TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnologías de Información

Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

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

Elaborado por: Daniela Brenes Gutiérrez

Prof. Tutor: MSc. Laura Alpízar Chaves

Cartago, Costa Rica

Julio, 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 Trabajo Final de Graduación de la estudiante Daniela Brenes Gutiérrez sea aceptado como requisito parcial para optar al grado académico de Licenciatura en Administración de Tecnología de Información.

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)

Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2022.06.17 18:25:13 -06'00'

Laura Alpízar Chaves

Profesor tutor

JUAN ANDRES SEGREDA JOHANNING (FIRMA)

Firmado digitalmente por JUAN ANDRES SEGREDA JOHANNING (FIRMA)
Fecha: 2022.06.18 22:00:10 -06'00'

Juan Andrés Segreda Johanning

Lector académico

David Chaverri P.

José David Chaverri Pérez

Lector externo

TEC | Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2022.06.20 23:05:02 -06'00'

Yarima Sandoval Sánchez

Coordinadora de Trabajo Final de Graduación

Dedicatoria

Dedico de manera especial el presente Trabajo Final de Graduación a mi abuela, Ana Lissia Gutiérrez Porras, quién con su esfuerzo me permitió llegar a esta etapa, por ser un apoyo incondicional durante los años de carrera y por ser mi mayor motivación para concluir este proceso de la mejor manera.

Gracias por ser mi pilar, por haberme forjado como la persona que soy en la actualidad, por impulsarme a buscar las mejores oportunidades y por demostrarme tanto amor.

Agradecimientos

A mi familia

Agradezco a mi familia por estar siempre presente y por su confianza. Especialmente, a mi madre, Ana Brenes, y hermano, Daniel Izaguirre, por acompañarme en los últimos dos años, durante momentos difíciles y por alentarme a concluir esta etapa.

A mis profesores

A todos los profesores que me acompañaron durante los años de carrera, por su tiempo y esfuerzo invertidos en nuestra formación como profesionales. En especial, a Laura Alpízar, quién ha sido mi tutora durante este proceso, por su retroalimentación e interés en la mejora continua del proyecto.

A mis amigas

A mis amigas, Hellen Cordero, Valeria Mata, Natalia Bonilla, Karen Vargas, Yariela Rodríguez y Maribel Cordero, por darme su apoyo incondicional, su amistad y por ser parte de las mejores experiencias que me dejó el TEC.

Al equipo de Auditoría de TI

Por todos los recursos y conocimientos proporcionados que hicieron posible la realización de este proyecto, por su colaboración y retroalimentación durante el proceso.

Resumen

El presente Trabajo Final de Graduación consiste en elaborar una propuesta de mejora de los controles generales de TI, específicamente para las áreas de "Accesos a Programas y Datos" y "Operaciones de Computadoras", considerados en la metodología actual para una firma de auditoría.

Este proyecto surge a partir del análisis de la situación problemática actual que enfrenta la organización, en donde se identifica una deficiencia en la calidad de los servicios de auditoría ofrecidos tanto a Auditoría Financiera como a clientes externos. Se destaca como principal causa que la metodología actual no está alineada a las mejores prácticas presentes en un marco de trabajo como COBIT 2019.

La propuesta solución es diseñada a partir de los resultados obtenidos de la realización de una comparativa de los controles presentes en la metodología actual para ambos procesos, con el marco de referencia COBIT 2019.

Con el desarrollo del presente proyecto se pretende brindar una herramienta de controles compensatorios para los procesos de "Acceso a Programas y Datos" y Operación de Computadoras, a partir de las brechas identificadas en la comparativa, con las pruebas de diseño y eficacia operativa correspondientes.

Adicionalmente, se pretende proporcionar un análisis financiero donde se determina la viabilidad económica de la propuesta.

Palabras clave: Auditoría de TI, Riesgos de TI, "Acceso a Programas y Datos", "Operaciones de Computadoras", Controles Generales de TI, COBIT 2019.

Abstract

This graduation final project consists of preparing a proposal to improve general IT controls, specifically for the areas of "Access to Programs and Data" and "Computer Operations" considered in the current methodology for an audit firm.

This project arises from the analysis of the current problematic situation facing the organization where a deficiency in the quality of the audit services offered to both Financial Audit and external clients is identified. It stands out as the main cause that the current methodology is not aligned with the best practices present in a framework such as COBIT 2019.

The proposed solution is designed based on the results obtained from a comparison of the controls present in the current methodology for both processes with the COBIT 2019 reference framework.

The development of this project aims to provide a compensatory control tool for the Access to Programs and Data and Computer Operation processes, based on the gaps identified in the comparison, with the corresponding design and operational effectiveness tests.

In addition, it is intended to provide a financial analysis where the economic viability of the proposal is determined.

Key words: Auditoría de TI, IT Risks, Access to Programs and Data, Computer Operations, IT General Controls, COBIT 2019.

Tabla de Contenidos

Índice de Figuras

Índice de Tablas

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 con relación al uso del "género inclusivo". Al mismo tiempo se aclara que estamos 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

1. Introducción

El Gobierno de Tecnología de Información hace referencia a la gestión y el control de todos los aspectos relacionados con la tecnología de información, requeridos para apoyar el logro de los objetivos empresariales y agregar valor a las compañías. Su propósito es alinear los objetivos, planes y operaciones de TI con los de la organización. (Gómez-Estupiñán, 2013)

La industria actual demanda que la planificación e implementación de Tecnología de Información sea lo suficientemente competente, de modo que apoye el cumplimiento de sus objetivos de negocio y operacionales. Para ello, es necesario estar alineado con las mejores prácticas y actuar con base en las condiciones de las entidades regulatorias.

El gobierno de Tecnología de Información integra un conjunto de buenas prácticas para su gestión, que permita justificar su inversión, asimismo, que asegure a la organización administrar estratégicamente la información, además, que se aprovechen al máximo las oportunidades que brinde el entorno y que se obtengan ventajas competitivas. (Gómez-Estupiñán, 2013)

Para la aplicación de estas mejores prácticas de TI existen varios marcos de referencia reconocidos a nivel global que se mantienen actualizados sobre las tendencias de la industria y los procedimientos por cumplir de las distintas áreas o procesos de TI.

Para el área de Auditoría de TI resulta fundamental tomar en consideración las mejores prácticas para el beneficio de las organizaciones a las que ofrecen sus servicios, asegurando un trabajo de calidad y también para cumplir con las normas de las entidades regulatorias.

Este proyecto busca efectuar una comparación de los procedimientos actuales de una firma de Auditoría de TI con las guías de la industria que contienen las mejores prácticas actualizadas y que cumplen globalmente con los estándares de calidad y las condiciones de las entidades regulatorias.

Además, el presente Trabajo Final de Graduación se enfocará en dos procesos de TI: “Acceso a Programas y Datos” y “Operaciones de Computadoras”. Para cada uno se analizará los controles de auditoría definidos en la guía actual de la firma y se determinará cuáles son las posibles brechas que tienen con respecto a las mejores prácticas.

En este apartado se encuentra una descripción general de la investigación, así como el contenido del documento, además, los antecedentes donde se incluye una descripción breve de la organización en la cual se desarrolla el proyecto, también se plantean otros puntos: organigrama general de la firma, misión, visión, valores, características relevantes y proyectos similares que se han llevado a cabo. De igual forma, se mencionan: proyectos similares externos a la organización que se usarán como referencia, la situación problemática, los objetivos y el alcance establecido que delimita el proyecto.

1.1. Descripción General

El presente documento plantea la propuesta del Trabajo Final de Graduación de la carrera de Administración de Tecnología de Información del Instituto Tecnológico de Costa Rica. La propuesta consiste en alinear la metodología de auditoría de TI actual para la evaluación de controles, de los procesos correspondientes a Operación de Computadoras y Accesos a Programas y Datos, con un marco de referencia por seleccionar, asimismo se busca identificar las posibles brechas con el fin de diseñar los controles compensatorios y/o adicionales.

En la primera sección del documento, se explica el contexto de la organización en la que se va a desarrollar el Trabajo Final de Graduación. Se describe la historia, la misión, visión y los valores de la organización.

Más adelante, se detalla la situación problemática y los beneficios que se obtienen a partir de la ejecución del proyecto planteado. Asimismo, se define el objetivo general y los objetivos específicos que describen el propósito y las actividades del proyecto.

Por último, se presenta la justificación y el alcance del proyecto incluyendo la definición de los entregables respectivos.

1.2. Antecedentes

En esta sección se especifican los antecedentes de la organización en donde se desarrolla el proyecto.

1.2.1. Descripción de la organización

DBG Auditores es una red global de firmas que presta servicios de Auditoría, Impuestos y Asesoría. Está presente en 147 países con más de 227.000 colaboradores trabajando alrededor del mundo. (DBG, 2021)

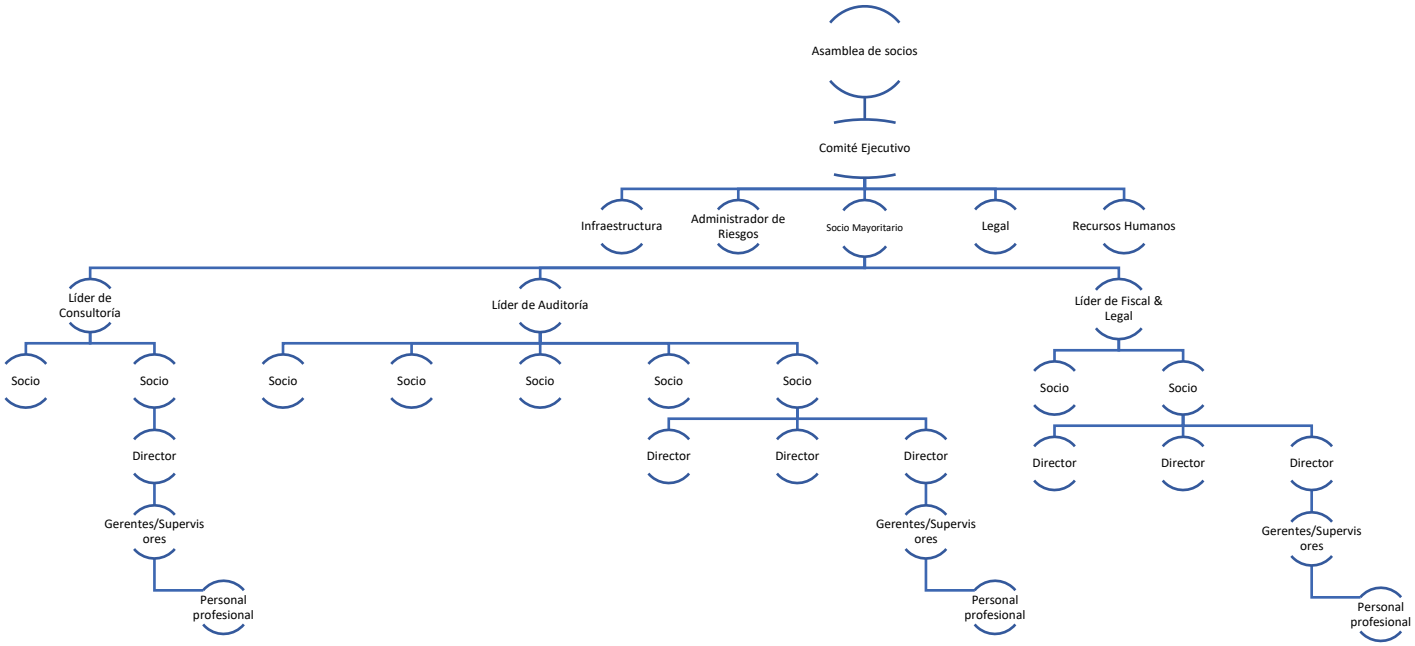
Fundada en 1958, DBG Auditores es en la actualidad una de las firmas profesionales de servicios más importantes del país. (DBG, 2021)

DBG Auditores cuenta con profesionales de diversas ramas agrupados en equipos disciplinarios, que buscan atender las necesidades especiales del mercado costarricense, a través de un profundo conocimiento del marco regulatorio local, una formación continua y especializada en la profesión y la dedicación total al servicio brindado al cliente. (DBG, 2021).

En el año 2005, la Firma de Auditoria comenzó a operar la nueva unidad de negocio integrada por las prácticas de la Firma en Costa Rica, Guatemala, Honduras, El Salvador, Nicaragua, Panamá y República Dominicana.

Como se observa en la Figura 1, la estructura de la firma está conformada por un director ejecutivo y un socio director, quienes brindan las directrices empresariales. En un nivel por debajo, se encuentran socios empresariales, responsables de definir las metas y los objetivos para cada uno de los departamentos a su cargo. (Masis-Álvarez, 2017)

Figura 1. Organigrama



Fuente: Adaptación información de la empresa DBG (2022).

1.2.1.1. Misión

"Proveer servicios de auditoría con el más alto nivel de calidad, buscando siempre la máxima satisfacción de nuestros clientes dentro de un marco de ética, independencia y confidencialidad." (DBG, 2021).

1.2.1.2. Visión

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

1.2.1.3. Valores

La firma DBG Auditores establece los siguientes valores: (DBG, 2021)

• Lideramos con el ejemplo en todos los niveles actuando de manera que ejemplifique lo que queremos de cada uno de nosotros.

• Trabajamos en equipo tomando lo mejor de cada uno y creando relaciones fuertes y duraderas.

• Respetamos a los individuos, respetando a las personas por lo que son y por su conocimiento, habilidades y experiencia como miembros individuales de un grupo.

• Investigamos los hechos y transmitimos conocimientos verificando los hechos y fortaleciendo nuestra reputación como asesores de negocios con credibilidad y objetividad.

• Nos comunicamos de forma abierta y honesta compartiendo información, conocimiento manejando situaciones difíciles con coraje y creatividad.

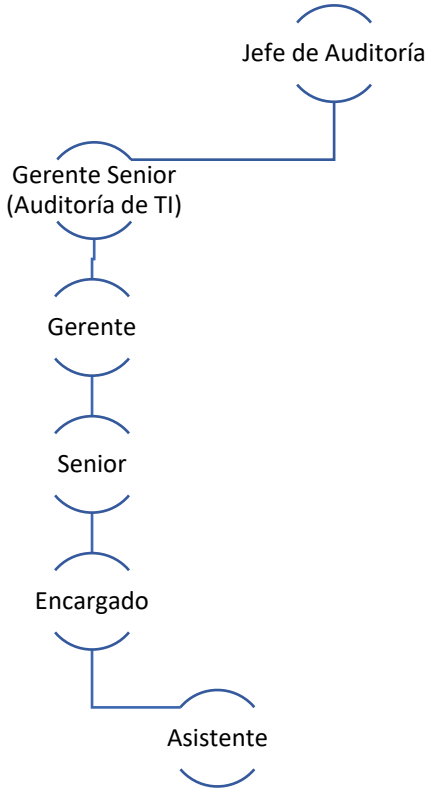
• Comprometidos con la Sociedad comportándonos como ciudadanos responsables y ampliando nuestras habilidades, experiencia y perspectiva de nuestras comunidades.

• Por encima de todo nos comportamos con integridad manteniendo elevados estándares profesionales en todo momento, proveyendo asesoría útil y conservando nuestra independencia con rigor.

1.2.1.4. Equipo de trabajo

El presente proyecto se desarrollará en el área de Auditoría de TI de la firma DBG Auditores. En la Figura 2, se muestra el diagrama actual del equipo de trabajo de Auditoría de TI.

Figura 2. Diagrama del área de Auditoría de TI



Fuente: Adaptación información de la empresa DBG (2022).

El equipo de Auditoría de TI se encarga de brindar un servicio al área de Auditoría Financiera, en donde evalúan los controles generales de TI y controles de aplicación de TI, relevantes para los sistemas de información financieros. El puesto que desempeña actualmente el estudiante es el de Asistente de Auditoría de TI.

1.2.1.5. Trabajos similares realizados dentro y fuera de la organización

En este apartado se presentan algunos de los proyectos similares al actual, se tomarán como punto de referencia para la ejecución del estudio. Se incluyen tanto proyectos realizados en la firma como también efectuados fuera de la organización, siempre y cuando pertenezcan a la misma área de conocimiento.

1.2.1.5.1. Proyectos internos a la organización

Los proyectos internos que corresponden al insumo de esta investigación son los servicios de Auditoría que el área de Auditoría de TI ofrece a Auditoría Financiera.

Además, se utiliza como insumo la Matriz de Controles Generales de TI para la comparación con el marco de referencia por seleccionar.

1.2.1.5.2. Proyectos externos a la organización

Se consideran como insumos para la propuesta del presente proyecto los siguientes TFG:

- *Propuesta de mejora de los controles generales de auditoría de TI en el tema de la seguridad de la Información* realizado por Cristopher Fabián Inces Martínez en el 2019. Este proyecto tenía como objetivo general: Elaborar una propuesta de mejora a los controles generales de TI y pruebas de control del área de IRM, en el proceso de Gestión de Seguridad de la Información, alineado con COBIT 5, que permita fortalecer el proceso de auditoría del área.
- *Propuesta de definición de controles de auditoría y pruebas sustantivas para la evaluación del proceso de Gestión del Cambio en las organizaciones auditadas, Caso JM Auditores*. realizado por Adán Josué Masis Álvarez en el 2017. Este proyecto tenía como objetivo general: Desarrollar los controles de auditoría y las pruebas sustantivas para el proceso de Gestión del Cambio de forma que se alinee a un marco de referencia internacional, con el fin de llevar a cabo una mejor evaluación de Controles Generales de TI para las empresas industriales auditadas en el año 2017.

1.3. Planteamiento del problema

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

1.3.1. Situación problemática

El área de Auditoría de TI se encarga de evaluar la efectividad de los controles mitigantes a los riesgos inherentes del uso de Tecnología de Información de las organizaciones, los cuales son denominados dentro de la firma como Controles Generales de TI.

Los Controles Generales de TI se clasifican en 4 categorías: Operación de Computadoras y Accesos a Programas y Datos, Cambios a Programas, Desarrollo de Programas y Operación de Computadoras. El presente análisis se enfoca en el proceso de Operación de Computadoras y Accesos a Programas y Datos.

Los controles asociados al proceso de "Operación de Computadoras y Accesos a Programas y Datos" se refieren a la evaluación de las medidas mitigantes en cuanto a la asignación de accesos en las organizaciones, donde se asegure que estén debidamente autorizados y los niveles de privilegio son asignados acordes a las responsabilidades y roles que correspondan.

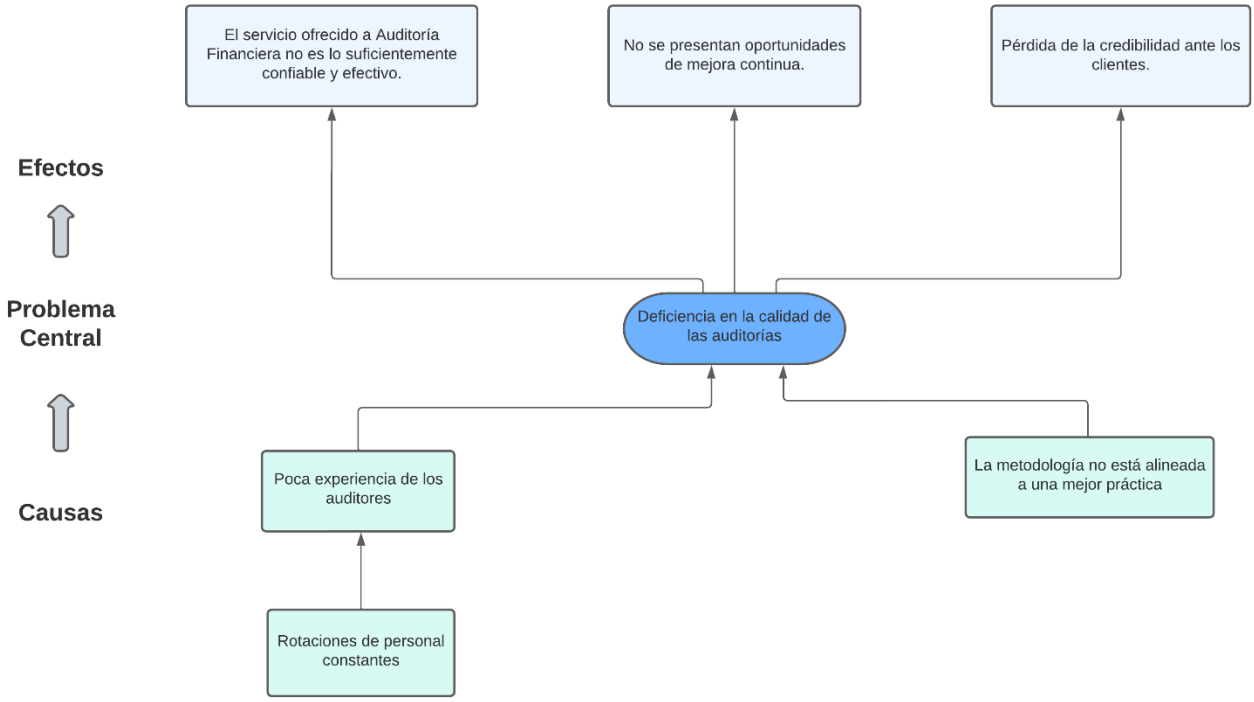
En ciertas organizaciones puede existir la posibilidad de que no se implementen algunos de los controles, para estos casos no se definen cuáles controles alternativos se podrían considerar como compensatorios donde se asegure que responden al riesgo de manera efectiva.

Asimismo, debido a la actualización continua de los marcos de referencia de la industria, puede que no se estén identificando posibles brechas con la metodología actual y se estén quedando por fuera controles relevantes del alcance de la auditoría.

El servicio que ofrece Auditoría de TI a Auditoría Financiera consiste en confirmar si los sistemas de información implementados por las organizaciones son lo suficientemente confiables para gestionar los reportes contables. Por lo tanto, la opinión emitida por Auditoría de TI debe de estar respaldada por una evaluación de controles completa. Por lo contrario, se pierde la credibilidad de los resultados emitidos y representa un riesgo significativo para Auditoría Financiera.

El problema central identificado, junto con sus causas y efectos, se pueden visualizar en la Figura 3.

Figura 3. Árbol de problemas



Fuente: Elaboración propia.

1.3.2. Justificación del proyecto

La evaluación de Controles Generales de TI es necesaria para determinar cuáles son las medidas para contrarrestar los riesgos de TI y financieros que las empresas están implementando en la actualidad.

Con esta revisión se asegura la efectividad y la confiabilidad de los sistemas de información responsables de la gestión financiera de las organizaciones. Indican el porcentaje de riesgos de materialidad de los reportes contables, ya sea por error o fraude.

La propuesta de esta investigación le ofrece al área de Auditoría de TI la identificación de oportunidades de mejora, en cuanto a pruebas de auditoría para los procesos de Operación de Computadoras y Accesos a Programas y Datos.

Adicionalmente, la ejecución de este proyecto aplica los conocimientos adquiridos por el estudiante a lo largo de la carrera. A continuación, algunos de los temas de TI relevantes:

- **Administración de Servicios de TI:** en este curso se introducen otros marcos de referencia reconocidos a nivel de industria que enseña las mejores prácticas a la hora de ofrecer servicios de TI. Abarca muchos de los procesos de negocio y de TI que se evalúan en una auditoría.
- **Administración de Proyectos:** este curso es el pilar para la compañía que conlleva la ejecución de un proyecto de negocio y de TI, introduciendo los factores críticos de éxito que se deben de tomar en consideración.
- **Ingeniería de Requerimientos:** este curso es una introducción a gran parte del trabajo que un profesional de ATI realiza a lo largo de su carrera profesional, independientemente del área que elija ejercer.
- **Auditoría de TI:** en este curso se entiende el rol del auditor de TI y lo que conlleva administrar un proyecto de auditoría.

1.3.3. Beneficios esperados o aportes del Trabajo Final de Graduación

En esta sección se indican cuáles son los beneficios directos e indirectos que conlleva la realización de este TFG para la firma.

1.3.3.1. Beneficios Directos

- Identificación de posibles brechas de la metodología actual con algún marco de referencia reconocido.
- Definición de controles compensatorios para los procesos de Operación de Computadoras y Accesos a Programas y Datos.

1.3.3.2. Beneficios Indirectos

- Brindar opiniones más completas y confiables a Auditoría Financiera.

1.4. Objetivos del Trabajo Final de Graduación

En esta sección, se define el objetivo general del presente proyecto, el cual indica su propósito. Asimismo, se describen los objetivos específicos que definen las actividades por realizar para cumplir con el objetivo general.

1.4.1. Objetivo General

Elaborar una propuesta de mejora de los Controles Generales de TI para los procesos "Acceso a Programas y Datos" y "Operación de Computadoras" por medio de una comparativa de la metodología actual con COBIT 2019 con el fin de identificar posibles brechas en los procesos; en un período de 15 semanas para una empresa de Auditoría.

1.4.2. Objetivos Específicos

- Comparar la metodología actual implementada por la firma para la evaluación de los Controles Generales de TI con un marco de referencia reconocido a nivel global para la identificación de las posibles brechas en los procesos de Operación de Computadoras y Accesos a Programas y Datos.
- Diseñar los controles generales de TI compensatorios para los procesos de "Acceso a Programas y Datos" y "Operación de Computadoras" tomando en consideración las brechas identificadas.
- Elaborar un análisis financiero para determinar la factibilidad y la obtención de los beneficios tangibles que se derivan de la implementación de este proyecto.

1.5. Alcance

La propuesta de este proyecto plantea seleccionar un marco de referencia reconocido a nivel global y alinearlo con la metodología de auditoría de TI actual, para la identificar posibles brechas en los procesos de Operación de Computadoras y Accesos a Programas y Datos.

A partir del mapeo se plantea la propuesta de los controles compensatorios y/o adicionales que completen la evaluación de los controles de Operación de Computadoras y Accesos a Programas y Datos, con el fin de reducir las brechas identificadas que respalden las opiniones emitidas por Auditoría de TI.

Se pretende desarrollar una herramienta con los controles diseñados a partir de la comparación de la metodología actual con el marco de referencia.

Este proyecto no incluye el análisis de las otras dos categorías de controles generales de TI, es decir: Cambios a Programas y Desarrollo de Programas.

1.6. Supuestos

En esta sección se indica cuáles son los factores que se asume que van a ser cumplidos o serán ciertos en la realización del proyecto.

- Se cuenta con el apoyo del área de Auditoría de TI en la propuesta de proyecto.

1.7. Entregables

En este apartado, se especifican los entregables generados a partir de la ejecución del proyecto.

- Matriz de controles generales de TI con los procesos de Operación de Computadoras y "Acceso a Programas y Datos" alineados con el marco de referencia.
- Propuesta de los controles compensatorios con las pruebas de auditoría.
- Análisis financiero del proyecto.

1.8. Limitaciones

En esta sección se indican cuáles serán los factores que en alguna medida restringen la realización del proyecto.

- Uso de la información de la organización.

2. Marco Conceptual

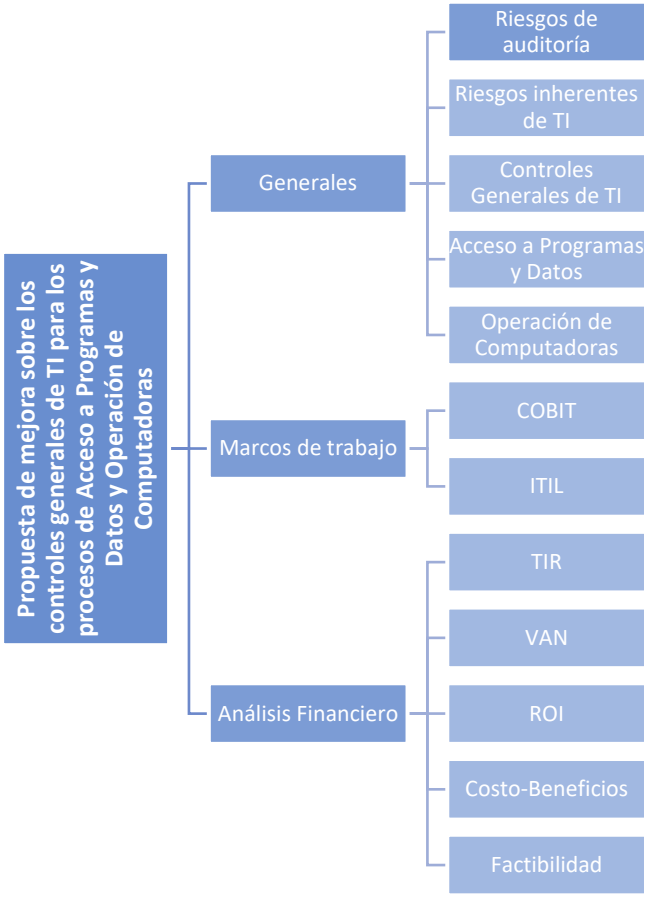
En el presente capítulo se presentan las definiciones que sustentan conceptualmente el desarrollo del Trabajo Final de Graduación, con el fin de brindar un entendimiento de la teoría implicada en el análisis de la problemática y la base de la propuesta de mejora.

Se realizó una búsqueda exhaustiva de artículos y proyectos similares para analizar los conceptos, fuentes e instrumentos de investigación que mejor responden al problema central identificado. Dentro de los temas abarcados se incluyen términos básicos del área de conocimiento en el que se enfoca el proyecto, los marcos de referencia que se utilizarán en el análisis de resultados, y el insumo principal para la comparación y el análisis de brecha. Asimismo, se indagan los componentes clave que conforman el análisis financiero de la propuesta.

2.1. Mapa conceptual

Como parte de la investigación, se determinaron las definiciones que sustentan teóricamente el desarrollo del proyecto. En la Figura 4 se observa un mapa conceptual con un resumen de los temas planteados.

Figura 4. Mapa conceptual



Fuente: Elaboración propia.

2.2. Generales

En esta sección se enfatizan aquellos conceptos básicos que forman parte del contexto de la problemática presentada, con el fin de obtener un entendimiento más detallado sobre las áreas de conocimiento implicadas y establecer una línea base sobre la propuesta de mejora que se desea plantear.

2.2.1. Riesgos de auditoría

PCAOB (2022) establece que en una auditoría de estados financieros el "riesgo de auditoría" se refiere a aquel riesgo de que el auditor exprese una opinión inapropiada de auditoría cuando los estados financieros contienen incorrecciones materiales, es decir, los estados financieros no se presentan fielmente de conformidad con el marco de información financiera aplicable.

2.2.2. Riesgos inherentes de TI

Según la metodología de la firma, un riesgo inherente de TI representa cualquier condición que pueda afectar la operación efectiva de los controles automáticos o la integridad de los datos de los sistemas de información de una entidad.

2.2.3. Controles generales de TI

La metodología de la firma establece que se refiere a los controles que se pueden aplicar a los sistemas de información de una entidad en sus diferentes capas, ya sea a nivel de base de datos, sistema operativo, aplicaciones e infraestructura de TI.

El objetivo de los controles generales de TI es asegurar la integridad del diseño y datos, así como la efectividad operativa de los sistemas de información de una organización.

2.2.4. Acceso a Programas y Datos

El proceso "Acceso a Programas y Datos" corresponde a un área de controles generales de TI que se enfoca en la evaluación del acceso lógico a los sistemas de información sobre cómo se mitigan los riesgos inherentes de TI asociados a dicho proceso.

Asimismo, según Pathlock (2022) se refiere a:

> Evaluar cómo la organización restringe el acceso e implementa medidas de control de acceso, para garantizar que solo las personas adecuadas puedan acceder física y electrónicamente a la información financiera confidencial. Esto incluye medidas de acceso físico como candados y videovigilancia para salas de servidores, y medidas digitales como autenticación y gestión de credenciales mediante una solución de gestión de acceso e identidad (párr.14).

2.2.5. Operación de computadoras

Los controles de "Operación de Computadoras" verifican si los sistemas de TI continúan funcionando como se espera, de manera consistente y precisa. Según O'Reilly (2022), una auditoría debe aplicar procedimientos en donde se asegure lo siguiente:

- Los *Jobs* de producción se completan de manera oportuna y la capacidad de producción es suficiente para satisfacer las necesidades de procesamiento a corto y largo plazo.

- Los procedimientos de copia de seguridad y recuperación protegen adecuadamente los datos y los programas contra la pérdida o destrucción accidental o intencional.
- Los procedimientos de mantenimiento protegen adecuadamente el hardware de la computadora contra fallas.
- El hardware, el software y los datos de la computadora están asegurados al costo de reposición.
- Los procedimientos de gestión de problemas garantizan que los problemas del sistema se documenten y resuelvan de manera oportuna y eficaz.

2.3. Marcos de trabajo

En esta sección, se describen los marcos de referencia pertinentes por considerar para la comparación con la metodología implementada por la firma y, consecuentemente, para el planteamiento de la propuesta de mejora.

2.3.1. COBIT

Según ISACA (2019), COBIT es un marco de trabajo reconocido globalmente creado para cerrar la brecha entre los riesgos de TI y los requisitos de control. En los Estados Unidos, COBIT es el marco más utilizado para lograr el cumplimiento de la Ley Sarbanes-Oxley (SOX).

En COBIT 2019 se definen seis principios considerados como los requisitos principales de un sistema de gobierno para administrar la información y la tecnología corporativa, se indican a continuación:

1. Cada empresa necesita un sistema de gobierno para satisfacer las necesidades de los interesados y agregar valor mediante el uso de TI.
2. Un sistema de gobierno para Enterprise I&T consta de una serie de componentes que pueden ser de diferentes tipos y trabajar juntos de manera integral.
3. Un sistema de gobierno debe ser dinámico. Esto significa que cualquier cambio en uno o más factores de diseño debe tener en cuenta el impacto de estos cambios en el sistema EGIT.
4. Un sistema de gobierno debe distinguir claramente entre el gobierno y las actividades y estructuras de gestión.
5. Un sistema de gobierno debe adaptarse a las necesidades de la empresa, utilizando un conjunto de factores de diseño como parámetros para adaptar y priorizar los componentes del sistema de gobierno.
6. Un sistema de gobierno debe cubrir a toda la empresa, centrándose no solo en la función de TI, sino en toda la tecnología y el procesamiento de información que la empresa utiliza para lograr sus objetivos. (González, 2018, párr.9)

Dentro del marco de referencia de COBIT 2019 se presentan varios aspectos que se deben de tener claros, entre ellos los instrumentos descritos para que las organizaciones se adapten a esta guía, según sus propios requerimientos y metas.

Objetivos: COBIT 2019 establece 'Objetivos de gobierno' y 'Objetivos de gestión', con un total de 40 como parte de su 'Modelo central'. Los profesionales priorizan estos objetivos en función de las necesidades de los clientes, las partes interesadas, los usuarios, etc., lo que les permite crear marcos y estrategias de TI integrales y personalizados.

Dominios: cada objetivo de COBIT se ajusta a un "Dominio" específico. Los objetivos de gestión están contenidos en 'Entregar, Servicio y Soporte (DSS)', 'Supervisar, Evaluar y Evaluar (MEA)', 'Construir, Adquirir e Implementar (BAI)' y 'Alinear, Planificar y Organizar (APO)'. Los objetivos de gobernanza se encuentran en 'Evaluar, dirigir y monitorear (EDM)'.

Cascada de objetivos: esta herramienta se utiliza para demostrar cómo los conductores crean necesidades y, posteriormente, "objetivos" más claramente definidos. En COBIT 2019, estos se conocen como 'Objetivos de alineación', a diferencia de los 'Objetivos de TI' de COBIT 5.

Componentes: anteriormente conocidos como "facilitadores", los componentes son elementos genéricos que influyen en TI. Incluyen 'Flujos de información', 'Habilidades', 'Infraestructura', 'Procesos', 'Políticas y procedimientos' y 'Estructuras organizacionales'. COBIT 2019 también introdujo 'variantes de genéricos', con las cuales los Componentes se pueden examinar y modificar en función de un 'Área de enfoque', como una legislación específica como el RGPD.

Factores de diseño: estos factores ayudan a definir las necesidades de una organización y cómo deben abordarse en un marco. Seguidamente, los factores contextuales, como los entornos corporativos y de amenazas, están fuera del control de la organización. Asimismo, los factores estratégicos reflejan decisiones de la organización, como la dirección de la estrategia empresarial y la priorización de diferentes elementos de TI. Finalmente, los factores tácticos se centran en las opciones de implementación con respecto a la tecnología (como los datos en la nube), los métodos (como DevOps, ITIL 4 o Agile) y los modelos de subcontratación. (Good E-Learning, 2021)

Por otro lado, se especifican algunos de los beneficios que ofrece una certificación COBIT 2019:

Alineación de TI: COBIT 2019 va más allá de las necesidades inmediatas de los usuarios y clientes, y garantiza que TI esté alineada con estrategias comerciales más grandes. Lograr esto junto con las complejidades de administrar las operaciones diarias requiere de una perspectiva de alto nivel integral y bien definida. COBIT proporciona esto y un vocabulario común para garantizar que los profesionales de TI, los equipos, los departamentos y las partes interesadas estén todos en sintonía.

Cumplimiento mejorado: la TI moderna debe permanecer alineada con la legislación comercial y de datos, como el RGPD. COBIT trata tales regulaciones como detalles cruciales al formular y actualizar marcos, asegurando que se aborden en todos los niveles de TI. Basado en el éxito de COBIT 5 en esta capacidad, los clientes ya tienen mucha confianza en COBIT 2019 para la gestión de riesgos.

Optimización: COBIT 2019 también es perfecto para la TI diaria, ya que ayuda a los profesionales a identificar prioridades y proporciona las herramientas y las mejores prácticas para realizar mejoras donde sea necesario. Como resultado, los profesionales pueden disfrutar

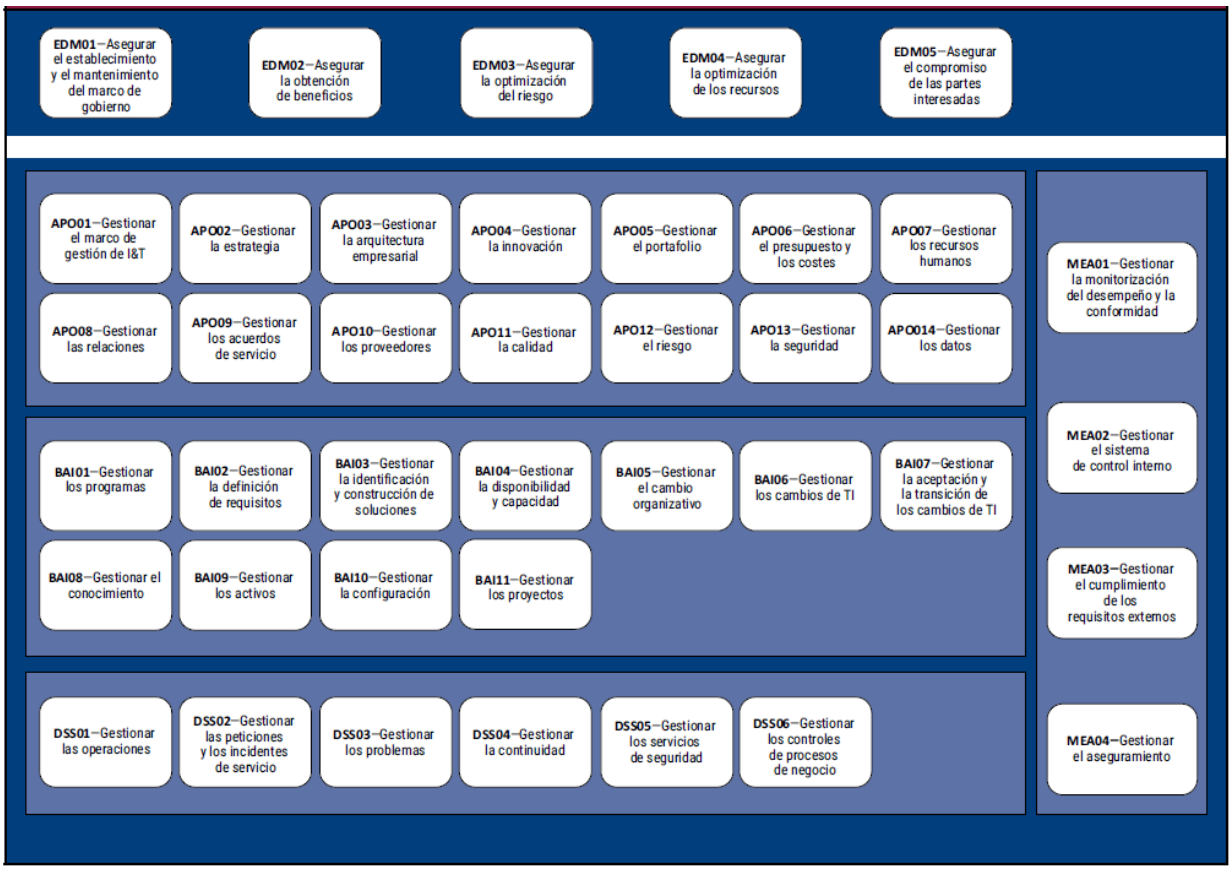
de operaciones de TI más eficientes, específicas y rentables, con funciones y responsabilidades claramente definidas en todos los equipos y departamentos.

Confianza: con la popularidad de COBIT, utilizarlo puede ayudar a aumentar la confianza de las partes interesadas, los usuarios y los clientes. La confiabilidad que COBIT permite en TI también puede elevar el perfil de una empresa con los clientes

Preparado para el futuro: COBIT 2019 es vanguardista y ofrece información sobre las últimas herramientas de TI, las mejores prácticas, etc. Sin embargo, también prepara a los profesionales para desarrollos futuros, gracias a su enfoque en las reevaluaciones del marco y su modelo de código abierto. Esto deja a las organizaciones perfectamente preparadas para evolucionar según sea necesario. (Good E-Learning, 2021)

En la Figura 5 se observa de manera gráfica el detalle del modelo principal definido para COBIT 2019.

Figura 5. Modelo principal de COBIT



Fuente: (ISACA, 2019)

Existen dos dominios en COBIT 2019 altamente relacionados con las áreas de “Acceso y Programas y Datos” y “Operación de Computadoras” los cuales corresponden a:

- **Alinear, Planear y Organizar (APO):** Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir mejor con los objetivos del negocio. Es importante mencionar que la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas; y finalmente, la implementación de una estructura organizacional y tecnológica apropiada. Proporciona la dirección para la entrega de soluciones y la entrega de servicios. (ISACA, 2019).

- **Entregar, Dar Servicio y Soporte (DSS):** Involucra la entrega en sí de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte a los usuarios del servicio, la administración de los datos y de las instalaciones operativas. El objetivo es lograr que los servicios de TI se entreguen de acuerdo con las prioridades del negocio, la optimización de costos, asegurar que la fuerza de trabajo utilice los sistemas de modo productivo y seguro, implantar de forma correcta la confidencialidad, la integridad y la disponibilidad. (ISACA, 2019).

2.3.2. ITIL

El acrónimo ITIL corresponde a *Information Technology Infrastructure Library*, que se traduce al español como Biblioteca de Infraestructura de Tecnología de la Información.

A continuación, Global Suite (2021) afirma que la ITIL:

> Es una guía de buenas prácticas para la gestión de servicios de tecnología de la información (TI). La guía ITIL se ha desarrollado para cubrir toda la infraestructura, el desarrollo y las operaciones de TI y gestionarla para mejorar la calidad del servicio (párr.1).

Los pilares de ITIL son los siguientes principios:

- Procesos: necesarios para la gestión de TI de acuerdo con el alineamiento de estos dentro de la organización.
- Calidad: entendida como la entrega al cliente del producto o servicio óptimo, es decir, con las características pactadas.
- Cliente: su satisfacción es el objetivo de mejorar los servicios, siendo, por tanto, el beneficiario directo de la implantación de las buenas prácticas ITIL.
- Independencia: se deben mantener siempre las buenas prácticas a pesar de los métodos establecidos para cada proceso y proveedores existentes. (Global Suite, 2021)

2.4. Análisis Financiero

En este apartado se definen los conceptos considerados para la elaboración del análisis financiero del presente proyecto.

2.4.1. TIR

Según establece (ACCA, s.f.), la Tasa Interna de Retorno (TIR) se puede definir como la tasa de descuento que, cuando se aplica a los flujos de efectivo de un proyecto, produce un valor actual neto (VAN) de cero. Esta tasa de descuento se puede considerar entonces como el retorno previsto para el proyecto. Si la TIR es mayor que un porcentaje objetivo preestablecido, se acepta el proyecto. Si la TIR es menor que el objetivo, el proyecto se rechaza.

En otras palabras, es un indicador implementado en los bancos para determinar el riesgo de crédito. Ayuda a comprobar la viabilidad de una inversión, es decir, en cuanto mayor sea el valor de TIR mejor la inversión.

2.4.2. VAN

El valor actual neto (VAN) es el valor de todos los flujos de efectivo futuros (positivos y negativos) durante toda la vida de una inversión descontada al presente. El análisis VAN es una forma de valoración intrínseca y se usa ampliamente en finanzas y contabilidad para determinar el valor de un negocio, seguridad de inversión, proyecto de capital, nueva empresa, programa de reducción de costos y cualquier cosa que involucre flujo de caja. (Corporate Finance Institute, s.f.)

En otras palabras, es un indicador implementado para evaluar el rendimiento de una inversión.

2.4.3. ROI

El retorno de la inversión (ROI) se refiere a un índice financiero empleado para calcular el beneficio recibido por un inversor, en relación con el costo de su inversión. Se mide más comúnmente como el ingreso neto dividido por el costo de capital original de la inversión. Cuanto mayor sea la relación, mayor será el beneficio obtenido. (Corporate Finance Institute, s.f.)

2.4.4. Costo-Beneficio

Stobierski (2009) afirma que un análisis de costo-beneficio es el proceso de comparar los costos y beneficios (u oportunidades) proyectados o estimados asociados con una decisión de proyecto, para determinar si tiene sentido desde una perspectiva empresarial.

Si los beneficios proyectados superan los costos, podría argumentar que la decisión es buena. Si, por otro lado, los costos superan los beneficios, entonces una empresa puede querer repensar la decisión o el proyecto.

El análisis de costo-beneficio es un método esencial en el proceso de toma de decisiones de una organización, cuyos principios básicos y el marco se pueden aplicar a cualquier tipo de negocio.

2.4.5. Factibilidad

Un estudio de factibilidad, en términos financieros, “evalúa la viabilidad económica de una empresa propuesta evaluando los costos de puesta en marcha, los gastos operativos, el flujo de caja y haciendo una previsión del rendimiento futuro”. (Woodruff, 2019, párr.17)

En resumen, el resultado obtenido de un estudio de factibilidad es determinar si la propuesta de un proyecto es financieramente posible.

3. Marco Metodológico

En este capítulo se presenta la línea de trabajo para el desarrollo de la investigación, con el fin de alcanzar los objetivos propuestos.

De igual manera, se definen los aspectos relevantes de la metodología como el enfoque, alcance, diseño, fuentes de datos e información, sujetos de investigación, técnicas y el procedimiento metodológico como tal para el alcance de los objetivos.

3.1. Tipo de investigación

En primer lugar, se presenta el concepto de investigación, esta se define como: "conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema con el resultado (o el objetivo) de ampliar su conocimiento." (Hernández Sampieri & Mendoza, 2018, p.4)

Según Hernández y Mendoza (2018) existen tres tipos o enfoques de investigación: cualitativa, cuantitativa y mixta. A continuación, se define brevemente el enfoque mixto, el cual es el método de investigación más apropiado para la propuesta.

- **Investigación mixta:** se refiere a la combinación del enfoque cuantitativo y cualitativo. Hernández y Mendoza (2018) afirman que:

  Los métodos mixtos o híbridos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos tanto cuantitativos como cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada (denominadas meta inferencias) y lograr un mayor entendimiento del fenómeno bajo estudio (Hernández-Sampieri y Mendoza, 2008, p.10).

3.2. Enfoque de la investigación

Por medio del análisis de la información anterior, se considera que el enfoque mixto es el más adecuado para el desarrollo del presente proyecto ya que se combina la recopilación de información para el entendimiento y resolución de una problemática y se aplican métodos matemáticos para determinar la factibilidad económica de la propuesta.

3.3. Alcance de la investigación

El alcance de la investigación está sujeto a la estrategia establecida para el estudio. Sin embargo, según Hernández y Mendoza (2018), se definen cuatro variaciones en el alcance de una investigación:

- **Explicativo:** pretenden establecer las causas de los sucesos o fenómenos que se estudian.
- **Descriptivo:** busca especificar propiedades y características importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población.
- **Correlacional:** asocian variables mediante un patrón predecible para un grupo o población

- **Exploratorio:** aplica cuando el objeto de estudio es muy reciente o poco estudiado.

El proyecto busca proponer una mejora sobre la metodología de auditoría de TI implementada actualmente, por lo que se considera adecuado aplicar un alcance de investigación descriptivo.

3.4. Diseño de la investigación

En este apartado, se detalla el diseño de la investigación cualitativa correspondiente para este proyecto.

En el caso de las investigaciones cualitativas el diseño puede ser cambiante, específicamente en las que se basan en la búsqueda de información de un fenómeno en particular y el desarrollo de procedimientos que se apliquen en el contexto del problema. En resumen, se considera que la investigación cualitativa es un diseño en sí.

Sin embargo, de acuerdo con Hernández y Mendoza (2018), varios autores definen diferentes tipos de diseños cualitativos. En la Tabla 1 se muestra los diferentes diseños cualitativos con las preguntas de investigación y la información que proporciona.

Tabla 1. Diseños cualitativos

Pregunta de investigación	**Diseño**, marco o abordaje	**Información que proporciona**
Preguntas sobre procesos y relaciones entre conceptos que conforman un fenómeno.	**Teoría fundamentada**	Categorías del proceso o fenómeno y sus vínculos. Teoría que explica el proceso o fenómeno (problema de investigación).
Preguntas sobre las características, estructura y funcionamiento de un sistema social (grupo, organización, comunidad, subcultura, cultura), desde una familia, hermandad o hinchada hasta una megaciudad.	**Etnográfico**	Descripción y explicación de los elementos y categorías que integran al sistema social: historia y evolución, estructura (social, política, económica, etc.), interacciones, lenguaje, reglas y normas, patrones de conducta, mitos y ritos.

Pregunta de investigación	**Diseño**, marco o abordaje	**Información que proporciona**
Preguntas orientadas a comprender una sucesión de eventos, a través de las historias o narrativas de quienes la vivieron (experiencias de vida bajo una secuencia cronológica). Eventos como una catástrofe, una elección, la biografía de un individuo, etcétera.	**Narrativo**	Historias sobre procesos, hechos, eventos y experiencias, siguiendo una línea de tiempo, ensambladas en una narrativa general. Categorías relacionadas con tales historias y narrativa.
Preguntas sobre la esencia de las experiencias: lo que varias personas experimentan en común respecto a un fenómeno o proceso.	**Fenomenológico**	Experiencias comunes y distintas. Categorías que se presentan frecuentemente en las experiencias.
Preguntas sobre problemáticas o situaciones de un grupo o comunidad (incluyendo cambios).	**Investigación-acción**	Diagnóstico de problemáticas sociales, políticas, laborales, económicas, etc., de naturaleza colectiva. Categorías sobre las causas y consecuencias de las problemáticas y sus soluciones.

Fuente: Hernández y Mendoza (2018)

El objetivo del desarrollo del proyecto es determinar la problemática de una compañía y plantear una propuesta de solución que mejore o solvente la situación identificada. Por lo tanto, y con base en la información proporcionada en la tabla anterior, se indica que el diseño Investigación-Acción es el adecuado para esta propuesta.

3.5. Fuentes de datos e información

En esta sección, se definen las fuentes de información utilizadas como referencia para el desarrollo de la investigación.

En cuanto a las fuentes de información primarias, Maranto & González (2015) afirman que: "...contienen información original es decir son de primera mano, son el resultado de ideas, conceptos, teorías y resultados de investigaciones. Contienen información directa antes de ser interpretada, o evaluada por otra persona." (párr.2).

A continuación, se describen las fuentes de información consideradas en el presente estudio:

- Recursos proporcionados por la organización, como la metodología, guías de trabajo y material de estudio de capacitaciones.

- Juicio experto del equipo de trabajo de Auditoría de TI.
- Marcos de referencia como COBIT e ITIL.

Por otro lado, las fuentes secundarias "... son las que ya han procesado información de una fuente primaria." (Maranto & González, 2015, párr.3)

A continuación, se especifican las fuentes secundarias consideradas en la investigación:

- Recursos brindados por la Biblioteca del Instituto Tecnológico de Costa Rica.
- Recursos consultados en la web relacionados con el tema de auditoría de TI.
- Trabajos finales de graduación relacionados con el tema de auditoría de TI.

3.6. Población y selección de muestra

En esta sección se define la población total a la cual se le aplicará las técnicas de recopilación de información.

Según Neuman (2009, citado por Hernández et al., 2014):

> En la indagación cualitativa el tamaño de muestra no se fija a priori (antes de la recolección de los datos), sino que se establece un tipo de unidad de análisis y a veces se perfila un número aproximado de casos, pero la muestra final se conoce cuando las nuevas unidades que se añaden ya no aportan información o datos novedosos (p. 385).

3.7. Sujetos de investigación

En esta sección se definen los involucrados como sujetos de investigación que aportan de su conocimiento para el desarrollo del proyecto.

En la Tabla 2 se muestra el detalle de los sujetos de investigación considerados para este proyecto con el nombre del puesto, los años de experiencia en el área, el rol que desempeña y el aporte que brinda a esta investigación.

Tabla 2. Sujetos de investigación

Puesto	Experiencia	Rol	Aporte al proyecto
Gerente, Auditoría de TI (3 personas)	8 a 20 años	Gestiona la cartera de clientes. Revisa y aprueba el trabajo realizado por los colaboradores del área.	Experiencia con el uso de la metodología y apoyo en la identificación de las posibles brechas con respecto a otros marcos de referencia.
Asistentes, Auditoría de TI (8 personas)	1 a 3 años	Responsables de aplicar los procedimientos de auditoría con los clientes que correspondan. Gestiona el presupuesto de cada proyecto de auditoría.	Conocimiento sobre la aplicación de la metodología.

Fuente: Elaboración propia con información de la empresa DBG (2022).

3.8. Variables o categorías de la investigación

En esta sección se establecen las variables de investigación que corresponden a los temas relevantes al presente estudio. En la tabla 3, para cada una de las variables se describe su relevancia en el proyecto.

Tabla 3. Variables de investigación

Variable	Relevancia
Procesos COBIT	Determinar los procesos relevantes para la comparación y la elaboración de la propuesta de mejora de los controles generales de TI
Resultado de la comparación	Identificar las posibles brechas entre la metodología de la firma y COBIT.
Propuesta de mejora	Herramienta con los controles diseñados como respuesta a la identificación de las brechas.
Análisis financiero	Identificar las variables para determinar la factibilidad y los beneficios de la realización del proyecto.

Fuente: Elaboración propia.

3.9. Técnicas e instrumentos de recolección de datos

En este apartado se especifican las técnicas e instrumentos de investigación seleccionadas para la recolección de información.

En este caso, la investigación es cualitativa, por lo tanto, los instrumentos adecuados serían la revisión documental para la comparación, las entrevistas al personal de Auditoría de TI y encuestas que permitan evaluar la propuesta y recibir retroalimentación del diseño de controles.

3.9.1. Revisión documental

La revisión documental "sirve para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal" (Hernández & Mendoza, 2018, p.462)

En la presente investigación, la revisión documental es utilizada a lo largo de las diferentes etapas, ya que la firma cuenta con varios recursos para el entendimiento de la metodología. Por otro lado, se analizan las mejores prácticas para el alineamiento con la metodología y la identificación de mejoras. La plantilla para la revisión documental puede ser consultada en el Apéndice K.

3.9.2. Entrevistas

La entrevista cualitativa es más íntima, flexible y abierta que la cuantitativa (Savin-Baden y Major, 2013, y King y Horrocks, 2010). Se define como una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados).

En la entrevista, a través de las preguntas y respuestas se logra una comunicación y la construcción conjunta de significados respecto a un tema (Janesick, 1998).

Entre los tipos de entrevistas que pueden aplicarse en una investigación se encuentran: estructuradas, semiestructuradas y abiertas.

En el caso de la presente investigación, se aplican entrevistas no estructuradas o abiertas para la recolección de información específica para el desarrollo de las fases orientadas al entendimiento de la situación actual y la obtención de los insumos para el planteamiento del modelo económico.

La entrevista planteada para el entendimiento de la situación actual se puede consultar en el Apéndice C, mientras que la entrevista planteada para la recolección de datos para el análisis financiero puede observarse en el Apéndice E.

3.9.3. Encuestas

Según García Ferrando (s.f., citado por Casas, 2002) la encuesta se define como:

> Una técnica que utiliza un conjunto de procedimientos estandarizados de investigación mediante los cuales se recoge y analiza una serie de datos de una muestra de casos representativa de una población o universo más amplio, del que se pretende explorar, describir, predecir y/o explicar una serie de características (p.527).

En las encuestas se pueden aplicar varios tipos de preguntas: abiertas, cerradas o mixtas.

En cuanto a las preguntas abiertas, estas permiten respuestas más extensas, así como obtener mucha más información, ya que la persona que responde la encuesta puede expresar su respuesta con creatividad, porque no está limitado a un número especifico de opciones. (Easy Csat, s.f.)

Con relación a las preguntas cerradas, se utilizan para respuesta corta y enfocada; normalmente pueden ser preguntas de "Sí o No" y considerarse más rápidas de responder, ya que las respuestas u opciones son limitadas, también pueden ser analizadas de manera automática y no requieren acciones manuales de evaluación de la respuesta. (Easy Csat, s.f.)

Para la presente investigación, se aplica una encuesta para determinar si la propuesta permite una evaluación adecuada de los procesos en el alcance y recibir retroalimentación de los colaboradores del área. La encuesta aplicada puede consultarse en el Apéndice J.

3.10. Matriz de cobertura de las variables

En la Tabla 4, se visualiza la matriz de cobertura de las variables y el instrumento de investigación que aplica.

Tabla 4. Matriz de cobertura de las variables

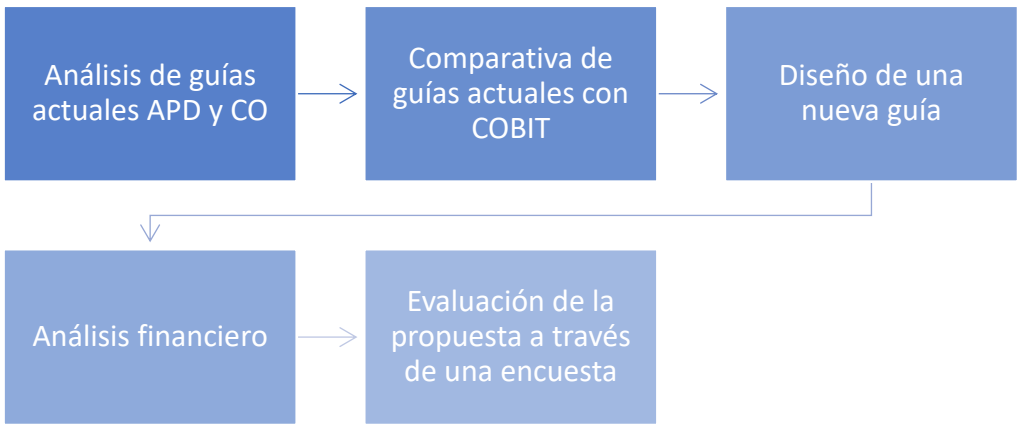
		Instrumento		
Variable		Entrevista	Encuesta	Revisión documental
	Procesos de COBIT	X		X
	Resultado de la comparación			X
	Propuesta de mejora		X	
	Análisis financiero	X		X

3.11. Procedimiento metodológico de la investigación

La metodología por utilizar para el desarrollo de la investigación se define de acuerdo con cuatro fases correspondientes a las etapas del ciclo de vida, contempladas dentro del alcance del proyecto. Con este procedimiento metodológico y con la ayuda de las técnicas e instrumentos mencionados en secciones anteriores, se espera alcanzar los objetivos establecidos.

En la Figura 6 se muestra el contenido de cada una de las fases definidas.

Figura 6. Fases de investigación



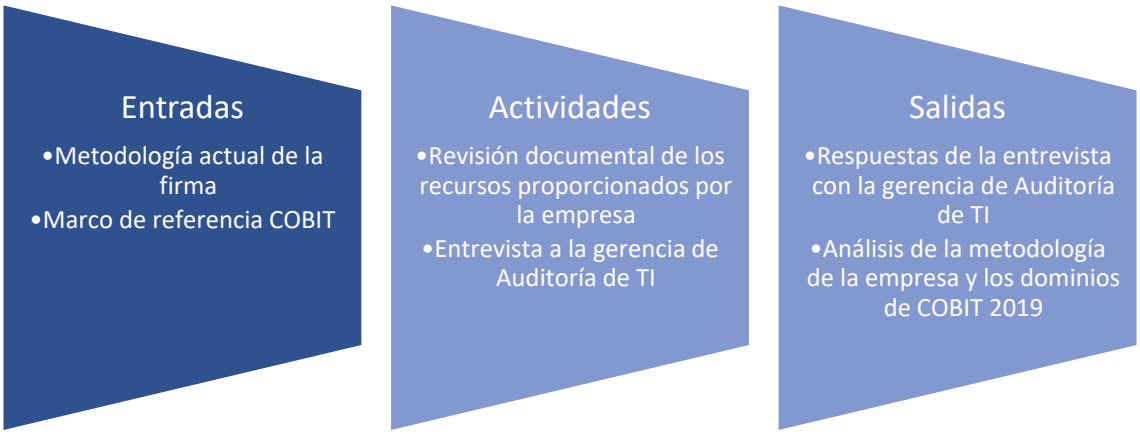
Fuente: Elaboración propia.

3.11.1. Fase 1: Análisis de guías actuales APD y CO

En esta fase se pretende realizar una revisión documental sobre la metodología actual implementada por la firma, específicamente la matriz de Controles Generales de TI para los procesos de Accesos a Programas y Datos y "Operaciones de Computadoras". De igual manera, se debe analizar el marco de referencia COBIT 2019 para efectos de la comparación con la metodología de la empresa.

En la Figura 7 se describen las entradas, actividades y salidas que conforman esta fase.

Figura 7. Fase 1: Entradas, actividades y salidas



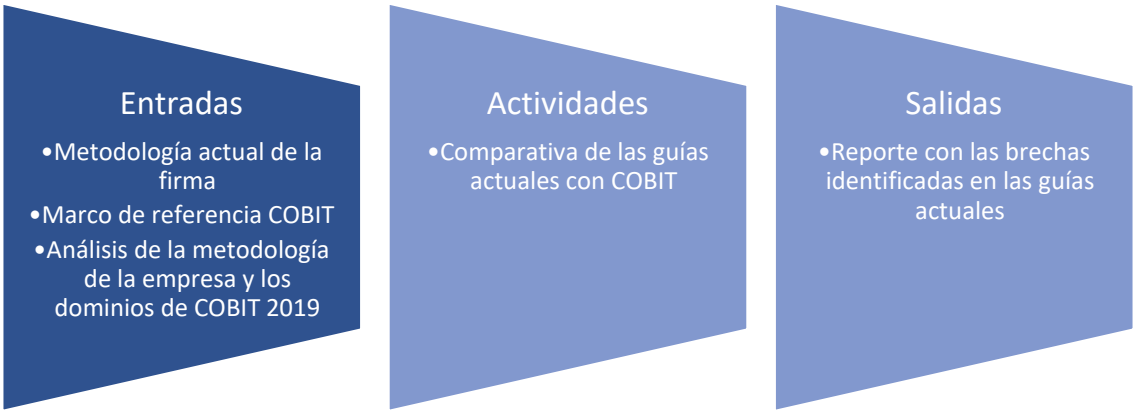
Fuente: Elaboración propia.

3.11.2. Fase 2: Comparativa de guías actuales con COBIT 2019

A partir del análisis y comparación de la metodología de la empresa con el marco de referencia COBIT 2019, en esta fase se identifican las posibles brechas en las guías actuales para los procesos de "Acceso a Programas y Datos" y "Operaciones de Computadoras".

En la Figura 8 se describen las entradas, actividades y salidas que conforman esta fase.

Figura 8. Fase 2: Entradas, actividades y salidas



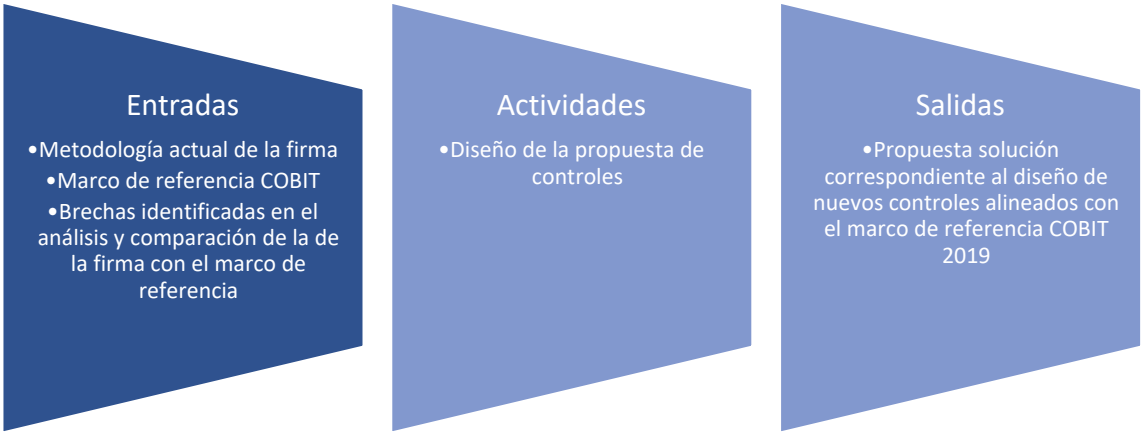
Fuente: Elaboración propia.

3.11.3. Fase 3: Diseño de una nueva guía

A partir del análisis y comparación de la metodología de la empresa con el marco de referencia COBIT 2019, en esta fase se diseña la propuesta de controles para los procesos de "Acceso a Programas y Datos" y "Operaciones de Computadoras" que solventan las brechas identificadas.

En la Figura 9 se describen las entradas, actividades y salidas que conforman esta fase.

Figura 9. Fase 3: Entradas, actividades y salidas



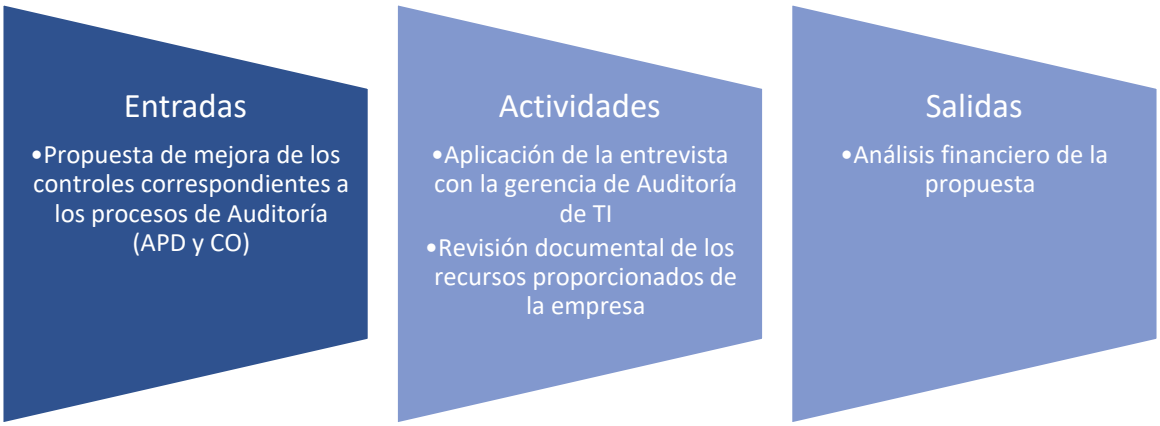
Fuente: Elaboración propia.

3.11.4. Fase 4: Análisis financiero

En esta fase, se analiza la factibilidad de la implementación de la propuesta de mejora desarrollada. Se determina, desde una perspectiva financiera, cuáles son los requerimientos necesarios para la aplicación de la propuesta y los beneficios que ofrece al área de Auditoría de TI.

En la Figura 10 se describen las entradas, actividades y salidas que conforman esta fase.

Figura 10. Fase 4: Entradas, actividades y salidas



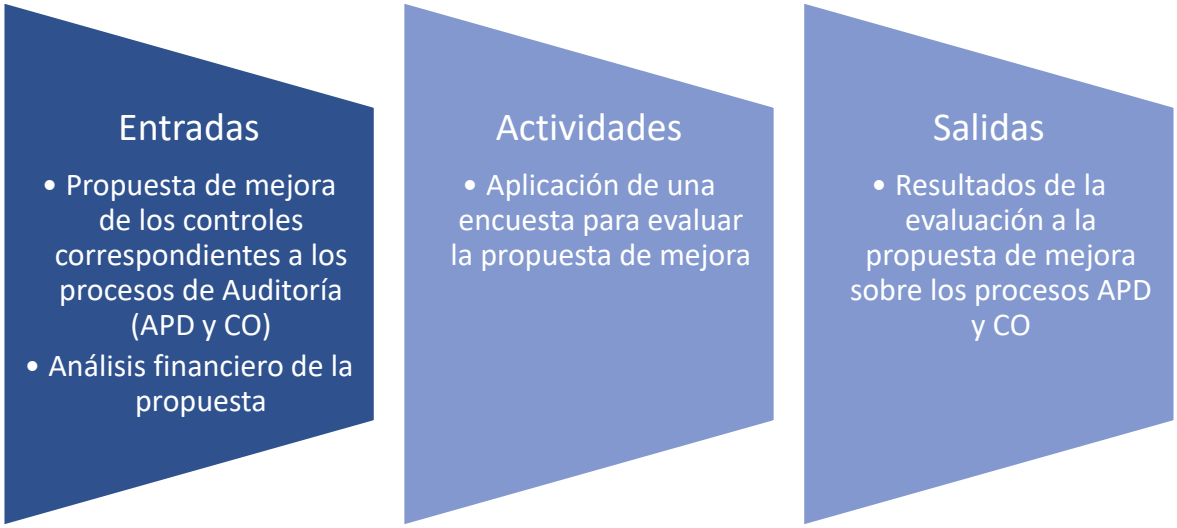
Fuente: Elaboración propia

3.11.5. Fase 5: Evaluación de la propuesta a través de una encuesta

Por último, con base en la propuesta de solución planteada, se aplica una evaluación a los sujetos de investigación. Lo anterior tiene como objetivo la obtención de retroalimentación del área de Auditoría de TI y sus opiniones sobre la viabilidad de la herramienta presentada en términos cualitativos y cuantitativos.

En la Figura 11 se describen las entradas, actividades y salidas que conforman esta fase.

Figura 11. Fase 5: Entradas, actividades y salidas



Fuente: Elaboración propia.

3.12. Operacionalización de las variables o categorías

En esta sección, se resume el marco metodológico incluyendo cada fase con su objetivo, instrumentos, variables y sujetos de investigación. En la Tabla 5 se logra apreciar dicha información de manera sintetizada.

Tabla 5. Matriz Operacionalización de las variables o categorías

Fase	Objetivo de la fase	Instrumentos	Variables	Sujetos de investigación
Fase 1: Análisis de guías actuales APD y CO	Identificar los procesos COBIT relacionados con Accesos a Programas y Datos y "Operaciones de Computadoras".	• Revisión documental • Entrevista	Procesos de COBIT Actividades COBIT 2019	Gerente Auditoría de TI
Fase 2: Comparativa de guías actuales con COBIT 2019	Identificar posibles brechas de la guía actual.	• Revisión documental	Resultado de la comparación	Gerente Auditoría de TI
Fase 3: Diseño de una nueva guía	Diseñar una guía para los procesos APD y CO, a partir de las oportunidades de mejora identificadas en la comparativa.	• Revisión documental	Resultado de la comparación	Gerente Auditoría de TI
Fase 4: Análisis financiero	Determinar la factibilidad de la propuesta.	• Revisión documental • Entrevista	Propuesta de mejora Análisis financiero	Gerente Auditoría de TI
Fase 5: Evaluación de la propuesta a través de una encuesta	Evaluar por medio de una encuesta la propuesta solución.	• Encuesta	Propuesta de mejora Análisis financiero	Gerente Auditoría de TI Asistentes Auditoría de TI

Fuente: Elaboración propia.

4. Análisis de Resultados

En este capítulo cuatro se determina el análisis de resultados para el presente Trabajo Final de Graduación, el cual tiene como objetivo explicar la investigación realizada mediante la aplicación de las distintas herramientas de investigación planteadas en el Marco Metodológico.

En el presente análisis se incluyen las primeras dos fases planteadas en el capítulo anterior, como parte del Procedimiento metodológico de la investigación. Estas dos fases corresponden a Fase 1: Análisis de guías actuales, tanto de la metodología actual de la organización como el marco de referencia COBIT y sus dominios, y la Fase 2: Comparativa de guías actuales con COBIT 2019 para los procesos de "Acceso a Programas y Datos" y Operación de Computadoras.

Como producto de estas fases se obtendrán los insumos necesarios para el diseño de la propuesta solución que responde a la situación problemática y objetivos planteados en el proyecto.

4.1. Fase 1: Análisis de guías actuales

En este apartado se presenta el desarrollo de la primera fase de la investigación, la cual tiene como objetivo principal adquirir un entendimiento sobre la situación actual de los controles aplicados para los procesos Accesos a Programas y Datos y Operación de Computadoras. De igual manera, se analizan los dominios y objetivos de gestión presentes en el marco de referencia COBIT 2019 que se relacionan los controles de los procesos del alcance de la guía actual de la organización.

Para el desarrollo de la Fase 1: Análisis de guías actuales, como instrumento de investigación, se aplicó una entrevista no estructurada a la gerencia de Auditoría de TI, con el fin de determinar la situación actual relacionada con los controles implementados en la metodología para los procesos de "Acceso a Programas y Datos" y Operación de Computadoras. Asimismo, se indaga sobre los controles que se consideran críticos como parte de los resultados obtenidos del servicio de auditoría.

4.1.1. Análisis de la metodología actual y el marco de referencia COBIT 2019

Primeramente, se debe identificar, en la metodología actualmente implementada por la firma, los procedimientos de auditoría que involucran los procesos correspondientes a ""Acceso a Programas y Datos" (APD)" y ""Operaciones de Computadoras" (CO)"

Luego, con base en la revisión documental del marco de referencia COBIT 2019, resulta pertinente determinar los procesos que se alinean con los procesos ""Acceso a Programas y Datos" (APD)" y ""Operaciones de Computadoras" (CO)".

Por último, elaborar un análisis de brecha, con el fin de puntualizar las oportunidades de mejora en la metodología de la firma.

4.1.1.1. Análisis de la situación actual

Con el fin de comprender los procedimientos de auditoría, relacionados con los procesos de "Acceso a Programas y Datos" y "Operaciones de Computadoras", se realizó una entrevista no estructurada dirigida a la gerencia de Auditoría de TI. En el Apéndice D se puede consultar la entrevista aplicada como herramienta de investigación para esta fase, en donde se determina si los controles utilizados actualmente permiten una evaluación completa y efectiva.

En esta entrevista se pretende indagar con los profesionales con experiencia en la firma si consideran que la metodología implementada permite realizar una adecuada evaluación del proceso y cuáles son las brechas que han identificado a lo largo del tiempo.

De la información obtenida, se determina que existe una necesidad de alinear los controles actuales con un marco de referencia para la mejora continua de las auditorías. Se menciona que muchos de los clientes cuestionan la revisión de los servicios de auditoría con una mejor práctica reconocida y actualizada, aspecto que puede restar confiabilidad y credibilidad.

Los controles definidos para el proceso de Accesos a Programas y Datos están conformados por evaluaciones a los mecanismos de autenticación en los diferentes aplicativos que implementa el cliente, en especial aquellos sistemas de información que influyen en alto nivel sobre los reportes financieros.

Luego, se evalúa la configuración sobre la parametrización de contraseñas, de modo que se cumplan las reglas de administración y sintaxis establecidas en la política de seguridad de la información definida en la organización y con los estándares de calidad y seguridad de la industria.

En cuanto a la administración de cuentas con alto nivel de privilegio, los procedimientos aseguran que las solicitudes para este tipo de acceso se pueden gestionar de modo que se les de trazabilidad de inicio a fin y que cuenten con las aprobaciones de las jefaturas respectivas en cada fase.

Se implementa un control referente al monitoreo de los accesos físicos a las instalaciones, donde se alojan los servidores locales que almacenan datos de evaluación de la compañía.

Para estos accesos físicos, se asegura que las organizaciones gestionen las solicitudes de acceso por medio de una herramienta, de modo que se le pueda dar trazabilidad a las autorizaciones de las jefaturas correspondientes y que estos permisos se alineen con los roles y responsabilidades de los colaboradores a los que se les asignan.

Asimismo, la evaluación toma en consideración si las organizaciones en proceso de auditoría mitigan los riesgos de accesos no autorizados, realizando revisiones periódicas de usuarios activos e inactivos y como resultado efectuar modificaciones o eliminaciones de accesos inapropiados.

En la Tabla 6. Guía actual para el proceso APD se resumen los controles definidos explicados anteriormente que se encuentran en la guía actual para el proceso de Accesos a Programas y Datos (APD).

Tabla 6. Guía actual para el proceso APD

Control APD
1. *La organización establece una política de seguridad de la información que está alineada apropiadamente con la organización.*
2. *La organización ha adoptado una política de seguridad formal que ofrece una guía para la seguridad de la información.*

Control APD
3. *La organización ha establecido un mecanismo de autenticación* 4. *Si las contraseñas son utilizadas para autenticación, la organización debe establecer reglas para su administración y sintaxis.* 5. *El acceso al ID con mayores privilegios, a nivel de sistemas operativos, base de datos y aplicativos, incluidos en el alcance está restringido al personal a cargo de la administración del sistema.* 6. *El acceso a los ID con privilegios funcionales en los aplicativos incluidos en el alcance que se utilizan para iniciar transacciones financieras críticas está restringido a los usuarios apropiados.* 7. *El acceso físico al equipo que resguarda la información de la organización está restringido al personal adecuado.* 8. *La organización tiene mecanismos efectivos para registrar la actividad en la seguridad e identificar violaciones potenciales, así como escalar esos incidentes a mandos superiores y tomar medidas oportunamente para reducir el riesgo de acceso inapropiado o autorizado a los datos o aplicaciones relevantes de reporte financiero.* 9. *Un mecanismo efectivo está implementado para asegurar que el acceso es otorgado, modificado apropiadamente o revocado (renuncio o despido) cuando ocurren cambios en las funciones o terminación del trabajo.* 10. *La organización revisa periódicamente los usuarios activos o inactivos y los derechos de acceso de usuarios para identificar y eliminar accesos inapropiados al sistema.* 11. *La auditoría interna o cualquier otro órgano interno revisa periódicamente la segregación de funciones de la organización. La administración de la organización resuelve los problemas identificados en la segregación de funciones modificando los roles funcionales o los privilegios de acceso de usuario relacionados.*

Fuente: Elaboración propia con datos de la empresa DBG.

Por otro lado, en la entrevista con la gerencia de Auditoría de TI se consulta cuáles son los controles críticos de cada proceso, según el conocimiento y experiencia de la gerente de Auditoría de TI. Para el proceso de accesos, se considera que los accesos administrativos con alto nivel de privilegio tienen gran prioridad en los procedimientos de auditoría y el aseguramiento de la segregación de funciones.

En segundo lugar, para el proceso de "Operaciones de Computadoras", se definen una serie de controles que se enfocan en el tema de configuración de *Jobs* o tareas automatizadas, respaldos, restauraciones de respaldos e incidentes.

Con el tema de *Jobs*, programas o tareas automatizadas se evalúa que en caso de fallos se gestione de forma que se asegure una corrección exitosa, dejando evidencia de la ejecución.

Con respecto al tema de incidentes, el enfoque abordado son los eventos que impactan *Jobs* de sistemas, procesos y/o programas críticos donde se asegure un monitoreo constante y la resolución dentro de una ventana de tiempo oportuna.

En este proceso también se toma en cuenta el tema de accesos, de forma que las organizaciones establezcan restricciones sobre los usuarios que tienen accesos a la configuración de *Jobs*, donde las jefaturas respectivas den el visto bueno requerido. Esto igual aplica con los usuarios que tienen acceso para modificar la configuración de los respaldos automáticos.

Estos controles procuran que los procedimientos relacionados con la configuración de *Jobs*, respaldos y el proceso de incidentes esté formalmente documentado y aprobado en las políticas de operaciones de TI.

Como parte de los resultados obtenidos de la entrevista con la gerencia de Auditoría de TI, en el caso del proceso de "Operaciones de Computadoras", la configuración de *Jobs* y respaldos son los puntos que consideran como críticos y pertinentes de tomar en cuenta al instante de evaluar estos controles.

En la Tabla 7 se resumen los controles que se encuentran en la guía actual para el proceso de Operación de Computadoras.

Tabla 7. Guía actual para el proceso CO

Control CO
1. *Los Jobs, procesos y programas son monitoreados y los procesos fallidos son corregidos asegurando una ejecución exitosa.*
2. *Los incidentes de sistemas de TI que impactan los Jobs de sistemas, procesos y/o programas relevantes son monitoreados y resueltos dentro de la ventana de tiempo definida.*
3. *Solo los usuarios autorizados tienen acceso a la configuración de Jobs.*
4. *Programas y datos son respaldados según la política de Operaciones de TI.*
5. *Solo usuarios autorizados tienen acceso a la configuración de respaldos automáticos.*

Fuente: Elaboración propia con datos de la empresa DBG.

4.1.2. Análisis de guías actuales APD y CO

En esta sección se presenta la segunda parte de la Fase 1: Análisis de guías actuales, la cual consiste propiamente en la alineación de las guías actuales para los procesos en el alcance implementados por la firma de auditoría, con respecto a la guía de mejores prácticas COBIT 2019.

En primer lugar, en la sección Procesos COBIT 2019 relacionados con "Acceso a Programas y Datos", se analiza cuáles son los dominios y objetivos de gestión presentes en COBIT 2019 relacionados con el proceso de Accesos a Programas y Datos, de forma que se pueda identificar las brechas que presenta la guía actual.

Luego, en la sección Procesos COBIT 2019 relacionados con "Operaciones de Computadoras", se identifican los dominios y objetivos de gestión presentes en COBIT 2019 que se vinculan con los controles actualmente implementados en la guía de la firma, para el proceso de "Operaciones de Computadoras".

Específicamente para este apartado, el instrumento de investigación que se emplea es la revisión documental de los insumos proporcionados por la empresa, como la metodología de los controles generales de TI, donde se incluyen los procesos en el alcance, las guías desarrolladas por la firma internacional y el material de capacitaciones. Asimismo, se utiliza como insumo el marco de referencia COBIT 2019 para determinar los dominios y objetivos de gestión que apliquen para efectos de la comparativa.

Esta fase tiene como objetivo producir un insumo para la comparación e identificación de brechas entre las guías y, posteriormente, diseñar los controles compensatorios que atienden dichas brechas como propuesta solución del proyecto.

4.1.2.1. Procesos COBIT 2019 relacionados con "Acceso a Programas y Datos"

El marco de referencia COBIT 2019 agrupa los objetivos de gobierno y gestión en cinco dominios. En este dominio, el órgano de gobierno evalúa las opciones estratégicas, guía a la alta gerencia con respecto a las opciones estratégicas elegidas y monitoriza el logro de la estrategia. (ISACA, 2019).

Mediante el análisis de modelo core de COBIT y sus 5 dominios, se identifican aquellos objetivos que se relacionan con la gestión de Accesos a Programas y Datos. Los dominios de estudio para este caso son: "Alinear, Planificar y Organizar (APO)" y "Entregar, Dar Servicio y Soporte (DSS)". (ISACA, 2019)

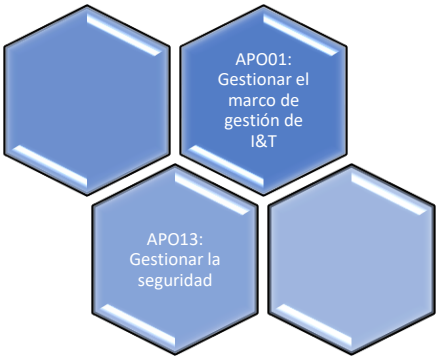
4.1.2.1.1. Alinear, Planificar y Organizar (APO)

En este dominio se aborda la organización general, estrategia y actividades de apoyo para la información y la tecnología (I&T) (ISACA, 2019). En este grupo se incluyen 14 objetivos de gestión que abordan la gestión de I&T (Información & Tecnología), la estrategia, la arquitectura empresarial, la innovación, el portafolio, presupuesto y costes, recursos humanos, las relaciones, los acuerdos de servicio, los proveedores, la calidad, el riesgo, la seguridad y los datos.

Específicamente para el proceso de "Acceso a Programas y Datos", es importante tomar en cuenta los objetivos presentados en la Figura 12, los cuales corresponden a la gestión del marco de gestión

de I&T y la gestión de la seguridad. Ambos están altamente relacionados con los controles que se implementan actualmente en la guía para el proceso APD.

Figura 12. Objetivos APO para APD



Fuente: Adaptación de COBIT 2019.

El objetivo de gestión APO01: Gestionar el marco de gestión de I&T está conformado por un conjunto de prácticas orientadas al diseño de sistema de gestión para la I&T de la empresa basados en las metas empresariales (ISACA, 2019). Debido a que el proceso de "Acceso a Programas y Datos" incluye controles sobre las políticas de seguridad de la información se debe asegurar que las auditorías tomen en consideración la alineación de estas con las regulaciones externas y los estándares de la industria.

En cuanto al objetivo APO13: Gestionar la seguridad, este se encuentra conformado por un conjunto de prácticas orientadas a definir, operar y monitorizar un sistema de gestión de seguridad de la información (ISACA, 2019). El proceso de "Acceso a Programas y Datos" tiene como objetivo gestionar la seguridad de la información en las organizaciones, por lo cual esta práctica COBIT es la más adecuada para la comparación y la identificación de posibles brechas.

En la Tabla 8 se resume la correlación del objetivo de gestión perteneciente al dominio APO con el proceso de estudio APD.

Tabla 8. Relación objetivos de gestión APO con APD

Objetivo APO	**Descripción**	**Relación con APD**
APO01: Gestionar el marco de gestión de I&T	Diseñar el sistema de gestión para la I&T de la empresa basándose en las metas empresariales y otros factores de diseño.	Esta práctica garantiza el cumplimiento de regulaciones externas y las políticas internas
APO13: Gestionar la seguridad	Definir, operar y monitorizar un sistema de gestión de seguridad de la información.	Este objetivo respalda la seguridad de la información, infraestructura y aplicaciones de procesamiento y privacidad.

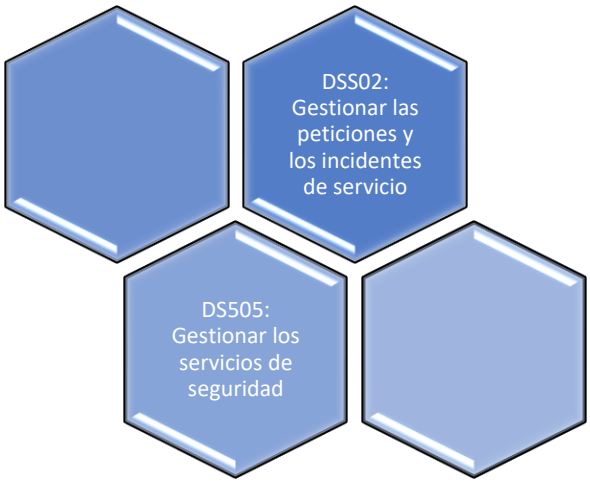
Fuente: Elaboración propia con datos de (ISACA, 2018)

4.1.2.1.2. Entregar, Dar Servicio y Soporte (DSS)

En este dominio se aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad (ISACA, 2019). Es decir, se enfoca en cómo se entrega el servicio relacionado con los sistemas a clientes internos y externos, y al mismo tiempo se asegura la confiabilidad y seguridad de los datos e información.

En cuanto a los objetivos de gestión para este dominio, los que están altamente relacionados con el proceso de "Acceso a Programas y Datos" son: DSS02- Gestionar las peticiones y los incidentes de servicio y DSS05- Gestionar los servicios de seguridad, presentados en la Figura 13.

Figura 13. Objetivos DSS para APD



Fuente: Adaptación de COBIT 2019.

En el objetivo de gestión DSS02: Gestionar las peticiones y los incidentes de servicio, se presentan las mejores prácticas para la administración de herramientas de incidentes y la atención de los distintos eventos y solicitudes que se procesan a través de esta. Como parte del proceso de "Acceso a Programas y Datos", los controles aseguran que se realice el procesamiento de solicitudes de nuevos accesos, modificaciones y eliminaciones para rastrear que los permisos asignados están alineados con roles y responsabilidades y se mantenga una segregación de funciones en los sistemas de información.

Por esta razón, se debe procurar que, a la hora de implementar herramientas, para la gestión de peticiones e incidentes, estas permitan una configuración que se ajuste a las necesidades de la organización y que apoyen en el cumplimiento de las políticas de seguridad de la información.

En segundo lugar, en cuanto al objetivo DSS05: Gestionar los servicios de seguridad, tiene como objetivo la protección de los datos e información de las organizaciones y ofrece una guía de las mejores prácticas para lograrlo.

Su relación con el "Acceso a Programas y Datos" es alta, ya que en ambos se busca que se gestione de manera correcta los permisos administrativos y se monitoree la operación de usuarios con este perfil, asegurando nuevamente una segregación de funciones.

En la Tabla 9 se resume la correlación del objetivo de gestión perteneciente al dominio DSS con el proceso de estudio APD.

Tabla 9. Relación objetivos de gestión APO con APD

Objetivo DSS	**Descripción**	**Relación con APD**
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.	Este objetivo de gestión permite que se implemente un control sobre las solicitudes de creaciones, modificaciones y eliminaciones de cuentas de usuario garantizando un tratamiento correcto de estas.
DSS05: Gestionar los servicios de seguridad	Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad.	Esta práctica garantiza el cumplimiento de regulaciones externas y las políticas internas.

Fuente: Elaboración propia con datos de COBIT 2019.

4.1.2.2. Procesos COBIT 2019 relacionados con "Operaciones de Computadoras"

En esta sección, nuevamente se presenta un análisis de los dominios y objetivos de gestión proporcionados por el marco de referencia COBIT 2019. Sin embargo, esta vez se realiza el análisis orientado al proceso de "Operaciones de Computadoras". Se busca conocer la correlación de las mejores prácticas con la gestión de programas y tareas automatizadas.

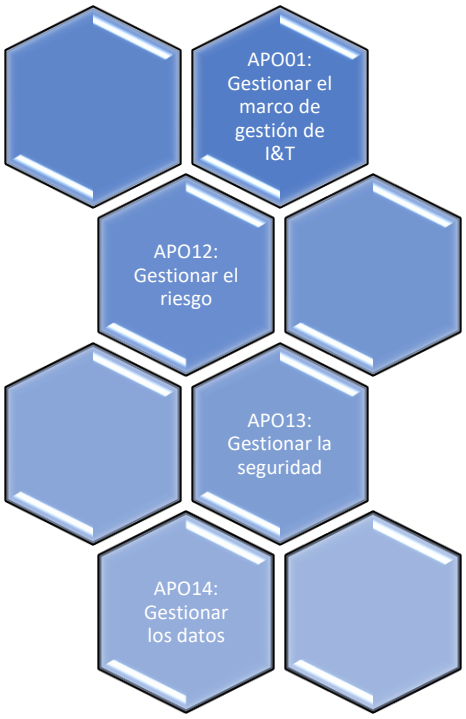
Mediante el análisis de modelo principal de COBIT y sus 5 dominios, se identifican aquellos objetivos que se relacionan con la gestión de "Operaciones de Computadoras". Los dominios de estudio para este caso son: "Alinear, Planificar y Organizar (APO)" y "Entregar, Dar Servicio y Soporte (DSS)". (COBIT, 2019).

4.1.2.2.1. Alinear, Planificar y Organizar (APO)

El dominio APO está orientado a las prácticas que procuran que la gestión operativa de los sistemas de información esté alineadas a las metas estratégicas de la organización. En este dominio se agrupan catorce objetivos para lograrlo. Dentro de los objetivos relacionados con el "Operaciones de Computadoras", se identifican: APO01: Gestionar el marco de gestión de I&T, APO12: Gestionar el riesgo, APO13: Gestionar la seguridad y APO14: Gestionar los datos.

En la Figura 14 se presentan los objetivos de gestión del dominio APO para el proceso de "Operaciones de Computadoras".

Figura 14. Objetivos APO para CO



Fuente: Adaptación de COBIT 2019.

En primer lugar, el objetivo APO01: Gestionar el marco de gestión de I&T tiene como objetivo diseñar un marco de gestión orientado al cumplimiento de los objetivos estratégicos de las organizaciones. Su correlación con el proceso de Operaciones a Computadoras se refiere a que en la guía actual se incluyen controles que evalúan la inclusión de estos procesos en las políticas de seguridad de la información.

El objetivo APO12: Gestionar el riesgo se enfoca en los procesos de identificar los riesgos y reducirlos a un nivel aceptable para la organización. Su correlación con el proceso "Operaciones de Computadoras" está orientado al aseguramiento de la reducción del riesgo que surge de la gestión de programas o tareas automatizadas que tienen incidencia en la operativa de las organizaciones.

El objetivo APO13: Gestionar la seguridad está orientado a definir un marco de seguridad de la información sobre los datos y reportes sensibles de las organizaciones. El proceso de "Operaciones de Computadoras" procura que la gestión de programas y tareas automatizadas se ejecute dentro de un margen de seguridad aceptable que cumpla con las regulaciones de la organización y de entidades externas.

Por último, el objetivo APO14: Gestionar los datos está orientado a las mejores prácticas que aseguran que se aplique un tratamiento de los datos que cumpla con los estándares de calidad y se encuentre dentro del margen de seguridad de la información.

En la Tabla 10 se detalla la correlación del objetivo de gestión perteneciente al dominio APO con el proceso de estudio CO, de acuerdo con las definiciones presentes en COBIT 19.

Tabla 10. Relación objetivos APO con CO

Objetivo APO	**Descripción**	**Relación con CO**
APO01: Gestionar el marco de gestión de I&T	Diseñar el sistema de gestión para la I&T de la empresa basándose en las metas empresariales y otros factores de diseño. Con base en este diseño, implementar todos los componentes necesarios del sistema de gestión.	Esta práctica garantiza el cumplimiento de regulaciones externas y las políticas internas
APO12: Gestionar el riesgo	Identificar, evaluar y reducir continuamente los riesgos relacionados con I&T dentro de los niveles de tolerancia establecidos por la gerencia ejecutiva de la empresa.	Esta práctica asegura que se reduzcan los riesgos asociados a la configuración de *Jobs* y respaldos que son críticos para los reportes financieros.

Objetivo APO	Descripción	Relación con CO
APO13: Gestionar la seguridad	Definir, operar y monitorizar un sistema de gestión de seguridad de la información.	Se relaciona con la gestión de *Jobs* y respaldos donde se evalúa que la configuración es correcta y solo los usuarios autorizados puedan administrarlos.
APO14: Gestionar los datos	Lograr y mantener la gestión eficaz de los activos de datos de la empresa durante todo el ciclo de vida de los datos, desde la creación hasta su entrega, mantenimiento y archivo.	Se relaciona ya que esta práctica garantiza que los *Jobs* configurados manipulen los datos de la manera correcta manteniendo su integridad.

Fuente: Elaboración propia con datos de COBIT 2019.

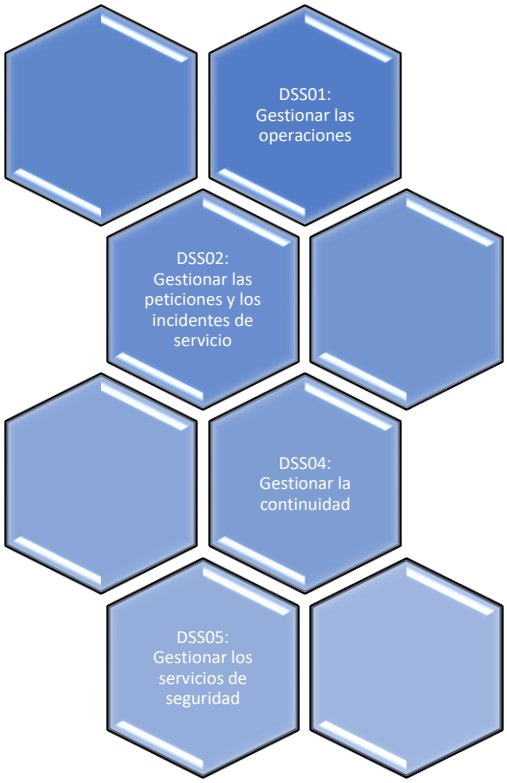
4.1.2.2.2. Entregar, Dar Servicio y Soporte (DSS)

En este dominio se aborda la entrega operativa y el soporte de los servicios de información y tecnología (I&T), incluida la seguridad (ISACA, 2019). Es decir, se enfoca en cómo se le entrega el servicio relacionado con los sistemas a clientes internos y externos, y al mismo tiempo se asegura la confiabilidad y seguridad de los datos e información.

Por lo tanto, su correlación con el proceso de "Operaciones de Computadoras" reside en que la entrega de servicios automatizados sea lo sumamente eficiente y confiable, ya que maneja información crítica para la organización, que tienen impacto en los informes financieros y cuentas contables.

En cuanto a los objetivos de gestión para este dominio, los que están altamente relacionados con el proceso de "Operaciones de Computadoras": DSS01: Gestionar las operaciones, DSS02: Gestionar las peticiones y los incidentes de servicio, DSS04: Gestionar la continuidad, DSS05: Gestionar los servicios de seguridad; los cuales se presentan gráficamente en la Figura 15.

Figura 15. Objetivos DSS para CO



Fuente: Adaptación de COBIT 2019.

Se considera el objetivo DSS01: Gestionar las operaciones, ya que permite establecer controles sobre la gestión de procedimientos operativos implicados en la entrega de servicios de tecnología de información.

El objetivo DSS02: Gestionar las peticiones y los incidentes de servicio está orientado a las mejores prácticas para la implementación de una herramienta que gestione peticiones e incidentes de servicio. En cuanto al proceso de Operación de Computadoras, los controles deben procurar que los fallos en la ejecución de tareas programadas se manejen correctamente, de manera que se asegure la reanudación de los servicios que trabajan con información que impactan los reportes financieros u operaciones críticas de las organizaciones.

Por otro lado, también se toma en consideración el objetivo DSS04: Gestionar la continuidad, el cual consiste en recordar a las organizaciones de tener un plan que atienda los incidentes y establezca las mejores técnicas de respuesta para mitigarlos.

Por último, se incluye el objetivo DSS05: Gestionar los servicios de seguridad; el cual está altamente relacionado con el proceso de "Operaciones de Computadoras", ya que los procedimientos de auditoría que se ejecuten deben atender las tareas programas o automatizadas de forma que se asegure que se encuentran reguladas bajo un marco de seguridad aceptable.

En la Tabla 11 se presenta un resume de la correlación del objetivo de gestión perteneciente al dominio DSS con el proceso APD en estudio.

Tabla 11. Relación objetivos DSS con CO

Objetivo DSS	**Descripción**	**Relación con CO**
DSS01: Gestionar las operaciones	Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar los servicios de I&T, internos y externalizados. Incluir la ejecución de procedimientos de operación estándar predefinidos y las actividades de supervisión requeridas.	Establece una guía sobre la coordinación ejecución de procesos automatizados que son críticos para la carga de información a los reportes financieros.
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.	Este objetivo de gestión permite que se implemente un control sobre las solicitudes de creaciones, modificaciones y eliminaciones de cuentas de usuario garantizando un tratamiento correcto de estas.
DSS04: Gestionar la continuidad	Establecer y mantener un plan que permita a las organizaciones empresariales y a TI responder a los incidentes y adaptarse rápidamente a las interrupciones. Esto permitirá la operación continua de los procesos críticos de negocio y de los servicios de I&T necesarios, y mantener la disponibilidad de recursos, activos e información en un nivel aceptable para la empresa.	Esta práctica responde a la necesidad de gestionar de manera correcta los casos en los que se presenten fallos en la ejecución de *Jobs* y respaldos. Además, se evalúa la herramienta de incidentes.
DSS05: Gestionar los servicios de seguridad	Proteger la información de la empresa para mantener el nivel de riesgo de la seguridad de la información aceptable para la empresa, conforme con la política de seguridad. Establecer y mantener roles y privilegios de acceso de seguridad de la información. Realizar una monitorización de la seguridad.	Esta práctica garantiza el cumplimiento de regulaciones externas y las políticas internas.

Fuente: Elaboración propia con datos de (ISACA, 2018)

4.2. Fase 2: Comparativa de guías actuales con COBIT 2019

En esta sección se presenta la comparativa de las guías actuales implementadas por la organización, con el marco de referencia COBIT 2019, con el objetivo de identificar cuáles procedimientos de auditoría de TI se están quedando fuera del alcance de evaluación.

En cuanto al desarrollo de la Fase 2: Comparativa de guías actuales con COBIT 2019, el instrumento de investigación aplicado fue la revisión documental de los insumos proporcionados por la organización, como metodologías, guías y material de capacitaciones del área. Por otro lado, se inspecciona el material correspondiente al marco de referencia en estudio COBIT 2019, específicamente los dominios que se alinean con los procesos del alcance: "Acceso a Programas y Datos" y Operación de Computadoras determinados en la Fase 1: Análisis de guías actuales.

En primer lugar, en la sección Comparativa de la guía APD con COBIT 2019, se realizará la comparativa de la guía actual con el marco de referencia COBIT 2019 para el proceso de "Acceso a Programas y Datos" para obtener las posibles brechas que se presenten.

Luego, en la sección Comparativa de la guía CO con COBIT 2019, se presenta el análisis realizado mediante la inspección de la guía actual para el proceso de "Operaciones de Computadoras" en relación con las mejores prácticas presentadas en COBIT 2019, con el fin de determinar cuáles son las posibles brechas.

4.2.1. Comparativa de la guía APD con COBIT 2019

A partir del análisis de la situación actual con las guías implementadas para el proceso de "Acceso a Programas y Datos" (APD) en la sección Fase 1: Análisis de guías actuales, se realiza una comparativa con los dominios y objetivos de gestión identificados para determinar las posibles brechas.

En la Tabla 12 se encuentra la lista de controles incluidos en la matriz de Controles Generales de TI para el proceso de "Acceso a Programas y Datos" asociados a los objetivos de gestión determinados en el análisis de la guía COBIT 2019. Como resultado, en la columna "Brecha" se justifica cuál es la variante encontrada a partir de la comparativa de ambos controles.

Tabla 12. Comparativa controles APD de la guía actual con COBIT 2019

Control APD	**Objetivo de Gestión**	**Brecha**
1. La organización establece una política de seguridad de la información que está alineada apropiadamente con la organización.	DSS05: Gestionar los servicios de seguridad	DSS05.02 Gestionar la seguridad de la conectividad y de la red. La empresa no evalúa las medidas de seguridad y procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.

Control APD	Objetivo de Gestión	Brecha
2. *La organización ha adoptado una política de seguridad formal que ofrece una guía para la seguridad de la información.*	DSS05: Gestionar los servicios de seguridad	DSS05.03 Gestionar la seguridad de *endpoint*. La empresa no evalúa que se definan mecanismos de seguridad para los distintos tipos de dispositivos para la protección de datos. Tampoco se toma en cuenta la gestión de dispositivos electrónicos, así como la asignación y eliminación de estos en la red de la empresa.
3. *La organización ha establecido un mecanismo de autenticación*	DSS05: Gestionar los servicios de seguridad	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. No se identifica alguna brecha.
4. *Si las contraseñas son utilizadas para autenticación, la organización debe establecer reglas para su administración y sintaxis.*	DSS05: Gestionar los servicios de seguridad	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. No se evalúa si se implementan mecanismos de autenticación sobre la información sensible.
5. *El acceso al ID con mayores privilegios -a nivel de sistemas operativos, base de datos y aplicativos incluidos en el alcance está restringido al personal a cargo de la administración del sistema.*	DSS05: Gestionar los servicios de seguridad	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. La empresa no evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura. Además, no se evalúa la actividad de estas cuentas con alto nivel de privilegio. DSS05.06: Gestionar documentos sensibles y dispositivos de salida. No se evalúa que se establezcan procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.
6. *El acceso a los IDs con privilegios funcionales en los aplicativos incluidos en el alcance que se utilizan para iniciar transacciones*	DSS05: Gestionar los servicios de seguridad	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. No se identifica alguna brecha.

Control APD	Objetivo de Gestión	Brecha
financieras críticas está restringido a los usuarios apropiados.		
7. El acceso físico al equipo que resguarda la información de la organización está restringido al personal adecuado.	DSS05: Gestionar los servicios de seguridad	DSS05.05: Gestionar el acceso físico a los activos de I&T. No se evalúa que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.
8. La organización tiene mecanismos efectivos para registrar la actividad en la seguridad e identificar violaciones potenciales, así como escalar esos incidentes a mandos superiores y tomar medidas oportunamente para reducir el riesgo de acceso inapropiado o autorizado a los datos o aplicaciones relevantes de reporte financiero.	DSS05: Gestionar los servicios de seguridad	DSS05.07: Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad. La empresa no evalúa si se aplican pruebas de vulnerabilidad y si se implementa algún plan de vulnerabilidades.
9. Un mecanismo efectivo está implementado para asegurar que el acceso es otorgado, modificado apropiadamente o revocado (renuncio o despido) cuando ocurren cambios en las funciones o terminación del trabajo	DSS02: Gestionar las peticiones y los incidentes de servicio	DSS02.02: Registrar, clasificar y priorizar las peticiones e incidentes. No se identifica alguna brecha.
10. La organización revisa periódicamente los usuarios activos o inactivos y los derechos de acceso de	DSS05: Gestionar los servicios de seguridad	DSS05.07: Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad. No se identifica alguna brecha.

Control APD	Objetivo de Gestión	Brecha
usuarios para identificar y eliminar accesos inapropiados al sistema.		
11. La auditoría interna o cualquier otro órgano interno revisa periódicamente la segregación de funciones de la organización. La administración de la organización resuelve los problemas identificados en la segregación de funciones modificando los roles funcionales o los privilegios de acceso de usuario relacionados.	DSS05: Gestionar los servicios de seguridad	DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad. No se identifica alguna brecha.

Fuente: Elaboración propia con los datos de (ISACA, 2018).

Como resultado de la comparación de cada control de la guía actual para el proceso de "Acceso a Programas y Datos" con los objetivos de gestión y mejores prácticas de COBIT 2019, se obtiene que siete actividades no se cumplen en la metodología de la empresa.

En la Tabla 13 se resumen las siete brechas identificadas en la comparativa para el proceso APD.

Tabla 13. Brechas identificadas en el proceso APD

Brechas identificadas en APD
1. ***DSS05.02 Gestionar la seguridad de la conectividad y de la red.*** *La empresa no evalúa las medidas de seguridad y procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.*
2. ***DSS05.03 Gestionar la seguridad de endpoint.*** *La empresa no evalúa que se definan mecanismos de seguridad para los distintos tipos de dispositivos para la protección de datos. Tampoco se toma en cuenta la gestión de dispositivos electrónicos, así como la asignación y eliminación de estos en la red de la empresa.*

Brechas identificadas en APD

3. ***DSS05.04: Gestionar la identidad del usuario y el acceso lógico.***
   No se evalúa si se implementan mecanismos de autenticación sobre la información sensible.

4. ***DSS05.04: Gestionar la identidad del usuario y el acceso lógico.***
   La empresa no evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura. Además, no se evalúa la actividad de estas cuentas con alto nivel de privilegio.

5. ***DSS05.06: Gestionar documentos sensibles y dispositivos de salida.***
   No se evalúa que se establezcan procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.

6. ***DSS05.05: Gestionar el acceso físico a los activos de I&T.***
   No se evalúa que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.

7. ***DSS05.07: Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.***
   La empresa no evalúa si se aplican pruebas de vulnerabilidad y si se implementa algún plan de vulnerabilidades.

Fuente: Elaboración propia con datos de COBIT 2019.

Con base en la tabla anterior, se puede observar que la mayoría de las deficiencias identificadas se relacionan con el dominio de DSS referente a la seguridad.

En primer lugar, la metodología no considera en el alcance de evaluación todos los dispositivos y métodos de conectividad en la gestión de accesos. Muchas organizaciones implementan en su modelo operacional variedad de dispositivos para cumplir con las tareas, las cuales pueden tener un impacto en la operativa general de las empresas.

En cuanto a la categorización de datos, no se evalúa que la información sensible se gestione dentro de un margen de seguridad que reduzca los riesgos a un nivel aceptable.

Otra de las observaciones destacadas que se relacionan con la gestión de la identidad del usuario y el acceso lógico se refiere a que no se incluye como buena práctica la reducción al mínimo necesario de la creación de cuentas administrativas con un alto nivel de privilegio y con acceso a funcionalidades críticas, a través de todos los sistemas de información que se implementen.

La gestión de documentos sensibles y dispositivos de salida es otro tema que difícilmente se toma en cuenta al momento de evaluar a los distintos clientes. No se cuestiona si las organizaciones tienen un plan o procedimientos para gobernar la recepción, uso, retiro y desecho de dispositivos electrónicos o información sensible.

En cuanto a la gestión de acceso físico a las instalaciones donde se alojan activos de TI, no hay suficientes procedimientos que aseguren la concienciación de la seguridad de la información física a los usuarios que corresponden.

Por último, en cuanto a temas de ciberseguridad, no se incluye algún procedimiento de evaluación exhaustiva que permita validar si se aplican al menos pruebas de vulnerabilidad y si hay un plan de atención a las vulnerabilidades identificadas.

4.2.2. Comparativa de la guía CO con COBIT 2019

Mediante el análisis realizado en la Fase 1: Análisis de guías actuales para el proceso de "Operaciones de Computadoras", se presenta a continuación una comparativa de los dominios y objetivos de gestión identificados para determinar las posibles brechas que se encuentren en la guía actual de este proceso.

En la Tabla 14 se plantea la lista de controles incluidos en la matriz de Controles Generales de TI para el proceso de "Operaciones de Computadoras" asociados a los objetivos de gestión determinados en el análisis de la guía COBIT 2019. Como resultado, en la columna "Brecha" se justifica cuál es la variante encontrada a partir de la comparativa de ambos controles.

Tabla 14. Comparativa controles CO de la guía actual con COBIT 2019

Control CO	**Objetivo de Gestión**	**Brecha**
Los Jobs, procesos y programas son monitoreados y los procesos fallidos son corregidos asegurando una ejecución exitosa	APO13: Gestionar la seguridad DSS01: Gestionar las operaciones	APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad. No se evalúa si existe una planificación, diseño de controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. DSS01.01 Ejecutar procedimientos operativos. No se evalúa la gestión del rendimiento y *throughput* de las actividades programadas.
Los incidentes de sistemas de TI que impactan los Jobs de sistemas, procesos y/o programas relevantes son monitoreados y resueltos dentro de la ventana de tiempo definida	DSS02: Gestionar las peticiones y los incidentes de servicio	DSS02.01 Definir esquemas de clasificación para incidentes y peticiones de servicio. No se identifica alguna brecha.

Control CO	Objetivo de Gestión	Brecha
Solo los usuarios autorizados tienen acceso a la configuración de Jobs	DSS05: Gestionar los servicios de seguridad	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. No se evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de *Jobs*.
Programas y datos son respaldados según la política de Operaciones de TI	DSS01: Gestionar las operaciones	DSS01.03: Monitorizar la infraestructura de I&T. No se evalúa si se establecen procedimientos para monitorizar los registros de eventos. Es recomendado llevar a cabo revisiones regulares sobre programas automatizados.
Solo usuarios autorizados tienen acceso a la configuración de respaldos automáticos	DSS05: Gestionar los servicios de seguridad	DSS05.04: Gestionar la identidad del usuario y el acceso lógico. No se evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de respaldos automáticos.

Fuente: Elaboración propia con datos de COBIT 2019.

Con base en los datos de la tabla anterior, se obtiene como resultado las deficiencias en la guía actual de Auditoría de TI para el proceso de "Operaciones de Computadoras". En total se identifican cinco brechas correspondientes a los objetivos de gestión de servicios de seguridad, gestión de operaciones y gestión de peticiones e incidentes de servicio pertenecientes a los dominios APO y DSS.

En la Tabla 15 se presenta un resumen de las cinco brechas identificadas.

Tabla 15. Brechas identificadas en el proceso CO

Brechas identificadas en CO
1. ***APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.*** *No se evalúa si existe una planificación, diseño de controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*
2. ***DSS01.01 Ejecutar procedimientos operativos.*** *No se evalúa la gestión del rendimiento y throughput de las actividades programadas.*
3. ***DSS05.04: Gestionar la identidad del usuario y el acceso lógico.*** *No se evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs.*
4. ***DSS01.03: Monitorizar la infraestructura de I&T.*** *No se evalúa si se establecen procedimientos para monitorizar los registros de eventos. Es recomendado llevar a cabo revisiones regulares sobre programas automatizados.*
5. ***DSS05.04: Gestionar la identidad del usuario y el acceso lógico.*** *No se evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de respaldos automáticos.*

Fuente: Elaboración propia con datos de COBIT 2019.

De acuerdo con los datos de la tabla anterior, se observa que la primera deficiencia identificada se asocia al dominio APO, en el objetivo de gestión relacionado con el tratamiento de riesgos. En la guía actual no se define un procedimiento donde evalúe que las organizaciones implementen un plan para la detección de eventos de seguridad y diseñen respuestas a incidentes de seguridad relacionados con las tareas automatizadas.

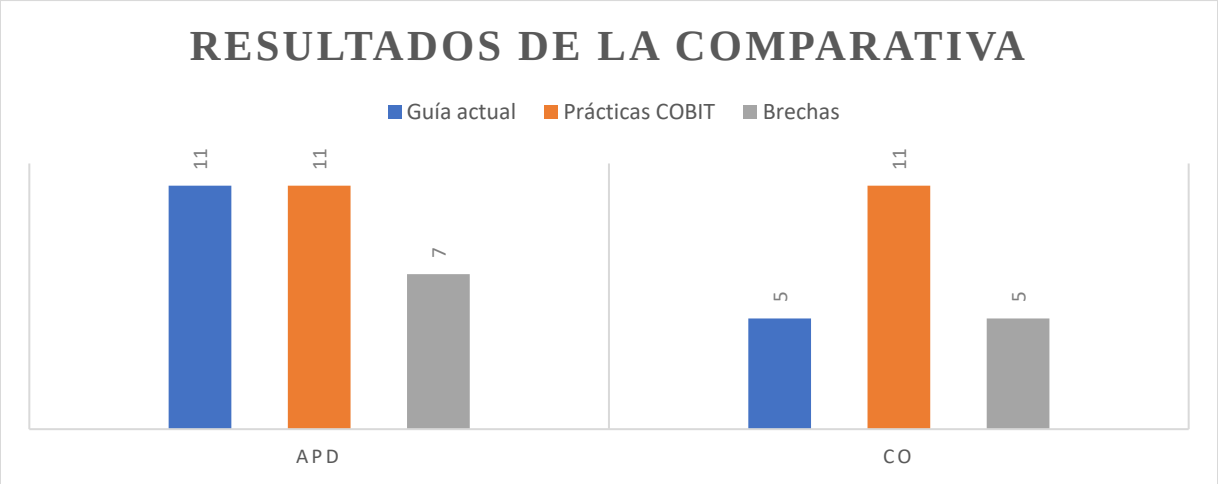
Se identifica que en la guía de CO no se evalúa si realizan una medición del rendimiento y *throughput de* las actividades programadas que permitan el monitoreo de la mejora continua.

Además, se determina que no se toma en consideración evaluar que se reduzca al mínimo necesario la cantidad de cuentas de usuario con acceso a la configuración de *Jobs*, respaldos y restauraciones.

Por último, para el proceso de "Operaciones de Computadoras", como buena práctica deberían aplicarse revisiones regulares sobre las tareas programadas, con el fin de monitorear los registros de eventos y tener un control sobre los riesgos de infraestructura de TI.

Como resultado de la comparativa, se identifica para ambas áreas deficiencias relacionados con aspectos de seguridad de la información y gestión de cuentas con alto nivel de privilegio. En el Gráfico 1. Resultados de la comparativa, se muestra que para un total de once controles en APD se identifican siete brechas y, en el caso de CO, para un total de cinco controles se identifican cinco brechas.

Gráfico 1. Resultados de la comparativa



Fuente: Elaboración propia

Con respecto al gráfico anterior, se puede determinar que, de las 11 prácticas identificadas, el 54.5% de los controles presentes en la matriz de Controles Generales de TI para el área de APD, abarcan las actividades incluidas en las mejores prácticas de los dominios relacionados con seguridad de la información. Sin embargo, se identifican siete oportunidades de mejores en cada uno de ellos.

En el caso de CO, se puede determinar que el 45% de los controles en la matriz de Controles Generales de TI, se abarcan actividades de las 11 prácticas de gestión analizadas en la comparativa. Sin embargo, se identifican cinco oportunidades de mejora.

A partir de las deficiencias identificadas para cada proceso en el alcance, en el siguiente capítulo se define la propuesta solución que solvente dichas brechas para la empresa.

5. Propuesta de Solución

A partir de los resultados obtenidos en la comparativa realizada en el Capítulo 4, correspondiente al Análisis de Resultados, se presenta la propuesta solución a la situación problemática descrita en la sección 1.3.1 Situación problemática.

Con el fin de asegurar el cumplimiento del objetivo general del presente Trabajo Final de Graduación, el cual consiste en la elaboración de una propuesta de mejora de los Controles Generales de TI para los procesos de "Accesos a Programas y Datos" y "Operación de Computadoras"; se diseñan una serie de controles compensatorios alineados con el marco de referencia COBIT 19 y sus mejores prácticas.

Tomando en cuenta el planteamiento del alcance del proyecto definido en la sección 1.5 Alcance, se elabora una herramienta estructurada con el diseño de los controles compensatorios que responden a las brechas identificados en el apartado Fase 2: Comparativa de guías actuales con COBIT 2019. Dicha herramienta es el producto que se le entrega a la organización, donde se abordan los procesos Accesos a Programas y Datos (APD) y "Operaciones de Computadoras" (CO).

Además, en este capítulo se incluyen tres fases del procedimiento metodológico de la investigación: la fase 3 con el diseño de la nueva guía para ambos procesos del alcance, la fase 4 con el análisis financiero de la propuesta solución y la fase 5 con la evaluación de la propuesta de mejora desarrollada.

5.1. Fase 3: Diseño de una nueva guía

Con base en la comparativa realizada en el Capítulo 4, correspondiente al Análisis de Resultados para los procesos de "Acceso a Programas y Datos" y "Operaciones de Computadoras", se definen los controles solución que solventan las brechas identificadas en la comparativa.

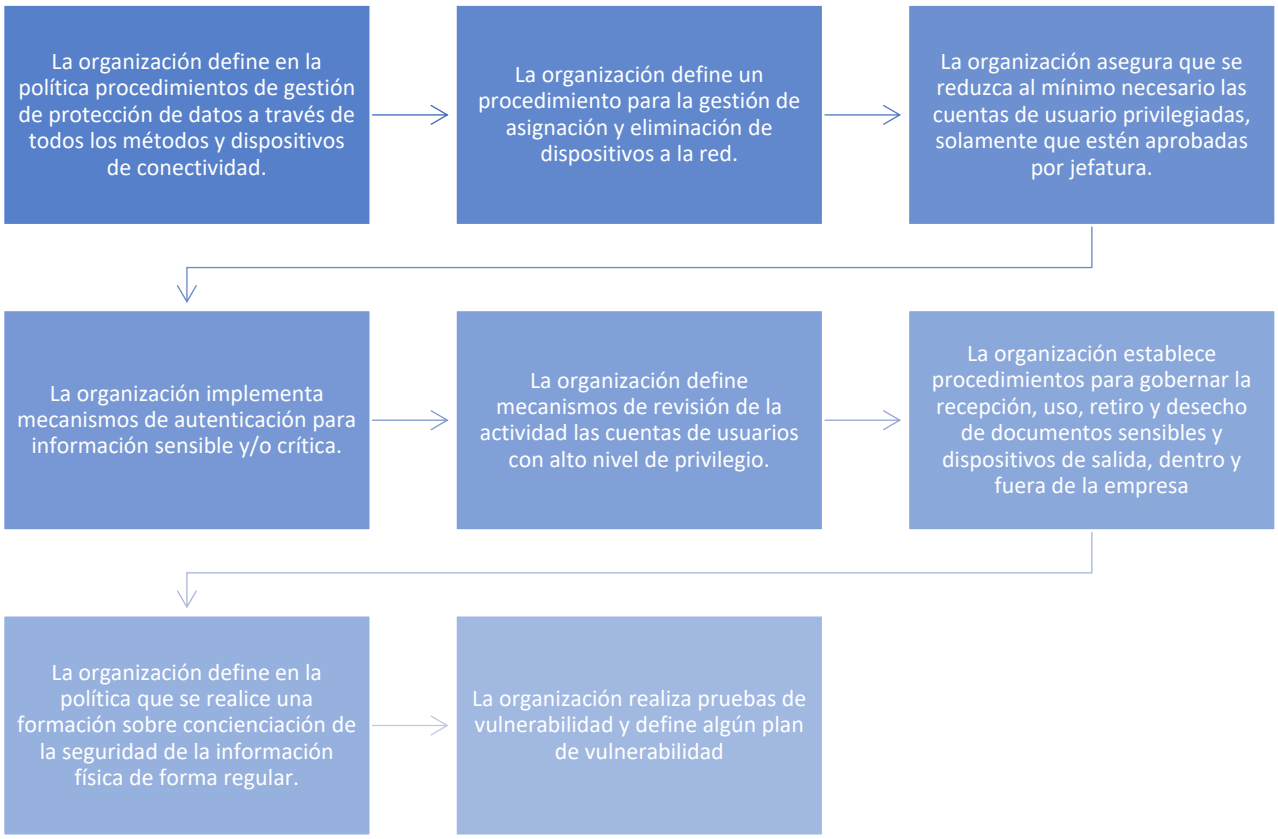
Para esta fase se aplica como instrumento de investigación la revisión documental de las mejores prácticas presentes en el marco de referencia COBIT 2019.

5.1.1. Guía de Controles Generales de TI para el proceso "Acceso a Programas y Datos"

Con respecto al proceso de "Acceso a Programas y Datos", se identificaron siete brechas entre la guía actual implementada por la empresa y el marco de referencia COBIT 2019 descritas en la sección 4.2.1 Comparativa de la guía APD con COBIT 2019.

Consecuentemente, se diseñaron los controles presentados en la Figura 16. Guía solución para APD.

Figura 16. Guía solución para APD



Fuente: Elaboración propia.

La figura anterior presenta los controles compensatorios para el área de “Acceso a Programas y Datos”; se contemplan temas relacionados con la protección de datos a través de la implementación de mecanismos de seguridad en los distintos tipos de dispositivos, aparte de la computadora, que se gestionan en una empresa. Además, sugiere la incorporación de mecanismos de autenticación específicamente para la gestión de información clasificada como sensible y/o crítica.

Se definen controles específicos para la gestión de los distintos dispositivos de conectividad, incluyendo los procesos de recepción, uso, retiro y desechos de estos equipos y documentos sensibles.

Estos controles sugieren que las organizaciones procuren reducir al mínimo necesario las cuentas privilegiadas donde se contemplen los factores de relevancia para siquiera considerar la asignación de este tipo de permisos.

Por última, en esta área se debería procurar la inclusión de controles y procedimientos de auditoría orientados a la evaluación de los procesos de ciberseguridad implementados actualmente en las organizaciones.

5.1.1.1. Alineación de la propuesta de controles APD con COBIT

Los controles presentados anteriormente se identificaron a partir del análisis de las mejores prácticas contenidas en COBIT 2019. Por lo tanto, es importante evidenciar que cada uno se encuentra asociado a un objetivo de gestión en particular en los dominios analizados en el capítulo anterior.

En la Tabla 16 se resumen los controles diseñados para el proceso de "Acceso a Programas y Datos" asociados con su respectivo objetivo de gestión COBIT.

Tabla 16. Controles nuevos alineados a COBIT 2019

Control APD nuevo	**Objetivo de gestión COBIT**
1. *La organización define en la política procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.*	DSS05.02 Gestionar la seguridad de la conectividad y de la red.
2. *La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.*	DSS05.03 Gestionar la seguridad de *endpoint*.
3. *La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.*	DSS05.04: Gestionar la identidad del usuario y el acceso lógico.
4. *La organización implementa mecanismos de autenticación para información sensible y/o crítica.*	DSS05.04: Gestionar la identidad del usuario y el acceso lógico.
5. *La organización define mecanismos de revisión de la actividad de las cuentas de usuarios con alto nivel de privilegio.*	DSS05.04: Gestionar la identidad del usuario y el acceso lógico.
6. *La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa*	DSS05.06: Gestionar documentos sensibles y dispositivos de salida.
7. *La organización define en la política que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.*	DSS05.05 Gestionar el acceso físico a los activos de I&T.
8. *La organización realiza pruebas de vulnerabilidad e implementa algún plan de vulnerabilidad*	DSS05.07 Gestionar las vulnerabilidades y monitorizar la infraestructura para detectar eventos relacionados con la seguridad.

Fuente: Elaboración propia.

5.1.1.2. Entregable a la organización para el proceso APD

Con el fin de proporcionarle a la organización un producto entregable con la propuesta solución para el proceso de "Acceso a Programas y Datos", se elaboró una herramienta con la lista de controles compensatorios para APD, junto con los posibles procedimientos de auditoría que se pueden aplicar en las pruebas de diseño e implementación y en las pruebas de eficacia operativa para cada control. En la Figura 17 se observa la herramienta elaborada con la descripción de los controles de la propuesta solución. De igual manera, se encuentra adjunta en el Apéndice I.

Figura 17. Matriz de controles generales para el proceso APD.

No. Control	Descripción del control	Pruebas de diseño e implementación	Pruebas de eficacia operativa
		Posibles procedimientos de auditoría	Posibles procedimientos de auditoría
APD001	La organización define en la política procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.	1. Indagar con el personal del departamento de TI el proceso relacionado a la gestión de proteción de datos a través de todos los métodos y dispositivos de conectividad. 2. Inspeccionar en la política de Seguridad de la Información de la compañía sobre el proceso de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad. 3. Inspeccionar, en caso de existir, el plan de gestión de protección de datos para cada método y dispositivo de conectividad.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
APD002	La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.	1. Indagar con el personal del departamento de TI el procedimiento definido para la asiganción y eliminación de dispositivos a la red. 2. Inspeccionar en la política o procedimientos de TI la descripción del proceso de asignación y eliminación de dispositivos de la red. 3. Inspeccionar en la política o procedimientos de TI el proceso de aprobación para la gestión de solicitudes de asignación y eliminación de dispositivos de la red.	1. Mediante la selección de una muestra de solicitudes de asignación y eliminación registradas durante el periodo, inspeccionar la evidencia donde se determine que la solicitud fue aprobada por el personal autorizado. 2. Mediante la selección de una muestra de solicitudes de asignación y eliminación registradas durante el periodo, inspeccionar la evidencia donde se determine que la solicitud se alinea con los roles y responsabilidades del usuario.
APD003	La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.	1. Indagar con el personal del departamento de TI el proceso de asignación de cuentas privilegiadas. 2. Inspeccionar en la política de TI de la Compañía el proceso de asignación de cuentas administrativas. 3. Inspeccionar una lista de usuarios administrativas para determinar si se alinean con los roles y responsabilidades. 4. Inspeccionar la lista de usuarios administrativos para determinar si se reduce al mínimo necesario las cuentas de usuario privilegiadas y aprobadas por jefatura.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
APD004	La organización implementa mecanismos de autenticación para información sensible y/o crítica.	1. Indagar con el personal de TI de la compañía el proceso relacionado a la gestión de información sensible y/o crítica. 2. Inspeccionar en la política de TI de la compañía la descripción del proceso de gestión de información sensible y/o crítica. 3. Indagar con el personal de TI de la compañías los mecanismos de autenticación implementados en la gestión de información sensible. 3. Inspeccionar si la configuración de los métodos de autenticación se alinean con los estándares de la industria y las políticas internas.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
APD005	La organización define mecanismos de revisión sobre la actividad de las cuentas de usuarios con alto nivel de privilegio.	1. Indagar con el personal de TI de la compañía el proceso relacionado con las revisiones periódicas y monitoreo de las actividades de las cuentas con alto nivel de privilegio. 2. Inspeccionar en la política de TI la descripción del proceso de revisiones de las actividaddes realizadas por las cuentas con alto nivel de privilegio. 3. Inspeccionar evidencia de la ejecución de las revisiones en la frecuencia establecida.	1. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si las revisiones fueron ejecutadas por el personal autorizado. 2. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si, a partir de los resultados de las revisiones, se tomaron las medidas oportunas ante inconsistencias identificadas.
APD006	La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa	1. Indagar con el personal de TI de la compañía el proceso relacionado a la gestión de la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa. 2. Inspeccionar en la política de TI la descripción del proceso de ecepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.	1. Inspeccionar evidencia de que los dispositivos el retiro y desecho de los dispositivos se ha realizado de forma segura siguiendo el proceso definido. Además, determinar si se ha retenido evidencia relevante de la gestión de dispositivos y documentación sensible.
APD007	La organización define en la política que se realice una formación sobre concientización de la seguridad de la información física de forma regular.	1. Indagar con el personal de TI de la compañía el proceso relacionado a la concentización de la seguridad de la información física de forma regular. 2. Inspeccionar en la política de TI la descripción del proceso de concientización de la seguridad de la información en cuanto al resguardo en las instalaciones físicas de forma regular.	1. Mediante la selección de una muestra de comunicaciones, ya sea correos electrónicos o reportes informativos, para determinar si la campaña sobre concientización de la seguridad de la información física se realiza en la periocidad establecida.
APD008	La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad	1. Indagar con el personal de TI de la compañía la aplicación de pruebas de vulnerabilidad. 2. Inspeccionar en la documentación proporcionada por el departamento de TI si definen un plan de pruebas de vulnerabilidad.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.

Fuente: Elaboración propia.

A continuación, se describen brevemente las columnas incluidas en la herramienta para los controles de APD:

- **No. del control:** representa el identificador del control conformado por las iniciales del proceso (APD) y un consecutivo numérico.
- **Descripción del control:** corresponde a la definición del control diseñado.
- **Las pruebas de diseño e implementación y posibles procedimientos de auditoría:** corresponde a la definición de los procesos por aplicar en la evaluación del diseño e implementación del control.
- **Las pruebas de eficacia operativa y posibles procedimientos de auditoría:** corresponde a la definición de los procesos por aplicar en la evaluación de la eficacia operativa del control.

Para aquellos controles que en la columna de pruebas de eficacia operativa se indica que "Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa", se validan por medio de los procedimientos realizados en las pruebas de diseño, ya que no requieren de técnicas adicionales para validar si son lo suficientemente efectivos.

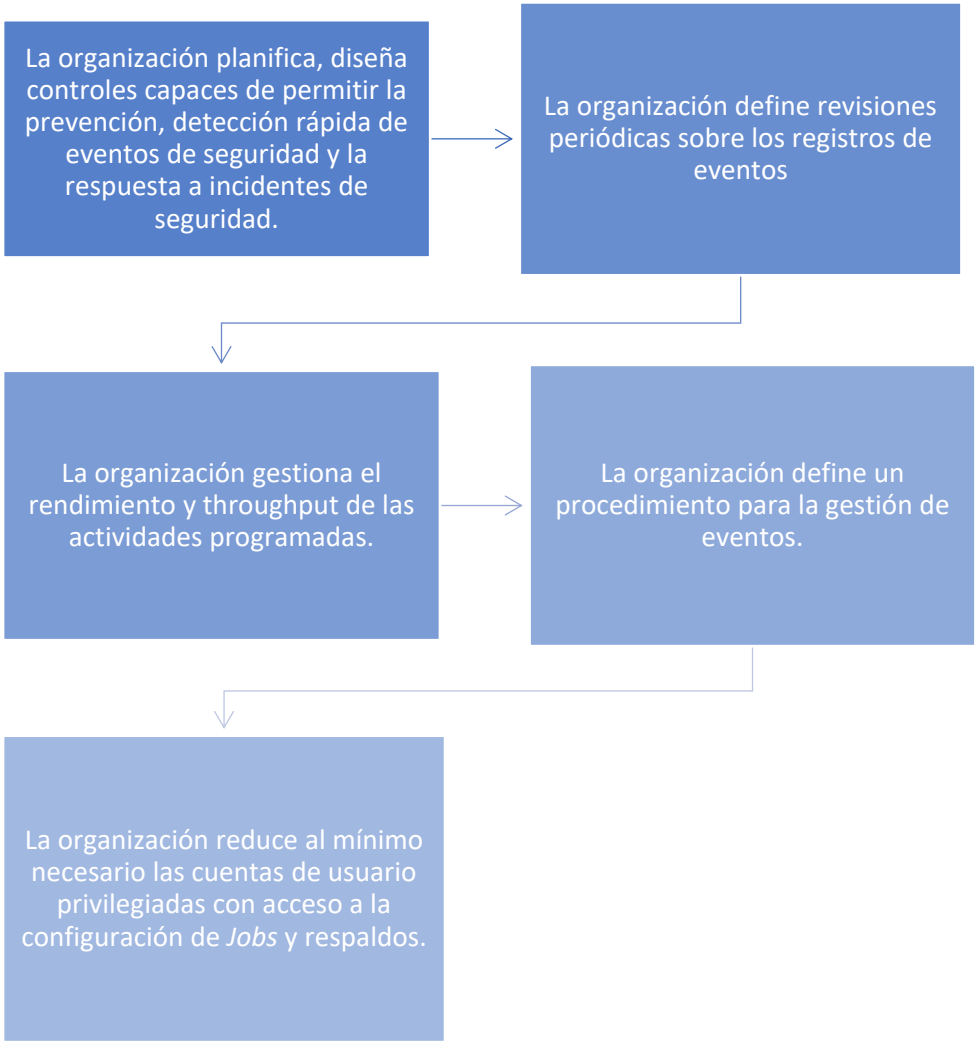
En la siguiente sección se definen los controles compensatorios diseñados, pero esta vez para el área de "Operaciones de Computadoras" junto con su respectiva alineación con COBIT 2019 y la herramienta con los posibles procedimientos para las pruebas de diseño e implementación y pruebas de eficacia operativa.

5.1.2. Guía de Controles Generales de TI para el proceso "Operaciones de Computadoras"

Con base en los resultados obtenidos en la sección 4.2.2 Comparativa de la guía CO con COBIT 2019, se identificaron siete brechas en la metodología actual para el proceso de "Operaciones de Computadoras" con respecto a las mejores prácticas presentes en COBIT 2019.

Como respuesta a las deficiencias identificadas, se diseñaron cinco controles como propuesta de mejora para el proceso CO en la evaluación de los Controles Generales de TI, mostrados en la Figura 18. Guía solución para CO.

Figura 18. Guía solución para CO



Fuente: Elaboración propia.

La figura anterior presenta los controles compensatorios diseñados para el proceso de Operación de Computadoras. Dentro de los temas considerados en la propuesta se incluyen gestión de eventos de seguridad y el registro de incidentes de seguridad, este último resultado de los procedimientos automatizados y configurados en los sistemas de información, que tienen un impacto sobre los reportes financieros.

Se recomienda monitorear el rendimiento de estas actividades programadas, debido al alto nivel de riesgo que representan sobre la operativa de los procesos de una organización, en especial una financiera.

Con base en el punto anterior, se sugiere que las organizaciones cuenten con un plan o un procedimiento definido para la gestión de eventos, debido al nivel de riesgo que se está manejando sobre la información operativa contable que algunas de las organizaciones asignan a estos programas o tareas automatizadas.

Finalmente, en el proceso de "Acceso a Programas y Datos" se debe procurar que se reduzca al mínimo necesario los permisos administrativos sobre la configuración de las tareas automatizadas.

5.1.2.1. Alineación de la propuesta de controles CO con COBIT

De acuerdo con la propuesta solución presentada en la figura anterior, resulta necesario que cada uno de los controles diseñados estén alineados con su respectivo objetivo de gestión COBIT 2019, de modo que se asegure que el control cumple con los estándares de calidad de las mejores prácticas.

A continuación, en la Tabla 17 se resumen los controles diseñados como propuesta solución a las brechas identificadas en el Análisis de Resultados. Además, se encuentran alineadas con su respectivo objetivo de gestión COBIT.

Tabla 17. Controles nuevos alineados a COBIT 2019

Control CO nuevo	**Objetivo de gestión COBIT**
1. *La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*	APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad.
2. *La organización define revisiones periódicas sobre los registros de eventos.*	DSS01.03: Monitorizar la infraestructura de I&T.
3. *La organización gestiona el rendimiento y throughput de las actividades programadas.*	DSS01.01 Ejecutar procedimientos operativos.
4. *La organización define un procedimiento para la gestión de eventos.*	DSS01.03: Monitorizar la infraestructura de I&T.
5. *La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos.*	DSS05.04: Gestionar la identidad del usuario y el acceso lógico.

Fuente: Elaboración propia.

5.1.2.2. Entregable a la organización para el proceso APD

Con el objetivo de brindarle a la organización el diseño de los controles compensatorios para el proceso de "Operaciones de Computadoras", se elaboró una herramienta con la lista de controles, junto con su descripción y los posibles procedimientos de auditoría que se pueden aplicar en las pruebas de diseño e implementación y las pruebas de eficacia operativa. En la Figura 19 se observa la herramienta elaborada con la descripción de los controles de la propuesta solución. De igual manera, se puede consultar en el Apéndice H.

Figura 19. Matriz de controles generales para el proceso CO

No. Control	Descripción del control	Pruebas de diseño e implementación	Pruebas de eficacia operativa
		Posibles procedimientos de auditoría	Posibles procedimientos de auditoría
CO001	La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.	1. Indagar con el personal del departamento de TI el proceso relacionado a la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 2. Inspeccionar en la política de Seguridad de la Información de la compañía sobre prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 3. Inspeccionar, en caso de existir, el plan de respuesta a eventos de seguridad.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
CO002	La organización define revisiones periódicas sobre los registros de eventos.	1. Indagar con el personal del departamento de TI el procedimiento definido sobre las revisiones periódicas sobre los registros de eventos. 2. Inspeccionar en la política o procedimientos de TI la descripción del proceso de revisiones periódicas sobre los registros de eventos.	1. Mediante la selección de una muestra de evidencia relacionadas a las revisiones periódicas sobre los registros de eventos para determinar que se ejecutaron durante el periodo. 2. Mediante la selección de una muestra de evidencia relacionadas a las revisiones periódicas que son ejecutadas por el personal autorizado.
CO003	La organización gestiona el rendimiento y throughput de las actividades programadas.	1. Indagar con el personal del departamento de TI el proceso de gestión del rendimiento y throughput de las actividades programadas. 2. Inspeccionar en la política de TI de la Compañía el proceso gestión del rendimiento y throughput de las actividades programadas. 3. Inspeccionar los criterios de medición utilizados en la gestión del rendimiento y throughput de las actividades programadas.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
CO004	La organización define un procedimiento para la gestión de eventos.	1. Indagar con el personal de TI de la compañía el proceso relacionado a la gestión de eventos 2. Inspeccionar en la política de TI de la compañía la descripción del proceso de gestión de eventos.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
CO005	La organización define mecanismos de revisión sobre la actividad de las cuentas de usuarios con alto nivel de privilegio. La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos	1. Indagar con el personal de TI de la compañía el proceso relacionado con las revisiones de acceso y actividades de las cuentas con alto nivel de privilegio. 2. Inspeccionar en la política de TI la descripción del proceso de revisiones de las actividaddes realizadas por las cuentas con alto nivel de privilegio. 3. Inspeccionar evidencia de la ejecución de las revisiones en la frecuencia establecida.	1. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si las revisiones fueron ejecutadas por el personal autorizado. 2. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si, a partir de los resultados de las revisiones, se tomaron las medidas oportunas ante inconsistencias identificadas.

Fuente: Elaboración propia.

A continuación, se describen brevemente las columnas incluidas en la herramienta para los controles de CO:

- **No. del control:** representa el identificador del control conformado por las iniciales del proceso (CO) y un consecutivo numérico.
- **Descripción del control:** corresponde a la definición del control diseñado.

- **Las pruebas de diseño e implementación y posibles procedimientos de auditoría:** corresponde a la definición de los procesos por aplicar en la evaluación del diseño e implementación del control.
- **Las pruebas de eficacia operativa y posibles procedimientos de auditoría:** corresponde a la definición de los procesos por aplicar en la evaluación de la eficacia operativa del control.

Para aquellos controles que en la columna de pruebas de eficacia operativa "Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa" se validan por medio de los procedimientos realizados en las pruebas de diseño, ya que no requieren de técnicas adicionales para validar si son lo suficientemente efectivos.

A partir de la propuesta y la herramienta desarrollada, en la siguiente sección se plantea un modelo económico para determinar la factibilidad de la implementación del proyecto y los beneficios tangibles que se pueden obtener.

5.2. Fase 4: Análisis financiero

Con el fin de evaluar la factibilidad de la propuesta solución que consiste en el diseño de controles compensatorios para los procesos de "Acceso a Programas y Datos" y "Operaciones de Computadoras", se desarrolló el cálculo para determinar el retorno de inversión de la propuesta.

Para el análisis financiero de la propuesta se realizó una entrevista no estructurada, presentada en el Apéndice G, con la gerente de Auditoría de TI y con los auditores del área. Lo anterior, con el objetivo de conocer los montos gestionados por la firma en cuanto a salarios estimados, incluyendo los salarios tanto de los colaboradores del área como de la gerencia. Los datos determinados se pueden apreciar en la Figura 20.

Figura 20. Cálculos del análisis financiero de la propuesta

Datos

Salarios - Auditoría de TI		
Puesto	Mensual	Hora
Gerente IT Audit	₡1 428 847,00	₡8 930,29
Auditores IT Audit	₡670 000,00	₡4 187,50
Estudiante	₡670 000,00	₡4 187,50

Ingresos - Área Auditoría de TI				
Área	Mensual	Salario por hora	Horas	Total de la semana
IT Audit	₡3 631 313,60	₡22 695,71	40	₡907 828,40

Aumento anual de salarios
5%

Ingresos

	Año 1	Año 2	Año 3	Total
Proyectos realizados	1	3	5	
Ingreso anual	₡907 828	₡2 723 485	₡4 539 142	₡8 170 456
Gerente IT Audit	₡1 428 847,00	₡1 500 289,35	₡1 575 303,82	
Auditores IT Audit	₡670 000,00	₡703 500,00	₡738 675,00	
Estudiante	₡670 000,00	₡703 500,00	₡738 675,00	
Gerente IT Audit	₡8 930,29	₡9 376,81	₡9 845,65	
Auditores IT Audit	₡4 187,50	₡4 396,88	₡4 616,72	
Estudiante	₡4 187,50	₡4 396,88	₡4 616,72	

Flujo de efectivo

	Inversión inicial	Año 1	Año 2	Año 3
Ejecución del proyecto	₡2 646 454,41			
Capacitación	₡201 000,00			
Costos de la implementación		₡67 000,00	₡211 050,00	₡346 253,91
Total	₡2 847 454,41	₡67 000,00	₡211 050,00	₡346 253,91

Retorno de inversión	186,94%

Fuente: Elaboración propia con datos proporcionados por la firma.

A partir de los datos obtenidos mediante la entrevista y la investigación por medio de fuentes externas, como periódicos y datos emitidos por el Colegio de Contadores Públicos, se desarrolla un desglose de los salarios mensuales y por hora del gerente de Auditoría de TI, los Auditores Auditoría de TI y los estudiantes que participan en el equipo.

Posteriormente, se realiza un desglose de los ingresos, pero a nivel del departamento de Auditoría de TI que se determina a partir del costo por hora del servicio brindado a Auditoría Financiera. De igual manera, se determina el aumento anual de salarios obtenido en la indagación realizada con la gerencia del área.

Se procede a calcular los ingresos anuales del área según los montos estimados correspondientes a los salarios por el aumento anual proporcionado. También se toma en cuenta la cantidad de proyectos que se desarrollarían cada año aplicando la matriz de controles de la propuesta solución. Para el primer año, se consideraría solamente emplearlo en un proyecto y luego en los siguientes dos se plantea la suposición de que la guía propuesta se utilizaría en tres y cinco proyectos, respectivamente.

Esta proyección también se desarrolla para los salarios de los colaboradores del área a tres años, mensual y por hora. Considerando el aumento anual proporcionado por la empresa.

En cuanto al cálculo de la inversión inicial, se determina el monto a partir de las horas invertidas por el estudiante, las cuales están conformadas por las 15 semanas del desarrollo del proyecto multiplicado por el salario. Asimismo, se toma en consideración las horas invertidas de asesoramiento y revisión por parte de la gerencia de Auditoría de TI en las 15 semanas.

Se determina el monto a invertir en capacitación del equipo de Auditoría de TI, el cual se encuentra conformado por ocho colaboradores, donde cada uno de ellos requeriría seis horas laborales de entrenamiento.

Como resultado del cálculo, donde se toman los ingresos anuales menos la inversión inicial, se obtiene que el retorno de inversión (ROI) de la propuesta es de 186,94%. Es decir, la propuesta es factible debido a que el beneficio que se obtendrá es 187 veces más que el costo de la inversión inicial.

El desarrollo del análisis financiero y del cálculo respectivo se puede consultar en el Apéndice G. Análisis Financiero (ROI).

En la siguiente sección se presenta los resultados obtenidos de la encuesta aplicada a los colaboradores del área de Auditoría de TI y la retroalimentación sobre los controles propuestos para ambas áreas.

5.3. Fase 5: Evaluación de la propuesta a través de una encuesta

En esta sección se detalla el desarrollo de la última fase de investigación definida para el presente proyecto, la cual corresponde a la evaluación de la propuesta solución, por parte de los colaboradores del área de Auditoría de TI de la organización.

El instrumento de investigación aplicado en esta fase fue la realización de una encuesta compuesta por dos preguntas, cuyas respuestas pueden consultarse en el Apéndice J.

La primera pregunta es si los colaboradores consideran que se puede llevar a cabo una evaluación adecuada y completa con el grupo de controles diseñados como propuesta solución específicamente para el proceso de "Acceso a Programas y Datos".

La segunda pregunta plantea lo mismo, es decir, si los colaboradores consideran que se puede llevar a cabo una evaluación adecuada y completa con el grupo de controles diseñados como propuesta solución, pero, específicamente, para el proceso de "Operación de Computadoras".

La encuesta fue enviada a los ocho colaboradores actuales, sin embargo, se obtuvieron solo cinco respuestas, ya que es la cantidad de auditores que tienen mayor tiempo de estar en la firma, por lo tanto, conocen a profundidad la metodología.

Dentro de las respuestas obtenidas se identifica un acuerdo en común, en resumen, el grupo de controles propuestos permitirían realizar una evaluación adecuada y completa de los procesos. Sin embargo, también surgieron oportunidades de mejora.

La primera oportunidad de mejora está relacionada al control "La organización realiza pruebas de vulnerabilidad e implementa algún plan de vulnerabilidad" del proceso APD, donde se sugiere especificar los tipos de vulnerabilidades en el alcance de la prueba del control.

La segunda oportunidad de mejora está relacionada con el proceso de CO, donde se recomienda para el control "La organización define un procedimiento para la gestión de eventos" especificar los tipos de eventos para delimitar el alcance de las pruebas.

En cuanto al control "La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de *Jobs* y respaldos" se recomienda especificar los métodos para reducir al mínimo los accesos a las configuraciones, asimismo, que se asegure que se incluya, como atributo del control, la consideración de que sea personal confiable quien lo gestione.

Por último, se considera como oportunidad de mejora la inclusión del tema de respaldos en el control de gestión de eventos.

Con base en las respuestas obtenidas, se determina que la propuesta es adecuada y efectiva para la evaluación de Controles Generales de TI que consideran aspectos que carece la metodología actual, asimismo, puede abarcar otros temas en profundidad que no se encuentren en el marco de referencia.

6. Conclusiones

En este capítulo se exponen los hallazgos y recomendaciones derivadas de la elaboración del presente Trabajo Final de Graduación. Se reflejan los descubrimientos relevantes obtenidos en el Análisis de Resultados y, para cada objetivo específico planteado se describen las conclusiones y recomendaciones respectivas con el propósito de evidenciar su cumplimiento.

Las conclusiones surgidas de los objetivos específicos de este estudio se presentan a continuación.

En relación con el Objetivo Específico 1: Comparar la metodología actual implementada por la firma para la evaluación de los Controles Generales de TI con un marco de referencia reconocido a nivel global para la identificación de las posibles brechas en los procesos de Operación de Computadoras y Accesos a Programas y Datos, se determinan las siguientes conclusiones:

- De la entrevista aplicada en la sección 4.1.1.1Análisis de la situación actual, se determina que la metodología actual de la firma incluye cuatro áreas de evaluación relacionadas con los Controles Generales de TI.

- La compañía cuenta con una guía propia para la evaluación de controles generales de TI donde se abordan los procesos "Acceso a Programas y Datos" y "Operación de Computadoras".

- Con respecto al proceso de "Acceso a Programas y Datos", la metodología actual de la firma cuenta con cinco controles en el alcance que abarcan los temas de accesos privilegiados, mecanismos de autenticación, parametrización de contraseñas, accesos temporales, accesos de cuentas genéricas y compartidas y accesos a las instalaciones físicas a Centro de Datos.

- Con respecto al proceso de "Operación de Computadoras", la metodología actual de la firma cuenta con cinco controles en el alcance, en los cuales se abarcan temas relacionados a tareas, procesos y/o programas automatizados, respaldos de información y gestión de incidentes.

- La organización describe que los controles de segregación de funciones y accesos privilegiados son los que considera como críticos en el proceso de "Acceso a Programas y Datos".

- En cuanto al proceso de "Operaciones de Computadoras", la organización considera que los controles relevantes son aquellos relacionados con los programas o tareas automatizadas.

- Las conclusiones relacionadas con la comparativa realizada en la sección 4.2 Fase 2: Comparativa de guías actuales con COBIT 2019 provienen de la revisión documental de los insumos proporcionados por la firma (metodología actual) y el marco de referencia COBIT 2019.

- A partir de los resultados obtenidos en la comparativa, se identificaron siete brechas para el proceso de "Acceso a Programas y Datos", y cinco para el proceso de "Operaciones de Computadoras".

- A partir de los resultados obtenidos en la sección 4.2.1 Comparativa de la guía APD con COBIT 2019, se identificaron siete brechas dentro de las que se encuentran:

    1. DSS05.02 Gestionar la seguridad de la conectividad y de la red: La empresa no evalúa las medidas de seguridad y procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.

    2. DSS05.03 Gestionar la seguridad de *endpoint*: La empresa no evalúa que se definan mecanismos de seguridad para los distintos tipos de dispositivos para la protección de datos. Tampoco se toma en cuenta la gestión de dispositivos electrónicos, así como la asignación y eliminación de estos en la red de la empresa.

    3. DSS05.04: Gestionar la identidad del usuario y el acceso lógico: No se evalúa si se implementan mecanismos de autenticación sobre la información sensible.

- A partir los resultados obtenidos en la sección 4.2.2 Comparativa de la guía CO con COBIT 2019, se identificaron cinco brechas, dentro de las que se encuentran:

    1. APO13.02 Definir y gestionar un plan de tratamiento de riesgos de seguridad de la información y privacidad: no se evalúa si existe una planificación, diseño de controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.

    2. DSS01.01 Ejecutar procedimientos operativos: no se evalúa la gestión del rendimiento y *throughput* de las actividades programadas.

    3. DSS05.04: Gestionar la identidad del usuario y el acceso lógico: No se evalúa que se reduzca al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de *Jobs*.

- A partir de la inspección de COBIT 2019 realizada en la Fase 2: Comparativa de guías actuales con COBIT 2019**Análisis de Resultados**, se determinaron 11 prácticas en el objetivo de gestión relacionadas con la administración de accesos y seguridad de la información. Por lo tanto, se identificó que el proceso de "Acceso a Programas y Datos" está alineado con COBIT 2019 a un 54.5%.

- A partir de la inspección de COBIT 2019 realizada en la Fase 2: Comparativa de guías actuales con COBIT 2019, se determinaron 11 prácticas en el objetivo de gestión relacionadas con la administración de accesos y seguridad de la información. Por lo tanto, se identificó que el proceso de Operación de Computadoras está alineado con COBIT 2019 a un 45%.

En el caso del Objetivo 2: Diseñar los controles generales de TI compensatorios para los procesos de "Acceso a Programas y Datos" y "Operación de Computadoras" tomando en consideración las brechas identificadas, se concluyen los siguientes aspectos:

- Con base en la comparativa de la guía actual con COBIT 19 y la identificación de las brechas, en la Fase 3: Diseño de una nueva guía, se propone un set de controles que solventen dichas deficiencias para ambos procesos del alcance.
- En relación con el proceso de "Acceso a Programas y Datos", en la sección 5.1.1, se diseña una propuesta conformada por un set de ocho controles compensatorios. Dentro de los controles elaborados se encuentran los siguientes:
    1. La organización define en la política procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.
    2. La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.
    3. La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.
    4. La organización implementa mecanismos de autenticación para información sensible y/o crítica.
- En relación con el proceso de "Operaciones de Computadoras", en la sección 5.1.2, se diseña una propuesta conformada por un set de cinco controles. Dentro de los controles elaborados se encuentran los siguientes:
    1. La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.
    2. La organización define revisiones periódicas sobre los registros de eventos
    3. La organización gestiona el rendimiento y *throughput* de las actividades programadas.
    4. La organización define un procedimiento para la gestión de eventos.
- De la entrevista aplicada en el Análisis de la situación actual, con la gerencia de Auditoría de TI, se determina el interés por parte del área de una herramienta que describa los controles compensatorios con sus respectivas pruebas de diseño e implementación y pruebas de eficacia operativa, para ambos procesos.

En relación con el Objetivo 3: Elaborar un análisis financiero para determinar la factibilidad y la obtención de los beneficios tangibles que se derivan de la implementación de este proyecto, se derivan las siguientes conclusiones:

- De la entrevista aplicada en la Fase 4: Análisis financiero, se determinan las consideraciones a tomar en cuenta para el planteamiento de una propuesta y su modelo

económico como lo son: el costo del desarrollo por el rango de tiempo establecido, incluyendo la elaboración de la herramienta, las horas invertidas por la gerencia para revisión y asesoramiento y el costo en la capacitación del personal.

- De los resultados obtenidos en la Fase 4: Análisis financiero, se determina que la elaboración del proyecto es viable dado que se obtendrá un beneficio 187 veces más del costo de la inversión inicial, en un periodo de tres años.

7. Recomendaciones

En este capítulo se detallan las recomendaciones del presente proyecto, las cuales se derivan de los objetivos específicos y hallazgos detallados en el capítulo anterior.

En relación con el Objetivo Específico 1: Comparar la metodología actual implementada por la firma para la evaluación de los Controles Generales de TI con un marco de referencia reconocido a nivel global para la identificación de las posibles brechas en los procesos de Operación de Computadoras y Accesos a Programas y Datos, se detalla las siguientes recomendaciones:

- Considerar la capacitación al equipo de Auditoría de TI en temas relacionados con la aplicación de las mejores prácticas presentes en COBIT 2019 de modo que se promueva la mejora de la calidad de las pruebas que se realizan y, al mismo tiempo, se encuentren sustentadas por un marco de referencia, con las mejores prácticas, reconocido a nivel global.

- Capacitar a los colaboradores de Auditoría de TI en temas de seguridad de la información incluyendo ciberseguridad, planes de vulnerabilidad, pruebas de penetración, gestión de accesos críticos por medio de tareas y/o funcionalidades automatizadas, entre otros.

En el caso del Objetivo 2: Diseñar los controles generales de TI compensatorios para los procesos de “Acceso a Programas y Datos” y “Operación de Computadoras” tomando en consideración las brechas identificadas, se recomienda lo siguiente:

- Alinear los controles compensatorios definidos en la propuesta, para ambos procesos, con los riesgos definidos en la metodología de la firma y describir los atributos de control que delimitan las pruebas, con el fin de mejorar el servicio ofrecido a Auditoría Financiera.

- Antes de la implementación de nuevos controles en los servicios de auditoría, capacitar a los colaboradores de Auditoría de TI con un enfoque orientado a los diferentes escenarios que enfrentan actualmente las organizaciones, donde se asegure la entrega efectiva de los servicios.

En relación con el Objetivo 3: Elaborar un análisis financiero para determinar la factibilidad y la obtención de los beneficios tangibles que se derivan de la implementación de este proyecto, se derivan las siguientes recomendaciones:

- Considerar la implementación de esta propuesta de controles compensatorios para las áreas de “Acceso a Programas y Datos” y “Operaciones de Computadoras”, considerando que son los procesos que abarcan la gestión de seguridad de la información que tiene alto impacto sobre la opinión emitida por Auditoría Financiera.

- Considerar la alineación de las demás áreas incluidas en la guía actual de la firma con el marco de referencia COBIT 2019 y contemplar en el modelo económico los beneficios directos que se pueden obtener con una mejora de los controles generales de TI completos.

8. Referencias

ACCA. (n.d.). *The internal rate of return*. Retrieved from ACCA - Think Ahead: https://www.accaglobal.com/in/en/student/exam-support-resources/foundation-level-study-resources/ffm/ffm-technical-articles/the-internal-rate-of-return.html

Casa, J. (2002). *La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos.* Retrieved from https://www.sciencedirect.com/science/article/pii/S0212656703707288/pdf?md5=3a6894d69e3a107287a9c699414f6600&pid=1-s2.0-S0212656703707288-main.pdf

Casas, J. (2002). *La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos (I)*. Retrieved from https://www.elsevier.es/es-revista-atencion-primaria-27-articulo-la-encuesta-como-tecnica-investigacion--13047738

Corporate Finance Institute. (n.d.). *Net Present Value (NPV)*. Retrieved from CFI: https://corporatefinanceinstitute.com/resources/knowledge/valuation/net-present-value-npv/

Corporate Finance Institute. (n.d.). *ROI Formula (Return on Investment)*. Retrieved from CFI: https://corporatefinanceinstitute.com/resources/knowledge/finance/return-on-investment-roi-formula/

Easy Csat. (n.d.). *¿Que es una encuesta? y tipos de encuesta*. Retrieved from Easy Csat: https://easycsat.com/app-encuestas/que-es-una-encuesta-y-tipos.php

Global Suite. (2021, Diciembre 18). *What is ITIL and what is it for?* Retrieved from Global Suite: https://www.globalsuitesolutions.com/what-is-itil-and-what-is-it-for/

Gómez-Estupiñán, J. F. (2013). *El rol de la auditoría de sistemas de información en la evaluación del gobierno de tecnologías de información en las.* Colombia: Grupo de Investigación GIPROCAS.

Gonzalez, F. (2018, Noviembre 30). *COBIT 2019 — EL NUEVO MODELO DE GOBIERNO EMPRESARIAL PARA INFORMACIÓN Y TECNOLOGÍA.* Retrieved from https://ppglzr.medium.com/cobit-2019-el-nuevo-modelo-de-gobierno-empresarial-para-informaci%C3%B3n-y-tecnolog%C3%ADa-a7bf92b7288b

Good E-Learning. (2021). *What is COBIT 2019? Everything you Need to Know*. Retrieved from https://www.goodelearning.com/courses/it-governance/cobit-2019-foundation/what-is-cobit-2019

Hernández Sampieri, R., & Mendoza Torres, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativas, cualitativa y mixta.* Ciudad de México: McGRAW-HILL Interamericana Editores, S.A. de C.V.

ISACA. (2019). *COBIT: An ISACA framework*. Retrieved from ISACA: https://www.isaca.org/resources/cobit

O'Reilly. (2022). *Computer Operations*. Retrieved from O'Reilly Media, Inc.: https://www.oreilly.com/library/view/auditing-information-systems/9780471281177/9780471281177_computer_operations.html

Pathlock. (2021, Diciembre 20). *Internal Controls for SOX Compliance: A Practical Guide*. Retrieved from Pathlock: https://pathlock.com/learn/internal-controls-for-sox-compliance-a-practical-guide/

PCAOB. (n.d.). *Auditing Standard No. 8*. Retrieved from PCAOB. Public Company Accounting Oversight Board.: https://pcaobus.org/oversight/standards/archived-standards/pre-reorganized-auditing-standards-interpretations/details/auditing-standard-no-8_1838#:~:text=In%20an%20audit%20of%20financial%20statements%2C%20audit%20risk%20is%20the,the%20applicable%20financi

Stobierski, T. (2019, Setiembre 5). *How to do a Cost-Benefit analysis & why it's important.* Retrieved from Harvard Business School: https://online.hbs.edu/blog/post/cost-benefit-analysis

Woodruff, J. (2019, Marzo 3). *How to Prepare a Financial Feasibility Study.* Retrieved from BizFluent: https://bizfluent.com/how-8048004-prepare-financial-feasibility-study.html

9. Apéndices

Apéndice A. Plantilla de Minuta

Reunión No.	Es un núm. consecutivo para este proyecto	**Fecha:**	Indicar la fecha exacta de la reunión
Lugar:	Indicar dónde fue la reunión	**Hora Inicio/Finalización:**	xx:00 am. / yy:00 am
Objetivo de la reunión:			
Participantes:	Presentes:		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
2	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito
3	Debe ser detallado, explícito	Debe ser detallado, explícito	Debe ser detallado, explícito

Próxima reunión

Temas a tratar	Fecha	Convocados
En la próxima reunión	indicar	Nombre de quiénes asistirán a esta próxima reunión.

Apéndice B. Plantilla de 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			

Revisado por:

Nombre tutor

Firma

(Prof. tutor)

Elaborado por:

Nombre estudiante

Firma

(Estudiante)

Revisado por:

Nombre representante empresa

Firma

(Empresa)

Aprobado por:

Nombre Coordinadora TFG

Firma

(Coordinadora de TFG)

Apéndice C. Entrevista inicial

Entrevista – Análisis de la metodología actual

Detalles de la entrevista

Tipo de entrevista:	**Fecha:**
Objetivo:	
Entrevistado:	
Puesto:	

Preguntas

1. ¿Los controles de la metodología actual permiten realizar una adecuada evaluación de "Acceso a Programas y Datos"?

2. ¿Los controles de la metodología actual permiten realizar una adecuada evaluación de Operación de Computadoras?

3. ¿Cuáles controles de la metodología actual considera que son los más importantes para cada proceso?

4. Expectativa de la propuesta de mejora

Apéndice D. Entrevista inicial (aplicada)

Entrevista – Análisis de la metodología actual

Detalles de la entrevista

Tipo de entrevista: Estructurada
Fecha: 18 de abril del 2022
Objetivo: Análisis situación actual
Entrevistado: Angélica Sánchez
Puesto: Gerente de Auditoría de TI

Preguntas

1. ¿Los controles de la metodología actual permiten realizar una adecuada evaluación de "Acceso a Programas y Datos"?
En general sí. Sin embargo, la situación que se ha presentado con varios clientes es que cuestionan si las evaluaciones se alinean con mejores prácticas.

2. ¿Los controles de la metodología actual permiten realizar una adecuada evaluación de Operación de Computadoras?
En general sí. Sin embargo, la situación que se ha presentado con varios clientes es que cuestionan si las evaluaciones se alinean con mejores prácticas.

3. ¿Cuáles controles de la metodología actual considera que son los más importantes para cada proceso?
En cuanto APD, la segregación de funciones es la que más se presta atención ya que tienen alto nivel de riesgo. Y para CO, sería la configuración de *Jobs* y Respaldos y los usuarios autorizados a gestionarlos.

4. Expectativa de la propuesta de mejora
Identificar las posibles brechas que se están presentando de modo que podamos mejorar la calidad de las auditorías.

Apéndice E. Entrevista – Análisis financiero

Entrevista – Análisis financiero

Detalles de la entrevista

Tipo de entrevista: **Fecha:**
Objetivo:
Entrevistado:
Puesto:

Preguntas

1. ¿Cuáles son las consideraciones que se deben tomar en cuenta para el planteamiento de un modelo económico que apoye la propuesta?

2. ¿Cuáles fuentes de información pueden ser consideradas para la obtención de cifras y estimados?

3. Expectativa de la propuesta y su modelo económico.

Apéndice F. Entrevista - Análisis Financiero (aplicada)

Entrevista – Análisis financiero

Detalles de la entrevista

Tipo de entrevista: Estructurada
Fecha: 27 de abril del 2022
Objetivo: Obtener insumos para el modelo económico de la propuesta
Entrevistado: Angélica Sánchez
Puesto: Gerente Auditoría de TI

Preguntas

1. ¿Cuáles son las consideraciones que se deben tomar en cuenta para el planteamiento de un modelo económico que apoye la propuesta?
Considerar los ingresos del área por proyecto según los presupuestos con Auditoría Financiera. Tomar en cuenta la inversión en capacitaciones.

2. ¿Cuáles fuentes de información pueden ser consideradas para la obtención de cifras y estimados?
Se puede consultar con el Socio del área y estimados en internet.

3. Expectativa de la propuesta y su modelo económico.
Refleje el esfuerza en horas que involucra la implementación de la propuesta.

Apéndice G. Análisis Financiero (ROI)

Datos

Salarios - Auditoría de TI		
Puesto	Mensual	Hora
Gerente IT Audit	₡1 428 847,00	₡8 930,29
Auditores IT Audit	₡670 000,00	₡4 187,50
Estudiante	₡670 000,00	₡4 187,50

Ingresos - Área Auditoría de TI				
Área	Mensual	Salario por hora	Horas	Total de la semana
IT Audit	₡3 631 313,60	₡22 695,71	₡40,00	₡907 828,40

Aumento anual de salarios
5%

Ingresos

	Año 1	Año 2	Año 3	Total
Proyectos realizados	1	3	5	
Ingreso anual	₡907 828	₡2 723 485	₡4 539 142	₡8 170 456

Gerente IT Audit	₡1 428 847,00	₡1 500 289,35	₡1 575 303,82
Auditores IT Audit	₡670 000,00	₡703 500,00	₡738 675,00
Estudiante	₡670 000,00	₡703 500,00	₡738 675,00

Gerente IT Audit	₡8 930,29	₡9 376,81	₡9 845,65
Auditores IT Audit	₡4 187,50	₡4 396,88	₡4 616,72
Estudiante	₡4 187,50	₡4 396,88	₡4 616,72

Flujo de efectivo

	Inversión inicial	Año 1	Año 2	Año 3
Ejecución del proyecto	₡2 646 454,41			
Capacitación	₡201 000,00			
Costos de la implementación		₡67 000,00	₡211 050,00	₡346 253,91
Total	₡2 847 454,41	₡67 000,00	₡211 050,00	₡346 253,91

Retorno de inversión	186,94%

Apéndice H. Herramienta de la propuesta para el proceso CO

No. Control	Descripción del control	Pruebas de diseño e implementación	Pruebas de eficacia operativa
		Posibles procedimientos de auditoría	Posibles procedimientos de auditoría
CO001	La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.	1. Indagar con el personal del departamento de TI el proceso relacionado a la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 2. Inspeccionar en la política de Seguridad de la Información de la compañía sobre prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad. 3. Inspeccionar, en caso de existir, el plan de respuesta a eventos de seguridad.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
CO002	La organización define revisiones periódicas sobre los registros de eventos.	1. Indagar con el personal del departamento de TI el procedimiento definido sobre las revisiones periódicas sobre los registros de eventos. 2. Inspeccionar en la política o procedimientos de TI la descripción del proceso de revisiones periódicas sobre los registros de eventos.	1. Mediante la selección de una muestra de evidencia relacionadas a las revisiones periódicas sobre los registros de eventos para determinar que se ejecutaron durante el periodo. 2. Mediante la selección de una muestra de evidencia relacionadas a las revisiones periódicas que son ejecutadas por el personal autorizado.
CO003	La organización gestiona el rendimiento y throughput de las actividades programadas.	1. Indagar con el personal del departamento de TI el proceso de gestión del rendimiento y throughput de las actividades programadas. 2. Inspeccionar en la política de TI de la Compañía el proceso gestión del rendimiento y throughput de las actividades programadas. 3. Inspeccionar los criterios de medición utilizados en la gestión del rendimiento y throughput de las actividades programadas.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
CO004	La organización define un procedimiento para la gestión de eventos.	1. Indagar con el personal de TI de la compañía el proceso relacionado a la gestión de eventos 2. Inspeccionar en la política de TI de la compañía la descripción del proceso de gestión de eventos.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
CO005	La organización define mecanismos de revisión sobre la actividad de las cuentas de usuarios con alto nivel de privilegio. La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos	1. Indagar con el personal de TI de la compañía el proceso relacionado con las revisiones de acceso y actividades de las cuentas con alto nivel de privilegio. 2. Inspeccionar en la política de TI la descripción del proceso de revisiones de las actividaddes realizadas por las cuentas con alto nivel de privilegio. 3. Inspeccionar evidencia de la ejecución de las revisiones en la frecuencia establecida.	1. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si las revisiones fueron ejecutadas por el personal autorizado. 2. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si, a partir de los resultados de las revisiones, se tomaron las medidas oportunas ante inconsistencias identificadas.

Apéndice I. Herramienta de la propuesta para el proceso APD.

No. Control	Descripción del control	Pruebas de diseño e implementación	Pruebas de eficacia operativa
		Posibles procedimientos de auditoría	Posibles procedimientos de auditoría
APD001	La organización define en la política procedimientos de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad.	1. Indagar con el personal del departamento de TI el proceso relacionado a la gestión de proteción de datos a través de todos los métodos y dispositivos de conectividad. 2. Inspeccionar en la política de Seguridad de la Información de la compañía sobre el proceso de gestión de protección de datos a través de todos los métodos y dispositivos de conectividad. 3. Inspeccionar, en caso de existir, el plan de gestión de protección de datos para cada método y dispositivo de conectividad.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
APD002	La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.	1. Indagar con el personal del departamento de TI el procedimiento definido para la asiganción y eliminación de dispositivos a la red. 2. Inspeccionar en la política o procedimientos de TI la descripción del proceso de asignación y eliminación de dispositivos de la red. 3. Inspeccionar en la política o procedimientos de TI el proceso de aprobación para la gestión de solicitudes de asignación y eliminación de dispositivos de la red-	1. Mediante la selección de una muestra de solicitudes de asignación y eliminación registradas durante el periodo, inspeccionar la evidencia donde se determine que la solicitud fue aprobada por el personal autorizado. 2. Mediante la selección de una muestra de solicitudes de asignación y eliminación registradas durante el periodo, inspeccionar la evidencia donde se determine que la solicitud se alinea con los roles y responsabilidades del usuario.
APD003	La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.	1. Indagar con el personal del departamento de TI el proceso de asignación de cuentas privilegiadas. 2. Inspeccionar en la política de TI de la Compañía el proceso de asignación de cuentas administrativas. 3. Inspeccionar una lista de usuarios administrativas para determinar si se alinean con los roles y responsabilidades. 4. Inspeccionar la lista de usuarios administrativos para determinar si se reduce al mínimo necesario las cuentas de usuario privilegiadas y aprobadas por jefatura.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
APD004	La organización implementa mecanismos de autenticación para información sensible y/o crítica.	1. Indagar con el personal de TI de la compañía el proceso relacionado a la gestión de información sensible y/o crítica. 2. Inspeccionar en la política de TI de la compañía la descripción del proceso de gestión de información sensible y/o crítica. 3. Indagar con el personal de TI de la compañías los mecanismos de autenticación implementados en la gestión de información sensible. 3. Inspeccionar si la configuración de los métodos de autenticación se alinean con los estándares de la industria y las políticas internas.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.
APD005	La organización define mecanismos de revisión sobre la actividad de las cuentas de usuarios con alto nivel de privilegio.	1. Indagar con el personal de TI de la compañía el proceso relacionado con las revisiones periódicas y monitoreo de las actividades de las cuentas con alto nivel de privilegio. 2. Inspeccionar en la política de TI la descripción del proceso de revisiones de las actividaddes realizadas por las cuentas con alto nivel de privilegio. 3. Inspeccionar evidencia de la ejecución de las revisiones en la frecuencia establecida.	1. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si las revisiones fueron ejecutadas por el personal autorizado. 2. Mediante la selección de una muestra de revisiones realizadas durante el periodo, inspeccionar evidencia para determinar si, a partir de los resultados de las revisiones, se tomaron las medidas oportunas ante inconsistencias identificadas.
APD006	La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa	1. Indagar con el personal de TI de la compañía el proceso relacionado a la gestión de la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa. 2. Inspeccionar en la política de TI la descripción del proceso de ecepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa.	1. Inspeccionar evidencia de que los dispositivos el retiro y desecho de los dispositivos se ha realizado de forma segura siguiendo el proceso definido. Además, determinar si se ha retenido evidencia relevante de la gestión de dispositivos y documentación sensible.
APD007	La organización define en la política que se realice una formación sobre concientización de la seguridad de la información física de forma regular.	1. Indagar con el personal de TI de la compañía el proceso relacionado a la concentización de la seguridad de la información física de forma regular. 2. Inspeccionar en la política de TI la descripción del proceso de concientización de la seguridad de la información en cuanto al resguardo en las instalaciones físicas de forma regular.	1. Mediante la selección de una muestra de comunicaciones, ya sea correos electrónicos o reportes informativos, para determinar si la campaña sobre concientización de la seguridad de la información física se realiza en la periocidad establecida.
APD008	La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad	1. Indagar con el personal de TI de la compañía la aplicación de pruebas de vulnerabilidad. 2. Inspeccionar en la documentación proporcionada por el departamento de TI si definen un plan de pruebas de vulnerabilidad.	Los procedimientos del diseño e implementación cubren la prueba de eficacia operativa.

Apéndice J. Encuesta – Evaluación de la propuesta solución

Respuesta 1

Ver resultados

Encuestado

1 Anónimo

07:19

Tiempo para completar

1. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso APD:

1. *La organización define en la política procedimientos de gestión de protección de datos a través de todos los método y dispositivos de conectividad.*
2. *La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.*
3. *La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.*
4. *La organización implementa mecanismos de autenticación para información sensible y/o crítica.*
5. *La organización define mecanismos de revisión de la actividad las cuentas de usuarios con alto nivel de privilegio.*
6. *La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa*
7. *La organización define en la política que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.*
8. *La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Si, debido a que los controles definidos estan redactados de una manera que delimita el alcance de los procedimientos que se realizarian para evaluarlos, lo cual permite enfocarse solomente en aquellos atributos importantes para determinar la eficiencia o no del control relacionado al proceso.

2. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso CO:

1. *La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*
2. *La organización define revisiones periódicas sobre los registros de eventos.*
3. *La organización gestiona el rendimiento y throughput de las actividades programadas.*
4. *La organización define un procedimiento para la gestión de eventos.*
5. *La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos.*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Si, debido a que estos controles se enfocan en atender partes importantes del proceso en los cuales pueden presentarse riesgos que afecten la generación de información financiera o relevante para la compañia.

Respuesta 2

Ver resultados

Encuestado

2 Anónimo

19:12
Tiempo para completar

1. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso APD:

1. *La organización define en la política procedimientos de gestión de protección de datos a través de todos los método y dispositivos de conectividad.*
2. *La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.*
3. *La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.*
4. *La organización implementa mecanismos de autenticación para información sensible y/o crítica.*
5. *La organización define mecanismos de revisión de la actividad las cuentas de usuarios con alto nivel de privilegio.*
6. *La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa*
7. *La organización define en la política que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.*
8. *La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Si, porque abarcan los temas relevantes en la evaluación del proceso de acceso a programas y datos que debe tener una empresa.

2. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso CO:

1. *La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*
2. *La organización define revisiones periódicas sobre los registros de eventos.*
3. *La organización gestiona el rendimiento y throughput de las actividades programadas.*
4. *La organización define un procedimiento para la gestión de eventos.*
5. *La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos.*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Si, porque abarcan los temas relevantes en la evaluación del proceso de CO

Respuesta 3

Ver resultados

Encuestado

3 Anónimo

03:31
Tiempo para completar

1. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso APD:

1. *La organización define en la política procedimientos de gestión de protección de datos a través de todos los método y dispositivos de conectividad.*
2. *La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.*
3. *La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.*
4. *La organización implementa mecanismos de autenticación para información sensible y/o crítica.*
5. *La organización define mecanismos de revisión de la actividad las cuentas de usuarios con alto nivel de privilegio.*
6. *La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa*
7. *La organización define en la política que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.*
8. *La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad*

2. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso CO:

1. *La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*
2. *La organización define revisiones periódicas sobre los registros de eventos.*
3. *La organización gestiona el rendimiento y throughput de las actividades programadas.*
4. *La organización define un procedimiento para la gestión de eventos.*
5. *La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos.*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Sí, pero considero que se podría agregar un control enfocado en la ejecución de respaldos

Respuesta 4

Ver resultados

Encuestado

4 Anónimo

12:38
Tiempo para completar

1. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso APD:

1. *La organización define en la política procedimientos de gestión de protección de datos a través de todos los método y dispositivos de conectividad.*
2. *La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.*
3. *La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.*
4. *La organización implementa mecanismos de autenticación para información sensible y/o crítica.*
5. *La organización define mecanismos de revisión de la actividad las cuentas de usuarios con alto nivel de privilegio.*
6. *La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa*
7. *La organización define en la política que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.*
8. *La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Parte 8. A que tipo de vulnerabilidad están considerando ya que existen pruebas de penetracion relacionada con ciberseguridad, pero específicamente no hace mención de algún tipo de esta.

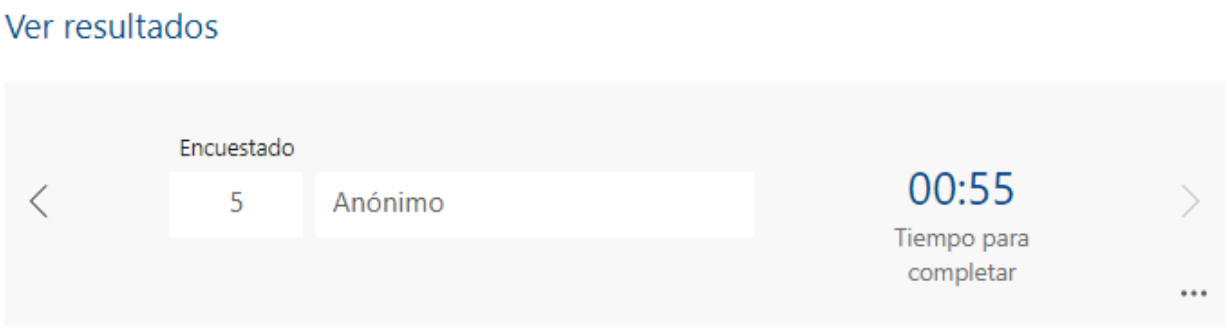
2. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso CO:

1. *La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*
2. *La organización define revisiones periódicas sobre los registros de eventos.*
3. *La organización gestiona el rendimiento y throughput de las actividades programadas.*
4. *La organización define un procedimiento para la gestión de eventos.*
5. *La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos.*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

4. Rescatar que eventos son.
5. Como reducir al mínimo, y como hacer que el mínimo sea personal confiable para el manejo de éstas.

Respuesta 5



1. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso APD:

1. *La organización define en la política procedimientos de gestión de protección de datos a través de todos los método y dispositivos de conectividad.*
2. *La organización define un procedimiento para la gestión de asignación y eliminación de dispositivos a la red.*
3. *La organización asegura que se reduzca al mínimo necesario las cuentas de usuario privilegiadas, solamente que estén aprobadas por jefatura.*
4. *La organización implementa mecanismos de autenticación para información sensible y/o crítica.*
5. *La organización define mecanismos de revisión de la actividad las cuentas de usuarios con alto nivel de privilegio.*
6. *La organización establece procedimientos para gobernar la recepción, uso, retiro y desecho de documentos sensibles y dispositivos de salida, dentro y fuera de la empresa*
7. *La organización define en la política que se realice una formación sobre concienciación de la seguridad de la información física de forma regular.*
8. *La organización realiza pruebas de vulnerabilidad y si implementa algún plan de vulnerabilidad*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Si, se puede evaluar la gestión de acceso.

2. A continuación, se presentan los controles como parte de la propuesta para la evaluación del proceso CO:

1. *La organización planifica, diseña controles capaces de permitir la prevención, detección rápida de eventos de seguridad y la respuesta a incidentes de seguridad.*
2. *La organización define revisiones periódicas sobre los registros de eventos.*
3. *La organización gestiona el rendimiento y throughput de las actividades programadas.*
4. *La organización define un procedimiento para la gestión de eventos.*
5. *La organización reduce al mínimo necesario las cuentas de usuario privilegiadas con acceso a la configuración de Jobs y respaldos.*

¿Considera que los controles permiten una evaluación adecuada y completa del proceso? Justifique su respuesta. *

Si, se puede evaluar la operaciones computarizadas

Apéndice K. Revisión documental

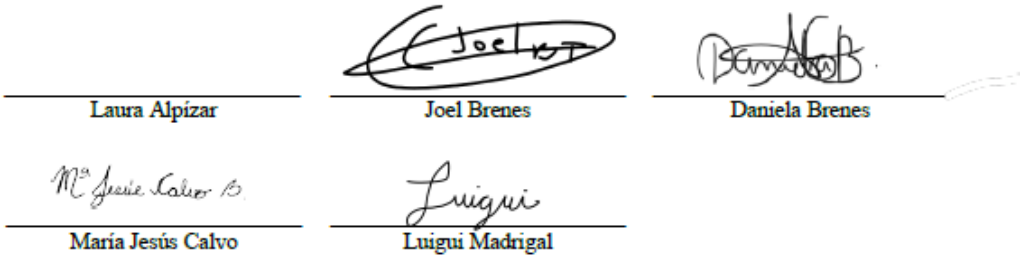
Revisión documental
Documento revisado [Se indica la referencia documental revisada]
Resultados de la revisión [Se indican resultados puntuales de la revisión]

Apéndice L. Minutas

Minuta 1

Minuta de Reunión			
Información general			
Reunión Nº:	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

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	2	**Fecha:**	18 de febrero del 2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	03:00 pm. / 03:30 pm
Objetivo de la reunión:	I Reunión Tutor, estudiante y la contraparte		
Participantes:	Presentes: Daniela Brenes (estudiante), Laura Alpízar (tutora) y Angélica Sánchez (contraparte)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Cronograma del proceso de TFG	Se le explicó a la contraparte la estructuración del cronograma para el presente I Semestre del año 2022.	El estudiante coordinará las tres reuniones correspondientes con la contraparte.
2	Responsabilidades de los involucrados (contraparte, tutora y estudiante)	La tutora indica cuáles son las responsabilidades de los involucrados tanto como del estudiante como la contraparte.	La contraparte se compromete a brindar el espacio de tiempo para que el estudiante realice las actividades relacionadas con el TFG.
3	Evaluación del TFG	La tutora expone cuáles son los criterios y porcentajes involucrados en la evaluación del TFG y los responsables de cada rubro.	Los presentes se comprometen a realizar las evaluaciones en las fechas correspondientes.

Próxima reunión

Temas por tratar	Fecha	Convocados
Se entrega el primer avance del TFG a la tutora.	10/03/2022	Laura Alpízar (profesora-tutora) Daniela Brenes (estudiantes)

Uso Confidencial Pág. 1/1

Minuta 3

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	3	**Fecha:**	10/03/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	01:30 pm. / 02:00 pm
Objetivo de la reunión:	Entrega del primer avance del TFG.		
Participantes:	Presentes: Daniela Brenes (estudiante) y Laura Alpízar (tutora)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Entrega del primer Avance del TFG	La estudiante entrega el primer avance correspondiente al Trabajo Final de Graduación.	El estudiante revisó e hizo las mejores respectivas correspondientes al primer capítulo del TFG.
2	Observaciones de la tutora	La tutora indica las oportunidades de mejora correspondientes al entregable del primer capitulo del TFG.	El estudiante se compromete a realizar las modificaciones indicaciones realizadas por la tutora incluyendo: mejores en los objetivos y problemática.

Próxima reunión

Temas por tratar	Fecha	Convocados
Segunda reunión con la contraparte	31/03/2022	Laura Alpízar (profesora-tutora) Daniela Brenes (estudiantes) Angélica Sánchez (contraparte)

Uso Confidencial Pág. 1/1

Minuta 4

Minuta de Reunión			
Información general			
Reunión N°:	4	**Fecha:**	24/03/2022
Lugar:	Microsoft Teams	**Hora de inicio y finalización:**	2:00pm - 3:00pm
Objetivo de la reunión:	Estudio de un ejemplo de marco metodológico		
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 de cada estudiante)	Notificar a la profesora si se tienen problemas con la empresa.
Próxima reunión			
Temas por tratar		**Fecha**	**Convocados**
Por definir		Por definir	Por definir

Minuta 5

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	5	**Fecha:**	31/03/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	01:30 pm. / 02:00 pm
Objetivo de la reunión:	II Reunión con la contraparte		
Participantes:	Presentes: Daniela Brenes (estudiante), Laura Alpízar (tutora) y Angélica Sánchez (contraparte)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Presentación del avance del TFG	La estudiante presenta a la tutora y a la contraparte el avance hasta el momento que incluye los primeros dos capítulos.	El estudiante se compromete a realizar un cronograma de los entregables y presentar las fechas relevantes.

Próxima reunión

Temas por tratar	Fecha	Convocados
Cronograma de la investigación	04/04/2022	Laura Alpízar (profesora-tutora) Daniela Brenes (estudiantes)

Uso Confidencial Pág. 1/1

Minuta 6

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	6	**Fecha:**	04/04/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	02:00 pm. / 02:30 pm
Objetivo de la reunión:	Cronograma de la investigación		
Participantes:	Presentes: Daniela Brenes (estudiante) y Laura Alpízar (tutora)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Presentación del cronograma de investigación	La estudiante presenta a la tutora el cronograma solicitado indicando las fechas relevantes para los entregables.	El estudiante se compromete a seguir el cronograma definido y aprobado por la tutora.

Próxima reunión

Temas por tratar	Fecha	Convocados
Entrevista – Entendimiento situación actual	18/04/2022	Daniela Brenes (estudiante) Angélica Sánchez (contraparte)

Uso Confidencial Pág. 1/1

Minuto 7

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	7	**Fecha:**	18/04/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	10:00 am. / 11:00 am
Objetivo de la reunión:	Entrevista inicial – Entendimiento de la situación actual		
Participantes:	Presentes: Daniela Brenes (estudiante) y Angélica Sánchez (contraparte)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Aplicación de la entrevista inicial con la contraparte	La estudiante aplica la entrevista inicial con la contraparte para obtener un entendimiento actual de la metodología implementada.	La contraparte ofrece todos los insumos necesarios para la realización del proyecto y responde las preguntas de la entrevista inicial. El estudiante se compromete de mantener actualizado a la contraparte de los hallazgos obtenidos del análisis.

Próxima reunión

Temas por tratar	Fecha	Convocados
Avance del análisis de resultados Análisis financiero	27/04/2022	Daniela Brenes (estudiante) Angélica Sánchez (contraparte)

Uso Confidencial Pág. 1/1

Minuto 8

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	8	**Fecha:**	27/04/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	04:00 pm. / 05:00 pm
Objetivo de la reunión:	Avance del análisis de resultados Análisis financiero		
Participantes:	Presentes: Daniela Brenes (estudiante) y Angélica Sánchez (contraparte)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Avance del análisis de resultados	La estudiante expone el avance del análisis de resultados y los hallazgos obtenidos hasta el momento.	La contraparte brinda retroalimentación sobre el avance presentado a la fecha. El estudiante se compromete a realizar los cambios correspondientes.
2	Datos para el análisis financiero	Se aplicó una entrevista a la contraparte para obtener los datos que se utilizarán como insumo para el análisis financiero	La contraparte brinda datos estimados según la experiencia de la entrevistada. El estudiante se compromete a indagar e inspeccionar las fuentes indicadas por la contraparte para la obtención de información que sirvan como insumo para la elaboración del análisis financiero.

Próxima reunión

Temas por tratar	Fecha	Convocados
Avance V del TFG	28/04/2022	Daniela Brenes (estudiante) Laura Alpízar (tutora)

Uso Confidencial Pág. 1/1

Minuta 9

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	9	**Fecha:**	28/04/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	02:30 pm. / 03:00 pm
Objetivo de la reunión:	Avance V del TFG		
Participantes:	Presentes: Daniela Brenes (estudiante) y Laura Alpízar (tutora)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Avance V del TFG	La estudiante presenta el Avance V de TFG a la profesora tutora.	La tutora brinda retroalimentación sobre el documento entregado. La estudiante se compromete a realizar los cambios solicitados con respecto al análisis de resultados y propuesta solución.

Próxima reunión

Temas por tratar	Fecha	Convocados
Correcciones del análisis de resultados y propuesta solución del TFG	10/05/2022	Daniela Brenes (estudiante) Laura Alpízar (tutora)

Uso Confidencial Pág. 1/1

Minuta 10

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	10	**Fecha:**	10/05/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	01:30 pm. / 02:30 pm
Objetivo de la reunión:	Correcciones del análisis de resultados y propuesta solución del TFG		
Participantes:	Presentes: Daniela Brenes (estudiante) y Laura Alpízar (tutora)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Correcciones al avance del TFG	La estudiante presenta las correcciones realizadas al análisis de resultados y la propuesta solución.	La tutora brinda retroalimentación sobre el documento entregado. La estudiante se compromete a realizar los cambios solicitados con respecto al análisis de resultados y propuesta solución.

Próxima reunión

Temas por tratar	Fecha	Convocados
III Reunión con la contraparte	25/05/2022	Daniela Brenes (estudiante) Laura Alpízar (tutora) Angélica Sánchez (contraparte)

Uso Confidencial Pág. 1/1

Minuta 11

MINUTA DE REUNIÓN

Proyecto: Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Reunión No.	11	**Fecha:**	25/05/2022
Lugar:	Vía Microsoft Teams	**Hora Inicio/Finalización:**	01:30 pm. / 02:30 pm
Objetivo de la reunión:	III Reunión con la contraparte		
Participantes:	Presentes: Daniela Brenes (estudiante), Laura Alpízar (tutora) y Angélica Sánchez (contraparte)		
	Ausentes: N/A		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Finalización del proyecto y entrega de herramienta a la organización	La estudiante presenta la versión final del proyecto y los entregables correspondientes a la organización (herramienta con la propuesta solución)	NA

Próxima reunión

Temas por tratar	Fecha	Convocados
NA	NA	NA

Uso Confidencial Pág. 1/1

Minuta firmada (Contraparte)

Minutas de Reunión

Aprobación de las minutas de reunión de la contraparte

En este documento se agrupan y aprueban parte de las minutas correspondientes al proyecto de graduación "Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras", realizado por la estudiante Daniela Brenes Gutiérrez, carné 2015088274, cédula 116570301. En este, la contraparte de la empresa, Angélica Sánchez, valida su participación en las siguientes minutas del proyecto:

- Minuta 02 – I Reunión Tutor, estudiante y la contraparte
- Minuta 05 – II Reunión con la contraparte
- Minuta 07 – Entrevista inicial: Entendimiento de la situación actual
- Minuta 08 – Avance del análisis de resultados y Análisis financiero
- Minuta 11 – III Reunión con la contraparte

Firma

Angélica Sánchez Digitally signed by Angélica Sánchez Date: 2022.05.26 11:11:58 -06'00'

Minuta firmada (Tutora)

Minutas de Reunión

Aprobación de las minutas realizadas en el semestre por parte de la tutora

En este documento se agrupan y aprueban parte de las minutas correspondientes al proyecto de graduación "Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras", realizado por la estudiante Daniela Brenes Gutiérrez, carné 2015088274, cédula 116570301. En este, la tutora del proyecto, Laura Alpízar Chaves, valida su participación en las siguientes minutas del proyecto:

- Minuta 01 – Bienvenida y organización del curso
- Minuta 02 – I Reunión Tutor, estudiante y la contraparte
- Minuta 03 – Entrega del primer avance del TFG.
- Minuta 04 – Estudio de un ejemplo de marco metodológico
- Minuta 05 – II Reunión con la contraparte
- Minuta 06 – Cronograma de la investigación
- Minuta 09 – Avance V del TFG
- Minuta 10 – Correcciones del análisis de resultados y propuesta solución del TFG
- Minuta 11 – III Reunión con la contraparte

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)

Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2022.05.25 16:21:07 -06'00'

Firma

10. Anexo

Anexo A. Primera evaluación de la contraparte

Carnet: 2015088274

Título: Alinear la metodología de Auditoría de TI para la evaluación de los controles de Accesos a Programas y Datos con un marco de referencia reconocido a nivel global.

(41743)

Tipo: (X/boilerplate)

Fecha en que se realiza la evaluación (41667)

Tipo: (D/date)

26/05/2022

Evaluación número: (41674)

Tipo: (L/list-radio)

3

Firma del Evaluador/Contraparte de la Organización:: Angélica Sánchez Digitally signed by Angélica Sánchez Date: 2022.04.04 10:55:07 -06'00'

(41675)

Tipo: (X/boilerplate)

Anexo B. Segunda evaluación de la contraparte

Carnet: 2015088274

Título: Alinear la metodología de Auditoría de TI para la evaluación de los controles de Accesos a Programas y Datos con un marco de referencia reconocido a nivel global.

(41743)

Tipo: (X/boilerplate)

Fecha en que se realiza la evaluación (41667)

Tipo: (D/date)

09/05/2022

Evaluación número: (41674)

Tipo: (L/list-radio)

2

Firma del Evaluador/Contraparte de la Organización:: Angélica Sánchez Digitally signed by Angélica Sánchez Date: 2022.05.09 14:25:47 -06'00'

(41675)

Tipo: (X/boilerplate)

Anexo C. Tercera evaluación de la contraparte

Carnet: 2015088274

Título: Alinear la metodología de Auditoría de TI para la evaluación de los controles de Accesos a Programas y Datos con un marco de referencia reconocido a nivel global.

(41743)

Tipo: (X/boilerplate)

Fecha en que se realiza la evaluación (41667)

Tipo: (D/date)

26/05/2022

Evaluación número: (41674)

Tipo: (L/list-radio)

3

A3

Firma del Evaluador/Contraparte de la Organización::_____

(41675)

Tipo: (X/boilerplate)

Angélica Sánchez Digitally signed by Angélica Sánchez Date: 2022.05.26 11:11:58 -06'00'

Anexo D. Carta de la filóloga

Alajuela, 28 de mayo del 2022

A quien interese:

Yo, Gisela Alfaro Chaves, cédula de identidad 2-0701-0506 profesional en Filología Española y en Enseñanza del Castellano y la Literatura, perteneciente al Colegio de Licenciados y Profesores en Letras, Filosofía, Ciencias y Artes; leí y corregí el proyecto final de graduación:

Propuesta de mejora de los Controles Generales de TI para los procesos de Acceso a Programas y Datos y Operación de Computadoras

Documento realizado por el estudiante Daniela Brenes Gutiérrez, con el número de cédula 1-1657-0301, con el fin de optar por el grado de Licenciatura en Administración de Tecnología de Información, del Tecnológico de Costa Rica.

Por este motivo, se revisaron y corrigieron aspectos como la construcción de párrafos, organización discursiva, vicios del lenguaje trasladados al campo escrito, ortografía, puntuación, barbarismos, coherencia, cohesión y otros elementos relacionados con el campo filológico.

Realizadas las correcciones, doy fe de que el documento está listo para ser presentado.

Se suscribe de ustedes cordialmente,

Gisela Alfaro Chaves, céd 207010506
Carné de colegiada 67138