muestra las herramientas realizadas y la tutora brinda realimentación.	La estudiante debe corregir aspectos dados por la tutora en las herramientas.
02	Consultas de la evaluación piloto	Aclaración de las pruebas piloto.	La estudiante debe realizar las pruebas piloto en un contexto hipotético de un cliente que ya haya sido auditado por la empresa.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Minuta 14

Minuta de Reunión			
Información general			
Reunión N°:	14	**Fecha:**	Del 17-may-2022 al 18-may-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	4:00 pm a 5:00 pm
Objetivo de la reunión:	Aplicación de Grupo focal		
Participantes	Presentes:	Angélica Chavarría Yeiny Cubero Alonso Vargas José Pablo Calvo Yohani Martínez María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Ejecución del grupo focal de la matriz de requerimientos.	Se realiza el ejercicio de grupo focal con la matriz de requerimientos.	La estudiante debe realizar las correcciones pertinentes a la propuesta de solución y documentar los hallazgos del grupo focal.
02	Ejecución del grupo focal para el instructivo de gestión.	Se realiza el ejercicio de grupo focal con el instructivo de gestión.	
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 15

Minuta de Reunión			
Información general			
Reunión N°:	15	**Fecha:**	24-may-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	1:00 pm a 1:30 pm
Objetivo de la reunión:	Tercera reunión entre empresa y profesora tutora.		
Participantes	Presentes:	Yeiny Cubero Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Presentación final del TFG	La estudiante presenta el resultado de su TFG.	-
02	Cierre	Se realiza el cierre formal con la empresa.	-
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Minuta 16

Minuta de Reunión			
Información general			
Reunión N°:	16	**Fecha:**	27-may-2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	11:00 am a 11:30 am
Objetivo de la reunión:	Revisión conclusiones y recomendaciones		
Participantes	Presentes:	Laura Alpízar María Jesús Calvo	
	Ausentes:	-	
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
01	Conclusiones y recomendaciones	Revisión con la tutora sobre conclusiones y recomendaciones.	La estudiante realiza los ajustes necesarios.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
-		-	-

Firmas:

Laura Alpízar Chaves (Tutora)

María Jesús Calvo (Estudiante)

Firma de Minutas Empresa

Firma de Minutas por parte de la empresa

Por medio de este documento, se agrupan y firman las minutas de reuniones realizadas a lo largo del desarrollo del Trabajo Final de Graduación titulado "Propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en el marco de referencia COBIT 2019", y elaborado por la estudiante María Jesús Calvo Bolaños, carnet 2017090398.

La contraparte, Yeiny Cubero, Supervisora del equipo de TI, valida su participación y la del equipo, en las siguientes minutas:

- Minuta 2: Primera reunión entre empresa y profesora tutora.
- Minuta 4: Problema y tema oficial del Trabajo Final de Graduación (Capítulo 1).
- Minuta 9: Segunda reunión entre empresa y profesora tutora.
- Minuta 10: Entrevistas de Situación Actual.
- Minuta 12: Resultados de Situación Actual.
- Minuta 14: Aplicación de Grupo focal.
- Minuta 15: Tercera reunión entre empresa y profesora tutora.

YEINY CUBERO BENAVIDES (FIRMA)

Yeiny Cubero (Contraparte)

María Jesús Calvo (Estudiante)

Firma de Minutas Tutora

Firma de Minutas por parte de la profesora tutora

Por medio de este documento, se agrupan y firman las minutas de reuniones realizadas a lo largo del desarrollo del Trabajo Final de Graduación titulado "Propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en el marco de referencia COBIT 2019", y elaborado por la estudiante María Jesús Calvo Bolaños, carnet 2017090398.

La profesora tutora, Laura Alpízar, valida su participación en las siguientes minutas:

- Minuta 1: Bienvenida y organización del curso.
- Minuta 2: Primera reunión entre empresa y profesora tutora.
- Minuta 3: Delimitación del problema y objetivos del TFG.
- Minuta 5: Correcciones del Capítulo 1 e instrucciones para el Capítulo 2.
- Minuta 6: Revisión del Capítulo 3.
- Minuta 7: Metodología del TFG.
- Minuta 8: Evaluación de presentación para empresa.
- Minuta 9: Segunda reunión entre empresa y profesora tutora.
- Minuta 11: Revisión del Capítulo 4 y consultas del Capítulo 5.
- Minuta 13: Revisión de avance del Capítulo 5.
- Minuta 15: Tercera reunión entre empresa y profesora tutora.
- Minuta 16: Revisión conclusiones y recomendaciones.

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)

Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2022.05.28 11:58:33 -06'00'

Laura Alpízar (Tutora)

Mª Jesús Calvo B.

María Jesús Calvo (Estudiante)

10. ANEXOS

Anexo I. Plantilla para minutas

Minuta de Reunión			
Información general			
Reunión N°:		**Fecha:**	
Lugar:		**Hora de inicio y finalización:**	
Objetivo de la reunión:			
Participantes	Presentes:		
	Ausentes:		
Temas tratados			
ID	**Asunto**	**Comentarios**	**Acuerdos**
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**

Anexo II. Plantilla para el control de cambios

Hoja de Control de Cambios			
Datos Generales del Cambio			
N° Cambio			
Solicitante		**Fecha de solicitud del cambio**	
Responsable de la implementación		**Fecha de realización del cambio**	
Estado	☐Aprobado ☐ En Revisión ☐Rechazado		
Detalles del Cambio			
Categoría	Introducción / Alcance / Marco Teórico / Metodología /….		
Descripción detallada			
Justificación			
Implicaciones de realizar el cambio			
Impacto	Especificar si el cambio genera impacto en otras áreas del proyecto, tales como recursos, cronogramas, otros proyectos, entre otros.		
Comentarios / Observaciones			
Firmas			
Revisado por: Nombre tutor Firma (Prof. tutor)		**Revisado por:** Nombre representante empresa Firma (Empresa)	
Elaborado por: Nombre estudiante Firma (Estudiante)		**Aprobado por:** Nombre Coordinadora TFG Firma (Coordinadora de TFG)	

Anexo III. Carta Filológica

Esparza, 29 de mayo de 2022

Señores:
Área Académica de Administración de TI
Tecnológico de Costa Rica
Cartago, Costa Rica

Por este medio hago constar que he revisado y corregido la sintaxis, la morfología y la semántica del texto: "Propuesta de actualización de la matriz de requerimientos de procesos tecnológicos y un instructivo de gestión de ejecución de la auditoría basados en el marco de referencia COBIT 2019", propiedad de María Jesús Calvo Bolaños, presentado como requisito para optar por el grado de Licenciatura en Administración de Tecnología de Información.

Cordialmente,

MAGDALENA VENEGAS PORRAS (FIRMA)

Firmado digitalmente por MAGDALENA VENEGAS PORRAS (FIRMA)
Fecha: 2022.05.29 21:29:46 -06'00'

Lcda. Magdalena Venegas Porras
Filóloga
Carné 10785
Cédula 6-230-116

Anexo IV. Evaluaciones de la Organización

Evaluación I de la Organización

Evaluación por parte de la Organización sobre el trabajo del estudiante de TFG - 2022

Datos del estudiante (1515)

Institución o Empresa (41666)

Tipo: (!/list-dropdown)

A18 - KPMG

Nombre del estudiante (41692)

Tipo: (!/list-dropdown)

A1 - María Jesús Calvo Bolaños

Carnet: 2017090398

Título: Elaboración de una propuesta de mejora al proceso de auditoría de tecnología de información utilizado por el equipo de TI del área de Management Consulting, en la firma KPMG S.A.

(41742)

Tipo: (X/boilerplate)

Fecha en que se realiza la evaluación (41667)

Tipo: (D/date)

31/03/2022

Evaluación número: (41674)

Tipo: (L/list-radio)

1

A1

Calificación al estudiante (1516)

A. HABILIDADES ESTRATÉGICAS DEL ESTUDIANTE (41668)

Tipo: (K/numeric-multi)

3

a. Responsabilidad y puntualidad en las reuniones y entregas. (41695)

3

b. Comunicación asertiva y facilidad de expresión. (41696)

3

c. Proactividad. (41697)

3

d. Trabajo colaborativo y capacidad organizativa. (41698)

3

e. Acatamiento de lineamientos de la organización. (41699)

B. ACERCA DEL TRABAJO REALIZADO A LA FECHA (41669)

Tipo: (K/numeric-multi)

3

a. Disposición autodidacta. (41700)

3

b. Seguimiento a recomendaciones que se le dan. (41701)

3

c. Cumplimiento del cronograma de su trabajo. (41702)

3

d. Pensamiento sistemático o estratégico. (41703)

C. SOBRE LOS ENTREGABLES DEL ESTUDIANTE (41670)

Tipo: (K/numeric-multi)

3

a. Estructura lógica de los informes, minutas, correos que elabora, entre otros. (41704)

3

b. Claridad en la secuencia de ideas que expone. (41705)

3

c. Las minutas reflejan los acuerdos tomados en las reuniones. (41706)

3

d. Uso correcto de idioma oficial de la compañía. (41707)

3

e. Profundidad del contenido desarrollado dentro de sus documentos o propuestas. (41708)

D. ÉTICA PROFESIONAL DEL ESTUDIANTE (41671)

Tipo: (K/numeric-multi)

3

a. Compromiso con la calidad de su trabajo. (41709)

3

b. Respeto a la confidencialidad de la información brindada por la organización. (41710)

3

c. Honestidad en su actuar diario. (41711)

3

d. Tolerancia y aceptación a todo tipo de diversidad. (41712)

Observaciones generales (41672)

Tipo: (T/text-long)

Persona responsable y esforzada en las tareas ejecutadas hasta el día de hoy

Nombre del Evaluador/Contraparte de la Organización: (41673)

Tipo: (S/text-short)

Yeiny Cubero Benavides

Firma del Evaluador/Contraparte de la Organización::_____

(41675)

Tipo: (X/boilerplate)

Evaluación II de la Organización

Evaluación por parte de la Organización sobre el trabajo del estudiante de TFG - 2022

Datos del estudiante (1515)

Institución o Empresa (41666)

Tipo: (!/list-dropdown)

A18 - KPMG

Nombre del estudiante (41692)

Tipo: (!/list-dropdown)

A1 - María Jesús Calvo Bolaños

Carnet: 2017090398

Título: Elaboración de una propuesta de mejora al proceso de auditoría de tecnología de información utilizado por el equipo de TI del área de Management Consulting, en la firma KPMG S.A.

(41742)

Tipo: (X/boilerplate)

Fecha en que se realiza la evaluación (41667)

Tipo: (D/date)

06/05/2022

Evaluación número: (41674)

Tipo: (L/list-radio)

2

A2

Calificación al estudiante (1516)

A. HABILIDADES ESTRATÉGICAS DEL ESTUDIANTE (41668)

Tipo: (K/numeric-multi)

3

a. Responsabilidad y puntualidad en las reuniones y entregas. (41695)

3

b. Comunicación asertiva y facilidad de expresión. (41696)

3

c. Proactividad. (41697)

3

d. Trabajo colaborativo y capacidad organizativa. (41698)

3

e. Acatamiento de lineamientos de la organización. (41699)

B. ACERCA DEL TRABAJO REALIZADO A LA FECHA (41669)

Tipo: (K/numeric-multi)

3

a. Disposición autodidacta. (41700)

3

b. Seguimiento a recomendaciones que se le dan. (41701)

3

c. Cumplimiento del cronograma de su trabajo. (41702)

3

d. Pensamiento sistemático o estratégico. (41703)

C. SOBRE LOS ENTREGABLES DEL ESTUDIANTE (41670)

Tipo: (K/numeric-multi)

3

a. Estructura lógica de los informes, minutas, correos que elabora, entre otros. (41704)

3

b. Claridad en la secuencia de ideas que expone. (41705)

3

c. Las minutas reflejan los acuerdos tomados en las reuniones. (41706)

3

d. Uso correcto de idioma oficial de la compañía. (41707)

3

e. Profundidad del contenido desarrollado dentro de sus documentos o propuestas. (41708)

D. ÉTICA PROFESIONAL DEL ESTUDIANTE (41671)

Tipo: (K/numeric-multi)

3

a. Compromiso con la calidad de su trabajo. (41709)

3

b. Respeto a la confidencialidad de la información brindada por la organización. (41710)

3

c. Honestidad en su actuar diario. (41711)

3

d. Tolerancia y aceptación a todo tipo de diversidad. (41712)

Observaciones generales (41672)

Tipo: (T/text-long)

Persona proactiva la cual brinda alternativas a los problemas presentados durante el desarrollo de la propuesta; ademas es un persona muy responsable en las labores asiganadas.

Nombre del Evaluador/Contraparte de la Organización: (41673)

Tipo: (S/text-short)

Yeiny Cubero Benavides

Firma del Evaluador/Contraparte de la Organización::_____

(41675)

Tipo: (X/boilerplate)

Evaluación III de la Organización

Evaluación por parte de la Organización sobre el trabajo del estudiante de TFG - 2022

Datos del estudiante (1515)

Institución o Empresa (41666)

Tipo: (!/list-dropdown)

A18 - KPMG

Nombre del estudiante (41692)

Tipo: (!/list-dropdown)

A1 - María Jesús Calvo Bolaños

Carnet: 2017090398

Título: Elaboración de una propuesta de mejora al proceso de auditoría de tecnología de información utilizado por el equipo de TI del área de Management Consulting, en la firma KPMG S.A.

(41742)

Tipo: (X/boilerplate)

Fecha en que se realiza la evaluación (41667)

Tipo: (D/date)

28/05/2022

Evaluación número: (41674)

Tipo: (L/list-radio)

3

A3

Calificación al estudiante (1516)

A. HABILIDADES ESTRATÉGICAS DEL ESTUDIANTE (41668)

Tipo: (K/numeric-multi)

3

a. Responsabilidad y puntualidad en las reuniones y entregas. (41695)

3

b. Comunicación asertiva y facilidad de expresión. (41696)

3

c. Proactividad. (41697)

3

d. Trabajo colaborativo y capacidad organizativa. (41698)

3

e. Acatamiento de lineamientos de la organización. (41699)

B. ACERCA DEL TRABAJO REALIZADO A LA FECHA (41669)

Tipo: (K/numeric-multi)

3

a. Disposición autodidacta. (41700)

3

b. Seguimiento a recomendaciones que se le dan. (41701)

3

c. Cumplimiento del cronograma de su trabajo. (41702)

3

d. Pensamiento sistemático o estratégico. (41703)

C. SOBRE LOS ENTREGABLES DEL ESTUDIANTE (41670)

Tipo: (K/numeric-multi)

3

a. Estructura lógica de los informes, minutas, correos que elabora, entre otros. (41704)

3

b. Claridad en la secuencia de ideas que expone. (41705)

3

c. Las minutas reflejan los acuerdos tomados en las reuniones. (41706)

3

d. Uso correcto de idioma oficial de la compañía. (41707)

3

e. Profundidad del contenido desarrollado dentro de sus documentos o propuestas. (41708)

D. ÉTICA PROFESIONAL DEL ESTUDIANTE (41671)

Tipo: (K/numeric-multi)

3

a. Compromiso con la calidad de su trabajo. (41709)

3

b. Respeto a la confidencialidad de la información brindada por la organización. (41710)

3

c. Honestidad en su actuar diario. (41711)

3

d. Tolerancia y aceptación a todo tipo de diversidad. (41712)

Observaciones generales (41672)

Tipo: (T/text-long)

Muy profesional, acepto las recomendaciones brindadas por la empresa, y aplicó dichas recomendaciones a los productos finales en corto plazo

Nombre del Evaluador/Contraparte de la Organización: (41673)

Tipo: (S/text-short)

Yeiny Cubero Benavides

Firma del Evaluador/Contraparte de la Organización::_____

(41675)

Tipo: (X/boilerplate)