TEC | Tecnológico de Costa Rica

Área Académica de Administración de Tecnología de Información

Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

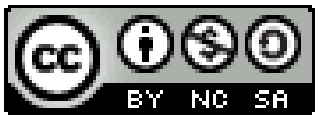
Trabajo final de graduación para optar por el título de Licenciatura en Administración de Tecnología de Información

Elaborado por: Deiber Jardel Ureña González

Profesor tutor: Laura Alpízar Chaves

Cartago

II semestre, 2021



ÁREA ACADÉMICA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÒN

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 del estudiante **Deiber Jardel Ureña González** 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: 2021.11.30 15:09:26 -06'00'

Laura Alpízar Chaves

Profesor tutor

CARLOS LUIS MATA MONTERO (FIRMA)

Firmado digitalmente por CARLOS LUIS MATA MONTERO (FIRMA)
Fecha: 2021.12.01 13:55:41 -06'00'

Carlos Luis Mata Montero

Lector académico

LUIS FELIPE PICADO VALVERDE (FIRMA)

Firmado digitalmente por LUIS FELIPE PICADO VALVERDE (FIRMA)
Fecha: 2021.12.03 23:23:18 -06'00'

Luis Felipe Picado Valverde

Lector externo

TEC Tecnológico de Costa Rica

Firmado digitalmente por YARIMA TATIANA SANDOVAL SANCHEZ (FIRMA)
Fecha: 2021.12.06 19:02:31 -06'00'

Yarima Sandoval Sánchez

Coordinadora de trabajo final de graduación

DEDICATORIA

En primera instancia doy gracias a Dios,

Por ser mi guía, proveerme con salud, sabiduría, paciencia, oportunidades.

A mi madre,

Por ser un ejemplo para seguir, donde la educación, consejos, apoyo, motivación y los valores que me inculcó, lo cual ha sido el pilar fundamental para la consecución de esta meta.

A mi padre,

Por el apoyo que me ha brindado durante mi formación.

A mis hermanos,

Quienes me demostraron su apoyo durante este periodo de formación.

que me ha dado han sido el pilar fundamental para la llegar hasta acá y seguir adelante.

A mi tutora,

Por el acompañamiento y apoyo brindado durante estos momentos de estrés y por toda la ayuda brindada para la elaboración de este proyecto.

A la familia Segura Campos,

Por todo el apoyo brindado durante esta etapa de mi carrera profesional.

A mis amigos de la Universidad,

Por el apoyo, y las vivencias durante todos los años de estudio, por los momentos inolvidables donde nunca faltaron las risas, y la motivación para seguir adelante.

A mi jefe y compañeros de trabajo,

Por brindarme la oportunidad de realizar este trabajo y todo el apoyo brindado durante el proceso.

RESUMEN

El presente trabajo final de graduación tiene como finalidad, diseñar una propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204, con el propósito de generar una mejora en la calidad de estas revisiones.

En la actualidad la tecnología es empleada de forma casi desmesurada en la mayor parte de procesos dentro de las organizaciones para automática y optimizarlos; y no es la excepción, su uso en organizaciones fiscalizadas por algún ente regulador para facilitar el cumplimiento de los requerimientos impuestos por alguna ley. Por lo tanto, empieza a ser importante considerar las buenas prácticas de gestión de tecnologías de información como COBIT 2019 y/o ISO9001 cuando existe algún componente tecnológico que es regulado por actividades de control.

Dado lo anterior, la presente investigación procederá a realizar un análisis del proceso actual realizado por una empresa que brinda servicios de auditoría externa sobre cumplimiento de la ley Nº8204, para determinar si el proceso se encuentra definido y delimitado de forma que todo colaborador realice un proceso unificado, estandarizado y con el mismo grado de calidad para cada cliente, asegurando resultados confiables y abordando los aspectos mínimos de la legislación nacional en temas de fraude y lavado de dinero.

Más adelante se consideran aspectos de la regulación nacional, específicamente el acuerdo SUGEF 12-10 y de los marcos de trabajo que contribuyen, fundamentan y consolidan la propuesta elaborada mediante este proyecto.

Posteriormente, se diseña la propuesta de controles basada en el análisis de brechas, con todas las oportunidades de mejora identificadas durante el desarrollo de la investigación, de forma que se pretende estandarizar el proceso de ejecución de las auditorías de TI de cumplimiento de la ley Nº8204 para que puedan ser ejecutadas por cualquier colaborador con poca experiencia sin sufrir cambios en la calidad del proceso o los resultados.

De esta forma, el presente trabajo final de graduación alcanzó a resolver la situación problemática planteada sin afectar los aspectos mínimos de la legislación nacional que deben considerarse durante la revisión.

Finalmente, mediante un modelo de costos se determinó que la propuesta es viable de implementar desde el punto de vista financiero pues presenta indicadores de inversión positivos.

Palabras clave: Auditoría, Auditoría de Tecnologías, Fraude y Lavado de Dinero, COBIT 2019, Tecnologías de Información, Ley Nº8204.

ABSTRACT

The purpose of this final graduation work is to design a proposal for a set of controls for an information technology audit in compliance with Law No. 8204, with the purpose of generating an improvement in the quality of these reviews.

At present, technology is used in an almost excessive way in most processes within organizations to automate and optimize them; and it is not the exception, its use in organizations supervised by a regulatory entity to facilitate compliance with the requirements imposed by any law. Therefore, it is becoming important to consider good information technology management practices such as COBIT 2019 and / or ISO9001 when there is a technological component that is regulated by control activities.

Given the above, this investigation proceeds to carry out an analysis of the current process carried out by a company that provides external audit services on compliance with Law No. 8204, to determine if the process is defined and delimited in such a way that all collaborators carry out a unified, standardized process with the same degree of quality for each client, ensuring reliable results and addressing the minimum aspects of national legislation on fraud and money laundering issues.

Later, aspects of national regulation are considered, specifically the SUGEF 12-10 agreement and the frameworks that contribute, base, and consolidate the proposal prepared through this project.

Subsequently, the control proposal is designed based on the analysis of gaps, with all the opportunities for improvement identified during the development of the investigation, in such a way that it is intended to standardize the process of executing IT audits in compliance with Law No. 8204 so that they can be executed by any collaborator with little experience without undergoing changes in the quality of the process or the results.

In this way, the present final graduation work managed to resolve the problematic situation raised without affecting the minimum aspects of the national legislation that must be considered during the review.

Finally, used a cost model to determine that the proposal is feasible to implement from a financial point of view, since it presents positive investment indicators.

Keywords: Audit, Technology Audit, Fraud and Money Laundering, COBIT 2019, Information Technology, Law No. 8204.

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

INTRODUCCIÓN

En Costa Rica, la ley N°8204, denominada: “Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo” (Procuraduría General de la República, 2021), es la responsable de regular las actividades financieras para evitar la legitimación de capitales en el país. Esta ley establece en el artículo uno del capítulo único que “(…) se regulan y sancionan las actividades financieras, con el fin de evitar la legitimación de capitales y las acciones que puedan servir para financiar actividades terroristas, tal como se establece en esta Ley. (Procuraduría General de la República, 2021).

Las entidades sujetas al cumplimiento de la ley N°8204 en materia financiera son aquellas que son reguladas, supervisadas y fiscalizadas por alguno de los siguientes órganos:

a. Superintendencia General de Entidades Financieras (SUGEF).
b. Superintendencia General de Valores (SUGEVAL).
c. Superintendencia de Pensiones (SUPEN).
d. Superintendencia General de Seguros (SUGESE).

Debido a lo antes indicado, se requiere que la entidad sometida a fiscalización contrate los servicios de una auditoría externa para que realice pruebas específicas sobre el cumplimiento de las medidas para prevenir y detectar la legitimación de capitales y el financiamiento al terrorismo, y posteriormente emitir un informe en el cual se brinde una valoración de la eficacia operativa que incluya al menos los requisitos mínimos solicitados en la Normativa para el cumplimiento de la "Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso no Autorizado, Legitimación de Capitales y Actividades Conexas", Ley N°8204. (SUGEF, 2017)

Producto de la regulación, la Firma brinda entre sus servicios la revisión del cumplimiento de la ley N°8204, cabe destacar que esta auditoría tiene un componente de TI y; por lo tanto, se requiere que el equipo auditor tenga conocimientos afines.

Actualmente, la Firma se basa en la Normativa para el cumplimiento de la Ley emitida por la SUGEVAL en la cual, se definen nueve artículos para evaluar los requisitos mínimos a los cuales debe apegarse la entidad fiscalizada. Sin embargo, el procedimiento de auditoría no ha definido controles ni sus atributos por lo que la revisión se enfoca únicamente en validar una serie de actividades relacionadas a cada uno de los artículos.

Debido a lo anterior, este Trabajo Final de Graduación se enfoca en la elaboración de una propuesta para un set de controles de TI apoyado tanto en el marco jurídico nacional como buenas prácticas internacionales como son las Normas Internacionales de Auditoría y COBIT 2019. Con el propósito de realizar una estandarización del proceso actual y generar un mayor valor agregado a los clientes de esta revisión, sin dejar de lado los requerimientos mínimos establecidos en la regulación. Cabe destacar que el producto final esperado es una matriz que incluya los atributos y procedimientos que conforman cada uno de los controles a evaluar en la revisión de la ley N°8204.

Capítulo I: Descripción general

1.1. Antecedentes

1.1.1. Descripción de la organización

En la siguiente sección se describen las características más relevantes de la organización, con el propósito de generar entendimiento sobre la misma, para esto se describe la misión, visión, valores e información general.

En adelante, la organización por motivo de confidencialidad será referida como La Firma, la cual según su sitio web, se encuentra conformada con alrededor 227 000 colaboradores trabajando a lo largo de 146 países. En Costa Rica empezó a brindar servicios en 1958 contando con más de 60 años de experiencia en el mercado nacional y en la actualidad es una de las firmas de servicios profesionales más importante del país. (La Firma, 2020)

La Firma cuenta con equipos profesionales multidisciplinarios en busca de atender las necesidades del mercado costarricense, a través de un profundo conocimiento del marco regulatorio local respaldada con la formación continua y la dedicación al servicio brindado a los clientes. (La Firma, 2020)

Adicionalmente, la estructura organizacional de la Firma se encuentra organizada con base en las líneas de servicios que ofrecen, las cuales son: Auditoría (*Audit*, nombre en inglés), Impuestos y Legal (*Tax & Legal*, nombre en inglés), y Asesoría (*Advisory*, nombre en inglés). Cabe destacar que cada línea de negocio se encuentra conformada por sublíneas. En la Figura 1, se muestra una adaptación del organigrama general de la Organización.

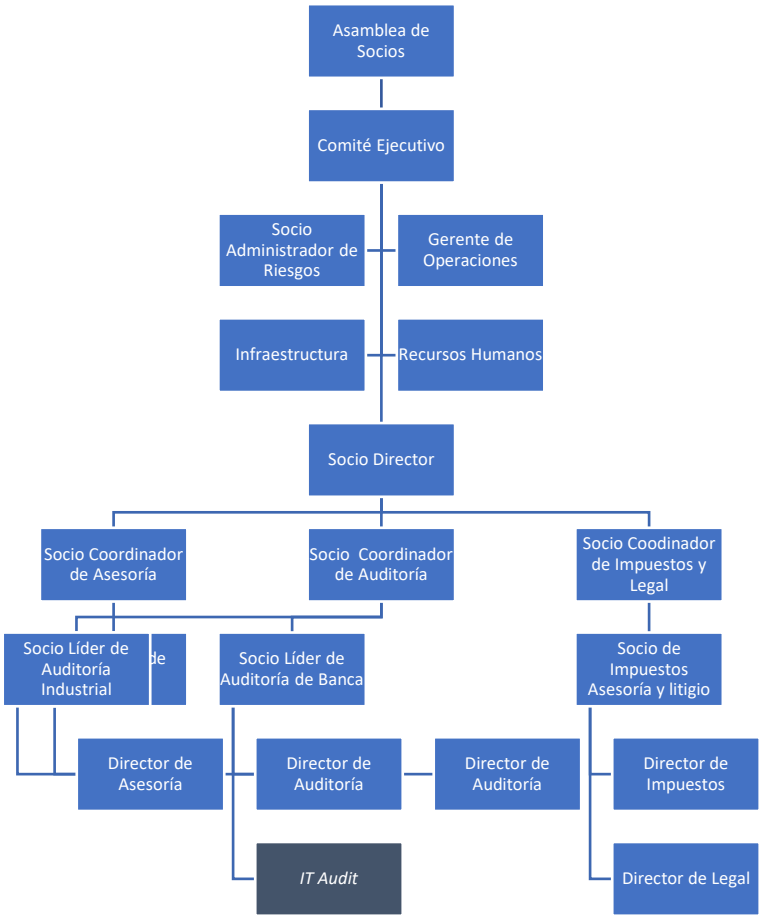


Figura 1. Organigrama General

Fuente: Adaptado de (La Firma, 2020)

1.1.1.1. Misión

La misión de la Firma es la siguiente, obtenida de su sitio web:

"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." (La Firma, 2020)

1.1.1.2. Visión

La visión de la Firma es la siguiente, obtenida de su sitio web:

"Ser la mejor firma de servicios profesionales, para nuestros clientes, para nuestra gente y para nuestra comunidad." (La Firma, 2020)

1.1.1.3. Valores

Los valores por los que ha optado la Firma son los siguientes: (La Firma, 2020)

- Lideramos con el ejemplo
- Trabajamos en equipo
- Respetamos a los individuos
- Investigamos los hechos y transmitimos conocimientos
- Nos comunicamos de forma abierta y honesta
- Comprometidos con la Sociedad
- Por encima de todo nos comportamos con integridad

1.1.1.4. Equipo de trabajo

De acuerdo con la Figura 1, la Firma cuenta con diferentes departamentos responsables de brindar servicios a los clientes, cabe destacar que el presente trabajo se desarrollará dentro del departamento de servicios de auditoría, propiamente en el área denominada Auditoría de TI (en adelante, *IT Audit*, por su nombre en inglés).

Como su nombre lo indica el área de *IT Audit* se encuentra conformada por especialistas de TI, los cuales tienen a su cargo brindar servicios de auditoría de TI como apoyo al equipo de auditoría financiera mediante la evaluación de los sistemas de información que tienen relación con la emisión de los estados financieros e infraestructura tecnológica que los soporta. Lo anterior, con el propósito de determinar deficiencias en controles y configuraciones que puedan provocar errores o registros indebidos en la información contable.

Actualmente, el área de *IT Audit* se encuentra conformada por un Gerente Sénior, un Gerente, un Supervisor, dos Encargados y un conjunto de especialistas con un grado de licenciatura o en proceso de su obtención; en carreras afines a tecnología de información. Cabe destacar que durante la elaboración del proyecto el estudiante conformará parte del grupo de asistentes.

En la Figura 2, se aprecia tanto la jerarquía existente dentro del área de *IT Audit* como la ubicación del estudiante que realiza el presente trabajo.

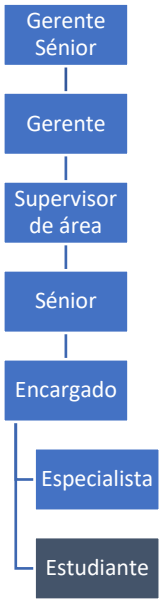


Figura 2. Organigrama de IT Audit

El equipo colaborador para la elaboración del Trabajo Final de Graduación, que brindará apoyo para facilitar el cumplimiento de los objetivos, se encuentra conformado por:

- **Gerente Sénior del área de *IT Audit*:** Tiene el rol de patrocinador del proyecto, será la parte encargada de revisar, aprobar y brindar retroalimentación al estudiante con respecto a los entregables del proyecto.
- **Supervisora del área de *IT Audit*:** Brindará la información operativa requerida como insumo para elaborar los diversos entregables, así como orientación para la coordinación de reuniones con el personal adecuado en la organización cuando así se requiera y finalmente, será un filtro dando su criterio durante una revisión previa al Gerente Sénior de los entregables.
- **Especialista de *IT Audit*:** Será una guía que brindará tanto apoyo como sus observaciones durante la ejecución del proyecto con base en sus propios conocimientos.
- **Estudiante:** Es el actor principal, responsable de recopilar y procesar la información necesaria para llevar a cabo el desarrollo del proyecto y alcanzar el objetivo por medio de la propuesta de controles para la revisión de la ley N°8204.

1.1.2. Trabajos similares realizados dentro y fuera de la organización

En esta sección se describen los proyectos que se han realizado en la organización y que están relacionados con el proyecto propuesto y que servirán como insumo. Algunos de estos realizados dentro de la organización en relación con mejoras de los procedimientos o controles de auditoría de TI son los siguientes:

1.1.2.1. Proyecto para la actualización de la matriz de controles de auditoría

Durante el 2015, la actual gerente del área de *IT Audit* realizó un proyecto el cual se identificó la necesidad de actualizar la matriz de controles de auditoría que se realizaban en ese momento. (Sánchez, 2015)

Utilizando el marco de trabajo COBIT 4.1 se inició con la actualización de Matriz de Controles Generales de TI que era utilizada para evaluar los sistemas de información como apoyo a las auditorías financieras que brinda la Firma. Por medio de este proyecto se realizó una restructuración a los controles del área de Acceso a Programas y Datos, definiendo un total de 11 controles los cuales son utilizados hasta la fecha durante el ejercicio de las auditorías financieras. (Sánchez, 2015)

Los controles que fueron definidos abarcan aspectos como la documentación de políticas de uso, seguridad de información, mecanismos utilizados por el departamento de TI de la organización auditada para garantizar el funcionamiento y la integridad de los sistemas financieros dentro de la misma. (Sánchez, 2015)

Adicionalmente, se identificó el área de gestión de cambios como un área crítica para evaluar y donde mayormente las organizaciones auditadas carecen de controles para ejecutar este proceso de la forma correcta. Por tal razón, una de las recomendaciones del proyecto fue realizar una actualización de controles de dicho apartado. (Sánchez, 2015)

Este proyecto es considerado un antecedente relevante debido a que presenta una propuesta de trabajo que puede ser considerada en la ejecución del Trabajo Final de Graduación. Adicionalmente, las actividades ejecutadas y el resultado obtenido de las mismas generan una matriz para la revisión de controles generales de la auditoría financiera la cuál es un insumo para la definición de la matriz con el set de controles que se busca realizar con el proyecto en cuestión.

1.1.2.2. Propuesta de una guía documental y procedimental según la norma ISO 9001 para el proceso de ejecución de una auditoría relacionada con Anti-Money Laundering (AML) siguiendo los objetivos establecidos por el negocio.

Otro trabajo realizado fue durante el 2019, donde se realizó una propuesta para una guía documental y procedimental según la norma ISO 9001 para el proceso de ejecución de una auditoría relacionada con Anti-Money Laundering (Antilavado de dinero, por su traducción al español) siguiendo los objetivos establecidos por el negocio, caso VYA. (Guzmán & Elizondo, 2019)

Dicho trabajo consistió en presentar una mejora que permitiera unificar y estandarizar el proceso de auditoría de cumplimiento sobre el fraude y lavado de dinero, para asegurar resultados confiables para los clientes sin dejar de lado todos los requerimientos de la legislación nacional. (Guzmán & Elizondo, 2019)

Finalmente, se considera relevante dado que se presenta una propuesta de diseño para una guía documental y procedimental basada en la norma ISO 9001, la cual busca estandarizar el proceso de recopilación de información otorgando mejores resultados y mayor agilidad a la hora de ejecutar la auditoría de la ley N°8204. (Guzmán & Elizondo, 2019)

1.2. Planteamiento del Problema

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

1.2.1. Situación problemática

El área de *IT Audit* de la Firma toma en consideración los requerimientos mínimos a revisar para validar el cumplimiento de la ley N°8204 desde un punto de vista de las tecnologías de información de la organización auditada. Debido a lo anterior, se definieron nueve objetivos los cuales son respaldados con artículos de la normativa para el cumplimiento de la "Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso no Autorizado, Legitimación de Capitales y Actividades Conexas", Ley N°8204.

Sin embargo, los procedimientos actuales para la revisión de la ley N°8204 presentan algunas deficiencias en su ejecución al no contar con instrucciones claras ni procesos que regulen la manera como el personal verifica cada objetivo. Pues, la auditoría

no se encuentra sustentada en ninguna práctica internacional, limitándose únicamente a los requerimientos mínimos para el cumplimiento de la ley.

Dado que las instrucciones son poco detalladas y que mayormente los auditores que realizan estas evaluaciones tienen poca experiencia, pues en su mayoría tienen puesto de asistente. El resultado de la revisión de la ley Nº8204 varia en cuanto a la calidad brindada a cada uno de los clientes e incluso se podría omitir algún aspecto importante indicado en la normativa.

Lo anterior, tiene un serio impacto en los clientes, pues en caso de no ejecutar la auditoría en concordancia con los artículos de la Norma para el Cumplimiento de la Ley Nº8204, el resultado podría ser afectado de tal forma que ambas partes pueden llegar a ser penalizados por los entes regulatorios.

Además, al no contar con instrucciones detalladas ni un enfoque de revisión de controles sustentado en buenas prácticas internacionales, en el momento de realizar la auditoría no es posible recomendar a la organización la inclusión y formalización de actividades de control interno acordes a los objetivos evaluados de la ley N°8204, para la prevención del lavado de dinero.

Por otra parte, la Firma cuenta con un sistema que permite la documentación centralizada de los proyectos de auditoría que realiza, donde se define para cada auditoría financiera el espacio de trabajo para documentar los controles tanto a nivel financiero como de TI que respaldan la generación de informes financieros. Dicha herramienta sigue una metodología de trabajo que la Firma ha adoptado con procedimientos propios apoyados por buenas prácticas internacionales.

Sin embargo, el proceso de revisión del cumplimiento de la ley Nº8204 no emplea esta herramienta; por lo tanto, cada auditor mantiene en su ordenador la documentación que soporta las conclusiones. Por lo cual, los revisores no tienen acceso para monitorear con frecuencia las actividades realizadas por el auditor, y en caso de que falte algún aspecto a considerar en la auditoría mayormente se dan cuenta cuando el tiempo se ha agotado, lo que conlleva al área de *IT Audit* recurrir en mayores costos.

Finalmente, es importante resaltar que, como parte de los procesos de mejora continua, la administración de la Firma ha adquirido el desafío de encontrar una forma de entregar mayor valor agregado a los clientes de la auditoría de cumplimiento de la ley N°8204, y que dicha responsabilidad fue asignada al departamento de *IT Audit*.

Por lo tanto, en busca de solventar las carencias y mejorar el valor entregado se define el problema como la **carencia de controles de TI que permitan evaluar y documentar el cumplimiento de la auditoría de la ley N°8204**, para evitar la legitimación de capitales y las acciones que puedan servir para financiar actividades terroristas, al mismo tiempo que entreguen mayor valor a los clientes.

1.2.2. Justificación del proyecto

En la presente sección, se explica la importancia de desarrollar el proyecto descrito en el presente documento.

El área de *IT Audit* de la Firma cuenta con una serie de objetivos con sus respectivos procedimientos los cuales adoptaron de la legislación nacional para auditar el cumplimiento de la ley N°8204 en temas de fraude y lavado de dinero a nivel operativo en las evaluaciones efectuadas en diversas organizaciones; sin embargo, se identifican las siguientes deficiencias:

- No existe una estandarización en la recolección de información, documentación y ejecución de este proceso de evaluación; por tanto, los resultados obtenidos en cada auditoría de cumplimiento podrían ser variantes entre los diversos auditores que ejecutan esta labor.
- Se carece de eficiencia a la hora del manejo del tiempo para el trabajo de recolección de información sobre la revisión del cumplimiento de la ley N°8204, dado que los recursos destinados a la auditoría se agotan rápidamente y el resultado muchas veces no es el esperado.
- Los procedimientos de la actual revisión del cumplimiento de la ley N°8204, son repetitivos en varios objetivos. Asimismo, las descripciones de estos no siempre generan el resultado esperado dado que no contemplan escenarios para favorecer el entorno de trabajo de los colaboradores con menos experiencia.

Adicionalmente, existe el desafío por parte de la Firma para mejorar el valor entregado a los clientes en las revisiones del cumplimiento de la ley N°8204, sin afectar los aspectos mínimos requeridos en cada evaluación. En consecuencia, el área de *IT Audit* debe considerar la regulación nacional vigente en conjunto con las buenas prácticas internacionales para mantenerse alineado con el objetivo de la revisión.

Dado lo anterior, para solventar las necesidades que tiene la Firma en relación con la revisión de la ley N°8204, este trabajo busca impulsar y mejorar el proceso de auditoría por medio de conocimientos en la práctica de auditoría de TI, sustentados con normas internacionales de auditoría, y buenas prácticas internacionales principalmente el ISO 9001 y los procesos DSS06 – Gestionar controles de procesos de negocio del marco de trabajo, BAI05 – Gestionar los cambios de COBIT 2019. Con el objetivo de definir los controles de TI que permitan entregar valor a la organización sin afectar los requerimientos mínimos solicitados en una auditoría de cumplimiento de la ley N°8204.

1.2.3. Beneficios esperados del proyecto

A partir del desarrollo del presente trabajo, se espera que la Firma obtenga diferentes beneficios. A continuación, se mencionan los posibles beneficios a generar.

1.2.3.1. Beneficios directos

- Mejora en la planificación de recursos para evaluar la ley N°8204, lo que conlleva a una reducción de los costos invertidos en la prestación del servicio.
- Mejora en los resultados al emitir el informe sobre la revisión del cumplimiento de la ley N°8204; lo anterior, por contar con controles estandarizados que brinden una mayor solidez a las conclusiones del equipo auditor.
- Mayor control con respecto a la documentación de resultados y papeles de trabajo.
- Mayor facilidad para detectar cualquier deficiencia en alguno de los procesos operacionales; así como, un mejor control y seguimiento sobre las mismas.
- Cumplimiento con la normativa nacional vigente y apego a buenas prácticas internacionales para brindar un mejor servicio con valor agregado para los clientes.

1.2.3.2. Beneficios indirectos

- Mayor confiabilidad sobre las evaluaciones de la ley Nº8204, al considerar mejores prácticas definidas en los marcos de referencia internacionales.
- Aumento y/o retención de clientes gracias al valor agregado brindado a las empresas cliente, a partir de resultados adecuados y precisos sobre la evaluación realizada.
- Mejora de la imagen del área de *IT Audit* y la Firma en general, al implementar la mejora continua sobre los controles de evaluación.

1.3. Objetivos

En la siguiente sección, se define objetivo general, el cual representa el propósito del desarrollo del Trabajo Final de Graduación. Asimismo, se definen los objetivos específicos que indican el cómo se logrará el objetivo general y los entregables del trabajo para dar una propuesta de solución a la problemática planteada.

1.3.1. Objetivo General

Elaborar una propuesta de un set de controles para una auditoría de tecnologías de información, que permita un fortalecimiento en la revisión del cumplimiento de criterios de control relacionados con el fraude y lavado de dinero de la ley N°8204, siguiendo los objetivos establecidos por la Firma, durante el segundo semestre del 2021.

1.3.2. Objetivos Específicos

a) Comprender el proceso establecido por la Firma en las auditorías de TI de cumplimiento de la Ley N°8204, por medio del análisis del proceso actual para el entendimiento de este.

b) Determinar brechas, deficiencias y oportunidades del proceso de auditoría de TI de la ley N°8204 de la Firma contra el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI, para la identificación del estado deseado del proceso.

c) Proponer un conjunto de controles y procedimientos de auditoría de TI de la ley N°8204 ejecutado por la Firma, para el cumplimiento del estado deseado del proceso y generación de valor a la organización auditada.

d) Construir un análisis financiero para la propuesta del proceso de auditoría TI de la ley N°8204, por medio de valoraciones financieras basadas en la industria y otras fuentes, para la obtención del impacto financiero aproximado que conllevan los beneficios y costos de esta.

1.4. Alcance del proyecto

El presente trabajo final de graduación tiene como propósito, definir un set de controles de TI para las auditorías de cumplimiento de la ley N°8204, para el área de *IT Audit*, que contemple los requisitos mínimos, específicamente los nueve objetivos adoptados de la Normativa para el cumplimiento de la "Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso no Autorizado, Legitimación de Capitales y Actividades Conexas", Ley N°8204. En la Tabla 1, se muestran las actividades evaluadas por la Firma.

Objetivo	Artículo	Descripción
1	Artículo 6	Criterios o variables para el análisis y descripción del perfil de riesgo del cliente.
2	Artículo 16	Programas informáticos.
3	Artículo 17	Análisis de las alertas generadas de los programas informáticos.
4	Artículo 18	Bitácoras.
5	Artículo 19	Operaciones únicas en efectivo.
6	Artículo 19 bis	Transferencias electrónicas.
7	Artículo 20	Operaciones múltiples
8	Artículo 21	Remisión de información a las Superintendencias
9	Artículo 38	Apartados mínimos del informe anual

Tabla 1. Actividades evaluadas por la Firma.

Fuente: (SUGEF, 2017)

En primera instancia, se procede a realizar una inspección que permita comprender el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI en temas de fraude y lavado de dinero, así como las pruebas empleadas por la Firma para cada uno de los objetivos de la auditoría de revisión.

Seguidamente, se considera en el desarrollo del trabajo, la elaboración de un marco teórico que, con base en las normas internacionales de auditoría desde un punto de vista de tecnologías de información, regulaciones contra el fraude y lavado de dinero, COBIT 2019 con énfasis en la gestión de controles de procesos de negocio y el control de cambios, así como otros conceptos y tecnologías relevantes, permitan realizar un abordaje sólido, y con profundidad desde distintos enfoques.

Posteriormente, se procederá a determinar brechas, deficiencias y oportunidades en el proceso actual realizado por la Firma en su revisión de la ley N°8204, al contrastarlo con el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI y el lavado de dinero.

Partiendo de lo anterior, se plantea diseñar un conjunto de controles y procedimientos alineados con la metodología de la Firma y sustentado por el marco teórico desarrollado, que permitan evaluar los requerimientos mínimos solicitados en la Normativa para el cumplimiento de la "Ley sobre Estupefacientes, Sustancias Psicotrópicas, Drogas de Uso no Autorizado, Legitimación de Capitales y Actividades Conexas", Ley N°8204.

Es importante destacar que estos controles conforman la propuesta de revisión de cumplimiento de la ley N°8204, contemplando los aspectos mínimos requeridos, facilitando la ejecución y seguimiento de auditorías en los clientes. Para lo cual, se construirá en un documento de Microsoft Excel una matriz que incluirá los aspectos a considerar en la revisión como la descripción, atributos, procedimientos y evidencia requerida para sustentar las pruebas.

Seguidamente, se elabora un instructivo que servirá como guía para la ejecución de una auditoría de cumplimiento de la ley N°8204 que incluye aspectos como la lista de requerimientos que deben ser solicitados al cliente, consideraciones generales durante la revisión de los controles, formato para documentar los resultados de las pruebas realizadas y plantilla de la carta para comunicar los resultados obtenidos.

Finalmente, considerando el tiempo invertido en el desarrollo de la propuesta por el estudiante y los integrantes de la Firma que han aportado su apoyo y conocimiento al estudiante, así como el tiempo estimado en la revisión de la ley N°8204, se realizará el modelo económico con valoraciones de la industria y otras fuentes, para brindar una aproximación al costo y valor de la propuesta.

1.5. Entregables del proyecto

Este apartado se describe todos los entregables que tendrá el proyecto, considerando la gestión, los académicos dirigidos a la coordinación del Trabajo Final de Graduación y el producto final solicitado por la Firma.

1.5.1. Entregables académicos

Corresponde al Informe de Trabajo Final de Graduación requerido para optar por la Licenciatura en Administración de Tecnología de Información. En el documento se detallan secciones como introducción, marco teórico, desarrollo metodológico, análisis de resultados, propuesta de solución, conclusiones, recomendaciones, anexos, apéndices y referencias bibliográficas.

1.5.2. Entregables del producto

En estos documentos se detalla el producto del proyecto, los cuales corresponden a los entregables que se realizarán para la organización. A continuación, se detallan estos:

1.5.2.1. Propuesta de controles para el cumplimiento de la ley

Mediante un documento Microsoft Excel, se entregará el listado completo de los controles de la propuesta para la revisión de la ley N°8204, dicho documento incluye los atributos de control, procedimientos sugeridos y evidencia que debería considerarse para sustentar las pruebas.

Adicionalmente, se entregará un instructivo que servirá como guía para evaluar los procedimientos de cada control, y que será un insumo para que el equipo de *IT Audit* realice las revisiones de la ley N°8204.

1.5.2.2. Análisis financiero de la propuesta

Se construirá un análisis para dar una aproximación del impacto financiero de la propuesta, donde se detallará por medio de valoraciones de la industria y otras fuentes, el costo de la propuesta y el valor financiero que trae a la organización.

1.5.3. Gestión del proyecto

Para un adecuado seguimiento y control del proyecto, en esta sección se define el cronograma inicial de trabajo donde se indican las fechas de entrega de los productos;

además, se establece el formato a utilizar para la elaboración de las minutas sobre las reuniones de seguimiento, control y cambios respecto al proyecto.

La gestión del presente proyecto se basa en el cumplimiento de los objetivos planteados en la sección Objetivos, para lo cual se establece el proceso de documentación de las reuniones y el cronograma del proyecto con las actividades por realizar durante el desarrollo del proyecto. Además, se define cómo será la gestión y el procedimiento para establecer cambios dentro del proyecto por ejecutar.

1.5.3.1. Minutas

Se emplearán minutas para mantener constancia de los temas conversados y acuerdos tomados por las partes involucradas en las reuniones que se lleven a cabo durante la ejecución del proyecto. Por lo anterior, la plantilla que será utilizada con este propósito se puede consultar en el Apéndice A.

1.5.3.2. Gestión del Cambio

Para la gestión de cambios se utilizará la plantilla definida en el Apéndice B, de manera que toda solicitud para ser considerada deberá contar con el formulario debidamente completado y seguir el siguiente procedimiento:

- **A.** El solicitante del cambio completa los campos de la plantilla del Apéndice B para este fin.
- **B.** Posteriormente, el estudiante en conjunto con el profesor tutor y el representante de la organización se dispondrán a evaluar la pertinencia del cambio, teniendo en cuenta aspectos como el costo-beneficio y el impacto que tendrá sobre el cronograma y alcance del proyecto.
- **C.** Finalmente, se notifica al solicitante mediante correo electrónico la resolución de la solicitud, y en caso de aceptarse se firma el acuerdo entre todas las partes involucradas.

1.5.3.3. Cronograma

El cronograma de proyecto sirve de como mecanismo de control de avance y apoyo para las fechas de entrega de los productos. El mismo se encuentra en el Apéndice C.

1.6. Supuestos del proyecto

A continuación, se presentan los elementos que se asumen como ciertos durante el desarrollo del presente trabajo.

a. Disposición de la Firma Auditora en brindar información, atender consultas y dar retroalimentación durante el desarrollo del proyecto.

b. Las personas involucradas en el proyecto tienen interés en su desarrollo.

c. Se dispondrá de todas las herramientas y recursos tanto físicos como tecnológicos necesarios en el trabajo.

1.7. Exclusiones del proyecto

En este apartado, se enumeran los aspectos que no serán tomados en cuenta durante el desarrollo del Trabajo Final de Graduación. En consecuencia, estos aspectos no formarán parte de resultados esperados ni de los entregables.

Es importante aclarar que el desarrollo del Trabajo de Graduación tiene como el definir un set de controles que permitan estandarizar la forma en cómo se establece el resultado de evaluación y entregar un mayor valor al cliente; sin embargo, no se realizará ninguna prueba de evaluación o implementación de los entregables producto del proyecto.

En particular, durante el desarrollo del proyecto no se incluirá los siguientes aspectos:

- No se contempla efectuar actividades con organizaciones clientes de la Firma Auditora, con el propósito de recolectar información.
- Las solicitudes de profesionales internos que no formen parte del equipo de trabajo no serán contempladas durante el desarrollo del trabajo, salvo que el supervisor considere adecuado hacerlo, en estos casos, se deberá seguir el procedimiento establecido para cambios en el proyecto.
- No se considera desarrollar revisiones en organizaciones clientes, a fin de probar los controles o pruebas formuladas.
- El desarrollo de capacitaciones o formación al personal del área sobre el uso de los productos del proyecto se efectuará fuera del periodo establecido para el desarrollo de la propuesta.

1.8. Limitaciones del proyecto

A continuación, se describen las restricciones o limitaciones que pueden afectar el desarrollo del trabajo final de graduación, que contemplan factores, personas o circunstancias:

- El apoyo e interés que brinda la institución sobre el desarrollo del proyecto se refiere únicamente en el área de *IT Audit*.
- La regulación establece los requerimientos mínimos que deben ser contemplados y estos no pueden ser alterados.
- Disponibilidad limitada del personal para atender consultas sobre el proyecto.
- Los objetivos definidos por la organización que regulan el control de fraude y lavado de dinero, pese a la que presente investigación, pueden detallar la normativa con los cuales debieron haber sido creados y los mismos podrían ser alterados durante la ejecución de la investigación actual, no es objetivo de este trabajo modificarlos.
- La no utilización de software u otros programas informáticos que no han sido avalados por la Firma.
- No se cuenta con acceso a la información financiera de la Firma, requerida para construir el modelo económico de la propuesta; por ende, se realizarán valoraciones financieras basadas en la industria y otras fuentes.

Capítulo II: Marco Conceptual

Este capítulo tiene como objetivo abordar todos los conceptos y definiciones que serán empleados, dado que fundamentan conceptualmente el desarrollo de este trabajo final de graduación, de manera que se construya una base teórica que apoye el entendimiento.

La estructura del capítulo toma como base un esquema de conceptos relacionados con el desarrollo tanto del objetivo general como los específicos del proyecto, teniendo en cuenta todos los conceptos relacionados con la auditoría de cumplimiento de la ley N°8204.

2.1. Mapa de Conceptos

Seguidamente, en la Figura 3, se muestra el mapa de conceptos, que incluye el detalle de los conceptos más relevantes del proyecto y aquellos que se derivan de este, para construir una base que apoye el entendimiento del problema que se pretende resolver.

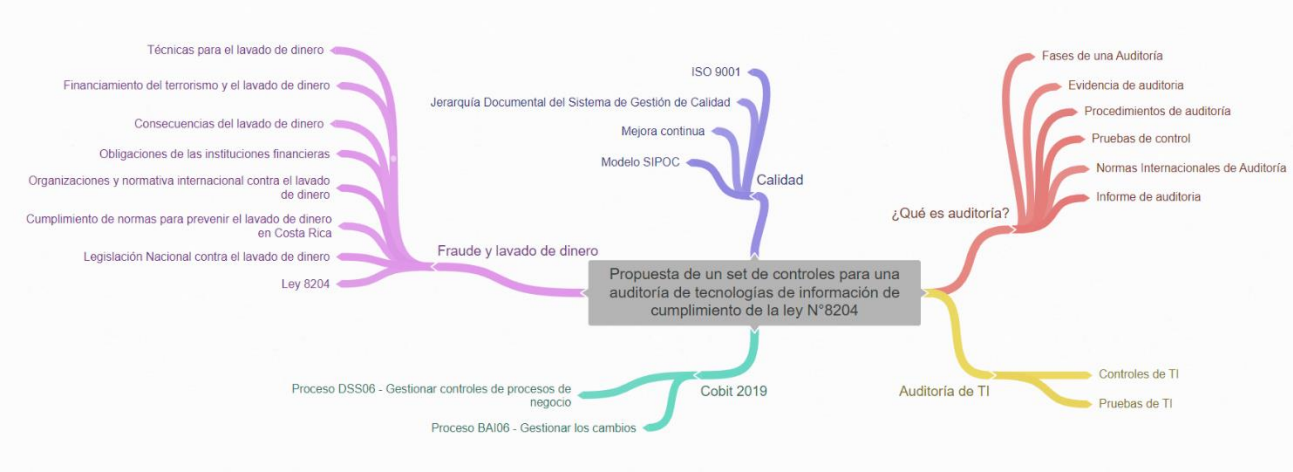


Figura 3. Mapa de conceptos

2.2. Auditoría

Julián Pérez Porto y Ana Gardey, segmentan el término de auditoría en tres partes, definiéndolo de la siguiente manera:

> "*Auditoría es un término que puede hacer referencia a tres cosas diferentes pero conectadas entre sí: puede referirse al trabajo que realiza un auditor, a la tarea de estudiar la economía de una empresa, o a la oficina donde se realizan estas tareas (donde trabaja el auditor)". (Pérez Porto & Gardey, 2021)*

Por otra parte, Nuño (2019) hace referencia al término de auditoría definiéndolo de la siguiente manera:

> *"La auditoría es un sistema de control e inspección que se da dentro de una empresa de cualquier sector de actividad, con el fin de mejorar los procesos, por ejemplo, o con el fin de comprobar que realmente actúa dentro de los términos legales en materia contable (…)." (Nuño, 2019).*

En términos generales, podemos ver el proceso de auditoría como un mecanismo que permite evaluar a empresas de cualquier ámbito o sector comercial, permitiendo establecer puntos de mejora al objeto o proceso auditado; además, permite validar que actúe en función de los términos definidos por la organización y que cumpla con las normas y legislación legal que se encuentra implícita en el objeto de estudio. (Nuño, 2019)

2.2.1. Fases de una Auditoría

Las auditorías se realizan siguiendo planes de acción o fases para respetar y cumplir un debido proceso. Según Uriarte (2021), estas fases son las siguientes:

- **Planeación:** Donde se informa a la empresa el modo de actuar del auditor y el tiempo que dura dicha auditoría. En esta etapa se le puede solicitar a la empresa determinadas cuestiones que faciliten la tarea del auditor. Por ejemplo, acceso a depósitos, a material contable o a oficinas. (Uriarte, 2021)
- **Ejecución**: Es la puesta en marcha de la etapa anterior, es la fase donde se realizan las pruebas necesarias para recopilar la información y que el auditor pueda generar opinión sobre el tema evaluado. (Uriarte, 2021)
- **Informe:** Es la presentación en forma escrita que incluye todos los datos revelados durante el trabajo del auditor, es una recopilación del material reunido durante la ejecución, con hincapié en resultados encontradas. (Uriarte, 2021)

2.2.2. Evidencia de Auditoría

El sitio web denominado Auditool (2017), describe la evidencia como "(…) el medio a través del cual se valida o se contradice que la información o procesos han sido realizados de acuerdo con las normas internas o políticas que deba cumplir la entidad en la jurisdicción donde se encuentre". (Auditool, 2017).

Adicionalmente, en el sitio de Auditool (2017), se indica que la evidencia debe ser suficiente, adecuada y cumplir una serie de características como la cantidad necesaria para que el auditor pueda concluir su opinión sobre la información revisada.

2.2.3. Procedimientos de auditoría para obtener evidencia

La NIA 500 indica los procedimientos para la recopilación de evidencia de auditoría suficiente y adecuada al contexto, estos son:

- **Inspección:** Implica examinar documentos que pueden ser físicos o electrónicos. (IAASB, 2021)
- **Observación:** Consiste en presenciar la ejecución de un proceso o procedimiento mientras es aplicado por otra persona.
- **Confirmación externa:** Consiste en evidencia obtenida mediante la respuesta directa escrita por un canal físico o electrónico y que está dirigida al auditor. (IAASB, 2021)
- **Recálculo:** Consiste en comprobar la exactitud de cálculos matemáticos de forma manual o por medios electrónicos. (IAASB, 2021)
- **Indagación:** Cosiste en realizar la búsqueda de información a través de personas expertas. (IAASB, 2021)

Es importante resaltar que, de acuerdo con la NIA 330, en el apartado A26 se indica que la indagación, por si sola, no es suficientemente segura para permitir probar la eficacia operativa de un control. Por lo tanto, se deberán aplicar otros procedimientos en conjunto a la indagación para sustentar la conclusión. (IAASB, 2021)

2.2.4. Pruebas de control

De acuerdo con la NIA 330 existen pruebas de control y procedimientos sustantivos, este último es utilizado para detectar incorreciones materiales en afirmaciones; por tanto, no es relevante considerarlo para una auditoría de TI. Por otra parte, las pruebas de control cuentan con procedimientos de auditoría diseñados para realizar la evaluación de eficacia operativa de los controles. (IAASB, 2021)

Según el gerente sénior de PWC, para que las tareas se ejecuten de manera consistente y no se cree dependencia de personal sobre actividades. Se debe contar con un ambiente de control de TI con políticas y procedimientos estandarizados, donde por medio de matrices de riesgo, facilite la evaluación del diseño actual de los controles, para validar que estos mitiguen de manera adecuada los riesgos relacionados. (Zuazo, 2021)

Cabe resaltar que los sistemas de información soportan el cumplimiento de tareas, estos traen consigo riesgos financieros, operacionales o de cumplimiento que deben ser abordados por la organización. Y en caso de no contar con una adecuada evaluación de riesgos, acompañada de una estrategia para abordarlos, el cumplimiento de objetivos de la compañía podría verse afectado. (Zuazo, 2021)

2.2.5. Normas Internacionales de Auditoría

Según el sitio de AOB Auditores (2021), las Normas Internacionales de Auditoría (en adelante, NIAS) deben aplicarse siempre en las auditorías de estados financieros, debido a que indican los aspectos de calidad, pues contienen principios y procedimientos básicos que son esenciales para el auditor.

En la Tabla 2, se indica las NIAs y una breve descripción de cada una.

NIA	Descripción
NIA 200	Objetivos globales del auditor independiente
NIA 210	Acuerdo de los términos de encargo de auditoría
NIA 220	**Control de calidad de la auditoría de estados financieros**
NIA 230	**Responsabilidad del auditor en la preparación de la documentación**
NIA 240	**Responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude**
NIA 250	Responsabilidad del auditor de considerar las disposiciones legales y reglamentarias
NIA 260	Responsabilidad que tiene el auditor de comunicarse con los responsables del gobierno
NIA 265	Responsabilidad que tiene el auditor de comunicar adecuadamente
NIA 300	Responsabilidad que tiene el auditor de planificar
NIA 315	Responsabilidad del auditor para identificar y valorar riesgos
NIA 320	Responsabilidad que tiene el auditor de aplicar concepto de importancia relativa
NIA 330	Responsabilidad del auditor de diseñar e implementar respuestas
NIA 402	Responsabilidad del auditor de la entidad usuaria de obtener evidencia de auditoría
NIA 450	Responsabilidad del auditor de evaluar el efecto de las incorrecciones identificadas
NIA 500	**Evidencia de auditoría en una auditoría de estados financieros**

NIA	Descripción
NIA 501	Consideraciones específicas del auditor
NIA 505	Procedimientos de confirmación externa
NIA 510	Relación con los saldos de apertura en un encargo inicial
NIA 520	Procedimientos analíticos como procedimientos sustantivos
NIA 530	**Muestreo de auditoría en la realización de procedimientos**
NIA 540	Responsabilidad del auditor en relación con las estimaciones contables
NIA 550	Relaciones y transacciones con partes vinculadas en una auditoría
NIA 560	Respecto a los hechos posteriores al cierre
NIA 570	Utilización de la dirección de hipótesis de empresa en funcionamiento
NIA 580	Obtener manifestaciones escritas de los responsables
NIA 600	Consideraciones particulares aplicables a las auditorías del grupo
NIA 610	Auditor externo con respecto al trabajo de los auditores internos
NIA 620	Organización en un campo de especialización distinto
NIA 700	Formarse una opinión sobre los estados financieros
NIA 705	Emitir un informe adecuado
NIA 706	Comunicaciones adicionales
NIA 710	Relación con la información comparativa
NIA 720	Información incluida en documentos que contienen estados financieros auditados

Tabla 2. Normas Internacionales de Auditoría

Fuente: (AOB, 2021)

A continuación, se describen algunas de las NIAS que se consideran con mayor relevancia para el desarrollo del trabajo final de graduación.

2.2.5.1. NIA 220 - Control de calidad de la auditoría de estados financieros

Según el sitio de AOB Auditores (2021), el objetivo del auditor con respecto en esta NIA es implementar procedimientos de control de calidad que proporcionen seguridad razonable sobre que el informe emitido sea adecuado a las circunstancias y que la auditoría cumple con las normas profesionales.

Entre los principales requerimientos destacables para cumplir lo indicado en la norma, se encuentra la responsabilidad de liderazgo en la calidad de auditoría, los requerimientos de ética aplicables a los auditores, aceptación y continuidad de las

relaciones con clientes y encargados de la auditoria, asignación de equipos a estos últimos, seguimiento y documentación del procedimiento. (AOB Auditores, 2021)

2.2.5.2. NIA 230 - Responsabilidad del auditor en la preparación de la documentación

Según el sitio de AOB Auditores (2021), esta norma abarca la responsabilidad del auditor para preparar la documentación de auditoría correspondiente, que proporcione un registro suficiente y adecuado sustentando las bases del informe, y que la evidencia obtenida sea de conformidad con las NIAS, requisitos legales y reglamentarios que apliquen.

Como principales requerimientos destacables para cumplir con lo indicado en la norma, se encuentra la preparación oportuna de la documentación de auditoría, documentación de los procedimientos de auditoría aplicados con la respectiva evidencia obtenida y la compilación del archivo final. (AOB Auditores, 2021)

2.2.5.3. NIA 240 - Responsabilidades del auditor en la auditoría de estados financieros con respecto al fraude

Según el sitio de AOB Auditores (2021), los objetivos del auditor con respecto a en esta NIA son:

- Identificar y valorar los riesgos de incorrección material en los estados financieros debido al fraude.
- Obtener evidencia de auditoría suficiente y adecuada con respecto a los riesgos, mediante el diseño y la implementación de respuestas apropiada.
- Dar respuesta al fraude o indicios de fraude identificados.

Entre los principales requerimientos destacables en la norma se encuentran el escepticismo profesional, procedimientos de valoración del riesgo, evaluación de evidencia de auditoría, documentación, comunicación al gobierno de la entidad y autoridades reguladoras. (AOB Auditores, 2021)

2.2.5.4. NIA 500 - Evidencia de auditoría en una auditoría de estados financieros

Según el sitio de AOB Auditores (2021), esta norma explica los temas relacionados con la evidencia de auditoría, y sobre la responsabilidad del auditor para diseñar y aplicar procedimientos de auditoría para obtener evidencia suficiente y adecuada que permita realizar conclusiones razonables en las cuales basar su opinión.

Esta NIA es aplicable a toda la evidencia obtenida durante la ejecución de la auditoría. (AOB Auditores, 2021)

2.2.5.4. NIA 530 - Muestreo de auditoría en la realización de procedimientos

Esta norma trata sobre el muestreo a realizar para la selección de información en los procedimientos de auditoría. En busca que la información que conforma la muestra sea suficiente, representativa y adecuada para proporcionar una base razonable sobre la cual el auditor pueda alcanzar conclusiones sobre la población de la que se seleccionó la muestra. (AOB Auditores, 2021)

2.2.6. Informe de Auditoría

Según Donoso (2017), el informe de auditoría es realizado por un auditor al concluir el proceso de ejecución de la auditoría, y expresa una opinión sobre las cuentas o estados financieros que presenta una empresa.

Cabe resaltar que, al momento de realizar un informe de auditoría, se debe tener en cuenta cual es el objetivo de estos, y que aspectos debe de considerar. Los siguientes son casos involucrados en los informes de auditoría:

- El auditor puede ser una persona física o una empresa dedicada a la auditoría.
- El auditor deberá ser externo, esto quiere decir que no pertenece a la empresa auditada, y en caso de ser interno el método de informe de auditoría es para ser utilizado como mecanismo de control.
- El informe de auditoría expresa una opinión que no debe vincular al auditor. Lo que quiere decir es que, la expresión es sobre las cuentas de la empresa. Por lo que el informe de auditoría expresa la percepción del auditor.

El informe de auditoría incluye los siguientes aspectos: (Donoso, 2017).

- Portada: Incluye los datos más importantes de la compañía que se examinó, además de la dirigencia de esta.
- Opinión de auditoría: Muestra el conjunto de los resultados que involucra los tipos de auditoría presentes en la revisión (revisión de estados, AML, impuestos, etc.).
- Estados financieros: Revela la condición de los estados financieros que, se revisaron durante la auditoría.

- Notas a los estados financieros: Se explica cómo están conformadas las cuentas significativas de la empresa; además, están referenciadas a las cuentas que se ligan con los estados financieros.

2.3. Auditoría de TI

Según Gómez (2014, pág. 40), la auditoría informática consiste en la revisión y evaluación de todos o parte de los aspectos considerados en los sistemas automáticos de procesamiento de información, que incluyen procedimientos manuales e interfaces relacionadas.

Aunque se asocie con un término introducido recientemente, este concepto data de finales de la década de los años 70, a partir de un cambio en el paradigma de la fiscalización que provocó una clasificación de acuerdo con la actividad realizada por el negocio y los elementos que intervenían. (Mora Quirós, 2017, pág. 1)

Este proceso es necesario para verificar y asegurar que las políticas y procedimientos establecidos en la gestión y uso de tecnologías de información en las organizaciones, se encuentre implementadas de manera eficiente y oportuna. Donde se pretende garantizar que exista un entorno adecuado para el procesamiento de datos de recursos tecnológicos, y dar seguridad de que la información sea integral, exacta y confiable.

Según Gantz (2018) la auditoría de TI difiere de manera significativa de la auditoría de registros financieros, operaciones generales o proceso de negocio; no obstante, es un componente fundamental en otras auditorías por la utilización de las tecnologías en la mayor parte de los procesos de las organizaciones.

Un ejemplo de lo anterior, son las auditorías financieras dado que las organizaciones han adoptado sistemas de información para el desarrollo de prácticas contables y financieras. Confirmando esto, Gantz (2018), indica que:

> “las auditorías financieras deben abordar los controles basados en la tecnología y su contribución para respaldar eficazmente los controles financieros internos.” (Gantz, 2018, pág. 28)

Otra de las similitudes que presenta la auditoría de TI con los otros tipos, es su lugar de aplicación, pues puede ser desarrollada a modo interno o externo; por lo cual, Gantz

(2018) afirma que la línea base de una auditoría externa generalmente es definida por las reglas, requisitos legales o regulaciones. Por otra parte, en el caso de la auditoría interna a menudo existe flexibilidad para definir o adoptar estándares de calidad, marcos de trabajo u otros requisitos que deban considerarse. (Gantz, 2018, pág. 4)

Adicionalmente, es importante resaltar que las auditorías internas y externas de TI presentan un factor en común, pues ambas revisiones se basan en la implementación controles internos para gestionar de manera adecuada los procesos con algún componente tecnológico. Gantz (2018), afirma que los controles son el elemento clave para la gestión de tecnologías de información, y se encuentra definidos por medio de estándares, guías, metodologías y marcos de trabajo sobre los procesos del negocio, los servicios y la operación de los sistemas.

2.3.1. Controles de auditoría de TI

Como se indicó anteriormente, los controles son el elemento base para la gestión de TI y, por ende, las auditorías pretenden evaluar su eficacia operativa. Sin embargo, se debe considerar que el proceso de auditoría de TI tiene diferentes tipos de revisión, acordes al enfoque y alcance. Además, según afirma Carbajal (2013), las revisiones en sistemas de información se encuentran categorizadas principalmente en dos distintos enfoques de controles, y los define de la siguiente manera:

- **Controles Generales:** Corresponden a políticas y procedimientos aplicados a las operaciones con algún componente tecnológico, sustentando la base sobre la cual se respaldan los controles de aplicación y de usuario. (Carbajal Romero, 2013)
- **Controles de Aplicaciones:** Son un tipo de control más específico incorporado a cada una de las aplicaciones para proporcionar seguridad razonable sobre el ingreso, procesamiento y salida de los datos. (Carbajal Romero, 2013)

2.3.2. Pruebas de control en auditorías de TI

Son pruebas de cumplimiento orientadas a conocer el nivel de confianza razonable sobre la eficacia operativa de los controles internos implementados en los sistemas de información que soportan procesos de negocio o regulaciones impuestas.

En la NIA 330 se establece que este tipo de pruebas consisten en procedimientos para evaluar la eficacia operativa de los controles de auditoría, y prevenir o detectar incorreciones materiales en las afirmaciones. (IAASB, 2021)

Por lo tanto, estas pruebas permiten al auditor concluir sobre la funcionalidad y vigencia de los controles internos evaluados, y si estos aseguran la correcta ejecución de las actividades del negocio, al evitar posibles fallos. No obstante, se debe considerar aspectos regulatorios para identificar la existencia, carencia u oportunidades de mejora sobre controles de TI.

Es importante destacar que la prueba de control debe de realizarse únicamente sobre aquellos controles debidamente documentados y aprobados por la organización, pues esto afecta el alcance de la auditoría. En este sentido, la NIA 330 menciona que las pruebas de controles se realizan únicamente sobre los controles que se consideran adecuadamente diseñados para la prevención, detección o corrección de una incorreción material en una afirmación. (IAASB, 2021)

2.4. Fraude y lavado de dinero

De acuerdo con la Revista Digital de Aseguramiento publicada por la Empresa Deloitte se define el fraude como “Un acto intencional por uno o más individuos entre la administración, quienes tienen a cargo el gobierno, empleados, o terceros, que involucra el uso de engaño para obtener una ventaja injusta o ilegal” (Deloitte, 2016).

Cabe recalcar, tal como lo menciona Deloitte en su revista que, a pesar de la posibilidad de errores, un fraude es visto como un acto intencional en donde se genera un engaño para ocultar una acción injusta o ilegal para beneficio propio.

Gibson (2015) para la revista Forbes, define el lavado de dinero como “las operaciones con recursos obtenidos de manera ilícita, con procedimientos orientados a dar apariencia de legitimidad a los recursos, bienes o derechos”. Además, estos procedimientos se dividen en tres etapas, en la primera se introducen los fondos ilegales en el sistema financiero, posteriormente, se pretende realizar transacciones que eviten la trazabilidad de los fondos para finalmente dar una apariencia legítima a la riqueza ilícita.

De lo anterior, se puede concluir que el lavado de dinero tiene como objetivo hacer parecer que los activos provienen de actividades legales, de esta manera poder hace uso de estos, escondiendo el trasfondo u origen delictivo de donde fueron obtenidos.

Por otra parte, el diario digital del dinero, indica en su sitio que el antilavado de dinero es un concepto utilizado principalmente en el mundo financiero y legal para describir los controles legales que deben cumplir las instituciones financieras y otras entidades

reguladas para prevenir, detectar e informar sobre posibles actividades sospechosas del blanqueo de capitales. (OroyFinanzas.com, 2015).

2.4.1. Principales técnicas para el lavado de dinero

Existen varias formas de lavar dinero o legitimar capitales; sin embargo, entre las más comunes se encuentra las siguientes:

2.4.1.1. Depósitos bancarios

Este es uno de los métodos más utilizados, en donde se pretende deshacer del dinero en efectivo y poder colocarlo en el sistema financiero; sin embargo, gracias a las medidas implementadas por los bancos y sus reguladores, cada vez es más difícil realizar estos movimientos sin generar sospechas al intentar ingresar una suma considerable de efectivo sin justificación de su procedencia. (Gutiérrez, 2016).

Por esta razón, y para evadir estos controles, se utiliza una técnica donde se fracciona la totalidad del dinero para generar varios ingresos en un periodo de tiempo determinado. (Gutiérrez, 2016).

Otro mecanismo utilizado para eludir estos controles se ha dado con el desarrollo tecnológico y la implementación de nuevos cajeros automáticos, en los cuales se permiten realizar depósitos incluso fuera de horarios de oficina, haciendo más difícil determinar y rastrear la fuente del efectivo ingresado. (Gutiérrez, 2016).

2.4.1.2. Instrumentos de títulos valores

La definición de títulos de valores según el sitio de BBVA, es un documento que contiene un derecho. Este derecho puede ser de pago y cobro, además es transmisible, por lo que pasa de una persona a otras. Un ejemplo muy común de un título de valor es un cheque. (BBVA, 2020).

Al igual que los depósitos suelen utilizarse en el fraude y lavado de dinero para ocultar fondos, el instrumento más utilizado para estos fines es la letra de cambio, ya que se presta en las operaciones de títulos de valores librados al portador y para la transmisión simplemente basta con una entrega a otra persona. (OAS, 2014).

2.4.2. Financiamiento del terrorismo y el lavado de dinero

Según el sitio web *ACAMS Today,* los fondos que son legítimos destinados al terrorismo, en muchos casos no son lavados, simplemente son encubiertos. No obstante,

lo que tienen en común la financiación del terrorismo y el lavado de dinero es, que, a pesar de tener rumbos distintos en sus objetivos, crean oscuridad del proceso en el que fluyen los fondos.

Se entiende que el lavado de dinero es la práctica donde los activos son obtenidos de forma ilícita, que se transfieren para proporcionar un estado de legitimidad. Y para tener éxito, se debe reservar la relación de los fondos con la actividad delictiva por medio de tres etapas para obtener el activo. Permitiendo que los activos obtenidos de forma ilícita parezcan legítimos. (AcamsToday, 2019).

En la Figura 4, se muestran las etapas para legitimar capitales.

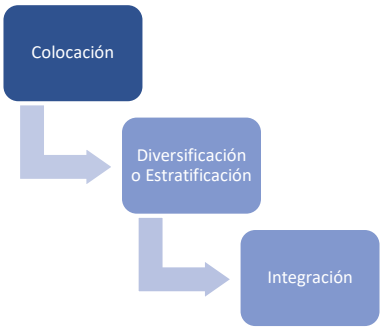


Figura 4. Etapas del lavado de dinero.

Fuente: Adaptado de (AcamsToday, 2019).

Por su parte, la financiación del terrorismo facilita la capacidad de almacenar y distribuir fondos; sin embargo, se realiza en una serie menor en comparación con la magnitud de mover el dinero de forma delictiva. (AcamsToday, 2018).

Finalmente, en la financiación del terrorismo, una parte del dinero de estos es producto del delito; sin embargo, no quiere decir que el dinero es sucio desde el inicio de las operaciones realizadas. (AcamsToday, 2018).

2.4.3. Consecuencias del lavado de dinero

Azofeifa (2016), menciona que una de las principales consecuencias del lavado de dinero a nivel costarricense e internacional es la afectación de las relaciones internaciones y de comercio con el exterior, pues provocan barreras, pérdida de imagen, pérdida de ventas, fuga de empresas extranjeras, poca calificación de riesgo, entre otras.

Es importante mencionar que todas las consecuencias, producto del lavado de dinero, forman parte de un deterioro de las personas y el país donde se encuentran,

generando conflictos o presiones sociales. En el momento de bajar la guardia, o descuidarse, incluso pensar que eso no pasará, podría inducir a error que contribuirá en la legitimación de activos. (Azofeifa, 2016).

2.4.4. Obligaciones de las instituciones financieras

La Superintendencia General de Entidades Financieras cuenta con el acuerdo 12-10 Normativa para el cumplimiento de la ley Nº8204, en el cual se menciona que toda persona física o jurídica inscrita ante la SUGEF por desempeñar alguna actividad comercial relacionada con el artículo 15 de la "Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo", se encuentra en la obligación de registrarse ante la Superintendencia y someterse a supervisión en materia de legitimación de capitales y de las acciones que puedan servir para financiar actividades terroristas u organizaciones terroristas, cuando se realice alguna de las siguientes actividades: (SUGEF, 2017)

- Operaciones de canje de dinero y transferencias, mediante instrumentos tales como cheques, giros bancarios, letras de cambio o similares.
- Operaciones de emisión, venta, rescate o transferencia de cheques.
- Transferencias de fondos, realizadas por cualquier medio.
- Administración de fideicomisos o de cualquier tipo de administración de recursos, efectuada por personas, físicas o jurídicas, que no sean intermediarios financieros.
- Remesas de dinero de un país a otro.

2.4.5. Organizaciones y normativa internacional contra el lavado de dinero

Como se menciona anteriormente, la lucha contra el lavado de dinero busca reducir la fuerza de los grupos sumergidos en actividades ilícitas previniendo acciones terroristas. Por esta razón existen organizaciones y grupos a nivel internacional que establecen lineamientos y normativas para prevenir el blanqueo de capitales. A continuación, se mencionan algunas de las principales organizaciones y normativas a nivel internacional en esta materia.

2.4.5.1. Comité de Supervisión Bancaria de Basilea

El Comité de Supervisión Bancaria de Basilea (BCBS, por sus siglas), es el principal organismo normativo internacional para la regulación prudencial de los bancos y constituye un foro de cooperación en materia de supervisión bancaria. Su mandato es mejorar la

regulación, la supervisión y las prácticas bancarias en todo el mundo con el fin de afianzar la estabilidad financiera. (Banco de Pagos Internacionales, 2013).

2.4.5.2. Banco Mundial y Fondo Monetario Internacional

El Banco Mundial cuenta con un programa de lucha contra el lavado de dinero y el financiamiento del terrorismo. Este programa fue creado en el 2001, y trata de ser un componente obligatorio del programa de evaluación del sector financiero. La estrategia, refleja la integridad del sistema financiero de un país y la forma primordial para mantener la estabilidad y el desarrollo. (Banco Mundial, 2014).

Por otra parte, durante los últimos años el Fondo Monetario Internacional ha realizado numerosos esfuerzos y aportes, colaborando en la definición de políticas en la lucha contra el lavado de dinero y el financiamiento del terrorismo a nivel internacional, esto gracias a la amplia experiencia en el ejercicio de supervisión de sistemas económicos de los países miembros, y la ejecución de diversas evaluaciones en el sector financiero. (Fondo Monetario Internacional, 2016).

2.4.6. Legislación nacional contra el lavado de dinero

Como se ha mencionado anteriormente, en la actualidad Costa Rica cuenta con la Ley Nº8204 o Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo. Esta ley busca combatir y evitar el blanqueo de capitales; a continuación, se detallan algunos de los puntos más importantes de esta. (Procuraduría General de la República, 2019).

2.4.6.1. Ley Nº8204

La ley N°8204, denominada: “Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo” (Procuraduría General de la República, 2021), es la responsable de regular y sancionar las actividades financieras con el fin de evitar la legitimación de capitales en el país. Esta ley establece en el artículo uno del capítulo único que “(…) se regulan y sancionan las actividades financieras, con el fin de evitar la legitimación de capitales y las acciones que puedan servir para financiar actividades terroristas, tal como se establece en esta Ley. (Procuraduría General de la República, 2021).

Las entidades sujetas al cumplimiento de la ley N°8204 en materia financiera son aquellas que son reguladas, supervisadas y fiscalizadas por alguno de los siguientes órganos: (Procuraduría General de la República, 2021).

e. Superintendencia General de Entidades Financieras (SUGEF).
f. Superintendencia General de Valores (SUGEVAL).
g. Superintendencia de Pensiones (SUPEN).
h. Superintendencia General de Seguros (SUGESE).

2.4.6.2. Normativa de cumplimiento de la ley Nº8204

La normativa fue aprobada por el Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF, por sus siglas) el 22 de diciembre del 2010. Indica los aspectos mínimos requeridos para cumplir con la regulación de la ley Nº8204 en materia de fraude y lavado de dinero. (SUGEF, 2017)

2.5. COBIT 2019

El marco de referencia de Objetivos de Control para la Información y Tecnologías Relacionadas (COBIT, por sus siglas en inglés) es un marco de referencia desarrollado por ISACA con un enfoque en el gobierno y gestión de TI, que proporciona principios, prácticas, herramientas analíticas y modelos globalmente aceptados que ayudan a aumentar la confianza y el valor de los sistemas de información. (ISACA, 2018).

El marco COBIT 2019 establece una división clara entre gobierno y gestión, donde el primero “asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas” y la gestión posee visión que “planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales.” (ISACA, 2020)

2.5.1. Dominios de COBIT

COBIT 2019 se encuentra conformado por un total de 37 procesos, los cuales se encuentran agrupados en cinco dominios que forman un marco integrado que permiten un correcto gobierno y gestión del entorno tecnológico en las organizaciones. Los dominios son nombrados por verbos que comunican la idea clave y las áreas de actividad, el primer

dominio EDM (Evaluar, Dirigir y Monitorizar) hace referencia a los objetivos de gobierno y los objetivos de gestión se reúnen en cuatro dominios APO (Alinear, Planificar y Organizar), BAI (Construir, Adquirir e Implementar), DSS (Entregar, dar Servicio y Soporte) y MEA (Monitorizar, Evaluar y Valorar). En la Figura 5, se muestran los 37 procesos y su agrupación en cada dominio.

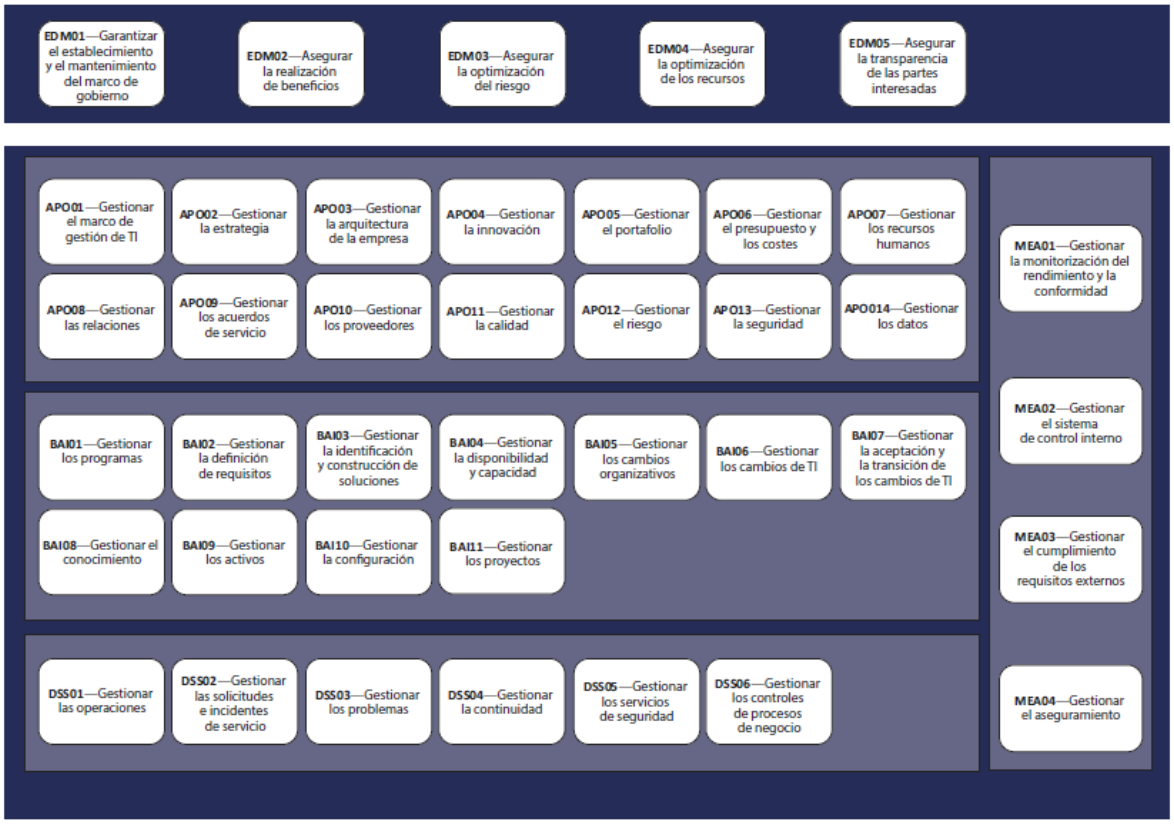


Figura 5. Mapa de procesos COBIT 2019.

Fuente: (ISACA, 2018)

Entre los 37 procesos, se considera que los siguientes son los de mayor relevancia para el desarrollo del presente trabajo final de graduación.

2.5.2. Proceso DSS06 – Gestionar controles de procesos de negocio de COBIT 2019

Encargado de entregar servicio y soporte, el proceso DSS06 se encarga de detallar y suministrar controles adecuados de procesos de negocio para garantizar que la información relacionada y procesada dentro de la organización o en manera externa satisface todos los requerimientos relevantes para el control de la información.

Busca mantener la integridad de la información y la seguridad de los activos de información manejados en los procesos de negocio dentro de la empresa o analizados con el propósito de este objetivo. En la Tabla 3, se muestra un resumen de las prácticas de gestión para este proceso.

Práctica de Gestión	Descripción
DSSA06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	Evalúa y supervisa continuamente la realización de las actividades de los procesos de negocio y controles relacionados, basados en el riesgo corporativo para asegurar que el procesamiento y controles está alineado con las condiciones de negocio.
DSSA06.02 Controlar el procesamiento de la información.	Opera la ejecución de las actividades de procesos de negocio y controles relacionados, basadas en el riesgo corporativo para asegurar que el procesamiento de la información es válido, completo, preciso, oportuno y seguro.
DSSA06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Gestiona los roles de negocio, responsabilidades, niveles de autoridad y segregación de tareas necesarias para apoyar los objetivos del proceso de negocio. Autorizar el acceso a cualquier activo de información relativo a los procesos de información del negocio, incluyendo aquellos bajo la custodia de negocio, de TI y de terceras partes. Esto asegura que el negocio sabe dónde están los datos y quién los está manejando.
DSSA06.04 Gestiona errores y excepciones.	Gestiona las excepciones y errores de los procesos de negocio y facilitar su corrección. Incluir escalada errores y excepciones en los procesos de negocio y la ejecución de acciones correctivas y definidas. Esto proporciona garantía de precisión e integridad del proceso de información del negocio.
DSSA06.05 Asegurar la trazabilidad de los eventos, responsabilidades y la información.	Asegura que la información del negocio pueda ser rastreada hasta los responsables y eventos que la originan. Esto permite trazabilidad de la información a lo largo de su ciclo de vida y procesos relacionados. Proporciona garantías de que la información que conduce el negocio es de confianza y ha sido procesada acorde a los objetivos definidos.
DSSA06.06 Asegurar los activos de la información.	Asegura los activos de la información accesibles por el negocio a través de los métodos aprobados, incluyendo la información en formato electrónico (tales como métodos para crear nuevos

Práctica de Gestión	Descripción
	activos en cualquier forma dispositivos portátiles, aplicaciones de usuario y dispositivos de almacenamiento) información en formato físico tales como documentos fuentes o informes de salida) e información en tránsito. Esto beneficia al negocio proporcionando una salvaguarda.

Tabla 3. Proceso DSS06

Fuente: (ISACA, 2018)

2.5.3. Proceso BAI06 – Gestionar los cambios de TI

El objetivo perteneciente al dominio (BAI) procura gestionar todos los cambios de una forma controlada, incluyendo cambios estándar, de mantenimiento y de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.

Se establece que su propósito es posibilitar una entrega de los cambios pronta y segura para el negocio, mientras modera cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno donde se aplica el cambio. En la Tabla 4, se muestra un resumen de las prácticas de gestión para este proceso.

Práctica de Gestión	Descripción
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.	Evalúa todas las peticiones de cambio para determinar su efecto en los desarrollos de negocio y los servicios TI, y analizar si el cambio afectará negativamente al entorno operativo e introducirá un riesgo inaceptable. Asegura que los cambios son apuntados, priorizados, categorizados analizados, autorizados, planificados y programados.
BAI06.02 Gestionar cambios de emergencia.	Gestiona atentamente los cambios de emergencia para minimizar futuras incidencias y conseguir que el cambio está controlado y se realiza de forma segura. Verificar que los cambios de emergencia son evaluados debidamente y autorizados una vez hecho el cambio.
BAI06.03 Hacer seguimiento e informar de cambios de estado	Mantiene un sistema de seguimiento e informe que documenta los cambios rechazados comunique el estado de cambio permitidos y en proceso de cambios completados. Asegura que los cambios admitidos son implementados como está previsto.

Práctica de Gestión	Descripción
BAI06.04 Cerrar y documentar los cambios	Siempre que el cambio haya sido implementado actualizar de forma constante la documentación de la solución y del usuario, así como los procedimientos a los que afecta el cambio.

Tabla 4. Proceso BAI06

Fuente: (ISACA, 2018)

2.6. ISO 9001

La ISO 9001 es una norma internacional que toma en cuenta las actividades de una organización, sin distinción de sector de actividad. Esta norma se concentra en la satisfacción del cliente y en la capacidad de proveer productos y servicios que cumplan con las exigencias internas y externas de la organización. (Lopez, 2016).

2.6.1. Sistemas de gestión de calidad

Los Sistemas de Gestión de Calidad son un conjunto de normas y estándares internacionales que se interrelacionan entre sí, para hacer cumplir los requisitos de calidad que una empresa requiere y satisfacer los requerimientos acordados con sus clientes a través de una mejora continua, de una manera ordenada y sistemática. *(Lopez, 2016)*.

Los estándares internacionales contribuyen a facilitar e incrementar la efectividad de los procesos y servicios de uso diario, ayudando a asegurar que los materiales, productos, procesos y servicios sean los adecuados para sus propósitos. Existen varios Sistemas de Gestión de la Calidad, dependiendo del giro de la organización. Todos los sistemas se encuentran normados bajo un organismo internacional no gubernamental llamado ISO, *International Organization for Standardization* (Organización Internacional para la Estandarización, por su traducción al español). *(Lopez, 2016)*.

2.6.2. Los pasos básicos para realizar la estandarización de procesos

La estandarización de los procesos consiste en establecer un nivel de operación basado en un estándar para cumplir con el servicio brindado. Los siguientes son los pasos para realizar la estandarización de procesos: (ISO 9001 Calidad Total , 2019).

- Definir el método actual por estandarizar
- Realizar el análisis del método actual comparando con el estándar o la norma establecida que se pretende implementar

- Identificar las diferencias y realizar los ajustes al método, incluyendo la utilización de registros de control.
- Ensayar o probar el nuevo método.
- Documentar el método, desplegarlo al personal y aplicarlo.

2.6.3. Jerarquía Documental del Sistema de Gestión de Calidad

La documentación en un Sistema de Gestión de Calidad tiene diversos propósitos y beneficios dentro de los cuales se mencionan: establecer un marco claro de trabajo para las operaciones de la organización, mantener consistencia en los procesos; además, puede proporcionar evidencias para el logro de los objetivos y metas *(Meskovska, 2019)*.

La documentación que se defina en un Sistema de Gestión de Calidad puede ser variada y estar conformada por diversos tipos de documentos, estos pueden ser jerarquizados y representados en una escala tal como se muestra en la Figura 6. *(Meskovska, 2019)*.

Figura 6. Pirámide Documental de un Sistema de Gestión de Calidad

Fuente: (Meskovska, 2019)

2.6.4. Mejora continua

La calidad y su aplicación llevan factores que involucran los términos, la mejora continua es uno. Dentro de los beneficios que se obtienen se encuentran los siguientes: (Sinnaps, 2019).

- Incremento del rendimiento de tu equipo
- Empresas más productivas
- Reducción de costes
- Reducción de plazos de ejecución
- Optimización de procesos
- Errores minimizados
- Resultados cada vez más eficaces
- Productos y servicios mejor dirigidos al cliente final
- Aumento de la motivación de los equipos de trabajo.

La mejora continua cree en implementar la actitud dentro del equipo para volverlo competitivo. La motivación es parte de la certeza que se ve involucrado en la toma de decisiones en el bienestar laboral. (Sinnaps, 2019)

2.7. Gestión de procesos de negocio

Dumas et al. (2018, p.1) definen la gestión de procesos de negocio (BPM, por sus siglas en inglés) como: “el arte y la ciencia de supervisar cómo se realiza el trabajo en una organización para garantizar resultados consistentes y aprovechar las oportunidades de mejora.

La gestión de procesos de negocio emplea distintas herramientas, metodologías y tecnologías para identificar en los procesos de las organizaciones, de forma gráfica el conjunto de oportunidades de mejora para optimizar el rendimiento de estos y facilitar la alineación con el negocio.

2.7.1. Modelado de Procesos de Negocio

Utiliza una notación estandarizada, basada en diagramas de flujos para definir los procesos de negocio, para proveer un camino que genere un proceso ejecutable. En la Tabla 5. Notación BPMN. se indica una descripción de los elementos utilizados en la notación BPMN 2.0.

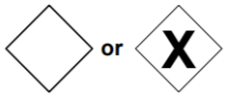
Figura	Descripción
Actividad 	Las actividades representan acciones.
Eventos **Evento de Inicio:**  **Evento intermedio:**  **Evento de Fin:** 	Representan algún factor que afecta el proceso, existen tres tipos de eventos. Los disparan el inicio del proceso, los que pueden surgir durante la ejecución o aquellos que finaliza el flujo.
Compuertas **Compuerta Exclusiva**  **Compuerta Paralela**  **Compuerta Inclusiva** 	Son puntos de control dentro del proceso, de manera unificadora o divisoria, que pueden tener múltiples entradas y salidas.
Conectores **Flujo de secuencia** 	Indica la dirección que sigue el flujo.
Pool  **Lane** 	Son contenedores gráficos que organizan las tareas, procesos y subprocesos, al mayor se le denomina *pool.* Y las divisiones son conocidas como canales. Cada proceso debe estar contenido en un *pool.* Un *pool*, representa una entidad, y los canales representan un área organizacional o puesto de trabajo.

Tabla 5. Notación BPMN.

Fuente: (Freund J. et al, 2014)

Capítulo III: Marco Metodológico

El presente capítulo tiene como fin abordar toda aquella información referente al marco metodológico del presente proyecto; por ende, en esta sección se definieron todos los temas relacionados con el tipo de investigación empleada para abordar la problemática, de igual manera se explica la metodología, fuentes, sujetos de información, variables e instrumentos de investigación utilizados.

A mayor detalle en este capítulo se aborda la forma en que se realizó la investigación y se obtuvieron los datos para el análisis; también se describen los instrumentos y técnicas empleadas para recolectar los datos.

3.1. Tipo de Investigación

De acuerdo con Hernández Sampieri, Fernández Collado, & Baptista Lucio (2014, p.4) el concepto de investigación hace referencia al conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema.

Además, según Hernández *et al*. (2014, p.3) existen tres tipos de investigación o enfoques los cuales son cualitativo, cuantitativo y mixto, estos se utilizan con base en el resultado que se espera alcanzar. A continuación se describe cada tipo de investigación:

- **Investigación Cuantitativa:** Es probatoria y secuencial, donde se emplea la recolección de datos para probar hipótesis con base en mediciones numéricas y análisis estadístico, con el propósito de establecer pautas de comportamiento o comprobar teorías.
- **Investigación Cualitativa:** A diferencia de la cuantitativa, presenta un enfoque no lineal con orientación por la recolección y análisis de datos mediante planeamiento de hipótesis y preguntas. De manera que el investigador pueda descubrir respuestas para interrogantes o bien descubrir nuevas.
- **Investigación Mixta:** Es una combinación de las anteriores mencionadas, donde los resultados se generalizan basándose en los métodos de recolección de datos y los análisis de estos, pero a su vez permitiendo flexibilidad en los datos a pesar de seguir un proceso parcialmente secuencial.

Por lo tanto, el presente trabajo utilizó un modelo de investigación cualitativa, en el cual, según (Hernández *et al.*, 2014) se enfoca en comprender los fenómenos desde la perspectiva de los participantes, permitiendo definir las condiciones y aspectos requeridos.

En este caso, las características que se requieran para la definición de controles y pruebas sustantivas que ayuden a reforzar la auditoría de TI.

De acuerdo con (Hernández *et al.*, 2014) especifica que el enfoque cualitativo utiliza la recolección y análisis de los datos para afinar las preguntas de investigación o revelar nuevas interrogantes en el proceso de interpretación. Lo anterior, permite la capacidad de realizar preguntas e hipótesis durante todo el ciclo de desarrollo del proyecto, brindado así la oportunidad de reformar y mejorar aspectos que no fueron identificados desde el planteamiento del proyecto.

Este punto es reforzado por (Hernández *et al*., 2014) que indica que los estudios cualitativos pueden desarrollar preguntas e hipótesis antes, durante o después de la recolección y el análisis de los datos. En la Figura 7, se muestra el proceso de investigación cualitativo propuesto por Hernández et al. (2014).

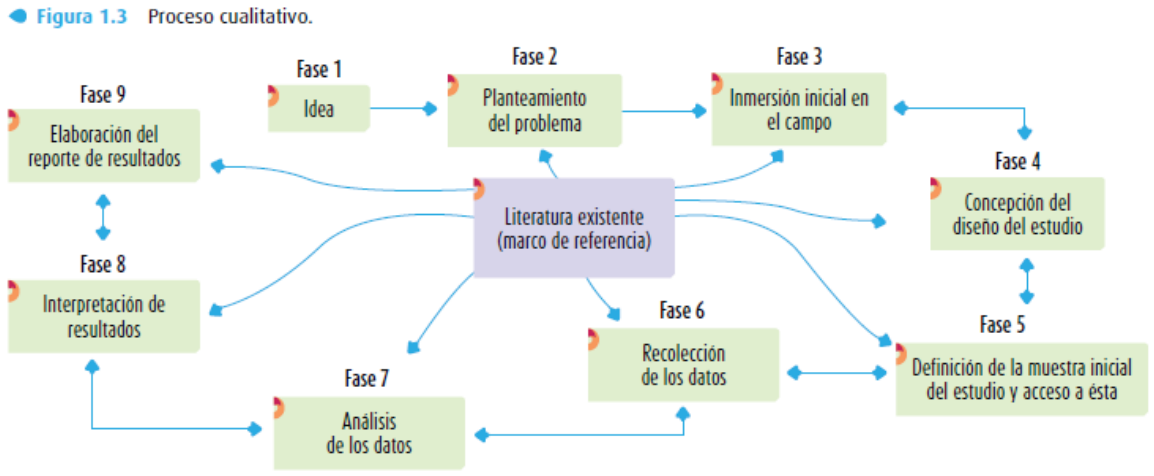


Figura 7. Proceso investigación cualitativa.

Fuente: Tomado de Metodología de la Investigación por Hernández, Fernández y Baptista (2014).

3.2. Alcance de la Investigación

Hernández *et al.* (2014) señalan que el: "Alcance del estudio depende la estrategia de investigación" (p. 90) y es el resultado de la revisión literaria y permite indicar el resultado que obtendrá con el estudio. Dicho esto, Hernández *et al.* (2014) establecen cuatro alcances de causalidad para una investigación de enfoque cualitativo.

- **Exploratorio:** Según Hernández *et al.* (2014), los estudios exploratorios se realizan cuando el objetivo es examinar un tema o problema de investigación que

generalmente es poco estudiado o novedoso, y en el que se mantienen muchas interrogantes.

- **Descriptivo:** El alcance descriptivo busca especificar las propiedades y las características importantes de cualquier fenómeno que se someta a un análisis. Este alcance pretende medir o recolectar información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, pero sin mostrar cómo se relacionan estas. (Hernández *et al.,* 2014, p.92)
- **Correlacional:** La investigación correlacional pretende asociar variables mediante un patrón predecible para un grupo o población, en busca de responder preguntas de investigación en un contexto específico. (Hernández *et al.,* 2014, p.93)
- **Explicativo:** Según Hernández et al. (2014), busca establecer las causas de los sucesos o fenómenos estudiados. Su nombre indica que, se debe explicar el "por qué" de las cosas y las condiciones relacionadas.

Adicionalmente, Hernández *et al.* (2014) explican que el alcance descriptivo consiste en: "Describir fenómenos, situaciones, contextos y sucesos; esto es, detallar cómo son y se manifiesta" (p. 92).

Por lo tanto, el presente trabajo utilizó un alcance descriptivo, donde se busca describir el procedimiento actual empleado por la Firma para la revisión del cumplimiento de la ley Nº8204, contrastado con el marco normativo nacional e internacional para diseñar un conjunto de controles que brinden mejoras en cuanto a la calidad de estas revisiones.

3.3. Diseño de la Investigación

El diseño de la investigación depende del enfoque, en este caso se abordó una investigación cualitativa con alcance descriptivo; por lo tanto, el diseño cualitativo se refiere al abordaje general que será empleado en el proceso de investigación.

Además, Hernández et al. (2014) mencionan que existen diversas tipologías de diseño cualitativo, pero las más importantes se presentan en la Figura 8*,* las cuales se encuentran vinculadas con preguntas de investigación e información que se proporciona en el estudio.

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.
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.

Figura 8. Diseños de la investigación cualitativa

Fuente: Tomado de Metodología de la Investigación por Hernández et al. (2014).

Por lo anterior, para el desarrollo de este trabajo, se utilizó el enfoque de investigación – acción; dado que, según Hernández et *al.,* (2014) tiene la finalidad de comprender y resolver problemas específicos vinculados a un ambiente aplicando la teoría y mejores prácticas de acuerdo con el planteamiento.

Este tipo de investigación se encuentra estructurado por ciclos y es caracterizado por su flexibilidad, pues como se indicaba anteriormente, permite realizar ajustes conforme se avanza con la investigación hasta llegar al resultado deseado. Por otra parte, en cuanto

las etapas que conforman los ciclos en un proceso investigación – acción, según Pavlish y Pharris (2011, citados por Hernández *et al*., 2014) se presentan los siguientes ciclos:

a. Detectar el problema de investigación, clarificarlo y diagnosticarlo (ya sea un problema social, la necesidad de un cambio, una mejora, entre otros).
b. Formulación de un plan o programa para resolver el problema o introducir el cambio.
c. Implementar el plan o programa y evaluar resultados.
d. Realimentación, la cual conduce a un nuevo diagnóstico y a una nueva espiral de reflexión y acción.

Este diseño permite generar insumos para la toma de decisiones en proyectos o reformas estructurales. Según Hernández *et al.* (2014) pretende propiciar el cambio social, transformar la realidad y generar conciencia en las personas sobre su papel en dicha transformación. Por lo tanto, desde el contexto del presente trabajo, el diseño de investigación empleado ofrece las condiciones y aspectos requeridos para la definición de controles y procedimientos para la evaluación de la ley Nº8204.

3.4. Fuentes de Investigación

Con el propósito de obtener la información necesaria para el desarrollo del presente trabajo final de graduación, se emplearon diversas fuentes de información para estudiar la problemática en la Firma, específicamente con el proceso de revisión de la ley Nº8204 por parte del equipo de *IT Audit.*

3.4.1. Fuentes de investigación primarias

Hernández et al. (2014, p.61) explican: “Las referencias o fuentes primarias proporcionan datos de primera mano, pues se trata de documentos que incluyen los resultados de los estudios correspondientes”. En la Tabla 6, se describen las fuentes de información primarias utilizadas y el sitio donde fue consultado.

Fuente	Sitio consultado
Juicio experto de personal clave en la Firma: Debido al conocimiento en el tema de auditoría de TI, así como revisiones de cumplimiento de la ley Nº8204 que han realizado durante su tiempo en la Firma.	Reuniones virtuales con el gerente sénior y gerentes del área de *IT Audit.*

Fuente	Sitio consultado
Normativas y regulaciones vigentes en Costa Rica: • Ley Nº8204 sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo. • Acuerdo SUGEF 12-10 Normativa Para El Cumplimiento de la Ley Nº8204.	Sitio web oficial de la Superintendencia General de Entidades Financieras (SUGEF) y Procuradoría General de la República.
Metodología de la Firma	Documentación interna de la Firma, relacionada con marcos de trabajo, plantillas, guías, y otra documentación soporte relacionada con el tema.
Equipo de *IT Audit*	Encuestas aplicadas a los profesionales que conforman el área de *IT Audit,* se consideraron durante las fases de entendimiento del proceso y determinación de brechas y oportunidades de mejora, debido a su participación en auditorías de la ley Nº8204.
COBIT 2019 y sus diferentes guías oficiales	Sitio web oficial de Asociación de Auditoría y Control de Sistemas de Información (ISACA), organización encargada del Marco de COBIT.

Tabla 6. Fuentes primarias

3.4.2. Fuentes de investigación secundarias

Asimismo, las fuentes secundarias de información utilizadas durante el desarrollo del presente trabajo son las siguientes:

- Bases de datos otorgadas por la biblioteca del Instituto Tecnológico de Costa Rica.
- Proyectos de graduación referentes a temas de auditoría de TI.
- Sitios *web* de Internet con información relativa al tema.

- Normas Internacionales de Información Financiera que proporcionan un conjunto de normas aceptadas a nivel internacional que rigen la forma en cómo se debe procesar la información contable por parte de las organizaciones.

Todas las anteriores, son las fuentes de información válidas y verificables que sustentan en bases sólidas el desarrollo del presente trabajo final de graduación.

3.5. Sujetos de Investigación

Los sujetos de la investigación se describen para tener una muestra de las personas que participan en el proceso de recopilación de información de la investigación. Con respecto a este apartado Hernández *et al*. (2014, p.384) señala que la muestra en el proceso cualitativo hace referencia a un grupo de personas, eventos, sucesos, comunicades y otros, sobre el cual se recolectarán los datos, sin que necesariamente sea estadísticamente representativo del universo o población que se estudia.

Para efectos del presente trabajo final de graduación, los participantes corresponden a los colaboradores del área de *IT Audit* de la Firma, los cuales, se encuentran involucrados directamente en las auditorías de TI de cumplimiento de la ley Nº8204. En la Tabla 7, se identifica y describe cada sujeto y su rol, así mismo, se menciona la importancia que aporta al proyecto.

Sujeto de Investigación	Características del Rol	Importancia en el Proyecto
Gerente sénior del área de IT *Audit*	Profesional experto en auditoría de tecnologías de información, cuenta con más de 17 años de laborar para la Firma y participa constantemente en todos los servicios de auditoría, así como en la toma de decisiones. De manera resumida algunas de las responsabilidades que mantiene son: a) Planificar y crear la estrategia de la auditoría, identificación de riesgos y diseño de las pruebas de control. b) Diseñar, planear y elaborar de pruebas de cumplimiento para la evaluación de la estructura de control interno del cliente. c) Administrar la ejecución de los proyectos a cargo de acuerdo con las normas de la Firma con respecto a calidad y servicio al cliente.	Es el principal punto de contacto con el investigador, ya que es el coordinador y encargado del departamento de *TI Audit.* Debido a su amplia experiencia en el funcionamiento del área, conoce ampliamente el servicio de evaluación del cumplimiento de la ley Nº8204.

Sujeto de Investigación	Características del Rol	Importancia en el Proyecto
Gerente sénior del área de IT *Audit*	d) Controlar financieramente los presupuestos de los proyectos a cargo. e) Supervisar el personal a cargo en los proyectos, respecto a la calidad y ejecución de los proyectos a cargo.	
Gerentes de *IT Audit*	Profesionales expertos que cuentan con más de 10 años de laborar para la Firma en el área de *IT Audit,* y participan constantemente en todos los servicios de auditoría, así como en la toma de decisiones. De igual forma comparten responsabilidades con el gerente sénior, apoyándole en los procesos de decisión; sin embargo, solo tiene una parte de los proyectos a su cargo.	Tienen a su cargo las inducciones de nuevos profesionales al equipo de IT Audit, y dentro de dichos entrenamientos contemplan el procedimiento de revisión de la ley Nº8204. Dado lo anterior, comprenden muy bien el proceso actual de auditoría de TI de cumplimiento de dicha ley.
Equipo *de IT Audit*	Entre los perfiles considerados destacan: • Asistentes: Responsables de realizar auditorías de la ley Nº8204 en diversos clientes, cuentan aproximadamente con un año de experiencia. • Encargados: Participan en el proceso de planificación y ejecución de las auditorías de TI, cuentan aproximadamente con dos años de experiencia en el área.	Son profesionales con menor experiencia en comparación con los gerentes; sin embargo, han participado en varias auditorías de TI de cumplimiento de la ley Nº8204. Es de suma importancia considerar su opinión debido a que ellos ejecutan actualmente el proceso de auditoría de TI de la ley Nº8204.

Tabla 7. Sujetos de investigación

3.6. Variables de la Investigación

Según indican Hernández *et al.* (2014, p.277) las variables de investigación se refieren a las propiedades medibles que forman parte de la hipótesis o que se pretenden describir con el desarrollo de la investigación, también mencionan que se requiere un solo indicador para que las variables sean medidas.

Por consiguiente, las variables de la investigación para efectos de este proyecto se definen como las características que se estudiaron y fueron generadas a partir de los objetivos específicos. En la Tabla 8, se detallan las variables que se emplearon con el presente trabajo final de graduación.

Objetivo específico	Variable	Importancia en la Investigación	Indicadores	Definición instrumental
Comprender el proceso establecido por la Firma en las auditorías de TI de cumplimiento de la Ley N°8204, por medio del análisis del proceso actual para el entendimiento de este.	Situación actual en auditorías de TI de cumplimiento de la ley Nº8204.	Permite comprender y diagnosticar el estado del proceso actual de revisión de la ley Nº8204.	Listado de actividades que se utilizan actualmente en el proceso auditoría de la ley Nº8204.	• Entrevista • Encuesta • Revisión documental
Determinar brechas, deficiencias y oportunidades del proceso de auditoría de TI de la ley N°8204 de la Firma contra el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI, para la identificación del estado deseado del proceso.	Oportunidades de mejora y recomendaciones a la situación actual para solventar brechas o deficiencias.	Permite identificar cuales aspectos mejorar para fortalecer la revisión de la ley Nº8204.	Listado de oportunidades de mejora a situación actual.	• Revisión documental
Proponer un conjunto de controles y procedimientos de auditoría de TI de la ley N°8204 ejecutado por la Firma, para el cumplimiento del estado deseado del proceso y generación de valor a la organización auditada.	Controles para la revisión del cumplimiento de la ley Nº8204 en materia de tecnologías de información.	Permite identificar las mejoras en la revisión a raíz de la propuesta de controles.	Diseño de controles para auditoría de la ley Nº8204.	• Entrevista • Revisión documental

Objetivo específico	Variable	Importancia en la Investigación	Indicadores	Definición instrumental
Construir un análisis financiero para la propuesta del proceso de auditoría TI de la ley N°8204, por medio de valoraciones financieras basadas en la industria y otras fuentes, para la obtención del impacto financiero aproximado que conllevan los beneficios y costos de esta.	Beneficios financieros y no financieros de la propuesta de auditoría de TI de la ley Nº8204.	Permite cuantificar los costos y beneficios del desarrollo e implementación de la propuesta.	Indicadores financieros para determinar la viabilidad de la propuesta.	• Entrevista • Revisión documental

Tabla 8. Variables de la investigación

3.7. Instrumentos de Investigación

Los instrumentos de recolección de datos deben estar alineados al tipo de investigación que se realiza, según indican Hernández *et al. (2014)*; para efectos del presente proyecto final de graduación como se indicó anteriormente, la investigación es de tipo cualitativa con un diseño de investigación - acción.

Según Hernández *et al*. (2014, p. 396) para el enfoque cualitativo, la recolección de datos resulta fundamental para obtener datos con la finalidad de analizarlos y comprenderlos, convirtiéndose en información que buscará responder las preguntas de investigación y generar conocimiento.

Adicionalmente, los autores recomiendan para las investigaciones cualitativas que "los investigadores deben establecer formas inclusivas para descubrir visiones múltiples de los participantes y adoptar papeles más personales e interactivos con ellos." (Hernández *et al.,* 2014, p.398)

A continuación, se detallan las técnicas que se utilizaron con el propósito de conocer la situación actual del proceso de auditoría de TI de cumplimiento de la ley Nº8204.

3.7.1. Entrevista

Según Hernández *et al.* (2014, p. 403), las entrevistas se definen como: "Una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados)". Según Ryen (2013) y Grinnell y Unrau (2011, citados por Hernández *et al*., 2014, p. 403) mencionan:

> *"Las entrevistas se dividen en estructuradas, semiestructuradas y no estructuradas o abiertas. En las primeras, el entrevistador realiza su labor siguiendo una guía de preguntas específicas y se sujeta exclusivamente a ésta (el instrumento prescribe qué cuestiones se preguntarán y en qué orden). Las entrevistas semiestructuradas se basan en una guía de asuntos o preguntas y el entrevistador tiene la libertad de introducir preguntas adicionales para precisar conceptos u obtener más información. Las entrevistas abiertas se fundamentan en una guía general de contenido y el entrevistador posee toda la flexibilidad para manejarla."*

Para efectos de este proyecto se hace uso de entrevistas semiestructuradas a las gerentes de IT Audit, se utilizó el Apéndice D con el objetivo de generar un entendimiento de la situación actual del proceso de revisión de la ley Nº8204.

3.7.2. Revisión documental

Según Hernández *et al.* (2014, p. 414) los documentos son una fuente muy valiosa de datos cualitativos, dado que permiten ayudar a entender el fenómeno central de estudio, y sirven al investigador para conocer los antecedentes de un ambiente, así como las vivencias o situaciones que se producen en él y su funcionamiento cotidiano y anormal.

Para efectos del proyecto, se utilizó esta técnica durante todo el ciclo de desarrollo, en primera instancia para revisar la documentación interna de la Firma, con el fin de comprender el marco de referencia y la metodología para las auditorías de TI de cumplimiento de la ley Nº8204.

Posteriormente, se estudian las regulaciones nacionales y las mejores prácticas en temas relacionados con el fraude y lavado de dinero que podrían aplicarse al construir la propuesta de controles de este proyecto.

En el Apéndice E, se encuentra el instrumento para la revisión documental empleada para este trabajo final de graduación.

3.7.3. Encuesta

Según Niño Rojas (2011), esta técnica de recolección de datos se obtiene a partir de las opiniones, apreciaciones, perspectivas y puntos de vista, así como experiencias. Adicionalmente, Niño Rojas (2011) menciona que existen encuestas abiertas, las cuales presentan la característica de ser espontáneas y darle libertad al encuestado de emitir una respuesta. Por otra parte, las encuestas cerradas contienen preguntas específicas y concisas con respuestas predefinidas.

Para efectos del presente trabajo final de graduación, se aplicó una encuesta con un enfoque mixto, pues se consideraron preguntas cerradas para obtener datos concisos y relevantes para la investigación; sin embargo, también se realizaron preguntas abiertas para obtener una mejor percepción del encuestado sobre algunos temas más puntuales.

El instrumento utilizado se encuentra en el Apéndice F, y se aplicó a los sujetos de investigación referentes al equipo de *IT Audit,* ya que estos son los encargados de ejecutar las auditorías de TI de cumplimiento de la ley Nº8204.

3.8. Procedimiento metodológico de la Investigación

Esta sección pretende describir la metodología de trabajo empleada para el desarrollo del presente trabajo final de graduación. Incluyendo el detalle de cada fase del proyecto para construir la propuesta de controles para la auditoría de TI de cumplimiento de la ley Nº8204.

Con respecto al procedimiento metodológico abordado, se definieron cuatro fases, las cuales pretenden asegurar el cumplimiento de los objetivos Figura 9, se muestran las fases de la metodología.

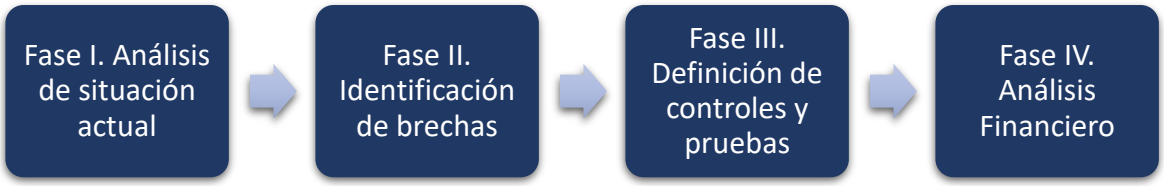


Figura 9. Fases de la metodología

3.8.1. Fase 1. Análisis de situación actual

Esta primera fase del proyecto se desarrolla durante el Capítulo IV: Análisis de Resultados, contemplando las reuniones iniciales para comprender el estado actual del proceso de auditoría de TI de cumplimiento de la ley Nº8204, para lo cual se utilizaron instrumentos como la encuesta al equipo de *IT Audit* y entrevista al Gerente de *IT Audit.*

Lo anterior, para obtener información detallada que describa la situación actual y definir la línea base para la ejecución de este proyecto final de graduación.

3.8.2. Fase 2. Identificación de brechas

Esta fase del proyecto se desarrolla durante el Capítulo IV: Análisis de Resultados, una vez se obtuvo el entendimiento de la situación actual, y utilizando como insumo la fase anterior.

Por su parte, esta fase tendrá como objetivo identificar las deficiencias, debilidades y oportunidades de mejora del proceso de auditoría de TI de cumplimiento la ley Nº8204,

con base en la normativa nacional e internacional relacionada con fraude y lavado de dinero, así como el marco de referencia COBIT 2019.

En síntesis, una vez se analicen las debilidades y deficiencias del procedimiento actual, se podrá identificar con detalle las brechas existentes que deberán ser solventadas por la propuesta de solución, así como el detalle de los puntos clave de mejora.

3.8.3. Fase 3. Definición de controles y pruebas

Esta fase del proyecto se desarrolla a lo largo de los capítulos: Capítulo IV: Análisis de Resultados y Capítulo V: Propuesta de Solución. Para lo cual, por medio de una serie de consultas a diferentes marcos de referencia aplicables en temas de fraude y lavado de dinero, así como buenas prácticas de TI; se procede a determinar qué características deberán considerarse para diseñar una serie de controles que permitan solventar las brechas y abordar las oportunidades de mejora que han sido identificadas como parte del procedimiento actual de auditoría de la ley Nº8204 evaluado por la Firma.

Por lo tanto, la salida principal de esta fase es el diseño de la propuesta de controles, así como una guía para la utilización de estos, que brindarán una mejoría en el procedimiento actual de auditoría de TI de la ley Nº8204, abarcando los entregables definidos en la sección 161.5.2.1. Propuesta de controles para el cumplimiento de la ley.

3.8.4. Fase 4. Análisis financiero

Esta última fase del proyecto se desarrolla en el Capítulo V: Propuesta de Solución, una vez se obtiene la propuesta de controles para la auditoría de TI de cumplimiento de la ley Nº8204. Se procede a aplicar una serie de indicadores para valorar la viabilidad desde el punto de vista financiero de esta, considerando un aproximado del costo inicial, capacitación en el uso de la herramienta al personal de *IT Audit*, así como un flujo de efectivo que considera una cantidad de proyectos de auditoría de cumplimiento de la ley Nº8204 a lo largo de tres años.

Por lo anterior, se elaboró un análisis que brinda una aproximación del impacto financiero de la propuesta, para lo cual se utilizaron instrumentos como la entrevista al Gerente de *IT Audit,* valoraciones financieras de la industria y otras fuentes.

3.9. Operacionalización del marco metodológico

A modo de síntesis de las secciones anteriores del Capítulo III: Marco Metodológico, en la Tabla 9, se muestra una alineación entre los objetivos específicos con la fase metodológica, instrumento utilizado, la variable de investigación y el sujeto involucrado.

Objetivo específico	Fases	Variables de Investigación	Instrumento	Sujetos de Investigación
Comprender el proceso establecido por la Firma en las auditorías de TI de cumplimiento de la Ley N°8204, por medio del análisis del proceso actual para el entendimiento de este.	Análisis de situación actual	Análisis de la situación actual en auditorías de TI de cumplimiento de la ley Nº8204.	Apéndice D. Entrevista semiestructurada Apéndice F. Entrevista personal IT Audit	**Gerentes de *IT Audit*** **Equipo *de IT Audit***
Determinar brechas, deficiencias y oportunidades del proceso de auditoría de TI de la ley N°8204 de la Firma contra el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI, para la identificación del estado deseado del proceso.	Identificación de brechas	Oportunidades de mejora y recomendaciones a la situación actual para solventar brechas o deficiencias.	Apéndice E Apéndice F. Entrevista personal IT Audit	**Gerentes de *IT Audit*** **Equipo *de IT Audit***
Proponer un conjunto de controles y procedimientos de auditoría de TI de la ley N°8204 ejecutado por la Firma, para el cumplimiento del estado deseado del proceso y generación de valor a la organización auditada.	Definición de controles y pruebas	Controles para la revisión del cumplimiento de la ley Nº8204 en materia de tecnologías de información.	Apéndice E	**Gerente sénior del área de IT *Audit*** **Gerentes de *IT Audit***
Construir un análisis financiero para la propuesta del proceso de auditoría TI de la ley N°8204, por medio de valoraciones financieras basadas en la industria y otras fuentes, para la obtención del impacto financiero aproximado que conllevan los beneficios y costos de esta.	Análisis financiero	Beneficios financieros y no financieros de la propuesta de auditoría de TI de la ley Nº8204.	Apéndice E	**Gerente sénior del área de IT *Audit*** **Gerentes de *IT Audit***

Tabla 9. Cuadro de Operacionalización de Variable

Capítulo IV: Análisis de Resultados

El presente capítulo tiene como fin presentar el análisis de los resultados obtenidos a través de la aplicación de los instrumentos de investigación que se definieron en el Capítulo III: Marco Metodológico.

De forma que el presente análisis aborda las tres primeras fases de la metodología, generando los insumos para desarrollar la propuesta de controles para mejorar el proceso de auditoría de TI de cumplimiento de la ley Nº8204 empleado por la Firma. Asimismo, en cada fase se consideran los datos que se recolectaron al aplicar los diversos instrumentos.

4.1. Análisis de la situación actual

Con el propósito de construir un entendimiento del proceso actual de auditoría de TI de cumplimiento de la ley Nº8204, se emplearon diversos instrumentos de investigación, los cuales fueron previamente definidos en la metodología, específicamente en la sección 3.7. Instrumentos de Investigación.

Los instrumentos utilizados para la recopilación de datos fueron la aplicación de una entrevista semiestructurada a una de las gerentes de *IT Audit,* para conocer ampliamente cuál es la metodología acogida por el área para los servicios de auditoría de TI de la ley Nº8204. Adicionalmente, se contrastó mediante una encuesta con preguntas cerradas y abiertas a otros profesionales del área, para conocer su percepción del proceso actual, dado que han realizado estas evaluaciones en clientes durante el último año.

4.1.1. Diagrama BMPN As-Is

Se utilizó una entrevista a través de *Microsoft Teams,* en el instrumento Apéndice G. Entrevista semiestructurada (aplicada), el día 29 de setiembre del presente año mediante una reunión con una gerente del área de *IT Audit,* para recabar las actividades de cada fase del proceso*.* Posteriormente, se procede a realizar el diagrama BPMN del proceso actual, el cual se presenta gráficamente en la Figura 10.

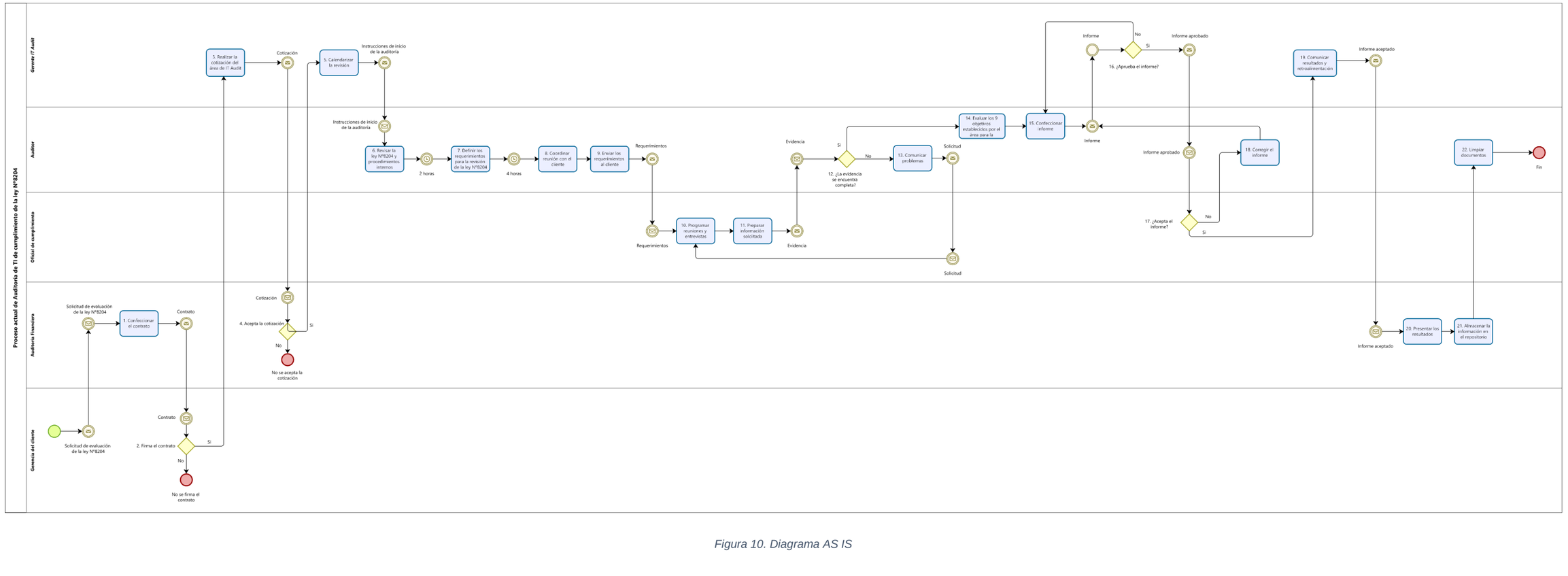


Figura 10. Diagrama AS IS

Para un mejor abordaje del entendimiento de la situación actual, se procedió a granular el proceso de auditoría de TI de cumplimiento de la ley Nº8204 en cuatro fases, las que se observan en la Figura 11.

Figura 11. Fases del procedimiento actual de revisión de la ley Nº8204.

Seguidamente, se describe el proceso de auditoría de TI de cumplimiento de la ley Nº8204.

4.1.2. Descripción del proceso de planificación

El proceso inicia cuando un cliente de la Firma requiere una evaluación del cumplimiento de la ley Nº8204; por tanto, contrata el servicio al área de auditoría financiera, los cuales, debido a que la revisión cuenta con un componente tecnológico solicitan al área de *IT Audit* el apoyo en la revisión de los temas relacionados con tecnología de información.

Seguidamente, un gerente o supervisor de *IT Audit* procede a realizar la cotización del tiempo requerido para la evaluación de las actividades relacionadas con la ley Nº8204, y procede a coordinar con el departamento de auditoría financiera la fecha de ejecución, para posteriormente incluir en la planificación de proyectos el tiempo que el profesional estará apoyando en la revisión.

Faltando dos semanas para realizar la evaluación, el profesional a cargo de la auditoría de la ley Nº8204 se comunica con el responsable de coordinación por parte del cliente, para informarle la fecha de inicio y enviarle el listado de requerimientos de evidencia que el cliente deberá tener listos al momento que inicia la fase de ejecución.

4.1.1.1. Resumen de actividades del proceso de planificación

En la Tabla 10, se muestra un resumen de las principales actividades realizadas por el proceso actual de planificación de la auditoría de TI de cumplimiento de la ley Nº8204 por parte del área de *IT Audit.*

Actividades	Responsable
Cotización	Gerente o supervisor del área de *IT Audit*
Calendarización	Gerente de *IT Audit*
Coordinación con el cliente para programar reuniones y entrevistas	Profesional del equipo de *IT Audit*, generalmente es un asistente o encargado.
Envío de requerimientos	Profesional del equipo de *IT Audit*, generalmente es un asistente o encargado.

Tabla 10. Resumen de actividades de la planeación

4.1.3. Descripción del proceso de ejecución

Para obtener una mejor comprensión de la situación actual de la fase de ejecución del proceso adoptado por la Firma, mediante la aplicación del instrumento Apéndice H. Revisión documental Metodología de la firma (aplicada), se revisó la documentación soporte de la metodología que actualmente utiliza el área de *IT Audit.*

Para el proceso de ejecución se determinó que el procedimiento de auditoría actual para velar por el cumplimiento de la ley N°8204 se encuentra fundamentado en nueve objetivos del Anexo 1: Acuerdo SUGEF 12-10 Normativa para el Cumplimiento de la Ley Nº8204. Estos nueve objetivos se muestran en la Tabla 11, y que representan los criterios de evaluación del área.

Número de objetivo	Requerimiento de TI del Acuerdo 12-10
1	Artículo 6. Criterios o variables para el análisis y descripción del perfil de riesgo del cliente.
2	Artículo 16. Programas informáticos.
3	Artículo 17. Análisis de las alertas generadas de los programas informáticos.
4	Artículo 18. Bitácoras.
5	Artículo 19. Operaciones únicas.
6	Artículo 20. Operaciones múltiples.
7	Artículo 19. bis Transferencias electrónicas
8	Artículo 38. Apartados Mínimos del Informe Anual. Inciso g) Servicios de Transacciones Electrónicas.
9	Artículo 21. Remisión de información a las Superintendencias

Tabla 11. Objetivos evaluados por el área de TI

Como parte de la ejecución de la evaluación de esta temática la Firma tiene una serie de procedimientos para cada objetivo. Estos procedimientos son aplicados por los auditores recabando evidencia a partir de una lista de requerimientos de información solicitada de previo al cliente en la fase anterior, para respaldar las conclusiones del auditor.

Seguidamente, conforme el auditor revisa la evidencia, debe etiquetar los aspectos mínimos que se indican en el Acuerdo 12-10 para cumplir con la ley Nº8204, y elaborar un memorando con los resultados obtenidos para cada objetivo evaluado. En dicho documento, se indican cuáles son los procedimientos evaluados para concluir sobre cada objetivo, se hace referencia a la evidencia revisada y se describen las pruebas con los resultados obtenidos a partir de estas.

A continuación, se procede a indicar de forma más detallada los requerimientos de información para cada objetivo evaluado por el área de *IT Audit,* con los cuales basan sus procedimientos para determinar si el cliente cumple satisfactoriamente o existe alguna oportunidad de mejora.

4.1.2.1. Objetivo 1 – Criterios o variables para el análisis y descripción del perfil de riesgo del cliente

Este objetivo abarca el artículo 6 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. Por lo tanto, la evaluación pretende determinar si existe una configuración a nivel del sistema para categorizar al cliente de acuerdo con su perfil de riesgo y cuáles son las variables o criterios empleadas para dicho fin. En la Tabla 12, se indican los requerimientos para su revisión.

Número de requerimiento	Descripción
1	Metodología para la clasificación de riesgos de los clientes.
2	Lista de variables implementadas en el sistema para el análisis y descripción del perfil de riesgo del cliente.
3	Revisión en sitio de las variables implementadas en el sistema.
4	Se requiere preparar un ambiente de pruebas para la creación de un cliente y verificar la funcionalidad de la clasificación de riesgo.

Tabla 12. Requerimientos objetivo 1

4.1.2.2. Objetivo 2 – Programas informáticos

Por su parte el objetivo 2, aborda el artículo 16 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. Por lo tanto, la evaluación pretende determinar si cuenta con programas informáticos para realizar el monitoreo continuo para asegurar que el patrón transaccional sea congruente con el perfil de riesgo. Adicionalmente, se verifican las alertas que han sido configuradas cuando se detectan operaciones inusuales, y que estas se generen de manera automáticamente y de manera oportuna. En la Tabla 13, se indican los requerimientos para su revisión.

Número de requerimiento	Descripción
5	Lista de programas informáticos especializados para realizar un monitoreo continuo de los clientes. (Perfil transaccional del cliente, productos, servicios o transacciones de alto riesgo).
6	Políticas y/o procedimientos relacionados con el monitoreo continuo de los clientes.
7	Revisión en sitio de los programas que están operando para el monitoreo continuo de los clientes.
8	Muestra de reportes generados por los programas informáticos de monitoreo de los clientes

Tabla 13. Requerimientos del objetivo 2

4.1.2.3. Objetivo 3 - Análisis de las alertas generadas de los programas informáticos.

En lo que respecta el objetivo 3, hace referencia al artículo 17 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. Donde se evalúa la operatividad y seguimiento de las alertas a transacciones inusuales; además, cuando deja evidencia del motivo, documentación y responsable de descartar una transacción inusual. En la Tabla 14, se indican los requerimientos revisados.

Número de requerimiento	Descripción
9	Lista de alertas implementadas en el sistema para determinar transacciones que desvíen el comportamiento esperado del cliente.
10	Muestra de alertas generadas sobre transacciones que desvíen el comportamiento esperado de los clientes.
11	Manual de cumplimiento.

12	Muestra de transacciones inusuales descartadas. (Documentación de respaldo, responsable).
13	Se requiere preparar un ambiente de pruebas para verificar la funcionalidad de las alertas.

Tabla 14. Requerimientos del objetivo 3

4.1.2.4. Objetivo 4 - Bitácoras.

Este objetivo abarca el artículo 18 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. Donde el proceso pretende validar se cuente con una bitácora de acceso y uso de los sistemas de banca electrónica que registre las transacciones realizadas por algún medio electrónico. Es importante destacar que la bitácora tiene que cumplir con los lineamientos sobre tecnología de información que emita cada Superintendencia. En la Tabla 15, se indican los requerimientos para su revisión.

Número de requerimiento	Descripción
14	Detalle de las bitácoras de acceso y uso de banca electrónica (Indicar nombre de las tablas de la base de datos, nombre y detalle de los campos que se registran, periodo de retención de los datos).
15	Se requiere preparar un ambiente de pruebas para verificar la funcionalidad de las bitácoras.

Tabla 15. Requerimientos del objetivo 4

4.1.2.5. Objetivo 5 – Operaciones únicas.

Por su parte el objetivo 5, aborda el artículo 19 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. El equipo de *IT Audit* valida el registro de las transacciones únicas en efectivo que superen o igualen a los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en colones u otra moneda extranjera; además, que el registro cuente con:

- Datos personales y firma del sujeto físico que realiza la transacción.
- Datos de la persona a cuyo nombre se realiza la transacción.
- Descripción de la transacción.
- Origen de los recursos.
- Datos del destinatario.
- Nombre del funcionario que tramita la transacción.

En la Tabla 16, se indican los requerimientos para la revisión de este objetivo.

Número de requerimiento	Descripción
16	Muestra de formularios físicos con el registro de las transacciones únicas (ROE).
17	Se requiere preparar un ambiente de pruebas para verificar el registro de las transacciones únicas.

Tabla 16. Requerimientos del objetivo 5

4.1.2.6. Objetivo 6 – Operaciones múltiples.

El objetivo 6, hace referencia al artículo 20 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. El equipo de *IT Audit* valida el registro de las transacciones realizadas en efectivo, desde o hacia el exterior durante un mes calendario, que en conjunto superen o igualen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otros colones u otra moneda extranjera; además, que el registro cuente con datos de la persona física o jurídica, una descripción de la transacción, y para cada transacción debe haber constancia de la fecha, medio de pago utilizado, entre otros aspectos mínimos requeridos. En la Tabla 17, se indican los requerimientos para la revisión de este objetivo.

Número de requerimiento	Descripción
18	Muestra de reportes con el registro de transacciones múltiples (ROM).
19	Se requiere preparar un ambiente de pruebas para verificar el registro de las transacciones múltiples.

Tabla 17. Requerimientos del objetivo 6

4.1.2.7. Objetivo 7 – Transferencias electrónicas.

En lo que respecta el objetivo 7, hace referencia al artículo 19 bis para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. El equipo de *IT Audit* valida el registro electrónico de las transacciones únicas que superen o igualen a los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otros colones u otra moneda extranjera; además, que el registro cuente con:

- Datos de la persona a cuyo nombre se realiza la transacción.
- Descripción de la transacción con detalle del tipo, número de operación, fecha y hora exacta, monto y moneda.

- Datos personales y firma del sujeto físico que realiza la transacción, que permitan rastrear los fondos.

Adicionalmente, el profesional encargado de la revisión valida si cuentan con políticas y procedimientos aprobados, que se encuentren basados en el riesgo para determinar cuándo ejecutar, rechazar o suspender una transferencia electrónica que no cumpla los requisitos de información solicitados y la acción de seguimiento apropiada.

En la Tabla 18, se indican los requerimientos revisados.

Número de requerimiento	Descripción
20	Políticas y/o procedimientos relacionados con el registro de transferencias desde y hacia el exterior.
21	Reportes electrónicos con el registro de transacciones desde y hacia el exterior.
22	Revisión en sitio de los controles implementados para el registro y control de las transferencias desde y hacia el exterior.
23	Bitácora con el registro de movimientos realizados por transferencias desde y hacia el exterior.

Tabla 18. Requerimientos del objetivo 7

4.1.2.8. Objetivo 8 – Apartados Mínimos del Informe Anual, inciso g) Servicios de Transacciones Electrónicas.

El objetivo 8, hace referencia al artículo 20 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. El equipo de *IT Audit* valida cuales son los canales electrónicos automatizados, y la implementación de políticas sobre los servicios de transacciones electrónicas en los sistemas. En la Tabla 19, se indican los requerimientos revisados.

Número de requerimiento	Descripción
24	Políticas y/o procedimientos relacionados con las transacciones electrónicas.
25	Políticas y/o procedimientos sobre los servicios de transacciones electrónicas.
26	Lista de los canales y transacciones electrónicos que automatiza la entidad.

Tabla 19. Requerimientos del objetivo 8

4.1.2.9. Objetivo 9 – Remisión de información a las Superintendencias

En lo que respecta el objetivo 9, hace referencia al artículo 21 para el cumplimiento de la ley Nº8204 en materia de tecnologías de información. Donde, el profesional de *IT Audit* valida que se reporte a la Superintendencia respectiva, en los 20 días posteriores al cierre mensual, las transacciones realizadas por sus clientes en efectivo o transferencias desde o hacia el exterior durante el mes calendario, ya sean únicas o múltiples, que igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otra moneda. Además, la validación incluye que el registro cuente con al menos los campos siguientes:

- Nombre completo o razón social del cliente.
- Número de identificación.
- Monto del ingreso o egreso.
- Tipo de operación.
- Fecha.
- Detalle de la transacción.
- Origen de los recursos.
- Nombre o identificador de la entidad.

En la Tabla 20, se indican los requerimientos para la revisión de este objetivo.

Número de requerimiento	Descripción
27	Reporte generado con el registro de las transacciones únicas y múltiples enviado a la Superintendencias.
28	*Select* (verificar en sitio o documento) del reporte de transacciones únicas y múltiples enviados a las Superintendencias.

Tabla 20. Requerimientos del objetivo 9

4.1.2.10. Resumen de actividades del proceso de ejecución

En la Tabla 21, se muestra un resumen de las principales actividades realizadas por el profesional del área de *IT Audit,* durante el proceso actual de ejecución de la auditoría de TI de cumplimiento de la ley Nº8204.

Actividades
Atender reuniones para generar evidencia
Coordinar reuniones y solicitar de evidencia al cliente

Actividades
Revisión del objetivo 1 - Inspeccionar la metodología de clasificación de los clientes. - Inspeccionar la lista de variables implementadas en el sistema. - Verificar en un ambiente de pruebas la creación de un cliente para determinar la funcionalidad de clasificación de riesgo. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 2 - Inspeccionar la lista de programas informáticos utilizados para el monitoreo de los clientes. - Inspeccionar las políticas o procedimientos relacionados al monitoreo de los clientes. - Revisar en el sitio de los programas que están monitoreo de los clientes. - Inspeccionar una muestra de reportes generados por los programas de monitoreo. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 3 - Inspeccionar la lista de alertas implementadas en el sistema para determinar transacciones que desvíen el comportamiento del cliente. - Inspeccionar una muestra de alertas generadas sobre transacciones que desvíen el comportamiento del cliente. - Inspeccionar el manual de cumplimiento. - Inspeccionar una muestra de transacciones inusuales descartadas. - Verificar en un ambiente de pruebas las alertas configuradas. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 4 - Inspeccionar las bitácoras de acceso y uso de banca electrónica. - Verificar en un ambiente de pruebas la funcionalidad de las bitácoras. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 5 - Inspeccionar los formularios con el registro de transacciones únicas. - Verificar en un ambiente de pruebas el registro de transacciones únicas. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores.

Actividades
- Documentar los resultados en el memorando.
Revisión del objetivo 6 - Inspeccionar los formularios con el registro de transacciones múltiples. - Verificar en un ambiente de pruebas el registro de transacciones múltiples. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 7 - Inspeccionar las políticas y/o procedimientos relacionados con el registro de transferencias. - Inspeccionar los reportes electrónicos con el registro de transferencias. - Revisar los controles para el registro y control de transferencias desde y hacia el exterior. - Inspeccionar la bitácora con registro de movimientos realizados por transferencias. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 8 - Inspeccionar las políticas y/o procedimientos relacionados con transferencias electrónicas. - Inspeccionar las políticas y/o procedimientos sobre los servicios de transacciones electrónicas. - Inspeccionar la lista de los canales y transacciones electrónicos que automatiza la entidad. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 9 - Inspeccionar los campos del reporte generado con el registro de transacciones únicas y múltiples enviado a la Superintendencia respectiva. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.

Tabla 21. Resumen de actividades de la ejecución

4.1.4. Descripción del proceso de elaboración del informe

El proceso de elaboración del informe da inicio cuando el profesional de *IT Audit* finaliza la documentación de los memorandos para cada objetivo evaluado, y procede a generar un memorando resumen donde indica a modo resumen los procesos evaluados

por objetivo y los resultados obtenidos, indicando si determinó oportunidades de mejora o la revisión del objetivo fue satisfactoria.

Una vez confeccionado el informe, el Gerente de *IT Audit* a cargo realiza una revisión de calidad para verificar el contenido del informe, haciendo hincapié en la estructura, que los procedimientos estuvieran acordes a lo indicado en la metodología del área y en los resultados obtenidos.

Posteriormente, el profesional a cargo de la revisión envía el informe aprobado al cliente para que valide los resultados y confirme si los acepta, o en caso contrario, puede apelar entregando evidencia que respalde sus afirmaciones.

4.1.3.1. Resumen de actividades del proceso de elaboración del informe

En la Tabla 22, se muestra un resumen de las principales actividades realizadas en el proceso actual de elaboración del informe de auditoría de TI de cumplimiento de la ley Nº8204 por parte del área de *IT Audit.*

Actividades	Responsable
Confeccionar el informe	Profesional del equipo de *IT Audit*, generalmente es un asistente o encargado.
Revisar y aprobar el informe	Gerente de *IT Audit.*
Enviar confirmación al cliente	Profesional del equipo de *IT Audit*, generalmente es un asistente o encargado.
Confirmación o apelación del cliente	Oficial de cumplimiento del cliente auditado.
Correcciones al informe producto de la apelación del cliente -si aplica-	Profesional del equipo de *IT Audit*, generalmente es un asistente o encargado.

Tabla 22. Resumen de actividades de la elaboración del informe

4.1.5. Descripción del proceso de cierre

El proceso de cierre culmina la participación de *IT Audit* en la auditoría de cumplimiento de la ley Nº8204, donde el gerente del área retroalimenta al gerente sénior del proceso y resultados obtenidos; y se envía el informe con los resultados al equipo de auditoría financiera para que presenten los resultados. Posteriormente, se almacenan la documentación que soporta las conclusiones del proceso en el repositorio para tal fin, y el

profesional del área de *IT Audit* elimina de su computadora toda la información de la cliente proporcionada como insumo para la revisión.

4.1.4.1. Resumen de actividades del proceso de cierre

En la Tabla 23, se muestra un resumen de las principales actividades realizadas en el proceso actual de elaboración del informe de auditoría de TI de cumplimiento de la ley Nº8204 por parte del área de *IT Audit.*

Actividades	Responsable
Comunicar los resultados y retroalimentación del proceso	Gerente de *IT Audit.*
Enviar el informe al gerente de auditoría financiera	Profesional del equipo de *IT Audit*, generalmente es un asistente o encargado.
Presentar los resultados a la gerencia del cliente	Gerente de *IT Audit* en conjunto con el gerente de auditoría.
Almacenar la documentación en el repositorio	Gerente de auditoría, equipo de riesgo.
Limpiar los documentos del cliente	Profesional del equipo de *IT Audit*, que realizó la auditoría.

Tabla 23. Resumen de actividades del cierre

4.2. Identificación de brechas

Partiendo del entendimiento obtenido del análisis de la situación actual del proceso de auditoría de TI de cumplimiento de la ley Nº8204, se procede a determinar deficiencias y brechas que, por medio de oportunidades de mejora, busca identificar el estado deseado del proceso, para lo cual, se procede a emplear diversos instrumentos de investigación, los cuales fueron previamente definidos en la metodología, específicamente en la sección 3.4. Fuentes de Investigación.

Los instrumentos utilizados para la recopilación de datos fueron la aplicación de una encuesta con preguntas cerradas y abiertas, dirigida a profesionales del área de *IT Audit* con puestos de asistente y encargado, para conocer su percepción del proceso actual, dado que han realizado estas evaluaciones en clientes durante el último año. El instrumento Apéndice L, se aplicó el 4 de octubre del presente año.

Seguidamente, se procede a determinar cuáles actividades son aplicables del marco jurídico nacional, y las buenas prácticas de auditorías de TI para identificar el estado deseado del proceso.

4.2.1. Revisión del acuerdo SUGEF 12-10 Normativa para el cumplimiento de la ley Nº8204

Para analizar los aspectos mínimos requeridos por esta normativa en materia de tecnologías de información, se procedió a realizar la aplicación del instrumento Apéndice I. Revisión documental Acuerdo 12-10 (aplicada).

Se determinó que la ley cuenta con cuatro apartados estrechamente relacionados con tecnologías de información, los cuales involucran sistemas que clasifican, monitorean y/o registran transacciones e información de los clientes. Estos apartados se describen a continuación.

4.2.1.1. Clasificación del riesgo de los clientes

En este apartado el Acuerdo SUGEF 12-10, menciona los requerimientos relacionados con los criterios o variables para el análisis y descripción del perfil de riesgo de los clientes, así como la metodología de clasificación del riesgo. (SUGEF, 2017)

En la Tabla 24, se indican los requerimientos mínimos para cada objetivo del apartado en cuestión, que involucran un componente tecnológico.

Objetivo	Requerimientos mínimos

Artículo 4. Categorización y perfil de riesgo de clientes	- Categorización del riesgo de los clientes.
	- Diseñar e implementar una metodología de clasificación de riesgo.
	- Establecer programas de monitoreo.
	- Consideraciones para definir la categoría de riesgo:
	  o Utilizar al menos tres categorías de riesgo (alto, moderado, bajo).
	  o Los criterios para establecer la categorización del riesgo.

Artículo 5. Metodología para la clasificación de riesgo de los clientes.	- Consideraciones el diseño de la metodología de categoría de riesgo:
	  o Los criterios para establecer la categorización del riesgo de los clientes.
	  o Descripción de la clasificación y categorización del riesgo de los clientes.
	  o Descripción y diseño automatizado del modelo para establecer el perfil del cliente.
	- Debe ser revisada y aprobada por la Junta Directiva.

Objetivo	Requerimientos mínimos
Artículo 6. Criterios o variables para el análisis y descripción del perfil de riesgo del cliente	- Los criterios para el análisis del perfil del riesgo cuentan con justificación para ser incluidos o excluidos de la metodología. Y considerar al menos: o Nacionalidad o País de origen o País de domicilio o Profesión u oficio o Zona geográfica de las actividades del negocio y si está involucrado con países considerados de alto riesgo según consideraciones de organismos internacionales. o Actividad económica. o Estructura de la propiedad. o Tipo de activos propios de la entidad cliente. o Tipo, monto y frecuencia de las transacciones. o Utilización de efectivo. o Origen de los recursos. o Temporalidad de la actividad que genera los recursos. o Personas expuestas políticamente. o Productos y servicios utilizados por el cliente. o Comportamiento atípico de los movimientos de la cuenta. o Cuentas o relaciones de negocios inactivas. o Clientes con patrimonios importantes.

Tabla 24. Requisitos mínimos para la clasifciación de riesgo de los clientes

Fuente: (SUGEF, 2017)

De acuerdo con el análisis de la situación actual realizado en la sección 4.1.2.10. Resumen de actividades del proceso de ejecución, sobre los objetivos relacionados con los artículos que cubre el presente apartado. Se determinó que no se incluyen explícitamente actividades para indicar los aspectos puntuales realizar durante la auditoría, como los indicados en la Tabla 25.

Objetivo	Aspectos que no se incluyen explícitamente
Objetivo 1	Validar la aprobación de la metodología de clasificación de riesgo de los clientes.
	Comparar que las variables indicadas en la metodología e implementadas en el incluyan al menos las indicadas en el artículo 6 del acuerdo SUGEF 12-10.
	Inspeccionar/Indagar cual es el modelo documentado e implementado en el sistema para clasificar el perfil de riesgo.
	Verificar en un ambiente de pruebas la creación de un cliente físico y uno jurídico para cada nivel de riesgo, para determinar la funcionalidad de clasificación de riesgo.

Tabla 25. Aspectos por considerar para la clasificación del riesgo de los clientes

4.2.1.2. Monitoreo de transacciones y programas informáticos

En este apartado el Acuerdo SUGEF 12-10, menciona los requerimientos relacionados con el monitoreo, alerta y registro de transacciones que se desvíen del comportamiento esperado del cliente de acuerdo con su perfil de riesgo. (SUGEF, 2017)

En la Tabla 26, se indican los requerimientos mínimos para cada objetivo del apartado en cuestión, que involucran un componente tecnológico.

Objetivo	Requerimientos mínimos

Artículo 16. Programas informáticos	- Implementar programas de monitoreo continuo, para asegurar que el patrón transaccional sea congruente con el comportamiento esperado de acuerdo con el perfil de riesgo.
	- Establecer alertas y en consecuencia los tipos de monitoreo necesarios para identificar operaciones inusuales.
	- Implementar alertas automáticas y oportunas sobre transacciones que se desvíen del comportamiento esperado del cliente.
	- Generar reportes, que consideren como mínimo:
	  ○ Datos personales de cada cliente.
	  ○ Histórico de transacciones.
	  ○ Relación entre las cuentas de cada cliente.
	  ○ Históricos de las categorías de riesgo asignadas a cada cliente.
	  ○ Alertas generadas.
	- Las alertas se deben mantener actualizadas.

Artículo 17. Análisis de las alertas generadas de los programas informáticos	- Se debe realizar revisión de todas las alertas, y dar seguimiento a las transacciones inusuales. - En el caso de las transacciones que se descarten, se debe dejar evidencia del motivo, documentación de respaldo y el responsable.
Artículo 18. Bitácoras	- Se debe contar con una bitácora de acceso y uso del sistema, que permita registrar y rastrear las transacciones realizadas en el sistema de banca electrónica. - Cumplir con los lineamientos de la Superintendencia.

Tabla 26. Requisitos mínimos con el monitoreo de transacciones y programas informáticos

Fuente: (SUGEF, 2017)

De acuerdo con el análisis de la situación actual realizado en la sección 4.1.2.10. Resumen de actividades del proceso de ejecución, sobre los objetivos relacionados con los artículos que cubre el presente apartado. Se determinó que no se incluyen explícitamente actividades indicadas en la Tabla 27.

Objetivo	Aspectos que no se incluyen explícitamente
Objetivo 2	Validar que alertas se encuentran parametrizadas en los sistemas para identificar operaciones inusuales.
	Revisar que los programas informáticos están operando efectivamente de forma que generen automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.
	Validar que los reportes generados por los programas informáticos incluyan al menos los campos indicados en el artículo 16 del acuerdo SUGEF 12-10.
Objetivo 3	Indagar con el personal de cumplimiento de qué manera se revisan las alertas y cómo se registra el seguimiento.
	Validar que para las transacciones inusuales que se descarten, se registre el motivo, documentación de respaldo y el responsable.
Objetivo 4	Indagar con el oficial de cumplimiento, los lineamientos que deben cumplir las bitácoras de acuerdo con lo indicado por la Superintendencia.
	Verificar en un ambiente de pruebas el registro del acceso y transacciones en las bitácoras implementadas para cada uno de los medios electrónicos.

Tabla 27. Aspectos por considerar con el monitoreo de transacciones y programas informáticos.

4.2.1.3. Registro y notificación de transacciones

Se mencionan aspectos para la trazabilidad y registro de operaciones electrónicas o en efectivo que sean únicas o múltiples, así como, la remisión de esta información a la Superintendencia respectiva. (SUGEF, 2017)

En la Tabla 28, se indican los requerimientos mínimos para cada objetivo del apartado en cuestión, que involucran un componente tecnológico.

Objetivo	Requerimientos mínimos

Artículo 19. Operaciones únicas en efectivo.	- Registrar las transacciones únicas iguales o superiores a los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América).
	- El formulario debe considerar como mínimo:
	  ○ Datos personales de cada cliente.
	  - Nombre completo
	  - Teléfono
	  - Fechas de nacimiento
	  - Número de identificación
	  - Tipo de identificación
	  - Domicilio exacto
	  - Representante legal y agente residente para las personas jurídicas.
	  ○ Datos de la persona a cuyo nombre se realiza la transacción.
	  - Nombre completo o razón social

Objetivo	Requerimientos mínimos
	- Número de identificación - Tipo de identificación - Domicilio o Descripción de la transacción - Tipo de transacción - Tipo de operación - Número de operación - Fecha y hora de la transacción - Monto y moneda original transada - Monto total dolarizado o Origen de los recursos o Número de cuenta y nombre de la entidad destino o Nombre del funcionario que tramitó la transacción o Firma de la persona física que realiza la transacción.
Artículo 19 bis. Transferencias electrónicas.	- Registrar las transacciones electrónicas únicas desde o hacia el exterior, que sean iguales o superiores a los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América). Considerando como mínimo: o Datos de la persona a cuyo nombre se realiza la transacción. - Nombre completo o razón social - Número de identificación o Descripción de la transacción - Tipo de transacción - Tipo de operación - Número de operación - Fecha y hora de la transacción - Monto y moneda original transada - Monto total dolarizado - En lo que respecta a la contraparte del exterior, se deben registrar: o Información requerida sobre el originador. o Información requerida sobre el beneficiario. - Contar con políticas y procedimientos actualizados para determinar cuándo ejecutar, rechazar o suspender una transacción, y la respectiva acción de seguimiento.
Artículo 20. Operaciones múltiples	- Registrar las transacciones múltiples en efectivo y electrónicas que igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América), durante un mes calendario. - El registro debe considerar como mínimo: o Nombre completo o razón social o Teléfono o Fecha de nacimiento o constitución o Número y tipo de identificación o Descripción de la transacción - Por otra parte, cada transacción debe considerar como mínimo: o Fecha

Objetivo	Requerimientos mínimos
	○ Tipo de transacción ○ Medio de pago ○ Número de operación ○ Moneda ○ Monto individual y total
Artículo 21. Remisión de información a las Superintendencias	- Reportar a la Superintendencia las transacciones únicas y múltiples realizadas por sus clientes, durante los 20 días naturales posteriores al cierre mensual. - El reporte debe incluir al menos: ○ Nombre completo o razón social del cliente ○ Número y tipo de identificación ○ Monto del ingreso o egreso ○ Tipo de operación ○ Fecha ○ Detalle de la transacción ○ Origen de los recursos ○ Nombre o código de la entidad

Tabla 28. Requisitos mínimos para el registro y notificación de transacciones

Fuente: (SUGEF, 2017)

De acuerdo con el análisis de la situación actual realizado en la sección 4.1.2.10. Resumen de actividades del proceso de ejecución, sobre tres de los cuatro objetivos relacionados con los artículos que cubre el presente apartado. Se determinó que las actividades cumplen de forma explícita con los aspectos mínimos requeridos por la normativa de cumplimiento de la ley Nº8204. En la Tabla 29, se muestran algunas oportunidades de mejora identificadas para los objetivos actuales.

Objetivo	Oportunidades de mejora
Objetivo 5	Cumple con todas las actividades requeridas, únicamente no se indica de forma explícita en los requerimientos cuales son los datos para validar, para lo cual, se considerarán al menos los campos indicados en el artículo 19 del acuerdo SUGEF 12-10.
Objetivo 6	Cumple con todas las actividades requeridas, únicamente no se indica de forma explícita en los requerimientos cuales son los datos para validar, para lo cual, se considerarán al menos los campos indicados en el artículo 20 del acuerdo SUGEF 12-10.
Objetivo 7	Cumple con todas las actividades requeridas, únicamente no se indica de forma explícita en los requerimientos cuales son los datos para validar, para lo cual, se considerarán al menos los campos indicados en el artículo 19 bis del acuerdo SUGEF 12-10.

Tabla 29. Oportunidades de mejora con el registro y notificación de transacciones

Por otra parte, siguiendo la misma línea, se determinó que el objetivo restante no incluye explícitamente las actividades para indicar los aspectos puntuales en la revisión, como los indicados en la Tabla 30.

Objetivo	Oportunidades de mejora
Objetivo 9	Validar que el reporte incluya al menos los campos indicados en el artículo 21 del acuerdo SUGEF 12-10.
	Validar que el reporte sea remitido dentro de los 20 días naturales posteriores al cierre de cada mes.
	Si se utiliza una herramienta automatizada, validar uno de los aspectos siguientes: - Validar para una muestra que los datos del reporte sean congruentes a los registrados en el sistema. - Validar que la consulta o la delimitación del reporte generado se limite a transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario

Tabla 30. Aspectos por considerar con el registro y notificación de transacciones

4.2.1.4. Obligaciones y responsabilidades de la auditoría interna y externa con hincapié en los apartados mínimos del informe anual

En este apartado el Acuerdo SUGEF 12-10, se mencionan las obligaciones de la auditoría interna y externa, específicamente indica que la auditoría externa debe emitir un informe sustentado con pruebas de cumplimiento de las medidas para prevenir o detectar el fraude, lavado de dinero y financiamiento al terrorismo. Asimismo, se indica que el informe debe incluir una valoración de la eficacia operativa y/u oportunidades de mejoras identificadas. (SUGEF, 2017)

En la Tabla 31, se indican los requerimientos mínimos para cada objetivo del apartado en cuestión, que involucran un componente tecnológico.

Objetivo	Requerimientos mínimos
Artículo 38. Apartados mínimos del informe anual	- El informe debe referirse al apartado: o Servicios de transacciones electrónicas.

Tabla 31. Requisitos mínimos para el registro y notificación de transacciones

Fuente: (SUGEF, 2017)

De acuerdo con el análisis de la situación actual realizado en la sección 4.1.2.10. Resumen de actividades del proceso de ejecución. En lo que respecta a las actividades de revisión del objetivo 8, por parte del área de *IT Audit,* no se identificaron brechas u oportunidades de mejora contrastando con lo solicitado en el acuerdo SUGEF 12-10.

4.2.2. Actividades del proceso BAI06

Para evaluar las prácticas que indica el marco de trabajo COBIT 2019 con respecto a la gestión de cambios de TI, se procedió a aplicar el instrumento Apéndice K, con el propósito de identificar las actividades recomendadas para cumplir con este proceso.

De lo anterior, se determinó que COBIT 2019 respecto al proceso de gestión de cambios, busca que exista una entrega confiable y rápida de los cambios en el negocio, y que se mitigue el riesgo de afectar negativamente la estabilidad o integridad del ambiente de producción. Para lo cual, se definieron cuatro actividades de gestión que se encuentran granuladas en una serie de actividades de cumplimiento.

Cabe destacar que por la naturaleza de la revisión actualmente no se consideran actividades sugeridas del proceso BAI06 dentro del proceso de auditoría de TI de cumplimiento de la ley Nº8204.

Sin embargo, se determinó que las actividades indicadas en la Tabla 32, podrían aportar una mejora significativa a la revisión pues se consideran aspectos relacionados con los cambios aplicados a la configuración relacionada con el cumplimiento de la ley Nº8204.

Práctica de gestión	Actividades Consideradas
BAI06.01. Evaluar, priorizar y autorizar solicitudes de cambio.	Asegurar que todos los cambios se realicen a través del proceso de gestión de cambios.
	Planificar y evaluar todas las peticiones de una manera estructurada. Considerando todas las implicaciones de cumplimiento normativo del cambio solicitado.
	Aprobar formalmente cada cambio por parte de los propietarios, gestores de servicio, según corresponda.
	Planificar y programar los cambios aprobados.
BAI06.04. Cierre y documentación	Incluir los cambios en políticas y procedimientos en el proceso de gestión de cambio como parte integral.
	Someter a la documentación a la misma revisión que al cambio en sí mismo.

Tabla 32. Actividades consideradas del BAI06 para el proceso de auditoría de TI de la ley Nº8204

Fuente: (ISACA, 2018)

Lo anterior, aplica para los objetivos indicados en la Tabla 33.

Objetivo	Actividades BAI06
Objetivo 1	Indagar si ha habido cambios en la configuración de clasificación de clientes, y validar que los cambios cuenten con aprobación respectiva.

Objetivo	Actividades BAI06
Objetivo 2	Indagar si ha habido cambios en la configuración de alertas para determinar transacciones que se desvíen del comportamiento esperado del cliente, y validar que los cambios cuenten con aprobación respectiva.
Objetivo 4	Indagar con el oficial de cumplimiento y personal de TI si ha habido cambios en la configuración de bitácoras de acceso y uso de banca electrónica, y validar que los cambios cuenten con aprobación respectiva.
Objetivo 7	Indagar si ha habido cambios relacionados que involucren la ejecución, rechazo o suspensión las transacciones automáticas cuando se detecte sospechosa, y validar que los cambios cuenten con aprobación respectiva.
Objetivo 8	Indagar si ha habido cambios relacionados con los servicios de transacciones por medio del sitio web, y validar que los cambios cuenten con aprobación respectiva.

Tabla 33. Actividades BAI06 en la auditoría de TI de la ley Nº8204

Lo anterior, para evitar que existan cambios no aprobados o documentados en la parametrización de los programas y herramientas que cumplen con los requerimientos solicitados por la ley Nº8204. Y sin generar gran impacto en el alcance de la auditoría.

4.2.3. Actividades del proceso DSS06

Para evaluar las prácticas que indica el marco de trabajo COBIT 2019 con respecto a la gestión de controles de proceso de negocio, se procedió a aplicar el instrumento Apéndice K, con el propósito de identificar las actividades recomendadas para cumplir con este proceso.

De lo anterior, se determinó que COBIT 2019 respecto al proceso de gestión de controles de procesos de negocio, pretender definir controles adecuados para garantizar que la operación de entradas, procesamiento y salidas de los controles del negocio satisfagan todos los requerimientos de información integra y relevante.

Actualmente el enfoque de la auditoría de TI de cumplimiento de la ley Nº8204 es una revisión de las actividades mínimas requeridas de la regulación, por lo tanto, no se podría considerar que se cuente con una revisión de controles como tal.

Por lo anterior, se considera que las actividades indicadas en la Tabla 34, brindan una oportunidad de mejora al proceso, pues con base en los lineamientos establecidos permitirá elaborar una serie de controles para facilitar la evaluación y considerar otros aspectos fundamentales como la mejora continua del proceso, entre otros.

Práctica de gestión	Actividades
DSS06.01. Alinear las actividades de control integradas en los procesos comerciales con objetivos empresariales	Identificar y documentar las actividades de control de los procesos claves para satisfacer los requerimientos de control estratégicos, operacionales, de informes y cumplimiento.
	Asegurar la propiedad de las actividades de control.
	Supervisar continuamente las actividades de control de extremo a extremo para identificar oportunidades de mejora.
	Mejorar continuamente el diseño y operación de los controles de procesos de negocio.
DSS06.02. Controlar el procesamiento de la información.	Crear transacciones por individuos autorizados siguiendo los procedimientos establecidos, incluyendo la segregación de tareas en relación con el origen y aprobación de esas transacciones.
	Introducir transacciones en el momento oportuno y verificar que las transacciones son precisas, completas y válidas. Validar los datos de entrada y edición.
	Mantener la integridad y validez de los datos a través del ciclo de procesamiento.
	Mantener la integridad de los datos durante interrupciones no esperadas en el procesamiento de datos
	Manejar la salida de una forma automatizada, entregarla al beneficiario apropiado y proteger la información durante la transmisión. Verificar la precisión y completitud de la salida.
DSS06.03. Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocios asignadas.
	Asignar niveles de autoridad para la aprobación de transacciones, límites y cualquier otra decisión relativa al proceso de negocio basado en los roles de trabajo aprobados.
	Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar en las actividades de trabajo, basados en los roles de puesto predefinidos.
	Asignar roles para actividades sensibles de manera que exista una segregación de funciones.
	Revisar periódicamente las definiciones de control de acceso, registros e informe de excepciones para asegurar que todos los

Práctica de gestión	Actividades
	privilegios de acceso son válidos y alineados a los roles asignados.
DSS06.04. Gestionar errores y excepciones	Revisar errores, excepciones y desviaciones.
	Hacer seguimiento, corregir, aprobar y reenviar información.
	Mantener evidencia de las medidas correctivas.
DSS06.05. Asegurar la trazabilidad de eventos y responsables de información	Definir requerimientos de retención, basados en los requerimientos del negocio, y de cumplimiento.
	Capturar la fuente de información, evidencia que soporta y el registro y transacciones.
	Eliminar la fuente de información, la evidencia que la soporta y el registro de transacciones de acuerdo con la política de retención.

Tabla 34. Actividades consideradas del DSS06 para el proceso de auditoría de TI de la ley Nº8204.

Fuente: (ISACA, 2018)

Las actividades anteriores, aplicadas al procedimiento actual permiten realizar una revisión más estructurada de cada objetivo evaluado por la auditoría de TI de cumplimiento de la ley Nº8204. Al considerar aspectos clave en la definición de controles, como la alineación con la regulación, que se garantice la integridad de la información, consideraciones acerca de la segregación de funciones y la documentación de excepciones.

4.2.4. Revisión de NIAS aplicables

Para evaluar aspectos importantes a considerar en la auditoría de TI de cumplimiento de la ley Nº8204 se procede a aplicar el instrumento Apéndice I. Revisión documental Acuerdo 12-10 (aplicada), donde se revisan puntualmente los requisitos que debe contener la evidencia suficiente y adecuada para que el auditor respalde sus conclusiones, y también las técnicas de muestro que permitan garantizar que los resultados de la revisión sean válidos para el total de información procesada por los controles.

Se debe garantizar que la información utilizada como evidencia sea adecuada y suficiente para alcanzar conclusiones razonables.

4.2.2.1. Tamaños de muestra

La NIA 530, indica que, para diseñar una muestra que sea suficiente para reducir el riesgo de muestreo a un nivel bajo, el auditor deberá considerar el procedimiento y el

objetivo, así como las características de la población. La selección de elementos debe de garantizar que todos los elementos pueden ser seleccionados.

4.2.5. Resultado del análisis para definir estado deseado

En la Tabla 35, se muestra un resumen con las actividades del estado actual y las consideraciones adicionales, definiendo así el estado deseado del proceso de auditoría de TI de cumplimiento de la ley Nº8204.

Actividades
Revisión del objetivo 1 - Indagar si ha habido cambios en la configuración de clasificación de clientes, y validar que los cambios cuenten con aprobación respectiva. - Indagar sobre el diseño y la implementación de la metodología aprobada para la clasificación de riesgo de los clientes. - Inspeccionar/Indagar cuál es el modelo documentado e implementado en el sistema para clasificar el perfil de riesgo. - Comparar que las variables indicadas en la metodología e implementadas en el incluyan al menos las indicadas en el artículo 6 del acuerdo SUGEF 12-10. - Verificar en un ambiente de pruebas la creación de un cliente físico y uno jurídico para cada nivel de riesgo, para determinar la funcionalidad de clasificación de riesgo. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 2 - Indagar si ha habido cambios en la configuración de alertas para determinar transacciones que se desvíen del comportamiento esperado del cliente, y validar que los cambios cuenten con aprobación respectiva. - Inspeccionar las políticas o procedimientos relacionados al monitoreo de los clientes. - Validar cuales alertas se encuentra parametrizadas en los sistemas para identificar operaciones inusuales. - Revisar que los programas informáticos están operando efectivamente de forma que generen automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente. - Validar que los reportes generados por los programas informáticos incluyan al menos los campos indicados en el artículo 16 del acuerdo SUGEF 12-10. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.

Actividades
Revisión del objetivo 3 - Indagar con el personal de cumplimiento de qué manera se revisan las alertas y cómo se registra el seguimiento - Inspeccionar la lista de alertas implementadas en el sistema para determinar transacciones que desvíen el comportamiento del cliente. - Inspeccionar una muestra de alertas generadas sobre transacciones que desvíen el comportamiento del cliente. - Validar que para las transacciones inusuales que se descarten, se registre el motivo, documentación de respaldo y el responsable. - Verificar en un ambiente de pruebas las alertas configuradas. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 4 - Indagar con el oficial de cumplimiento y personal de TI si ha habido cambios en la configuración de bitácoras de acceso y uso de banca electrónica, y validar que los cambios cuenten con aprobación respectiva. - Indagar con el oficial de cumplimiento cuales son los lineamientos que deben cumplir las bitácoras de acuerdo con lo indicado por la Superintendencia. - Indagar con el personal de TI de qué manera se han implementado bitácoras - Verificar en un ambiente de pruebas el registro del acceso y transacciones en las bitácoras implementadas para cada uno de los medios electrónicos. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 5 - Inspeccionar los formularios con el registro de transacciones únicas, que incluyan al menos los campos indicados en el artículo 19 del acuerdo SUGEF 12-10. - Verificar en un ambiente de pruebas el registro de transacciones únicas. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 6 - Inspeccionar los formularios con el registro de transacciones múltiples, que incluyan al menos los campos indicados en el artículo 20 del acuerdo SUGEF 12-10. - Verificar en un ambiente de pruebas el registro de transacciones múltiples. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores.

Actividades
- Documentar los resultados en el memorando.
Revisión del objetivo 7 - Indagar si ha habido cambios relacionados que involucren la ejecución, rechazo o suspensión las transacciones automáticas cuando se detecte sospechosa, y validar que los cambios cuenten con aprobación respectiva. - Indagar si las transferencias desde y hacia el exterior realizadas en moneda local o extranjera, se registran automáticamente e incluyen que incluyan al menos los campos indicados en el artículo 19 bis del acuerdo SUGEF 12-10. - Revisar los controles para el registro y control de transferencias desde y hacia el exterior - Inspeccionar los reportes electrónicos con el registro de transferencias. - Inspeccionar la bitácora con registro de movimientos realizados por transferencias. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 8 - Indagar si ha habido cambios relacionados con los servicios de transacciones por medio del sitio web, y validar que los cambios cuenten con aprobación respectiva. - Inspeccionar las políticas y/o procedimientos relacionados con transferencias electrónicas. - Inspeccionar las políticas y/o procedimientos implementados en los sistemas sobre los servicios de transacciones electrónicas. - Inspeccionar la lista de los canales y transacciones electrónicos que automatiza la entidad. - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.
Revisión del objetivo 9 - Validar que el reporte incluya al menos los campos indicados en el artículo 21 del acuerdo SUGEF 12-10. - Validar que el reporte sea remitido dentro de los 20 días naturales posteriores al cierre de cada mes. - Si se utiliza una herramienta automatizada, validar uno de los aspectos siguientes: o Validar para una muestra que los datos del reporte sean congruentes a los registrados en el sistema. o Validar que la consulta o la delimitación del reporte generado se limite a transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario - Etiquetar y marcar la evidencia obtenida de las actividades anteriores. - Documentar los resultados en el memorando.

Tabla 35. Estado deseado

4.2.6. Diagrama TO BE

Partiendo del estado deseado del proceso con el detalle de las actividades a incluir, se procede a realizar el diagrama BPMN que contempla dichas actividades, el cual se presenta gráficamente en la Figura 12.

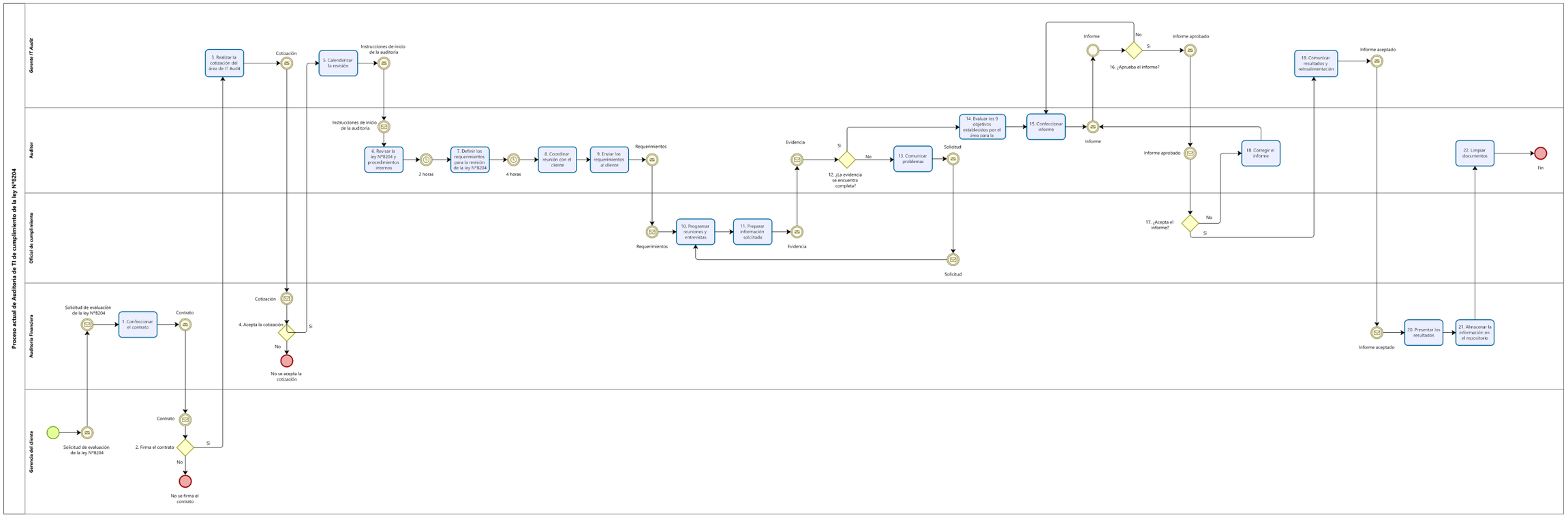


Figura 12. Diagrama To Be

Capítulo V: Propuesta de Solución

En el presente capítulo se presentan las oportunidades de mejora a las deficiencias descritas en la identificación de brechas del anterior capítulo, documentando la propuesta que pretende abordar los objetivos del proyecto.

Para el desarrollo de la propuesta de solución se considera la problemática identificada en la sección 1.2.2. Justificación del proyecto, la cual ha sido desarrollada de acuerdo con lo explicado en los capítulos anteriores del presente Trabajo Final de Graduación, con base en los aspectos mínimos de la normativa nacional contra el fraude y lavado de dinero de la ley Nº8204, y contrastando el proceso actual con mejores prácticas de TI de marcos de referencia internacionales para garantizar el cumplimiento de los objetivos del presente proyecto.

5.1. Definición de controles y pruebas

Los entregables presentados en esta sección son elaborados para apoyar el cumplimiento del objetivo general del proyecto; el cual, pretende generar una matriz de controles que contenga por cada uno de los objetivos evaluados, una lista de criterios que permitirán al área de *IT Audit,* valorar la situación de los clientes auditados respecto al cumplimiento de la ley Nº8204.

La estructura de la matriz de controles contiene nueve elementos, los cuales se detallan en la Tabla 36.

Elemento	Descripción
Número de objetivo.	Corresponde al número de objetivo del procedimiento actual de revisión.
Artículo SUGEF 12-10	Es el requerimiento regulatorio que sustenta la revisión del control.
Control	Nombre del control evaluado.
Riesgo asociado	Riesgo inherente asociado al control.
Procedimientos de diseño	Procedimientos realizados sobre el diseño del control.
Evidencia del diseño	Evidencia sugerida que sustenta los procedimientos de diseño.
Atributo	Variable no medible que pretende ser evaluada en la eficacia operativa del control.
Procedimientos del diseño	Procedimientos realizados para probar la eficacia operativa del control.
Evidencia	Evidencia sugerida que sustenta los procedimientos de eficacia operativa.

Tabla 36. Campos de la propuesta

La matriz que se propone para la auditoría de TI de cumplimiento de la ley Nº8204, se muestra en el Apéndice M: Matriz propuesta con los controles para la revisión de la ley Nº8204.

5.1.1. Instrucciones para realizar la evaluación utilizando los controles propuestos

Seguidamente se indican las instrucciones para la utilización de la matriz de controles en el proceso de revisión de cumplimiento de la ley Nº8204. Es importante resaltar que para la ejecución de las auditorías se requiere que el auditor cuente con:

- Conocimientos de auditoría de TI.
- Conocimientos de COBIT 2019.
- Capacitación del uso de la matriz y ejecución de las auditorías de la ley Nº8204.
- Grado de bachiller universitario en carreras afines.

Lo anterior dado que, el uso de la herramienta es un apoyo para realizar el proceso de auditorías, y se requiere un conocimiento previo sobre los procedimientos de diseño y eficacia operativa por evaluar.

Partiendo del envío de los requerimientos que se muestran en el Apéndice O, una vez realizadas las sesiones respectivas y el oficial de cumplimiento envía la información solicitada, el auditor procede a tomar la matriz y para cada control elaborar un memorando, tomando como guía la plantilla del Apéndice N.

En primera instancia, se parte de los procedimientos de diseño del control para los cuales se revisa que la evidencia entregada se encuentre completa, y se procede a marcar la información proporcionada haciendo hincapié en los aspectos de cumplimiento de los criterios evaluados por los procedimientos que se indican en la matriz. Además, deberá validar que toda información generada como evidencia cuente con un campo donde se muestre la fecha para garantizar que se está obteniendo durante el proceso de auditoría.

Los resultados obtenidos de la etapa de diseño son principalmente si la organización auditada cuenta con los controles diseñados para cumplir con lo indicado en los artículos del Acuerdo SUGEF 12-10, dichos resultados se documentan en el memorando de evaluación del control y si no cumpliera completamente con alguno de los procedimientos, se procede a indicarlo mediante un hallazgo de auditoría en dicho documento.

En caso de cumplir satisfactoriamente con el diseño del control, se procede a evaluar la eficacia operativa del control tomando los procedimientos de la matriz para este fin, y se procede a marcar la información proporcionada haciendo hincapié en el cumplimiento de los atributos.

Los resultados obtenidos se documentan en el memorando de evaluación del control, indicando todos los atributos se cumplen satisfactoriamente y haciendo referencia a la documentación marcada; en caso de no cumplir totalmente con alguno, se procede a indicarlo mediante un hallazgo de auditoría en dicho documento.

Posteriormente, se envía el memorando y la evidencia que soporta las conclusiones debidamente etiquetadas al gerente de *IT Audit* para su revisión, y en caso de tener alguna observación se procederá a corregir lo indicado.

Finalmente, una vez ejecutada la evaluación de los nueve controles, siguiendo la misma estructura se completa un memorando final con los resultados obtenidos, donde se indique para cada control evaluado si los resultados son satisfactorios; es decir, cumple completamente con los procedimientos de diseño y eficacia operativa evaluados, o bien se documentan las oportunidades de mejora identificadas producto de los hallazgos identificados.

5.1.2. Matriz RACI del proceso de ejecución de la auditoría de cumplimiento de la ley Nº8204

Para una mejor comprensión de las responsabilidades de cada involucrado, en la Tabla 37, se indican los principales roles que se involucran en el proceso, y su grado de participación en cada una de las actividades del proceso de revisión.

	Gerente de IT Audit	Auditor	Oficial de cumplimiento	Auditoría financiera	Gerencia del cliente
1. Confeccionar el contrato				**R**	
2. Firmar el contrato				**R**	**R**
3. Realizar la cotización	**R**			**I**	
4. Acepta cotización	**I**			**R**	
5. Calendarizar la revisión	**R**	**I**	**I**	**I**	**I**

	Gerente de IT Audit	Auditor	Oficial de cumplimiento	Auditoría financiera	Gerencia del cliente
6. Coordinar reunión con el cliente	**I**	**R**	**I**		
7. Enviar requerimientos al cliente		**R**			
8. Programar reuniones y entrevistas		**I**	**R**		
9. Preparar información solicitada		**I**	**R**		
10. ¿La evidencia se encuentra completa?		**R**	**I**		
11. Comunicar problemas	**I**	**R**	**I**		
12. Evaluar procedimientos de diseño para el control	**I**	**R**			
13. ¿Los procedimientos de diseño son correctos?	**C**	**R**			
14. Documentar los procedimientos de diseño del control o hallazgos identificados	**I**	**R**			
15. Evaluar procedimientos de eficacia operativa	**C**	**R**			
16. ¿Los procedimientos de diseño son correctos?	**I**	**R**			
17. Documentar los procedimientos de eficacia del control o hallazgos identificados	**R**	**I**			
18. Revisar el memorando	**R**	**I**			
19. ¿Hay observaciones?	**R**	**I**			
20. Confeccionar informe	**C**	**R**			
21. ¿Aprueba el informe?	**R**	**I**			
22. ¿Acepta el informe?			**R**		**I**
23. Corregir informe	**C**	**R**			

	Gerente de IT Audit	Auditor	Oficial de cumplimiento	Auditoría financiera	Gerencia del cliente
24. Comunicar resultados y retroalimentación	**R**	**C**		**I**	
25. Presentar los resultados	**I**			**R**	
26. Almacenar la información en el repositorio				**R**	
27. Limpiar documentos	**I**	**R**			
28. Documentar lecciones aprendidas	**I**	**R**		**I**	

Tabla 37. Matriz RACI

Adicionalmente, para brindar un mayor detalle a continuación, se presenta el detalle de los controles diseñados para cubrir los objetivos de la revisión realizada por el departamento de *IT Audit* con respecto a las auditorías de cumplimiento de la ley Nº8204.

5.1.3. AML01 - Configuración de la clasificación del riesgo de los clientes

Este control aborda el artículo 6 sobre el análisis de las alertas generadas de los programas informáticos del acuerdo SUGEF 12-10, donde se consideran dos procedimientos para el diseño y tres para la prueba de eficacia operativa, tal como se muestra en la Figura 13.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de TI sobre el diseño e implementación de la metodología aprobada para la clasificación del riesgo de los clientes. 2. **Indagar** con el personal de TI e **inspeccionar** cuáles criterios o variables fueron implementados en los sistemas, que como mínimo incluyan las siguientes: nacionalidad, país de origen, país de domicilio, profesión u oficio,zona geográfica, actividad económica, estructura de propiedad, tipos de activos propios de la actividad del cliente, origen de los recursos, utilización de efectivo, tipo, monto y frecuencia de las transacciones.	1. Metodología aprobada para la clasificación del riesgo de los clientes. 2. Lista de variables implementadas en el sistema.	a1. Los cambios efectuados en la configuración del control, fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración del cálculo del perfil de riesgo de los clientes; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con el cálculo de clasificación del riesgo. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
		a2. La clasificación del riesgo se realiza de acuerdo con la metodología aprobada para tal fin.	TOEa2. **Inspeccionar** el sistema para determinar la forma en la que los valores se encuentran parametrizados y cómo influyen en la categorización de los clientes.	1. Capturas de pantalla con la lista de variables implementadas en el sistema, y su asignación de peso.
		a3. Existe una diferenciación de las relaciones con los clientes, para lo cual se utilizan al menos tres categorías (Alto, medio, bajo).	TOEa3. Definir una muestra de clientes físicos y juridicos de cada categoría (alto, medio, bajo), y crearlos en una ambiente de pruebas para **observar** que la clasificación de riesgo funcione correctamente.	1. Capturas de pantalla de las pruebas realizadas.

Figura 13. AML01 - Configuración de la clasificación del riesgo de los clientes

5.1.4. AML02 - Configuración del monitoreo continuo.

Este control aborda el artículo 16 sobre programas informáticos del acuerdo SUGEF 12-10, donde se consideran dos procedimientos para el diseño y tres para la prueba de eficacia operativa, tal como se muestra en la Figura 14.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento las políticas o procedimientos relaciondas con el monitoreo de los clientes. 2. **Indagar** con el personal de TI e **inspeccionar** cuáles programas fueron implementados el monitoreo continuo del perfil transaccional del cliente, productos o servicios de alto riesgo y listas de personas vinculadas con organizaciones terroristas o lavado de dinero.	1. Políticas y procedimientos de monitoreo de clientes. 2. Captura de pantalla del sistema con la lista de alertas implementadas en este.	a1. Los cambios efectuados en la configuración del control, fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubieron cambios significativos en la configuración de los programas para alertar sobre determinar transacciones que se desvíen del comportamiento esperado del cliente, productos o servicios de alto riesgo y listas de personas vinculadas con organizaciones terroristas o lavado de dinero; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con la configuración de alertas. 2. Aprobación de los cambios realizados a la configuración del alertas.
		a2. Los programas de monitoreo continuo, generan automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.	TOEa2. **Observar** el funcionamietno de los programas para determinar que están operando efectivamente de forma que generen automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.	1. Capturas de pantalla de las pruebas realizadas.
		a3. Los reportes generados sobre alertas registran al menos los datos: a) Datos personales. b) Histórico transaccional. c) Relación existente de las cuentas de cada cliente con las de otros clientes u otros productos y servicios dentro de la institución, sea esta de tipo patrimonial, comercial o de parentesco, si la hubiere. d) Históricos de las categorías de riesgo asignadas a cada cliente. e) Alertas generadas.	TOEa3. Definir una muestra de reportes sobre la cual, **inspeccionar** que cuenten con al menos los datos: a) Datos personales. b) Histórico transaccional. c) Relación existente de las cuentas de cada cliente con las de otros clientes u otros productos y servicios dentro de la institución, sea esta de tipo patrimonial, comercial o de parentesco, si la hubiere. d) Históricos de las categorías de riesgo asignadas a cada cliente. e) Alertas generadas.	1. Muestra de reportes.

Figura 14. AML02 - Configuración del monitoreo continuo

5.1.5. AML03 – Seguimiento de alertas

Este control aborda el artículo 17 sobre el análisis de las alertas generadas de los programas informáticos del acuerdo SUGEF 12-10, donde se consideran dos procedimientos para el diseño y tres para la prueba de eficacia operativa, tal como se muestra en la Figura 15.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento de qué manera se revisan las alertas. 2. **Indagar** con el personal de cumplimiento el proceso para descartar transacciones inusuales, y si se registra el motivo, documento respaldo y responsable.	1. Políticas y procedimientos de monitoreo de clientes. 2. Lista de alertas configuradas. 3. Manual de cumplimiento.	a1. Se cuenta con alertas activas sobre transacciones inusuales.	TOEa1. Definir una muestra sobre las alertas generadas, e **inspeccionar** los campos registrados.	1. Bitácora de alertas de transacciones que desvíen el comportamiento del cliente.
		a2. Cuando se descarta una alerta, se registra el motivo, documento respaldo y responsable.	TOEa2. Definir una muestra de transacciones inusuales descartadas, para **inspeccionar** que registren el motivo, documento respaldo y responsable.	1. Muestra de transacciones inusuales descartadas.
		a3. Las alertas funcionan de acuerdo al funcionamiento esperado.	TOEa3. Definir una muestra de alertas y **observar** su adecuado funcionamiento en un ambiente de pruebas.	1. Capturas de pantalla de las pruebas realizadas.

Figura 15. AML03 – Seguimiento de alertas

5.1.6. AML04 - Configuración de bitácoras

Este control aborda el artículo 18 del acuerdo SUGEF 12-10, con respecto a bitácoras, donde se consideran dos procedimientos para el diseño y tres para la prueba de eficacia operativa, tal como se muestra en la Figura 16.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento los lineamientos que deben cumplir las bitácoras de acuerdo a lo indicado por la Superintendencia. 2. **Indagar** con el personal de TI e **inspeccionar** de qué manera se encuentran implementadas las bitácoras, considerando: a. Nombre de las tablas de la base de datos. b. Detalle de los campos que se registran.	1. Lineamientos de bitácoras emitidos por la Superintendencia. 2. Captura de pantalla de la consulta. 3. Políticas de retención de datos.	a1. Los cambios efectuados en la configuración del control, fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración de las bitácoras de acceso y uso del sitio de banca electrónica; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con la configuración de bitácoras. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
		a2. Las bitácoras regitran el acceso y uso del sistema de banca electrónica.	TOEa2. **Observar** en un ambiente de pruebas la funcionalidad de las bitácoras, ingresando con un usuario al sistema de banca electrónica y realizando transferencias.	1. Capturas de pantalla de las pruebas realizadas.

Figura 16. AML04 – Configuración de bitácoras

5.1.7. AML05 - Registro de transacciones únicas

Este control aborda el artículo 19 del acuerdo SUGEF 12-10, con respecto al registro de transacciones únicas, donde se considera un procedimiento para el diseño y dos para la prueba de eficacia operativa, tal como se muestra en la Figura 17.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento si las transacciones únicas el proceso de registro de los formularios electrónicos.	1. Politica o procedimiento para el registro de transacciones únicas.	a1. Los formularios de registro de transacciones únicas incluyen todos los campos requeridos.	TOEa1. Definir una muestra de formularios sobre la cual, **inspeccionar** que cuenten con al menos los datos: - Datos de la persona que físicamente realiza la transacción. - Datos de la persona a cuyo nombre realiza la transacción. - Descripción de la transacción. - Origen de los recursos. - Nombre del funcionario que tramita la transacción. - Firma de la persona que físicamente realiza la transacción (se podrá utilizar las bases de datos de entidades públicas o se debe obtener la copia del	1. Formularios con el registro de transacciones únicas.
		a2. Las transacciones únicas son registradas en los formularios para tal fin.	TOEa2. **Observar** en un ambiente de pruebas el registro de transacciones únicas.	1. Capturas de pantalla de las pruebas realizadas.

Figura 17. AML05 – Registro de transacciones únicas.

5.1.8. AML06 - Registro de transacciones múltiples

Este control aborda el artículo 20 del acuerdo SUGEF 12-10, con respecto al registro de transacciones múltiples, donde se considera un procedimiento para el diseño y dos para la prueba de eficacia operativa, tal como se muestra en la Figura 18.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento si las transacciones múltiples el proceso de registro de los formularios electrónicos.	1. Politica o procedimiento para el registro de transacciones múltiples.	a1. Los formularios de registro de transacciones múltiples incluyen todos los campos requeridos. - Nombre completo o razón social. - Teléfono. - Fecha de nacimiento o constitución. - Número de identificación. - Tipo de identificación. - Descripción de las transacciones. Asimismo para cada una de estas transacciones deberá quedar constancia de: - Fecha, tipo, medio de pago utilizado, número de operación, moneda, monto individual y monto total.	TOEa1. Definir una muestra de formularios sobre la cual, **inspeccionar** que cuenten con al menos los datos: - Nombre completo o razón social. - Teléfono. - Fecha de nacimiento o constitución. - Número de identificación. - Tipo de identificación. - Descripción de las transacciones. Asimismo para cada una de estas transacciones deberá quedar constancia de: - Fecha, tipo, medio de pago utilizado, número de operación, moneda, monto individual y monto total.	1. Fórmularios con el registro de transacciones múltiples.
		a2. Las transacciones múltiples son registradas en los formularios para tal fin.	TOEa2. **Observar** en un ambiente de pruebas el registro de transacciones múltiples.	1. Capturas de pantalla de las pruebas realizadas.

Figura 18. AML06 – Registro de transacciones múltiples.

5.1.9. AML07 - Registro de transacciones electrónicas

Este control aborda el artículo 19 bis del acuerdo SUGEF 12-10, con respecto al registro de transacciones electrónicas únicas o múltiples, donde se consideran dos procedimientos para el diseño y cuatro para la prueba de eficacia operativa, tal como se muestra en la Figura 19.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento y/o con el personal de TI si las transferencias desde y hacia el exterior realizadas, se registran automáticamente e incluyen al menos: a) Datos de la persona cuyo nombre se realiza la transacción. b) Descripción de la transacción Contraparte en el exterior a) Información requerida sobre el originador b) Información requerida sobre el beneficiario. 2. **Indagar** con el personal de TI si existen bitácoras para registrar los movimientos de transferencias electrónicas.	1. Política o procedimiento sobre controles de ejecución, rechazo o suspención de las transacciones electrónicas cuando se detecte actividad sospechosa.	a1. Los cambios efectuados en la configuración del control, fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración de controles de ejecución, rechazo o suspensión de las transacciones automáticas cuando se detecte actividad sopechosa; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con la configuración de controles de ejecución, rechazo o suspención de transacciones electrónicas. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
		a2. Se cuenta con controles implementados para la ejecución, rechazo o suspensión de las transacciones electrónicas.	TOEa2. **Inspeccionar** en el sistema los controles relacionados con la ejecución, rechazo o suspensión de transacciones cuando se determina actividad sospechosa.	1. Capturas de pantalla de los controles configurado.
		a3. Los formularios de registro de transacciones únicas incluyen todos los campos requeridos.	TOEa3. Definir una muestra de formularios sobre la cual, **inspeccionar** que cuenten con al menos los datos: - Datos de la persona a cuyo nombre realiza la transacción. - Descripción de la transacción. - Información requerida sobre el originador - Información requerida sobre el beneficiario.	1. Fórmularios con el registro de transacciones electrónicas.
		a4. Las bitácoras regitran los movimientos realizados por transferencias.	TOEa4. **Inspeccionar** la funcionalidad de las bitácoras, y verificar los registros relacionados.	1. Bitácoras de registro de transferencias electrónicas.

Figura 19. AML07 – Registro de transacciones electrónicas

5.1.10. AML08 - Canales electrónicos

Este control aborda el artículo 38 bis del acuerdo SUGEF 12-10, con respecto al registro de transacciones múltiples, donde se considera un procedimiento para el diseño y dos para la prueba de eficacia operativa, tal como se muestra en la Figura 20.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento las políticas y procedimientos relacionadas con transferencias electrónicas. 2. **Indagar** con el personal de TI e **inspeccionar** cual es la lista de canales y transacciones electrónicas que automatiza la entidad.	1. Políticas y procedimientos relacionadas con transferencias electrónicas. 2. Lista de canales y transacciones electrónicas automátizadas	a1. Los cambios efectuados en la configuración del control, fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubieron cambios significativos relacionados con los servicios de transacciones por medio del sitio web; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con los servicios de transacciones por medio del sitio web. 2. Aprobación de los cambios realizados a la configuración del alertas.
		a2. Los programas de monitoreo continuo, generan automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.	TOEa2. **Inspeccionar** que las políticas sobre los servicios de transacciones electrónicas se encuentren implementadas.	1. Capturas de pantalla de la implementación de políticas.

Figura 20. AML08 - Canales electrónicos.

5.1.11. AML09 - Remisión a Superintendencias

Este control aborda el artículo 21 del acuerdo SUGEF 12-10, con respecto al registro de transacciones múltiples, donde se considera un procedimiento para el diseño y dos para la prueba de eficacia operativa, tal como se muestra en la Figura 21.

Evaluación del diseño e implementación		Evaluación de eficacia operativa		
Procedimientos	**Evidencia**	**Atributo**	**Procedimientos**	**Evidencia**
1. **Indagar** con el personal de cumplimiento el proceso de envío a las Superintendencias del reporte de las transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario, ya sean únicas o múltiples, que igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otra moneda.	1. Politica o procedimiento para el envío del reporte de transacciones realizadas por sus clientes a la Superintendencia.	a1. Los formularios de registro de transacciones únicas o múltiples, son congruentes e incluyen todos los campos requeridos.	TOEa1. Definir una muestra de formularios sobre la cual, **inspeccionar** que los datos sean congruentes a los registrados en el sistema y que cuenten con al menos los datos: - Nombre completo o razón social. - Número de identificación. - Tipo de identificación. - Monto del egreso o ingreso - Tipo de operación. - Fecha. - Detalle de la transacción. - Origen de los recursos. - Nombre o código de la entidad.	1. Fórmularios con el registro de transacciones únicas o múltiples.
2. **Indagar** el personal de TI y/o el oficial de cumplimiento, si se utilizan herramientas automatizadas para la generación de las transacciones ya sean únicas o múltiple.		a2. El reporte es emitido a la Superintendencia dentro de los 20 días naturales posteriores al cierre mensual.	TOEa2. **Inspeccionar** la configuración y envío de los reportes a las Superintendencias; y validar que sea dentro de los 20 días posteriores al cierre mensual.	1. Capturas de pantalla de las pruebas realizadas.
			TOEa3. Inspeccionar el sistema para validar que la consulta o delimitación del reporte generado se limite a transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario	1. Capturas de pantalla de las pruebas realizadas.

Figura 21. AML09 – Remisión a Superintendencias.

5.1.12. Cumplimiento de las mejores prácticas COBIT 2019

En la Tabla 38, se indican cuáles son las prácticas de los procesos de gestión de controles de procesos de negocio que son incorporadas dentro de la propuesta de controles para la revisión del cumplimiento de la ley Nº8204.

Práctica de Gestión	Actividades	Cumple	No cumple
DSSA06.01 Alinear actividades de control embebidas en los procesos de negocio con los objetivos corporativos.	Identificar y documentar las actividades de control de los procesos de negocio claves para satisfacer los requerimientos de control para los objetivos estratégicos, operacionales, de informes y cumplimiento.	X	
	Priorizar las actividades de control basadas en el riesgo inherente del negocio e identificar controles clave.	X	

Práctica de Gestión	Actividades	Cumple	No cumple
	Asegurar la propiedad de las actividades de control claves.	X	
	Supervisar continuamente las actividades de control de extremo a extremo para identificar oportunidades de mejora.	X	
	Mejorar continuamente el diseño y operación de los controles de procesos de negocio.	X	
DSSA06.02 Controlar el procesamiento de la información.	Crear transacciones por individuos autorizados siguiendo los procedimientos establecidos, incluyendo, cuando sea apropiado, la adecuada segregación de tareas en relación con el origen y aprobación de esas transacciones.		X
	Autenticar la fuente de las transacciones y verificar que él o ella tiene la autoridad para originar las transacciones.		X
	Introducir transacciones en el momento oportuno. Verificar que las transacciones son precisas, completas y válidas. Validar los datos de entrada y la edición o, cuando sea aplicable, la devolución para su corrección tan cerca al punto de origen como sea posible.	X	
	Corregir y reenviar datos cuya entrada fue erróneamente aceptada, sin comprometer los niveles de autorización de la transacción original. Cuando sea apropiado para la reconstrucción, conservar los documentos fuentes originales durante tiempo apropiado.		X
	Mantener la integridad y validez de los datos a través del ciclo de procesamiento.	X	
	Mantener la integridad de los datos durante interrupciones no esperadas en el procesamiento de negocio y confirmar la integridad de los datos después de los fallos de procesamiento.	X	
	Manejar la salida de una forma autorizada, entregarla al beneficiario apropiado y proteger la	X	

Práctica de Gestión	Actividades	Cumple	No cumple
	información durante la transmisión. Verificar la precisión y completitud de la salida.		
	Antes de pasar datos de la transacción entre las aplicaciones internas y las funciones operacionales o de negocio (dentro o fuera de la organización), comprobar el correcto direccionamiento, autenticidad de origen e integridad del contenido. Mantener la autenticidad e integridad durante la transmisión o la generación del informe.	X	
DSSA06.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	Asignar roles y responsabilidades sobre la base de la descripción aprobada de puestos y actividades de procesos de negocio asignada		X
	Asignar niveles de autoridad para la aprobación de transacciones, límites y cualquier otra decisión relativa a los procesos de negocio, basadas en los roles de trabajo aprobados.		X
	Asignar derechos de acceso y privilegios solo sobre lo que es necesario para ejecutar las actividades de trabajo, basados en los roles de puesto predefinidos. Eliminar o revisar los derechos de acceso inmediatamente si el rol del puesto cambia o un miembro del personal deja el área de proceso de negocio. Revisar periódicamente para asegurar que el acceso es adecuado para las actuales amenazas, riesgos, tecnología y necesidades del negocio.		X
	Asignar roles para las actividades sensibles de manera que haya una segregación clara de funciones.		X
	Proporcionar concienciación y formación en relación con los roles y responsabilidades de forma regular para que todo el mundo entienda sus responsabilidades; la importancia de los controles; y la integridad, confidencialidad y		X

Práctica de Gestión	Actividades	Cumple	No cumple
	privacidad de la información de la empresa en todas sus formas.		
	Revisar periódicamente las definiciones de control de acceso, registros e informes de excepciones para asegurar que todos los privilegios de acceso son válidos y están alineados con el personal actual y sus roles asignados.		X
DSSA06.04 Gestiona errores y excepciones.	Definir y mantener procedimientos para asignar propiedad, corregir errores, remplazar errores y manejar las condiciones fuera de equilibrio.	X	
	Revisar errores, excepciones y desviaciones.	X	
	Hacer seguimiento, corregir, aprobar y reenviar documentos fuente y transacciones.	X	
	Mantener evidencia de las medidas correctivas.	X	
	Informar acerca de errores de proceso de información relevantes de manera oportuna para realizar el análisis de tendencias y causas raíz.	X	
DSSA06.05 Asegurar la trazabilidad de los eventos, responsabilidades y la información.	Definir requerimientos de retención, basados en los requerimientos de negocio, para conocer las necesidades operativas, de reporte financiero y cumplimiento.	X	
	Capturar la fuente de información, evidencia que la soporta y el registro de las transacciones.	X	
	Eliminar la fuente de información, la evidencia que la soporta y el registro de transacciones de acuerdo con la política de retención.	X	
DSSA06.06 Asegurar los activos de la información.	Aplicar las políticas de clasificación de datos y uso aceptable y seguridad y los procedimientos para proteger los activos de información bajo el control del negocio.		X

Tabla 38. Check list de cumplimiento del proceso DDS06 COBIT 2019

En la Tabla 39, se indican cuáles son las prácticas de los procesos de gestión de cambios son incorporadas dentro de la propuesta de controles para la revisión del cumplimiento de la ley Nº8204.

Práctica de Gestión	Actividades	Cumple	No cumple
BAI06.01 Evaluar, priorizar y autorizar peticiones de cambio.	Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y TI soliciten cambios. Asegurar que todos estos cambios surgen solo a través del proceso de gestión de peticiones de cambio.	X	
	Categorizar todas las peticiones de cambio y relacionarlas con los elementos de configuración afectados.	X	
	Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, así como razones contractuales, legales o de regulación que motivan el cambio.	X	
	Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio o partes interesadas.	X	
	Planificar y programar todos los cambios aprobados.	X	
BAI06.02 Gestionar cambios de emergencia.	Asegurar que hay un procedimiento documentado para declarar, evaluar, aprobar de forma preliminar, autorizar una vez hecho el cambio y registrar el cambio de emergencia.	X	
	Verificar que los accesos de emergencia acordados para realizar cambios están debidamente autorizados y son revocados una vez se ha aplicado el cambio.		X
	Supervisar todos los cambios de emergencia y realizar revisiones posteriores a la implementación.		X
	Definir qué constituye un cambio de emergencia.	X	
BAI06.03 Hacer seguimiento e informar de cambios de estado	Categorizar las peticiones de cambio en el proceso de seguimiento.	X	
	Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento.		X

Práctica de Gestión	Actividades	Cumple	No cumple
	Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo con su prioridad.		X
	Mantener un sistema de seguimiento e informe de todas las peticiones de cambio.	X	
BAI06.04 Cerrar y documentar los cambios	Incluir los cambios en la documentación en el procedimiento de gestión del cambio como parte integral del cambio.	X	
	Definir un periodo apropiado de conservación de la documentación del cambio-		X
	Someter la documentación a la misma revisión que el cambio en sí mismo.	X	

Tabla 39. Check list de cumplimiento del proceso BAI06 COBIT 2019

5.2. Análisis financiero

En el presente apartado se muestra el análisis que determinará la viabilidad y rentabilidad financiera del proyecto; para lo cual, se estimó el costo de la propuesta de acuerdo con valoraciones en la industria e indagación con el departamento de recursos humanos de la Firma. En la Figura 22, se indica el aumento salarial anual, los salarios aproximados de los asistentes y el gerente sénior, y también el salario promedio del equipo de *IT Audit.*

Insumos

Aumento del salario anual de la Firma	5%

	Por hora	Duración en horas	Total
Costo de una auditoría financiera de TI	₡ 21.233,54	40	₡ 849.341,64

Salario recursos		
Recurso	Salario mensual	Salario por hora
Estudiante	₡ 700.000,00	₡ 4.375,00
Gerente Senior	₡ 1.323.370,00	₡ 8.271,06
Personal IT Audit	₡ 700.000,00	₡ 4.375,00

Figura 22. Datos iniciales para el análisis financiero

Con los datos anteriores, se procedió a calcular el costo del desarrollo de la propuesta considerando las 40 horas invertidas del estudiante y las cinco horas del gerente sénior; posteriormente, se calculó el costo de capacitar al personal promediando el salario de los integrantes del equipo de *IT Audit,* y estimando una duración de cuatro horas de entrenamiento.

En la Figura 23, se indican el costo de la propuesta y la capacitación al personal sobre el uso de la herramienta para las revisiones de cumplimiento de la ley Nº8204, se determinó que la propuesta requiere una inversión inicial de ₡ 2.876.355,31.

Inversión inicial	Costo de la propuesta	Capacitación
	₡ 2.666.355,31	₡ 210.000,00

Figura 23. Inversión inicial

Posteriormente, se procedió a validar con el Colegio de Contadores Públicos el costo por hora realizar una auditoría externa financiera, de TI o cumplimiento. (Colegio de Contadores Públicos, 2020)

En la Figura 24, se elabora un flujo de efectivo para tres años considerando elaborar un proyecto el primer año, cinco proyectos el segundo y finalmente siete proyectos el tercer año. Donde se considera la ganancia anual considerando el tiempo de ejecución de cada auditoría.

		Año 1	Año 2	Año 3	Total
Ingreso anual	Cantidad de proyectos	1	5	7	13
	Ingreso anual	₡ 849.341,64	₡ 4.246.708,20	₡ 5.945.391,48	############
	Gerente Senior	₡ 1.323.370,00	₡ 1.389.538,50	₡ 1.459.015,43	
	Personal IT Audit	₡ 700.000,00	₡ 735.000,00	₡ 771.750,00	
	Gerente Senior	₡ 8.271,06	₡ 8.684,62	₡ 9.118,85	
	Personal IT Audit	₡ 4.375,00	₡ 4.593,75	₡ 4.823,44	

		Inversión inicial	Año 1	Año 2	Año 3	
Flujo de ejectivo	Desarrollo	₡ 2.666.355,31				
	Capacitación	₡ 210.000,00				
	Costos operativos	₡ -	₡ 175.000,00	₡ 918.750,00	₡ 964.687,50	
	Total	₡ 2.876.355,31	₡ 3.051.355,31	₡ 918.750,00	₡ 964.687,50	₡ 4.934.792,81

Figura 24. Flujo de efectivo

El análisis para determinar la viabilidad financiera del presente trabajo final de graduación se observa en el Apéndice O. En la Figura 25, se presentan los indicadores de rentabilidad de la inversión.

ROI	284%
VAN	₡ 73.299,00
TIR	44%

Figura 25. Indicadores de la propuesta

i. ROI

Con respecto a este indicador la propuesta es viable dado que para el caso propuesto se cuenta con un retorno del 2,84% del monto invertido en el desarrollo y capacitación del personal para implementar la propuesta que se desarrolló en este trabajo final de graduación.

ii. VAN

Por su parte este indicador permite valorar la viabilidad y rentabilidad de los proyectos, dado que el resultado 73.299,00 es positivo, es viable realizar el proyecto, pues quiere decir que refleja ganancia.

iii. TIR

Una tasa interna de retorno de 44% nos indica que se obtiene beneficio de la inversión; por lo tanto, el proyecto es viable de realizar.

iv. Valoración de resultados

Del análisis anterior, se determina que el proyecto es viable de realizar pues genera ganancia con una tasa de retorno de 2,84%. Adicionalmente, el proyecto pretende generar beneficios no financieros que no han sido cuantificados en la propuesta, tales como:

- Un aumento en la calidad de las auditorías.
- Eliminación de reprocesos.
- Mejora de la imagen del área de *IT Audit*
- Aumento y/o retención de clientes gracias al valor agregado brindado a las empresas cliente, a partir de resultados adecuados y precisos sobre la evaluación realizada.

Capítulo VI: Conclusiones

En este capítulo se detallan las conclusiones del Trabajo Final de Graduación con base en el logro de los objetivos específicos del proyecto, considerando los resultados obtenidos a través de la ejecución de esta investigación.

Seguidamente, se enlistan para cada objetivo específico sus respectivas conclusiones.

Para el objetivo específico 1, comprender el proceso establecido por la Firma en las auditorías de TI de cumplimiento de la Ley N°8204, para el entendimiento de este. Se concluye que:

1. En la actualidad, la Firma utiliza una herramienta basada en nueve objetivos para valorar los criterios de la ley Nº8204, donde se indica la lista de requerimientos que deben ser enviados al cliente; sin embargo, no se incluye explícitamente el detalle completo de las actividades a ejecutar durante las revisiones.

2. Actualmente el área de *IT Audit* no cuenta con una guía específica para realizar las auditorías de TI de cumplimiento de la ley Nº8204, pues, aunque los auditores con mayor experiencia entienden, no sucede lo mismo con aquellos que tienen menos experiencia, resultando en una falta de estandarización y variando la calidad de revisión de cada cliente.

Para el objetivo específico 2, determinar brechas, deficiencias y oportunidades del proceso de auditoría de TI de la ley N°8204 de la Firma contra el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI, para la identificación del estado deseado del proceso. Se concluye que:

3. De acuerdo con la información recolectada y estudiada como insumo para la investigación en cuestión, al realizar la comparación con el proceso actual, se evidencia que falta mayor detalle en la metodología empleada por los colaboradores del área de *IT Audit.*

4. Producto de la revisión de las mejores prácticas como COBIT, NIAs e incluso el Acuerdo SUGEF 12-10 Normativa de cumplimiento de la ley Nº8204, se obtuvieron insumos para fundamentar y consolidar la herramienta propuesta a la Firma.

5. Del análisis de la situación actual del proceso de revisión de la auditoría de TI de cumplimiento de la ley Nº8204 y las mejores prácticas aplicables, se obtuvo un estado deseado que definió los criterios para implementar en la herramienta propuesta.

6. A partir de las brechas identificadas, se determina como aspectos clave que las evaluaciones de la ley Nº8204 pueden brindar mejores resultados, con orientación al cumplimiento de la regulación por parte de los clientes evaluados.

Para el objetivo 3, proponer un conjunto de controles y procedimientos del proceso de auditoría de TI de la ley N°8204 de la Firma, para el cumplimiento del estado deseado del proceso y generación de valor a la organización auditada. Se concluye:

7. Como resultado de la investigación, se desarrolló una propuesta que incluye los elementos considerados en los controles para mejorar el proceso al estado deseado.

8. La herramienta propuesta e s fácil de utilizar y está orientada a que los colaboradores del área de *IT Audit,* independientemente del grado de experiencia, puedan aplicarla conservando el mismo grado de calidad en las revisiones de todos los clientes evaluados.

9. La propuesta incluye los procedimientos de auditoría para evaluar los artículos del acuerdo SUGEF 12-10 norma para el cumplimiento de la ley Nº8204, generando una facilidad de aplicación en los colaboradores del área de IT Audit.

Para el objetivo 4, construir el modelo económico de la propuesta del proceso de auditoría TI de la ley N°8204, por medio de valoraciones financieras basadas en la industria y otras fuentes, para la obtención de un aproximado del impacto financiero que conllevan los beneficios y costos de esta. Se concluye que:

10. De los resultados obtenidos de la propuesta económica, se determinó la viabilidad de este proyecto dado que se obtendrá una rentabilidad de ₡81.688,49 en tres años plazo.

11. Según el modelo económico de la propuesta, se determina que el proyecto es viable de realizar pues presenta indicadores de inversión positivos; además, otorga beneficios que no han sido cuantificados, como estandarizar el mismo nivel de calidad en las revisiones para los clientes.

Capítulo VII: Recomendaciones

En este capítulo se detallan las recomendaciones del Trabajo Final de Graduación, las cuales provienen del cumplimiento de los objetivos específicos y las conclusiones descritas en el capítulo anterior.

Dicho capítulo tiene como propósito que las recomendaciones sean aceptadas por el área de *IT Audit* y aplicadas en futuras auditorías de TI de cumplimiento de la ley Nº8204.

Seguidamente, se enlistan para cada objetivo específico sus respectivas recomendaciones.

Para el objetivo específico 1, comprender el proceso establecido por la Firma en las auditorías de TI de cumplimiento de la Ley N°8204, para el entendimiento de este. Se recomienda:

1. Comunicar y concientizar a todos los colaboradores del área de IT Audit sobre la importancia de utilizar un proceso de evaluación estandarizado y repetible de modo que los clientes reciban la misma calidad en las evaluaciones de cumplimiento de la ley Nº8204.

2. Se recomienda incluir en la fase de cierre de los proyectos de auditoría, un apartado de análisis de retroalimentación o lecciones aprendidas, que sirva como insumo para la mejora continua.

Para el objetivo específico 2, determinar brechas, deficiencias y oportunidades del proceso de auditoría de TI de la ley N°8204 de la Firma contra el marco jurídico nacional y las buenas prácticas internacionales aplicables a las auditorías de TI, para la identificación del estado deseado del proceso. Se recomienda:

3. Considerar las mejores prácticas en materias de auditoría y tecnologías de información, para estandarizar el proceso actual de revisión de la ley Nº8204.

4. Capacitar a los colaboradores en las mejores prácticas que incluye la propuesta, como lo son COBIT 2019, las NIAs y el acuerdo SUGEF 12-10 Normativa para el cumplimiento de la ley Nº8204.

Para el objetivo 3, proponer un conjunto de controles y procedimientos del proceso de auditoría de TI de la ley N°8204 de la Firma, para el cumplimiento del estado deseado del proceso y generación de valor a la organización auditada. Se recomienda:

5. Que el área de *IT Audit* elabore un plan piloto para probar el uso de la herramienta propuesta.

6. Capacitar a los colaboradores con respecto a la utilización de la herramienta propuesta para las auditorías de TI de cumplimiento de la ley Nº8204.

7. Incorporar dentro del ciclo de evaluación del área de IT Audit, la herramienta desarrollada durante este trabajo final de graduación.

Para el objetivo 4, construir el modelo económico de la propuesta del proceso de auditoría TI de la ley N°8204, por medio de valoraciones financieras basadas en la industria y otras fuentes, para la obtención de un aproximado del impacto financiero que conllevan los beneficios y costos de esta. Se recomienda:

8. El desarrollo de este proyecto pues proporcionará un estandariza del nivel de calidad en las revisiones para los clientes, durante las auditorías de la ley Nº8204; además, es viable desde un punto de vista financiero, lo cual se encuentra sustentado por el análisis económico realizado.

Capítulo VIII: Referencias

AcamsToday. (23 de Febrero de 2018). *Sondeo de viabilidad de las normas del GAFI*. Obtenido de AcamsToday: https://www.acamstoday.org/sondeo-de-viabilidad-practica-de-las-normas-del-gafi/

AcamsToday. (29 de Marzo de 2019). *Sondeo de viabilidad de las normas del GAFI*. Obtenido de AcamsToday: https://www.acamstoday.org/sondeo-de-viabilidad-practica-de-las-normas-del-gafi/

AOB. (23 de 08 de 2021). *NIAS*. Obtenido de AOB: https://aobauditores.com/nias/

AOB Auditores. (23 de 08 de 2021). *NIA 220*. Obtenido de AOB Auditores: https://aobauditores.com/nias/nia220/

AOB Auditores. (23 de 08 de 2021). *NIA 230*. Obtenido de AOB Auditores: https://aobauditores.com/nias/nia230

AOB Auditores. (23 de 08 de 2021). *NIA 240*. Obtenido de AOB Auditores: https://aobauditores.com/nias/nia240/

AOB Auditores. (23 de 08 de 2021). *NIA 500*. Obtenido de AOB Auditores: https://aobauditores.com/nias/nia500

AOB Auditores. (23 de 08 de 2021). *NIA 530*. Obtenido de AOB Auditores: https://aobauditores.com/nias/nia530

Asociación Española para la Calidad. (22 de 04 de 2019). *DIAGRAMA SIPOC*. Obtenido de Asociación Española para la Calidad: https://www.aec.es/web/guest/centro-conocimiento/diagrama-sipoc

Auditool. (17 de mayo de 2017). *La Auditoría y el Auditor en el Entorno de los Negocios*. Obtenido de www.auditool.org: https://www.auditool.org/blog/auditoria-externa/5328-la-auditoria-y-el-auditor-en-el-entorno-de-los-negocios

Auditool. (24 de 05 de 2019). *Auditoría en Prevención del Lavado de Dinero*. Obtenido de Auditool: https://www.auditool.org/blog/fraude/3229-auditoria-en-prevencion-del-lavado-de-dinero

Azofeifa, A. (30 de Noviembre de 2016). *Blanqueo de activos: la experiencia costarricense*. Obtenido de Investiga UNED: https://investiga.uned.ac.cr/revistas/index.php/espiga/article/view/1663/1884

Banco de Pagos Internacionales. (enero de 2013). *Carta Estatuaria.* Obtenido de Banco de Pagos Internacionales: https://www.bis.org/bcbs/charter_es.pdf

Banco Mundial. (14 de Febrero de 2014). *La lucha contra el "dinero sucio" y los flujos monetarios ilícitos para reducir la pobreza*. Obtenido de Banco Mundial: http://www.bancomundial.org/es/results/2013/04/04/helping-countries-establish-transparent-financial-systems-and-robust-mechanisms-for-asset-recovery

BBVA. (21 de mayo de 2020). *Finanzas para todos, los títulos de valores, letras de cambio,cheque y pagare*. Obtenido de BBVA: https://www.bbva.com/es/finanzas-para-todos-los-titulos-valores-letra-de-cambio-cheque-y-pagare/

Cabrera Libuy, R. (22 de 04 de 2019). *¿Cómo hacer un Mapeo de Procesos SIPOC?* Obtenido de Linkedin: https://www.linkedin.com/pulse/c%C3%B3mo-hacer-un-mapeo-de-procesos-sipoc-rolando-cabrera-libuy

CEUPE. (24 de 05 de 2019). *Responsabilidades de los particpantes en la auditoría*. Obtenido de CEUPE: https://www.ceupe.com/blog/cuales-son-las-responsabilidades-de-los-participantes-en-la-auditoria.html

Cheong, W., & Nicoll, A. (s.f.).

Colegio de Contadores Públicos. (2020). *Aviso de tarifas*. Obtenido de https://ccpa.or.cr/wp-content/themes/maximus/pdf/normativa-vigente/tarifa/aviso-tarifas.pdf

ConceptoDefinición.De. (23 de marzo de 2019). *ConceptoDefinición.De*. Obtenido de ConceptoDefinición.De: https://conceptodefinicion.de/calidad/

Deloitte. (2016). Auditoría de información financiera histórica: Principios y responsabilidades generales - Segunda parte. *Revista Digital de Aseguramiento*, https://www2.deloitte.com/content/dam/Deloitte/co/Documents/audit/revistadigital/RDANo7F.pdf. Obtenido de https://www2.deloitte.com/content/dam/Deloitte/co/Documents/audit/revistadigital/RDANo7F.pdf

Difiere. (23 de Marzo de 2019). *Aseguramiento, control y calidad*. Obtenido de Difiere: https://difiere.com/diferencia-aseguramiento-control-calidad/

Donoso, A. (30 de junio de 2017). *Informe de auditoría*. Obtenido de Economipedia: https://economipedia.com/definiciones/informe-de-auditoria.html

Dumas, M., Rosa, M. L., Mendelling, J., & Reijers, H. A. (2018). *Fundamentals of Business Process Management .* Berlin: Springer.

Escuela Europea. (23 de Marzo de 2019). *Principios de la gestión de la calidad*. Obtenido de Escuela Europea Excelencia: https://www.escuelaeuropeaexcelencia.com/2017/12/los-7-principios-de-la-gestion-de-la-calidad/

Federico, C. (29 de Marzo de 2019). *Economía Sumergida*. Obtenido de Economipedia: https://economipedia.com/definiciones/economia-sumergida.html

Firma, L. (2020). *¿Quiénes somos?* Obtenido de Sitio web de la firma de auditoría

Fondo Monetario Internacional. (21 de marzo de 2016). *El FMI y la lucha contra el lavado de dinero y el financiamiento del terrorismo*. Obtenido de Fondo Monetario Internacional: https://www.imf.org/es/About/Factsheets/Sheets/2016/08/01/16/31/Fight-Against-Money-Laundering-the-Financing-of-Terrorism

Freund, J., Rucker, B., & Hitpass, B. (2014). BPMN 2.0 Manual de Referencia y Guía Práctica (4ta. Edición ed.). Santiago, Chile: COMUNDA

Gestiopolis. (23 de Marzo de 2019). *Aseguramiento de la calidad*. Obtenido de Gestiopolis: https://www.gestiopolis.com/que-son-calidad-aseguramiento-de-la-calidad-y-control-de-calidad/

Gibson, R. G. (14 de 07 de 2015). *Forbes*. Obtenido de Las 3 etapas del lavado de diner: https://www.forbes.com.mx/las-3-etapas-del-lavado-de-dinero/

Gutiérrez, F. (20 de 10 de 2016). *Depósitos y transferencias, de lo más utilizado para lavado de dinero*. Obtenido de El economista: https://www.eleconomista.com.mx/economia/Depositos-y-transferencias-de-lo-mas-utilizado-para-lavado-de-dinero-20161020-0117.html

Guzmán, V., & Elizondo, A. (2019). Propuesta de una Guía Documental y Procedimental según la norma ISO 9001 para el proceso de ejecución de una auditoría relacionada con Anti-Money Laundering (AML) siguiendo los objetivos establecidos por el negocio, caso VYA. San José.

Hernández Sampieri, R. (2014). Metodología de la Investigación. En R. Hernández, *Metodología de la Investigación* (pág. 3). Distrito Federal, México: Mac Graw Hill.

IAASB. (2021). *NIA 330*. Obtenido de Ministerio de Ciencia, Innovación, Tecnologia y Comunicaciones: http://www.aplicaciones-mcit.gov.co/adjuntos/niif/17%20-%20NIA%20330.pdf

IAASB. (2021). *NIA 500*. Obtenido de Ministerio de Ciencia, Innovación Tecnología y Telecomunicaciones: http://www.aplicaciones-mcit.gov.co/adjuntos/niif/20%20-%20NIA%20500.pdf

ISACA. (2018). *COBIT 2019 Marco de Referencia - Objetivos de Gobierno y Gestión.* Illinois: ISACA.

ISO 9001 Calidad Total . (17 de 05 de 2019). *Estandarizar los procesos bajo la norma ISO 9001*. Obtenido de ISO 9001 Calidad Total : http://iso9001-calidad-total.com/como-estandarizar-los-procesos-bajo-la-norma-iso-9001/

La Firma. (2020). *¿Quiénes somos?* Obtenido de Sitio web de la Firma

Lopez, P. (31 de Marzo de 2016). *Novedades ISO 9001:2015.* Madrid, España: Fundación Confemetal. Obtenido de Normas 9000: http://www.normas9000.com/content/que-es-iso.aspx

Meskovska, A. (22 de 04 de 2019). *Cómo estructurar la documentación del sistema de gestión de calidad*. Obtenido de Advisera Expert Solutions Ltd: https://advisera.com/9001academy/es/knowledgebase/como-estructurar-la-documentacion-del-sistema-de-gestion-de-calidad/

Nueva ISO 9001. (23 de Marzo de 2019). *Conceptos básicos gestión de calidad*. Obtenido de Nueva ISO 9001: https://www.nueva-iso-9001-2015.com/2018/07/conoce-conceptos-basicos-gestion-de-calidad/

Nuño, P. (17 de 03 de 2019). *La auditoría interna*. Obtenido de EmprendePyme.net: https://www.emprendepyme.net/auditoria-interna.html

OAS. (16 de 05 de 2014). *Lavado Activos*. Obtenido de OAS: http://www.oas.org/es/ssm/ddot/publicaciones/LIBRO%20OEA%20LAVADO%20ACTIVOS%202018_4%20DIGITAL.pdf

OroyFinanzas.com. (26 de Mayo de 2015). *¿Qué es Anti-Money Laundering (AML) o prevención de blanqueo de capitales (PBC)?* Obtenido de OroyFinanzas.com: https://www.oroyfinanzas.com/2015/05/que-anti-money-laundering-aml-prevencion-blanqueo-capitales/

OroyFinanzas.com. (24 de Febrero de 2019). *¿Qué es Anti-Money Laundering (AML) o prevención de blanqueo de capitales (PBC)?* Obtenido de OroyFinanzas.com: https://www.oroyfinanzas.com/2015/05/que-anti-money-laundering-aml-prevencion-blanqueo-capitales/

Pérez Porto, J., & Gardey, A. (2021). *Definición de Auditoría*. Obtenido de Definición de: https://definicion.de/auditoria/

Procuraduría General de la República. (06 de 04 de 2019). *Reforma integral Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo.* Obtenido de Sistema Costarricense de Información Jurídica: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=48392&nValor3=93996&strTipM=TC

Procuraduría General de la República. (06 de junio de 2021). *Sistema Costarricense de Información Jurídica*. Obtenido de Reforma integral Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=48392&nValor3=93996&strTipM=TC

Rodríguez, Ó. (18 de 03 de 2019). *Costa Rica mejora en cumplimiento de normas*. Obtenido de La nación: https://www.nacion.com/economia/politica-economica/costa-rica-mejora-en-cumplimiento-de-normas-para/JFJC7YHPS5GLNJOECASAIDBSOQ/story/

Sánchez, A. (2015). Mejora de los controles de auditoría para la revisión de la seguridad de TI. San José.

Significados . (23 de Marzo de 2019). *Significados* . Obtenido de Significados : https://www.significados.com/calidad/

Sinnaps. (8 de Abril de 2019). *Proceso mejora continua una empresa*. Obtenido de Sinnaps: https://www.sinnaps.com/blog-gestion-proyectos/proceso-mejora-continua-una-empresa

Sistemas y Calidad Total. (31 de Marzo de 2019). *Sistemas de Gestión de la Calidad*. Obtenido de Sistemas y Calidad Total:

http://www.sistemasycalidadtotal.com/calidad-total/sistemas-de-gestion-de-la-calidad-%E2%94%82-historia-y-definicion/

SUGEF. (24 de mayo de 2017). *Acuerdo SUGEF 12-10 Normativa para el cumplimiento de la ely Nº8204*. Obtenido de SUGEF Normativa Vigente: https://www.sugef.fi.cr/normativa/normativa_consulta/historico_normativa_consulta/normativa_vigente/SUGEF%2012-10%20(v13%20%2024may2017)%20SUGEF%20R-SGF-1318-2017.pdf

SUGEF. (03 de Mayo de 2019). *Normativa 2012 - 10*. Obtenido de SUGEF: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2012-10%20(v13%20%2024may2017)%20SUGEF%20R-SGF-1318-2017.pdf

UCC. (23 de Marzo de 2019). *Sistema de gestión calidad*. Obtenido de UCC Edu Co: https://www.ucc.edu.co/sistema-gestion-integral/Paginas/sistema-gestion-calidad.aspx

Uriarte, J. M. (23 de Julio de 2021). *10 características de una auditoría*. Obtenido de Características: https://www.caracteristicas.co/auditoria/

Wiley, J. (2013). *Gestión de Procesos de Negocio para Dummies.* Nueva Jersey: John Wiley & Sons Inc.

Zuazo, R. (24 de Marzo de 2021). *DESAFÍOS PWC*. Obtenido de La importancia de los controles de tecnología de la información: https://desafios.pwc.pe/la-importancia-de-los-controles-de-tecnologia-de-la-informacion/

Capítulo IX: Apéndices

9.1. Apéndice A. Plantilla de bitácora

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

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.

9.2. Apéndice B: Plantilla de solicitudes de cambio

Control de Cambios <<Número de cambio>>	
Solicitante: Número de cambio:	**Fecha:**
Descripción detallada del cambio:	
Riesgos asociados al cambio:	
Estado:	
Nombre y firma del patrocinador:	**Nombre y firma del solicitante:**

9.3. Apéndice C: Cronograma

Actividades/semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Reunión inicial con partes interesadas.	X														
2. Desarrollo del Capítulo 1	X	X													
3. Reunión 1: tutor - organización		X													
4. Entrega Capítulo 1: tutor			X												
5. Entrega Capítulo 1 revisado: estudiante				X											
6. Desarrollo del Capítulo 2				X	X										
7. Entrega Capítulo 2: tutor					X										
8. Evaluación 1: empresa					X										
9. Reunión 2: tutor - organización						X									
10. Desarrollo del Capítulo 3						X	X								
11. Entrega Capítulo 3: tutor							X								
12. Entrega Capítulo 2 y 3 revisado: estudiante								X							
13. Reunión con tutor								X							
14. Evaluación 2: empresa									X						
15. Desarrollo del Capítulo 4 y 5									X	X	X				
16. Entrega Capítulo 4 y 5: tutor											X				
17. Reunión 3: tutor - organización												X			
18. Entrega Capítulo 4 y 5 revisado: estudiante												X			
19. Reunión con tutor													X		
20. Evaluación 3: empresa													X		
21. Desarrollo del Capítulo 6												X	X		
22. Entrega Capítulo 6: tutor													X		
23. Entrega Capítulo 6 revisado: estudiante														X	
24. Reunión con tutor														X	
25. Entrega Informe final con observaciones: estudiante														X	
26. Entrega de informe final a la coordinación del TFG															X

Tabla 40. Cronograma del proyecto

9.4. Apéndice D. Entrevista semiestructurada

***Sección 1**: Planificación de auditoría de ley Nº8204*

1. Desde su perspectiva, ¿Cómo es el proceso de planificación de las revisiones 8204?
2. Describa, ¿Cuáles son los requerimientos que se solicitan al cliente?
3. Describa, ¿Cuánto tiempo disponen los auditores para llevar a cabo la auditoría?

***Sección 2**: Ejecución de auditoría de ley Nº8204*

4. Describa, ¿Cuál es el procedimiento de revisión de ley Nº8204?
5. ¿Considera que las actividades de la evaluación son suficientemente claras para que un auditor con poca experiencia pueda realizar estas revisiones sin inconvenientes?
6. ¿Considera que el proceso actual es suficientemente claro sobre qué evidencia se deben documentar para cumplir con los objetivos?
7. Describa, ¿Cuáles son los procedimientos para verificar que la revisión de una actividad cumple con los criterios definidos?
8. ¿Cuáles son las fuentes de conocimiento que sustentan las actividades ejecutadas en la revisión?
9. ¿Existe una metodología de la Firma Internacional que regule el proceso de revisión de la ley Nº8204?

***Sección 3**: Resultados de auditoría de ley Nº8204*

10. Describa, ¿Cómo se presentan los resultados?
11. Describa, ¿Cuáles son los principales inconvenientes durante el proceso de revisión o entrega de resultados?
12. ¿Considera que el proceso se encuentra estandarizado y es aplicado de la misma forma por todo el personal?
13. Describa, ¿Cuáles factores considera que necesita el proceso para ser estandarizado?
14. ¿Existe un modelo para validar la satisfacción del cliente?
15. ¿Existen prácticas de mejora continua sobre el procedimiento de revisión?
16. ¿Qué mejoras consideraría respecto al estado actual del proceso de auditoría de la ley 8204?
17. Desde su perspectiva, ¿Considera que apoyar el proceso actual con algún *framework* de TI aportaría un aumento en la calidad del proceso actual de revisión?

9.5. Apéndice E. Plantilla para revisión documental

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

Tabla 41. Plantilla revisión documental

9.6. Apéndice F. Entrevista personal IT Audit

Sección 1*: Conocimientos generales sobre el proceso de revisión de la ley Nº8204*

1. En una escala del 1 al 5, ¿Qué tan familiarizado se encuentra con la ley Nº8204?, donde 1 es "Poco familiarizado y 5 "Muy familiarizado".
2. ¿Conoce otras normas nacionales o internacionales que regulen el tema de fraude y lavado de dinero?
3. Durante su tiempo laborando para la Firma, ¿Ha realizado revisiones de la ley Nº8204?

Sección 2*: Ejecución del proceso de revisión de la ley Nº8204*

4. En una escala del 1 al 5, ¿Considera que el proceso de revisión establecido por la Firma se encuentra estandarizado y es aplicado por todo el personal?, donde 1 es "En desacuerdo" y 5 "Muy de acuerdo".
5. ¿Cuál es su percepción sobre la calidad del proceso actual?
6. En una escala del 1 al 5, ¿Considera que los pasos a seguir al ejecutar la auditoría se encuentran definidos de manera clara y puntual facilitando la evaluación de los objetivos establecidos por la Firma para la revisión 8204?, donde 1 es "En desacuerdo" y 5 "Muy de acuerdo".
7. En una escala del 1 al 5, ¿Considera que la guía actual de la Firma para ejecutar la revisión de la ley 8204 brinda información suficientemente detallada acerca de qué información y en qué formato se debe documentar para soportar los procedimientos realizados?, donde 1 es "En desacuerdo" y 5 "Muy de acuerdo".

Sección 3*: Resultados del proceso de revisión de la ley Nº8204*

8. ¿Cómo considera el grado de satisfacción del cliente con los resultados?
9. Desde su experiencia, ¿Cuáles son los principales problemas que ha tenido durante la revisión de la ley Nº8204?
10. Indique brevemente, ¿Qué aspectos cambiaría del proceso actual?
11. En una escala del 1 al 5, ¿Considera que una matriz de controles con sus respectivos procedimientos fundamentada en buenas prácticas nacionales e internacionales en términos de tecnología, fraude y lavado de dinero mejoraría el proceso de revisión?, donde 1 es "En desacuerdo" y 5 "Muy de acuerdo".

9.7. Apéndice G. Entrevista semiestructurada (aplicada)

***Sección 1**: Planificación de auditoría de ley Nº8204*

1. **Desde su perspectiva, ¿Cómo es el proceso de planificación de las revisiones 8204?**

El proceso de planificación de las revisiones 8204 se encuentra un poco desalineado, ya que no existe un tipo de ejecución como si lo hay en las auditorías estatutarias. La planificación debe ser el centro y el inicio de la ejecución, sin embargo; muchas veces es débil a la hora de iniciarse.

2. **Describa, ¿Cuáles son los requerimientos que se solicitan al cliente?**

Los requerimientos se centran en los objetivos del acuerdo 12-10, el cual muchas veces se utiliza de forma desactualizada.

3. **Describa, ¿Cuánto tiempo disponen los auditores para llevar a cabo la auditoría?**

Cuentan con alrededor de 40 horas; sin embargo, hay clientes complejos que tardan hasta 120 horas.

***Sección 2**: Ejecución de auditoría de ley Nº8204*

4. **Describa, ¿Cuál es el procedimiento de revisión de ley Nº8204?**

Este procedimiento se centra en encontrar potencialmente las brechas en las instituciones sobre el ejercicio de fraude y lavado de dinero.

5. **¿Considera que las actividades de la evaluación son suficientemente claras para que un auditor con poca experiencia pueda realizar estas revisiones sin inconvenientes?**

Me parece que no son claras también deben actualizarse ya que algunos objetivos están mal enfocados.

6. **¿Considera que el proceso actual es suficientemente claro sobre qué evidencia se deben documentar para cumplir con los objetivos?**

No, si el auditor es relativamente nuevo en el campo no podrá entender el impacto que tienen los objetivos y su resultado.

7. **Describa, ¿Cuáles son los procedimientos para verificar que la revisión de una actividad cumple con los criterios definidos?**

Los procedimientos son la indagación, la observación y la inspección sobre los objetivos del control y para las actividades deberán solicitarse muestras que muchas veces quedan a criterio del auditor por lo que no existe nada definido y puede haber un conflicto si este decide solamente revisar una cantidad determinada.

8. **¿Cuáles son las fuentes de conocimiento que sustentan las actividades ejecutadas en la revisión?**

Los auditores deben conocer la ley 8204, el acuerdo 12-10 y en muchos casos deben de leer sobre el envío de información para SUGEF, SUGESE y SUGEVAL que eso varía en torno a los días.

9. **¿Existe una metodología de la Firma Internacional que regule el proceso de revisión de la ley 8204?**

No existe.

Sección 3*: Resultados de auditoría de ley Nº8204*

10. **Describa, ¿Cómo se presentan los resultados?**

Los resultados al igual que en una auditoría estatutaria se muestran en forma de una carta estilo borrador, el comité junto al auditor revisan las deficiencias.

11. **Describa, ¿Cuáles son los principales inconvenientes durante el proceso de revisión o entrega de resultados?**

Los principales inconvenientes que se presentan son por el juicio del auditor, por ejemplo; si en el acuerdo mencionan que todos los clientes deben de tener pesos para así asignarle una categoría, pero en lugar de eso les colocan una variante distinta el auditor puede alegar que se encuentran fuera del contexto, sin embargo; la institución puede indicar que si se cumple con el requerimiento, pero desde otro punto de vista.

12. **¿Considera que el proceso se encuentra estandarizado y es aplicado de la misma forma por todo el personal?**

No, me parece que es por criterio del auditor y no hay un estándar.

13. **Describa, ¿Cuáles factores considera que necesita el proceso para ser estandarizado?**

Los papeles de trabajo, las muestras y claridad con las pruebas y actividades a ejecutarse, así como el inicio y planeación de la revisión.

14. **¿Existe un modelo para validar la satisfacción del cliente?**

Me parece que no.

15. **¿Existen prácticas de mejora continua sobre el procedimiento de revisión?**

Me parece que no.

16. **¿Qué mejoras consideraría respecto al estado actual del proceso de auditoría de la ley 8204?**

Revisión completa de objetivos y restructuración de estos.

17. **Desde su perspectiva, ¿Considera que apoyar el proceso actual con algún *framework* de TI aportaría un aumento en la calidad del proceso actual de revisión?**

Si, ya que existiría una guía y aportaría calidad al trabajo realizado.

9.8. Apéndice H. Revisión documental Metodología de la firma (aplicada)

Revisión documental
Documento revisado Documentación soporte de la metodología actual de la Firma sobre la revisión Nº8204.
Resultados de la revisión Se determinó que el área de *IT Audit* cuenta con un manual donde con base en el acuerdo SUGEF 12-10 Normativa para el cumplimiento de la ley Nº8204, se seleccionaron nueve objetivos relacionados con tecnología de información. Cada uno de los objetivos seleccionados corresponde a una actividad evaluada por *IT Audit* e indican los procedimientos que realizan para cada uno de estos. Adicionalmente, con base en las pruebas diseñadas se cuenta con una lista de requerimientos para solicitar la información al cliente.

Tabla 42. Revisión documental aplicada a la metodología de la Firma

9.9. Apéndice I. Revisión documental Acuerdo 12-10 (aplicada)

Revisión documental
Documento revisado Acuerdo 12-10 Normativa para el cumplimiento de la ley Nº8204.
Resultados de la revisión Se revisan los artículos de la normativa, y se determinaron los aspectos mínimos requeridos que cuentan con un componente tecnológico para cada uno de los objetivos evaluados en el proceso de revisión de cumplimiento de la ley Nº8204. Y deben ser incluidos en la revisión de TI.

Tabla 43. Revisión documental aplicada al acuerdo 12-10

9.10. Apéndice J. Revisión documental NIAs (Aplicada)

Revisión documental
Documento revisado NIA 500 NIA 530
Resultados de la revisión Se determinaron aspectos a considerar relacionados con la obtención de evidencia que sustenta la opinión del auditor, así como los requerimientos relacionados con el muestreo para asegurar la integridad de la información y que sea representativa de la población total.

Tabla 44. Revisión documental aplicada a las NIAS

9.11. Apéndice K. Revisión documental COBIT (Aplicada)

Revisión documental
Documento revisado Proceso DSS06 – COBIT 2019 Proceso BAI06 – COBIT 2019
Resultados de la revisión Se revisaron las actividades de cada práctica de domino indicada en los procesos; posteriormente, se analizan cuáles pueden ser consideradas para mejorar sustancialmente los controles de revisión de la ley Nº8204.

Tabla 45. Revisión documental aplicada a los procesos DSS06 y BAI06 de COBIT 2019

9.12. Apéndice L. Encuesta personal de TI (Aplicada)

Sección 1: Conocimientos generales sobre el proceso de revisión de la ley Nº8204

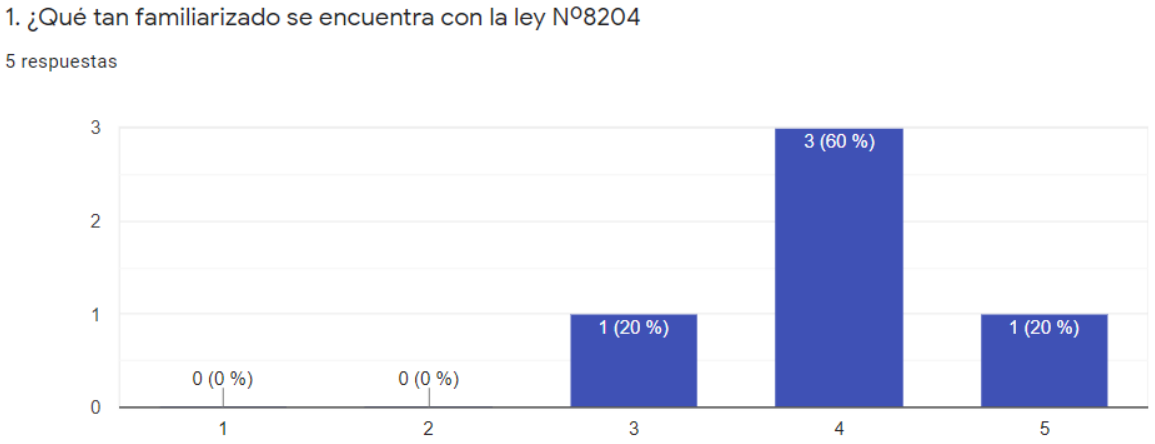


Figura 26. Resultados encuesta pregunta 1

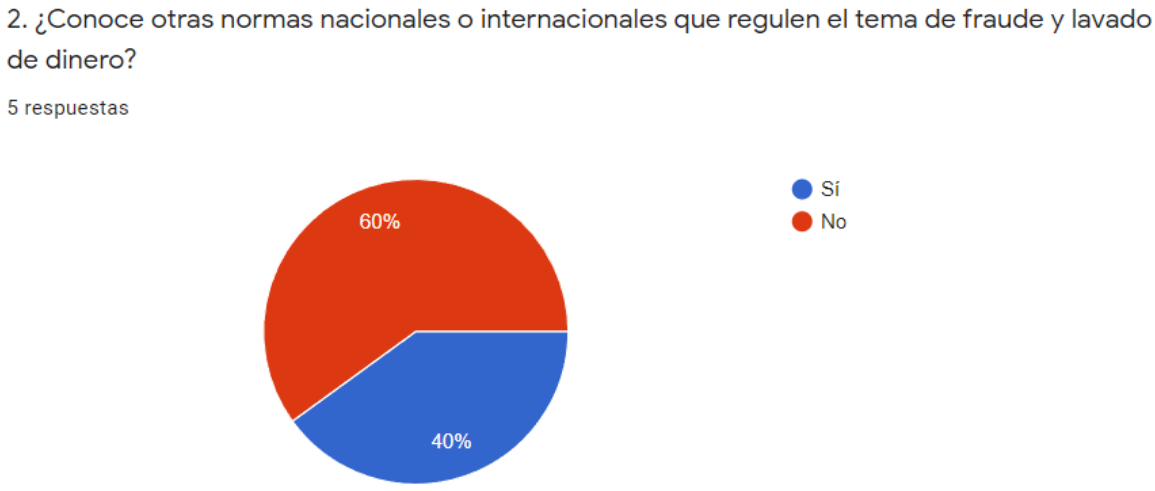


Figura 27. Resultados encuesta pregunta 2

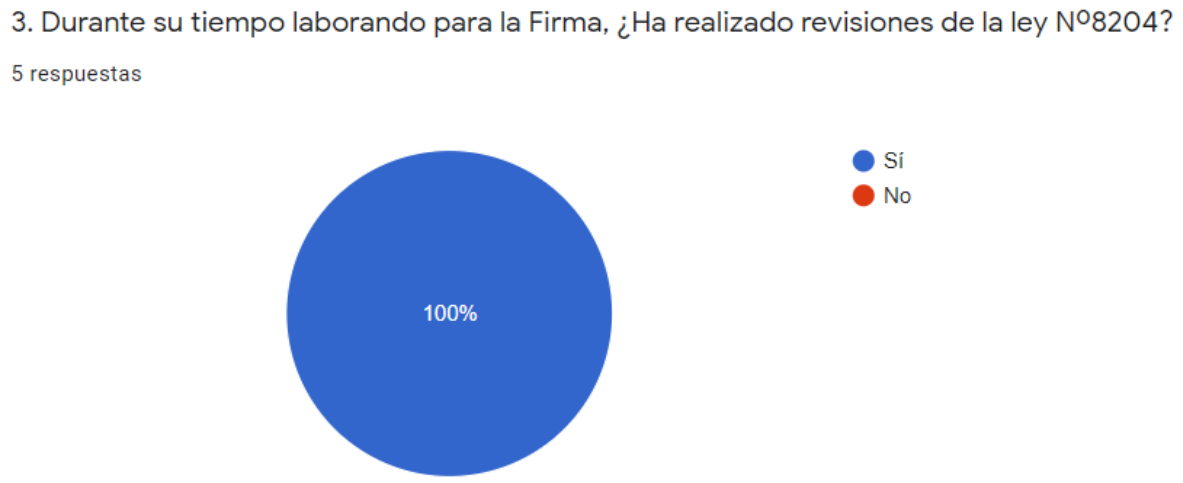


Figura 28. Resultados encuesta pregunta 3

***Sección 2**: Ejecución del proceso de revisión de la ley Nº8204*

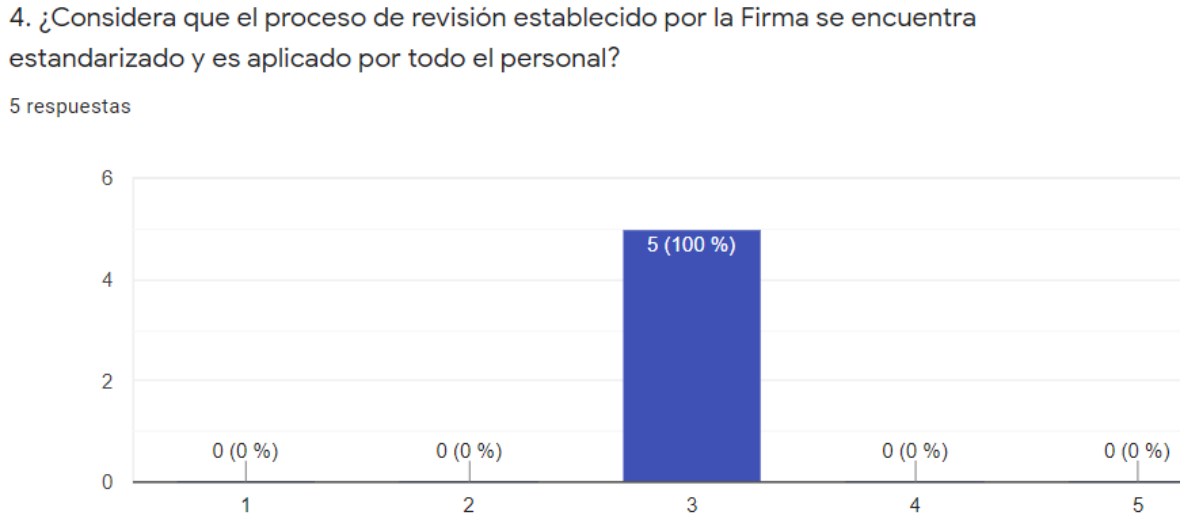


Figura 29. Resultados encuesta pregunta 4

Figura 30. Resultados encuesta pregunta 5

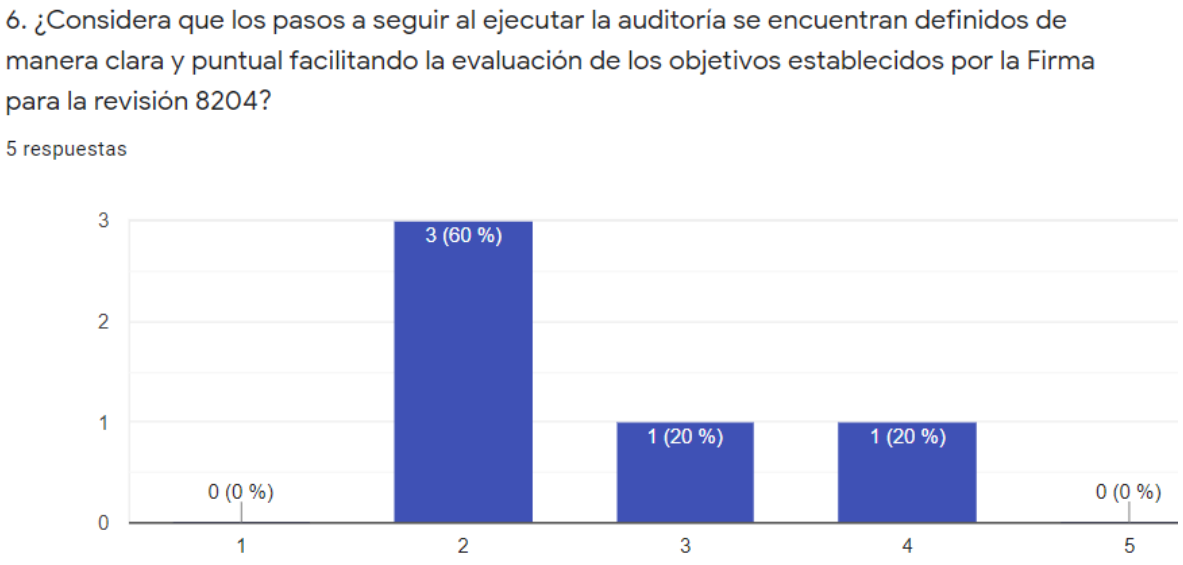


Figura 31. Resultados encuesta pregunta 7

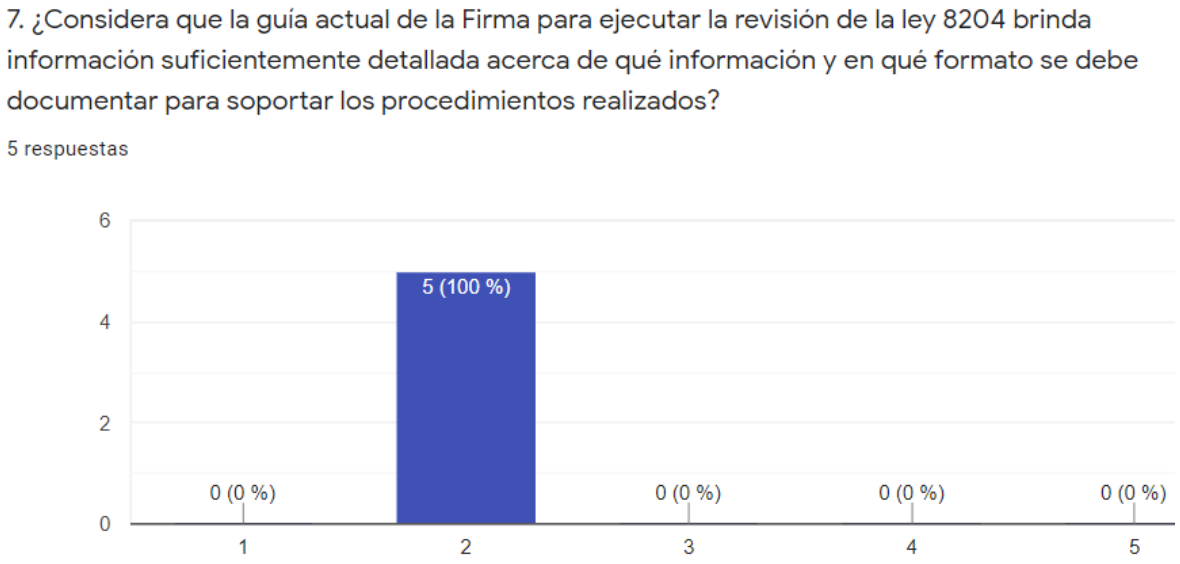


Figura 32. Resultados encuesta pregunta 7

***Sección 3**: Resultados del proceso de revisión de la ley Nº8204*

Figura 33. Resultados encuesta pregunta 8

9. Indique brevemente, ¿Cuáles son los principales problemas que ha tenido durante la revisión de la ley Nº8204?

5 respuestas

El proceso no está estandarizado y el material que hay actualmente que sirve de guía está desactualizado, hay cosas que están por fuera y solo los que tienen más experiencia saben

Los requerimientos a enviar al cliente no son del todo claro, para comprender que se debe revisar.

La descripción de las pruebas y la estandarización de la documentación

Requerimientos entregados al cliente poco claros y falta de una definición formal sobre el tamaño de muestra a utilizar en las revisiones.

poca claridad de instrucciones lo que afecta el manejo del tiempo

Figura 34. Resultados encuesta pregunta 9

10. Indique brevemente, ¿Qué aspectos cambiaría del proceso actual?

5 respuestas

Estandarizarlo, crear herramientas que ayuden y guíen a realizar la evaluación, sobretodo pensando en los que tenemos poca experiencia

Documentar los resultados en un software que lo haga más sencillo, ya que actualmente se debe completar un memo por objetivo evaluado.

El alcance de cada prueba y desarrollar un enfoque adecuado para cada modelo de negocio

Mejorar la vinculación de los requerimientos con los puntos en revisión para que los mismos sean congruentes. También, evaluar si los puntos en revisión responden las aspectos definidos en la Ley y a normativas asociadas (SUGEF 12-10).

La documentación (instrucciones) del proceso

Figura 35. Resultados encuesta pregunta 10

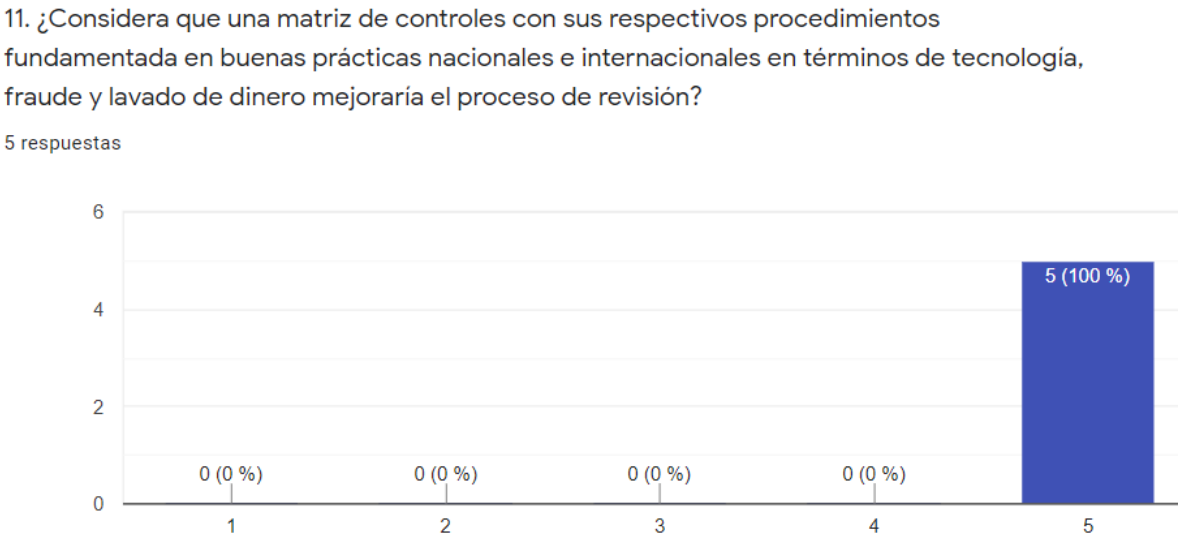


Figura 36. Resultados encuesta pregunta 11

9.13.Apéndice M: Matriz propuesta con los controles para la revisión de la ley Nº8204

Objetivo No.	SUGEF 12-10	Control	Riesgo Asociado	Procedimientos de diseño	Evidencia de diseño	Atributo	Procedimientos eficacia operativa	Evidencia de eficacia operativa
1	**Artículo 6.** Criterios o variables para el análisis y descripción del perfil de riesgo del cliente.	**AML01**- Configuración de la clasificación de riesgo de los clientes.	Configuración del sistema incorrecta relacionada con el cálculo del perfil del riesgo del cliente.	1. **Indagar** con el personal de TI sobre el diseño e implementación de la metodología aprobada para la clasificación del riesgo de los clientes. 2. **Indagar** con el personal de TI e **inspeccionar** cuáles criterios o variables fueron implementados en los sistemas, que como mínimo incluyan las siguientes: nacionalidad, país de origen, país de domicilio, profesión u oficio, zona geográfica, actividad económica, estructura de propiedad, tipos de activos propios de la actividad del cliente, origen de los recursos, utilización de efectivo, tipo, monto y frecuencia de las transacciones.	1. Metodología aprobada para la clasificación del riesgo de los clientes. 2. Lista de variables implementadas en el sistema.	a1. Los cambios efectuados en la configuración del control fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración del cálculo del perfil de riesgo de los clientes; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con el cálculo de clasificación del riesgo. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
						a2. La clasificación del riesgo se realiza de acuerdo con la metodología aprobada para tal fin.	TOEa2. **Inspeccionar** el sistema para determinar la forma en la que los valores se encuentran parametrizados y cómo influyen en la categorización de los clientes.	1. Capturas de pantalla con la lista de variables implementadas en el sistema, y su asignación de peso.
						a3. Existe una diferenciación de las relaciones con los clientes, para lo cual se utilizan al menos 3 categorías (Alto, medio, bajo).	TOEa3. Definir una muestra de clientes físicos y jurídicos de cada categoría (alto, medio, bajo), y crearlos en el sistema para **inspeccionar** que la clasificación de riesgo funcione correctamente.	1. Capturas de pantalla de las pruebas realizadas.
2	**Artículo 16.** Programas informáticos.	**AML02** - Configuración del monitoreo continuo.	Configuración de los programas de monitoreo incorrecta o inexistente.	1. **Indagar** con el personal de cumplimiento las políticas o procedimientos relacionadas con el monitoreo de los clientes. 2. **Indagar** con el personal de TI e **inspeccionar** cuáles programas fueron implementados para el monitoreo continuo del perfil transaccional del cliente, productos o servicios de alto riesgo y listas de personas vinculadas con organizaciones terroristas o lavado de dinero.	1. Políticas y procedimientos de monitoreo de clientes. 2. Captura de pantalla del sistema con la lista de alertas implementadas en este.	a1. Los cambios efectuados en la configuración del control fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración de los programas para alertar sobre transacciones que se desvíen del comportamiento esperado del cliente, productos o servicios de alto riesgo y listas de personas vinculadas con organizaciones terroristas o lavado de dinero; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con la configuración de alertas. 2. Aprobación de los cambios realizados a la configuración de las alertas.
						a2. Los programas de monitoreo continuo generan automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.	TOEa2. **Observar** el funcionamiento de los programas para determinar que están operando efectivamente de forma que generen automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.	1. Capturas de pantalla de las pruebas realizadas.
						a3. Los reportes generados sobre alertas registran al menos los datos: a) Datos personales. b) Histórico transaccional. c) Relación existente de las cuentas de cada cliente con las de otros clientes u otros productos y servicios dentro de la institución, sea esta de tipo patrimonial, comercial o de parentesco, si la hubiere. d) Históricos de las categorías de riesgo asignadas a cada cliente. e) Alertas generadas.	TOEa3. Definir una muestra de reportes sobre la cual, **inspeccionar** que cuenten con al menos los datos: a) Datos personales. b) Histórico transaccional. c) Relación existente de las cuentas de cada cliente con las de otros clientes u otros productos y servicios dentro de la institución, sea esta de tipo patrimonial, comercial o de parentesco, si la hubiere. d) Históricos de las categorías de riesgo asignadas a cada cliente. e) Alertas generadas.	1. Muestra de reportes.
3	**Artículo 17.** Análisis de las alertas generadas en los programas informáticos**.**	**AML03** – Seguimiento de alertas	Configuración de alertas errónea o inexistente	1. **Indagar** con el personal de cumplimiento de qué manera se revisan las alertas. 2. **Indagar** con el personal de cumplimiento el proceso para descartar transacciones inusuales, y si se registra el motivo, documento respaldo y responsable.	1. Políticas y procedimientos de monitoreo de clientes. 2. Lista de alertas configuradas. 3. Manual de cumplimiento.	a1. Se cuenta con alertas activas sobre transacciones inusuales.	TOEa1. Definir una muestra sobre las alertas generadas, e i**nspeccionar** los campos registrados.	1. Bitácora de alertas de transacciones que desvíen el comportamiento del cliente. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
						a2. Cuando se descarta una alerta, se registra el motivo, documento respaldo y responsable.	TOEa2. Definir una muestra de transacciones inusuales descartadas, para **inspeccionar** que registren el motivo, documento respaldo y responsable.	1. Muestra de transacciones inusuales descartadas.
						a3. Las alertas funcionan de acuerdo con el funcionamiento esperado.	TOEa3. Definir una muestra de alertas y **observar** su adecuado funcionamiento en un ambiente de pruebas.	1. Capturas de pantalla de las pruebas realizadas.

Objetivo No.	SUGEF 12-10	Control	Riesgo Asociado	Procedimientos de diseño	Evidencia de diseño	Atributo	Procedimientos eficacia operativa	Evidencia de eficacia operativa
4	**Artículo 18.** Bitácoras	**AML04** - Configuración de bitácoras	No se realiza seguimiento de transacciones y/o acciones sospechosas	1. **Indagar** con el personal de cumplimiento los lineamientos que deben cumplir las bitácoras de acuerdo con lo indicado por la Superintendencia. 2. **Indagar** con el personal de TI e **inspeccionar** de qué manera se encuentran implementadas las bitácoras, considerando: a. Nombre de las tablas de la base de datos. b. Detalle de los campos que se registran. c. Periodos de retención.	1. Lineamientos de bitácoras emitidos por la Superintendencia. 2. Captura de pantalla de la consulta. 3. Políticas de retención de datos.	a1. Los cambios efectuados en la configuración del control fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración de las bitácoras de acceso y uso del sitio de banca electrónica; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con la configuración de bitácoras. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
						a2. Las bitácoras registran el acceso y uso del sistema de banca electrónica.	TOEa2. **Observar** en un ambiente de pruebas la funcionalidad de las bitácoras, ingresando con un usuario al sistema de banca electrónica y realizando transferencias.	1. Capturas de pantalla de las pruebas realizadas.
5	**Artículo 19.** Operaciones únicas en efectivo	**AML05** - Registro de transacciones únicas	No se registran adecuadamente las operaciones únicas.	1. **Indagar** con el personal de cumplimiento si las transacciones únicas el proceso de registro de los formularios electrónicos.	1. política o procedimiento para el registro de transacciones únicas.	a1. Los formularios de registro de transacciones únicas incluyen todos los campos requeridos.	TOEa1. Definir una muestra de formularios sobre la cual, **inspeccionar** que cuenten con al menos los datos: - Datos de la persona que físicamente realiza la transacción. - Datos de la persona a cuyo nombre realiza la transacción. - Descripción de la transacción. - Origen de los recursos. - Nombre del funcionario que tramita la transacción. - Firma de la persona que físicamente realiza la transacción (se podrá utilizar las bases de datos de entidades públicas o se debe obtener la copia del documento de identificación).	1. Formularios con el registro de transacciones únicas.
						a2. Las transacciones únicas son registradas en los formularios para tal fin.	TOEa2. **Observar** en un ambiente de pruebas el registro de transacciones únicas.	1. Capturas de pantalla de las pruebas realizadas.
6	**Artículo 20.** Operaciones múltiples	**AML06** - Registro de transacciones múltiples	No se registran adecuadamente las operaciones múltiples	1. **Indagar** con el personal de cumplimiento si las transacciones múltiples el proceso de registro de los formularios electrónicos.	1. política o procedimiento para el registro de transacciones múltiples.	a1. Los formularios de registro de transacciones múltiples incluyen todos los campos requeridos.	TOEa1. Definir una muestra de formularios sobre la cual, **inspeccionar** que cuenten con al menos los datos: - Nombre completo o razón social. - Teléfono. - Fecha de nacimiento o constitución. - Número de identificación. - Tipo de identificación. - Descripción de las transacciones. Asimismo, para cada una de estas transacciones deberá quedar constancia de: - Fecha, tipo, medio de pago utilizado, número de operación, moneda, monto individual y monto total.	1. Formularios con el registro de transacciones múltiples.
						a2. Las transacciones múltiples son registradas en los formularios para tal fin.	TOEa2. **Observar** en un ambiente de pruebas el registro de transacciones múltiples.	1. Capturas de pantalla de las pruebas realizadas.
7	**Artículo 19 bis.** Transferencias electrónicas	**AML07 -** Registro de transacciones electrónicas	No se registran adecuadamente las operaciones desde o hacia el exterior	1. **Indagar** con el personal de cumplimiento y/o con el personal de TI si las transferencias desde y hacia el exterior realizadas, se registran automáticamente e incluyen al menos: a) Datos de la persona cuyo nombre se realiza la transacción. b) Descripción de la transacción Contraparte en el exterior a) Información requerida sobre el originador b) Información requerida sobre el beneficiario. 2. **Indagar** con el personal de TI si existen bitácoras para registrar los movimientos de transferencias electrónicas.	1. Política o procedimiento sobre controles de ejecución, rechazo o suspensión de las transacciones electrónicas cuando se detecte actividad sospechosa.	a1. Los cambios efectuados en la configuración del control fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos en la configuración de controles de ejecución, rechazo o suspensión de las transacciones automáticas cuando se detecte actividad sospechosa; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con la configuración de controles de ejecución, rechazo o suspensión de transacciones electrónicas. 2. Aprobación de los cambios realizados a la configuración del cálculo del perfil de riesgo.
						a2. Se cuenta con controles implementados para la ejecución, rechazo o suspensión de las transacciones electrónicas.	TOEa2. **Inspeccionar** en el sistema los controles relacionados con la ejecución, rechazo o suspensión de transacciones cuando se determina actividad sospechosa.	1. Capturas de pantalla de los controles configurado.
						a3. Los formularios de registro de transacciones únicas incluyen todos los campos requeridos.	TOEa3. Definir una muestra de formularios sobre la cual, **inspeccionar** que cuenten con al menos los datos: - Datos de la persona a cuyo nombre realiza la transacción. - Descripción de la transacción. - Información requerida sobre el originador - Información requerida sobre el beneficiario.	1. Formularios con el registro de transacciones electrónicas.
						a4. Las bitácoras registran los movimientos realizados por transferencias.	TOEa4. **Inspeccionar** la funcionalidad de las bitácoras, y verificar los registros relacionados.	1. Bitácoras de registro de transferencias electrónicas.

Objetivo No.	SUGEF 12-10	Control	Riesgo Asociado	Procedimientos de diseño	Evidencia de diseño	Atributo	Procedimientos eficacia operativa	Evidencia de eficacia operativa
8	**Artículo 21.** Remisión de información a las Superintendencias.	**AML08 -** Canales electrónicos	No hay seguimiento apropiado de los canales electrónicos.	1. **Indagar** con el personal de cumplimiento las políticas y procedimientos relacionadas con transferencias electrónicas. 2. **Indagar** con el personal de TI e **inspeccionar** cual es la lista de canales y transacciones electrónicas que automatiza la entidad.	1. Políticas y procedimientos relacionadas con transferencias electrónicas. 2. Lista de canales y transacciones electrónicas automatizadas	a1. Los cambios efectuados en la configuración del control fueron documentados y aprobados apropiadamente.	TOEa1. **Inspeccionar** si hubo cambios significativos relacionados con los servicios de transacciones por medio del sitio web; y de ser así, que dichos cambios cuenten con aprobación.	1. Información de los cambios implementados en el sistema, relacionados con los servicios de transacciones por medio del sitio web. 2. Aprobación de los cambios realizados a la configuración de las alertas.
						a2. Los programas de monitoreo continuo generan automática y oportunamente, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente.	TOEa2. **Inspeccionar** que las políticas sobre los servicios de transacciones electrónicas se encuentren implementadas.	1. Capturas de pantalla de la implementación de políticas.
9	**Artículo 38.** Apartados mínimos del informe anual	**AML09 -** Remisión a Superintendencia**s**	La información no es enviada a la Superintendencia dentro del tiempo establecido. No se encuentra bien parametrizados los reportes para generar las totalidades durante un mes calendario.	1. **Indagar** con el personal de cumplimiento el proceso de envío a las Superintendencias del reporte de las transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario, ya sean únicas o múltiples, que igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otra moneda. 2. **Indagar** el personal de TI y/o el oficial de cumplimiento, si se utilizan herramientas automatizadas para la generación de las transacciones ya sean únicas o múltiple.	1. polítca o procedimiento para el envío del reporte de transacciones realizadas por sus clientes a la Superintendencia.	a1. Los formularios de registro de transacciones únicas o múltiples son congruentes e incluyen todos los campos requeridos.	TOEa1. Definir una muestra de formularios sobre la cual, **inspeccionar** que los datos sean congruentes a los registrados en el sistema y que cuenten con al menos los datos: - Nombre completo o razón social. - Número de identificación. - Tipo de identificación. - Monto del egreso o ingreso - Tipo de operación. - Fecha. - Detalle de la transacción. - Origen de los recursos. - Nombre o código de la entidad.	1. Formularios con el registro de transacciones únicas o múltiples.
						a2. El reporte es emitido a la Superintendencia dentro de los 20 días naturales posteriores al cierre mensual.	TOEa2. **Inspeccionar** la configuración y envío de los reportes a las Superintendencias; y validar que sea dentro de los 20 días posteriores al cierre mensual.	1. Capturas de pantalla de las pruebas realizadas.
							TOEa3. Inspeccionar el sistema para validar que la consulta o delimitación del reporte generado se limite a transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario	1. Capturas de pantalla de las pruebas realizadas.

Tabla 46. Propuesta de set de controles para la auditoría de TI de cumplimiento de la ley Nº8204

9.14. Apéndice N. Machote para documentar el memo

Memo control AML<<XX>>
Cliente: Auditor: Gerente: Control: Procedimientos de diseño: **Procedimiento 1** **Procedimiento 2** Entrevistados: **<<Nombre/Puesto>>** Resultados: Procedimientos de eficacia operativa: **Procedimiento 1** **Procedimiento 2** Entrevistados: Resultados: Conclusiones generales sobre el diseño y la eficacia operativa:

9.15. Apéndice O: Requerimientos

ID	Control	Requerimiento	Estatus
1	CM01	Metodología para la clasificación de riesgos de los clientes.	Pendiente
2	CM01	Lista de variables implementadas en el sistema para el análisis y descripción del perfil de riesgo del cliente.	Pendiente
3	CM01	Revisión en sitio de las variables implementadas en el sistema.	Pendiente
4	CM01	Se requiere preparar un ambiente de pruebas para la creación de un cliente y verificar la funcionalidad de la clasificación de riesgo.	Pendiente
5	CM01	Lista de cambios en la configuración del cálculo del perfil de riesgo de los clientes; y de ser así, que dichos cambios cuenten con aprobación.	Pendiente
6	CM02	Lista de programas informáticos especializados para realizar un monitoreo continuo de los clientes. (Perfil transaccional del cliente, productos, servicios o transacciones de alto riesgo).	Pendiente
7	CM02	Políticas y/o procedimientos relacionados con el monitoreo continuo de los clientes.	Pendiente
8	CM02	Revisión en sitio de los programas que están operando para el monitoreo continuo de los clientes.	Pendiente
9	CM02	Muestra de reportes generados por los programas informáticos de monitoreo de los clientes. *** Nota: El tamaño de la muestra se definirá en la evaluación del control.	Pendiente
10	CM02	Lista de cambios en la configuración de los programas para alertar sobre determinar transacciones que se desvíen del comportamiento esperado del cliente.	Pendiente
11	CM03	Lista de alertas implementadas en el sistema para determinar transacciones que desvíen el comportamiento esperado del cliente.	Pendiente

ID	Control	Requerimiento	Estatus
12	CM03	Muestra de alertas generadas sobre transacciones que desvíen el comportamiento esperado de los clientes. *** Nota: El tamaño de la muestra se definirá en la evaluación del control.	Pendiente
13	CM03	Manual de cumplimiento.	Pendiente
14	CM03	Muestra de transacciones inusuales descartadas. (Documentación de respaldo, responsable) *** Nota: El tamaño de la muestra se definirá en la evaluación del control.	Pendiente
15	CM03	Se requiere preparar un ambiente de pruebas para verificar la funcionalidad de las alertas.	Pendiente
16	CM04	Detalle de las bitácoras de acceso y uso de banca electrónica (Indicar nombre de las tablas de la base de datos, nombre y detalle de los campos que se registran, periodo de retención de los datos).	Pendiente
17	CM04	Se requiere preparar un ambiente de pruebas para verificar la funcionalidad de las bitácoras.	Pendiente
18	CM04	Listado de cambios en la configuración de las bitácoras de acceso y uso del sitio de banca electrónica	Pendiente
19	CM05	Muestra de formularios físicos con el registro de las transacciones únicas (ROE). *** Nota: El tamaño de la muestra se definirá en la evaluación del control	Pendiente
20	CM05	Se requiere preparar un ambiente de pruebas para verificar el registro de las transacciones únicas.	Pendiente
21	CM06	Muestra de reportes con el registro de transacciones múltiples (ROM). *** Nota: El tamaño de la muestra se definirá en la evaluación del control	Pendiente
22	CM06	Se requiere preparar un ambiente de pruebas para verificar el registro de las transacciones múltiples.	Pendiente
23	CM07	Políticas y/o procedimientos relacionados con el registro de transferencias desde y hacia el exterior.	Pendiente

ID	Control	Requerimiento	Estatus
24	CM07	Reportes electrónicos con el registro de transacciones desde y hacia el exterior.	Pendiente
25	CM07	Revisión en sitio de los controles implementados para el registro y control de las transferencias desde y hacia el exterior.	Pendiente
26	CM07	Bitácora con el registro de movimientos realizados por transferencias desde y hacia el exterior.	Pendiente
27	CM07	Lista de cambios significativos en la configuración de controles de ejecución, rechazo o suspensión de las transacciones automáticas cuando se detecte actividad sospechosa	Pendiente
28	CM08	Políticas y/o procedimientos relacionados con las transacciones electrónicas.	Pendiente
29	CM08	Políticas y/o procedimientos sobre los servicios de transacciones electrónicas.	Pendiente
30	CM08	Lista de los canales y transacciones electrónicos que automatiza la entidad.	Pendiente
31	CM09	Reporte generado con el registro de las transacciones únicas y múltiples enviado a la Superintendencias.	Pendiente
32	CM09	Consulta (verificar en sitio o documento) del reporte de transacciones únicas y múltiples enviados a las Superintendencias.	Pendiente

Tabla 47. Requerimientos

1.1. Apéndice P: Análisis financiero de la propuesta

Insumos

Aumento del salario anual de la Firma		5%

	Por hora	Duración en horas	Total
Costo de una auditoría financiera de TI	₡ 21.233,54	40	₡ 849.341,64

Recurso	Salario recursos Salario mensual	Salario por hora
Estudiante	₡ 700.000,00	₡ 4.375,00
Gerente Senior	₡ 1.323.370,00	₡ 8.271,06
Personal IT Audit	₡ 700.000,00	₡ 4.375,00

Inversión inicial

Costo de la propuesta	Capacitación
₡ 2.666.355,31	₡ 210.000,00

Ingreso anual

	Año 1	Año 2	Año 3	Total
Cantidad de proyectos	1	5	7	13
Ingreso anual	₡ 849.341,64	₡ 4.246.708,20	₡ 5.945.391,48	₡11.041.441,32

Gerente Senior	₡ 1.323.370,00	₡ 1.389.538,50	₡ 1.459.015,43
Personal IT Audit	₡ 700.000,00	₡ 735.000,00	₡ 771.750,00

Gerente Senior	₡ 8.271,06	₡ 8.684,62	₡ 9.118,85
Personal IT Audit	₡ 4.375,00	₡ 4.593,75	₡ 4.823,44

Flujo de ejectivo

	Inversión inicial	Año 1	Año 2	Año 3	
Desarrollo	₡ 2.666.355,31				
Capacitación	₡ 210.000,00				
Costos operativos	₡ -	₡ 175.000,00	₡ 918.750,00	₡ 964.687,50	
Total	₡ 2.876.355,31	₡ 3.051.355,31	₡ 918.750,00	₡ 964.687,50	₡ 4.934.792,81

Retorno de inversión	**284%**

Indicadores de valoración

Inversión inicial	-₡ 2.876.355,31
Flujo de ejectivo año 1	₡ 3.051.355,31
Flujo de ejectivo año 2	₡ 918.750,00
Flujo de ejectivo año 3	₡ 964.687,50
Tasa de interés	0,417127441
VAN	**₡ 73.299,00**
TIR	**44%**

Figura 37. Modelo económico de la propuesta

9.16. Apéndice Q. Reunión #1 con el representante de la organización.

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley 8204

Reunión No.	01	**Fecha:**	06-08-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:30pm-5:15pm
Objetivo de la reunión:	Reunión inicial con la organización por parte del profesor tutor		
Participantes:	Presentes: Eric Mora, Laura Alpizar, Hellen Cordero, Deiber Ureña		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación de los trabajos de graduación**	Se presento el nombre del proyecto que va a realizar cada estudiante.	
2	**Responsabilidades de las partes**	Se presentaron las responsabilidades que debe cumplir cada parte durante el desarrollo del trabajo final de graduación (Estudiante y Organización)	
3	**Evaluación del trabajo final de graduación**	Se presento la evaluación correspondiente al trabajo final de graduación	
4	**Rubrica de la organización**	Se presenta la rúbrica de calificación de la organización	• Enviar rúbrica a la empresa en las semanas correspondiente a las evaluaciones. • Consultar con la coordinadora de trabajo de graduación por el formato de la rúbrica de la empresa ***Responsable: Deiber Ureña***
5	**Cronograma del proyecto**	Se presenta el cronograma del proyecto y se plantean las fechas tentativas para las próximas reuniones.	• Recordar evaluaciones • Fechas tentativas próximas reuniones: -Viernes 17 septiembre 2021, 4:30pm -Viernes 22 de octubre 2021, 4:30pm ***Responsable: Deiber Ureña***

Uso Confidencial Pág. 1/2

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Próxima reunión		
Temas para tratar	**Fecha**	**Convocados**
Avance del proyecto de graduación	Viernes 17 septiembre 2021 Hora: 4:30pm	Laura Alpizar Eric Mora Deiber Ureña

Eric Mora Rugama
Digitally signed by Eric Mora Rugama
Date: 2021.11.05 15:11:12 -06'00'

Firma del responsable de la organización Eric Mora Rugama

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.05 19:00:35 -06'00'

Firma de profesor Tutor
Laura Alpizar Chávez

Deiber Ureña González
Digitally signed by Deiber Ureña González
Date: 2021.11.05 17:42:58 -06'00'

Firma del estudiante
Deiber Ureña Gonzáles

Hellen Cordero Robles
Digitally signed by Hellen Cordero Robles
Date: 2021.11.05 17:56:57 -06'00'

Firma del estudiante
Hellen Cordero Robles

9.17. Apéndice R. Reunión #2 con el representante de la organización

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley 8204

Reunión No.	02	**Fecha:**	08-10-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	4:00pm-5:00pm
Objetivo de la reunión:	Reunió inicial de seguimiento con la empresa.		
Participantes:	Presentes: Eric Mora, Laura Alpízar, Hellen Cordero, Deiber Ureña		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación de la reunión**	Profesora indica el objetivo de la reunión y se menciona el orden en que presentaran los estudiantes.	
2	**Presentación de Avance Hellen Cordero**	Se realizó una pequeña presentación por parte de la estudiante Hellen Cordero donde se indica el trabajo realizado hasta el momento y el trabajo pendiente. También se indica el tiempo que falta para concluir con el TFG	
3	**Presentación de Avance Deiber Ureña**	Se realizó una pequeña presentación por parte del estudiante Deiber Ureña donde se indica el trabajo realizado hasta el momento y el trabajo pendiente.	
4	**Comentarios finales**	Se comenta que no se han presentado problemas con la empresa y los estudiantes tienen el apoyo de esta.	

Próxima reunión

Temas para tratar	Fecha	Convocados
Reunión final con la organización	Por definir	Laura Alpízar Eric Mora Deiber Ureña

Uso Confidencial Pág. 1/2

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un conjunto de herramientas de evaluación de riesgos cibernéticos, basado en el marco de trabajo NIST – Cybersecurity Framework

Eric Mora Rugama
Digitally signed by Eric Mora Rugama
Date: 2021.11.05 15:11:56 -06'00'

Firma del responsable de la organización
Eric Mora Rugama

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.05 19:01:44 -06'00'

Firma de profesor Tutor
Laura Alpizar Chávez

Deiber Ureña González
Digitally signed by Deiber Ureña González
Date: 2021.11.05 17:41:18 -06'00'

Firma del estudiante
Deiber Ureña Gonzáles

Hellen Cordero Robles
Digitally signed by Hellen Cordero Robles
Date: 2021.11.05 18:00:32 -06'00'

Firma del estudiante
Hellen Cordero Robles

9.18. Apéndice S Reunión #2 con el representante de la organización

MINUTA DE REUNIÓN CON LA ORGANIZACIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley 8204

Reunión No.	03	**Fecha:**	03-11-2021
Lugar:	Mediante Microsoft Teams	**Hora Inicio/Finalización:**	9:30am-10:30am
Objetivo de la reunión:	Reunió inicial con la organización por parte del profesor tutor		
Participantes:	Presentes: Eric Mora, Laura Alpízar, Hellen Cordero, Deiber Ureña		
	Ausentes: -		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	**Presentación de los resultados por parte de Hellen Cordero**	Se presentaron los resultados obtenidos, y se explicaron las herramientas realizadas por la estudiante Hellen Cordero	
2	**Presentación de los resultados por parte de Deiber Ureña**	Se presentaron los resultados obtenidos, y se explicó el set de herramientas realizadas por el estudiante Deiber Ureña	
3	**Comentarios finales**	• Agradecimiento a ambas partes por el apoyo brindado • Comentarios sobre la utilidad de las herramientas presentadas	

Eric Mora Rugama
Digitally signed by Eric Mora Rugama
Date: 2021.11.05 15:12:39 -06'00'

Firma del responsable de la organización
Eric Mora Rugama

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.05 19:01:07 -06'00'

Firma de profesor Tutor
Laura Alpízar Chávez

Hellen Cordero Robles
Digitally signed by Hellen Cordero Robles
Date: 2021.11.05 17:53:34 -06'00'

Firma del estudiante
Hellen Cordero Robles

Deiber Ureña González
Digitally signed by Deiber Ureña González
Date: 2021.11.05 17:45:30 -06'00'

Firma del estudiante
Deiber Ureña Gonzáles

9.19. Apéndice T. Minuta #1

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#1	**Fecha:**	31/07/2021
Lugar:	Zoom	**Hora Inicio/Finalización:**	3:00 am. / 4:00 am
Objetivo de la reunión:	Dar inicio al TFG		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González, Hellen Cordero,		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Inicio del proyecto		
2	Organización del trabajo		Se acordó coordinar con el responsable en la organización la primera reunión. Responsable: Deiber Ureña

Próxima reunión

Temas a tratar	Fecha	Convocados
En la próxima reunión	indicar	Hellen Cordero Deiber Ureña Eric Mora Laura Alpízar

9.20. Apéndice U. Minuta #2

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#2	**Fecha:**	28/08/01
Lugar:	Zoom	**Hora Inicio/Finalización:**	1:00 am. / 2:00 am
Objetivo de la reunión:	Revisión de los capítulos 1 y 2		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Correcciones del capítulo 1	Corregir los objetivos, y la problemática	
2	Correcciones del capítulo 2	Que aspectos podrían considerarse para sustentar la investigación	
3	Consideraciones generales	Definición de formato, utilizar tablas, y otras correcciones varias	Se acordó realizar todas las correcciones para la próxima sesión. Responsable: Deiber Ureña

Próxima reunión

Temas a tratar	Fecha	Convocados
	24/09/2021	Deiber Ureña Laura Alpízar

9.21. Apéndice V. Minuta #3

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#3	**Fecha:**	24/09/2021
Lugar:	Zoom	**Hora Inicio/Finalización:**	1:00 am. / 2:00 am
Objetivo de la reunión:	Revisión de los capítulos 1 y 2		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión de los capítulos 1 y 2	Se realizó revisión, correcciones a los objetivos, entre otros aspectos.	
2	Indicaciones para el capítulo 3	Se indicaron los aspectos y generalidades a considerar para el desarrollo del capítulo 3	

Próxima reunión

Temas a tratar	Fecha	Convocados
	07/10/2021	Deiber Ureña Laura Alpízar

9.22.*Apéndice W. Minuta #4*

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#4	**Fecha:**	07/10/2021
Lugar:	Zoom	**Hora Inicio/Finalización:**	3:00 pm. / 4:00 pm
Objetivo de la reunión:	Revisión de los capítulos 3 y 4		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión del capítulo 3	Guía para la elaboración de la metodología, y otros elementos del capítulo	Realizar correcciones para la próxima reunión, siendo puntual en las observaciones indicadas. Responsable: Deiber Ureña
2	Indicaciones para el capítulo 4	Se indicaron los aspectos y generalidades a considerar para el desarrollo del capítulo 4	

Próxima reunión

Temas a tratar	Fecha	Convocados
	22/10/2021	Deiber Ureña Laura Alpízar

9.23. Apéndice X. Minuta #5

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#5	**Fecha:**	22/10/2021
Lugar:	Teams	**Hora Inicio/Finalización:**	9:00 am. / 10:15 am
Objetivo de la reunión:	Revisión de los capítulos 4 y 5		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión del capítulo 4	Se brindó retroalimentación sobre la ejecución de la metodología.	Realizar correcciones para la próxima reunión, siendo puntual en las observaciones indicadas. Responsable: Deiber Ureña
2	Indicaciones para el capítulo 5	Se indicaron los aspectos y generalidades a considerar para el desarrollo del capítulo 5	

Próxima reunión

Temas a tratar	Fecha	Convocados
Revisión del capítulo 5 e instrucciones para el 6	29/10/2021	Deiber Ureña Laura Alpízar

9.24. Apéndice Y. Minuta #6

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#5	**Fecha:**	22/10/2021
Lugar:	Teams	**Hora Inicio/Finalización:**	09:00 am. / 10:15 pm
Objetivo de la reunión:	Revisión de los capítulos 4 y 5		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión del capítulo 4	Guía para la elaboración de la metodología, y otros elementos del capítulo	Realizar correcciones para la próxima reunión, siendo puntual en las observaciones indicadas. Responsable: Deiber Ureña
2	Indicaciones para el capítulo 5	Se indicaron los aspectos y generalidades a considerar para el desarrollo del capítulo 5	

Próxima reunión

Temas a tratar	Fecha	Convocados
	29/10/2021	Deiber Ureña Laura Alpízar

9.25. Apéndice Z. Minuta #7

MINUTA DE REUNIÓN

Proyecto: Propuesta de un set de controles para una auditoría de tecnologías de información de cumplimiento de la ley N°8204

Reunión No.	#7	**Fecha:**	05/11/2021
Lugar:	Teams	**Hora Inicio/Finalización:**	6:30 pm. / 8:00 pm
Objetivo de la reunión:	Revisión de los capítulos 6 y 7		
Participantes:	Presentes: Laura Alpízar Chaves, Deiber Ureña González		
	Ausentes:		

Temas Tratados

No.	Asunto	Comentarios	Acuerdos
1	Revisión de las conclusiones y recomendaciones	Se brindó retroalimentación sobre conclusiones y recomendaciones, así como otros capítulos.	
2	Otros temas pendientes en los capítulos		

Próxima reunión

Temas a tratar	Fecha	Convocados
		Deiber Ureña Laura Alpízar

9.26. Apéndice AA. Aprobación de minutas

TEC | Tecnológico de Costa Rica

ati
Área Académica de Administración de Tecnologías de Información
Licenciatura en Administración de Tecnología de Información

Cartago, Costa Rica, 08 de noviembre 2021

Asunto: Aceptación de las minutas de reunión del TFG

Mediante la presente yo Deiber Ureña González, carné universitario 2015148409, estudiante de la carrera Administración de Tecnología de Información, solicita a aprobación de las minutas realizadas durante el trabajo final de graduación (TFG) durante el II Semestre 2021.

Esta aprobación incluye las siguientes minutas:

- Minuta#1: 31/07/2021
- Minuta#2: 28/08/2021
- Minuta#3: 24/09/2021
- Minuta#4: 07/10/2021
- Minuta#5: 22/10/2021
- Minuta#6: 29/10/2021
- Minuta#7: 05/11/2021

Sin más que agregar me despido,

Muchas gracias de antemano.

Atentamente.

Deiber Ureña González
Digitally signed by Deiber Ureña González
Date: 2021.11.08 08:09:20 -06'00'

Deiber Ureña Gonzáles
Carné 2015148409

LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Firmado digitalmente por LAURA CRISTINA ALPIZAR CHAVES (FIRMA)
Fecha: 2021.11.08 08:55:07 -06'00'

Laura Alpízar Chaves
Profesora tutora

Capítulo X: Anexos

10.1. Anexo 1: Acuerdo SUGEF 12-10 Normativa para el Cumplimiento de la Ley Nº8204 (Extractos)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

ACUERDO SUGEF 12-10
NORMATIVA PARA EL CUMPLIMIENTO DE LA LEY N° 8204[a]

Aprobado por el Consejo Nacional de Supervisión del Sistema Financiero, mediante el artículo 12 del acta de la sesión 893-2010, celebrada el 3 de diciembre del 2010. Publicada en el diario oficial "La Gaceta" N° 248, del 22 de diciembre del 2010.

Rige a partir de su publicación en el diario oficial La Gaceta.

CONTENIDO

VER CONSIDERANDOS DEL ACUERDO ORIGINAL

VER REGLAMENTO

VER LINEAMIENTOS

VER MODIFICACIONES

VER HISTORIAL DE VERSIONES

Versión documento	Fecha de actualización
13	**24 de mayo de 2017**

[a] Ley sobre estupefacientes, sustancias psicotrópicas, drogas de uso no autorizado, actividades conexas, legitimación de capitales y financiamiento al terrorismo.

Figura 38. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

b) Los criterios para establecer las categorías de riesgo según lo establecido en el artículo 6 de esta normativa.
c) Los requisitos documentales adicionales a los establecidos en los artículos en esta Normativa, para cumplir con la Política Conozca a su Cliente para cada categoría de riesgo establecida por el sujeto fiscalizado.

Artículo 5. Metodología para la clasificación de riesgo de los clientes.

En el diseño de la metodología para la clasificación de riesgo de los clientes deben considerarse los siguientes elementos:

a) Conceptos y marco teórico.
b) Criterios o variables mínimas para el análisis del perfil de riesgo del cliente.
c) Descripción de la clasificación y categorización de riesgo de los clientes.
d) Definición de modelos para el establecimiento del perfil de riesgo de clientes.
e) Descripción y diseño para la automatización del modelo o modelos seleccionados.
f) Diseño y descripción de matrices de riesgo.
g) Apéndices, anexos.

Esta metodología de clasificación y sus modificaciones deben ser conocidas y aprobadas por la Junta Directiva u órgano colegiado equivalente.

Las Superintendencias pueden realizar las comprobaciones pertinentes para verificar que la metodología de clasificación de riesgo de los clientes es razonable de acuerdo con el volumen y naturaleza de las operaciones que lleva a cabo el sujeto fiscalizado, así como al perfil de cliente que atiende. En los casos en que se determine que la metodología de clasificación es inadecuada o insuficiente, la Superintendencia correspondiente debe requerir al sujeto fiscalizado que tome las medidas que corresponda para su corrección, aclaración o sustitución en el plazo que ésta establezca.

Artículo 6. Criterios o variables para el análisis y descripción del perfil de riesgo del cliente.

Para el análisis y descripción del perfil de riesgo de cada cliente, los sujetos fiscalizados seleccionarán entre los siguientes criterios o variables, sin estar limitados a estos:

a) Nacionalidad.
b) País de origen (país de nacimiento o país de constitución)
c) País de domicilio.
d) Profesión u oficio.
e) Zona geográfica de las actividades de negocios del cliente incluyendo la localización de las contrapartes con las cuales realiza transacciones y hace negocios, si está vinculado con países considerados como de alto riesgo, según lo recomendado por el Grupo de Acción Financiera del Caribe (GAFIC), Fondo Monetario Internacional, Banco Mundial, Grupo de Acción Financiera (GAFI) entre otros.

Figura 39. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

CAPÍTULO IV

MONITOREO DE TRANSACCIONES Y PROGRAMAS INFORMÁTICOS

Artículo 16. Programas informáticos

Los sujetos fiscalizados deben contar con programas informáticos especializados que permitan realizar un monitoreo continuo de las cuentas y servicios ofrecidos a los clientes, para asegurar que su patrón transaccional es congruente con el perfil de riesgo y la cuantía mensual estimada indicada por el cliente al inicio y durante la relación comercial.

El nivel de monitoreo de las transacciones lo determina la evaluación de riesgo de los clientes de la entidad. Con fundamento en su análisis de riesgo, el sujeto fiscalizado debe establecer señales de alerta particulares para su negocio y en consecuencia establecer los tipos de monitoreo necesarios para identificar operaciones inusuales.

Los programas informáticos deben generar, en forma automática y oportuna, alertas sobre transacciones que se desvíen del comportamiento esperado del cliente, así como reportes que incluyan, como mínimo pero no limitados a estos, la siguiente información:

a) Datos personales.
b) Histórico transaccional.
c) Relación existente de las cuentas de cada cliente con las de otros clientes u otros productos y servicios dentro de la institución, sea esta de tipo patrimonial, comercial o de parentesco, si la hubiere.
d) Históricos de las categorías de riesgo asignadas a cada cliente.
e) Alertas generadas.

Los sujetos fiscalizados son responsables de revisar regularmente los sitios de Internet de organizaciones como el Grupo de Acción Financiera (GAFI), Organización de Estados Americanos (OEA), Organización para la Cooperación y el Desarrollo Económico (OECD), Organización de las Naciones Unidas (ONU), Grupo de Acción Financiera Internacional del Caribe (GAFIC) entre otras, para mantener actualizadas sus señales de alerta.

Artículo 17. Análisis de las alertas generadas de los programas informáticos

El sujeto fiscalizado debe realizar una revisión de todas las alertas, con el objetivo de identificar las transacciones inusuales a las que debe dárseles seguimiento.

Para aquellas transacciones inusuales que se descarten, se debe dejar evidencia del motivo por el cual se descartó, la documentación de respaldo y el responsable.

19

Figura 40. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

Artículo 18. Bitácoras

El sujeto fiscalizado que ofrezca el servicio de banca electrónica debe llevar una bitácora de acceso y de uso del sistema que permita registrar y rastrear las transacciones que realiza el cliente.

Las transacciones financieras electrónicas comprenden aquellas operaciones que se realicen por medio de cajeros automáticos, Internet, transacciones telefónicas o cualquier otro servicio que pueda llevarse a cabo por medios electrónicos.

Estas bitácoras deben cumplir con los lineamientos sobre tecnología de información que al respecto emita cada Superintendencia.

CAPÍTULO V

REGISTRO Y NOTIFICACIÓN DE TRANSACCIONES

Artículo 19. Operaciones únicas en efectivo [4] [7k]

De conformidad con lo establecido en el artículo 20 de la Ley 8204 y su Reglamento, las personas físicas o jurídicas sujetas al cumplimiento de la Ley 8204, deben registrar en formularios físicos o electrónicos el ingreso o egreso de las transacciones únicas, entendiendo estas como todas las realizadas en moneda local o extranjera, que igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en colones u otra moneda extranjera, realizadas en efectivo; dicho formulario debe incluir la información que se detalla seguidamente:

a) Datos de la persona que físicamente realiza la transacción: nombre completo, teléfono, fecha nacimiento, número de identificación, tipo de identificación (cédula, pasaporte en el caso de extranjeros no residentes, documentos de identificación aceptados por la Dirección General de Migración y Extranjería para extranjeros residentes y documentos de identificación de diplomáticos emitidos por el Ministerio de Relaciones Exteriores y Culto; dicha información podrá ser obtenida de bases de datos oficiales y ser almacenada de forma electrónica), domicilio exacto. Para las personas jurídicas se debe consignar, para su representante legal y su agente residente, la misma información solicitada a las personas físicas.
b) Datos de la persona a cuyo nombre se realiza la transacción (cliente): nombre completo o razón social (para persona jurídica), número de identificación, tipo de identificación, domicilio.
c) Descripción de la Transacción: tipo de transacción (ingreso o egreso), tipo de operación, número de la operación, fecha y hora de la transacción, monto y moneda original transada y monto total dolarizado.

Figura 41. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

d) Origen de los recursos (breve descripción).
e) Datos del beneficiario o destinatario. Indicar el número de cuenta y nombre de la entidad de destino.
f) Nombre del funcionario que tramita la transacción (completar cuando el formulario es confeccionado por una persona distinta al cajero).
g) Firma de la persona que físicamente realiza la transacción (se debe verificar la identidad de las personas que realizan físicamente la transacción, para lo cual podrá utilizar las bases de datos de entidades públicas. En los casos en que no se pueda corroborar la identidad de la persona por ausencia de bases de datos de entidades públicas o porque la entidad no desee utilizar dicho medio, se debe obtener copia del documento de identificación).

La firma de la persona que físicamente realiza la transacción podrá ser registrada en el correspondiente recibo de caja, recibo de dinero, órdenes de inversión o retiro, que contengan como mínimo la siguiente información: nombre del sujeto obligado y agencia, número de comprobante, fecha y hora de la transacción, nombre del funcionario que tramita la transacción, número de identificación y nombre o razón social de la persona a cuyo nombre se realiza la transacción, número de cuenta en la entidad, tipo de transacción, monto, nombre completo, número de identificación, tipo de identificación y firma de la persona que físicamente realiza la transacción.

Para efecto de lo establecido en los artículos 20 a 23 de la Ley 8204, se entenderá como formulario cualquier registro o registros, sean físicos o electrónicos, que recopilen, capturen o integren la totalidad de la información requerida en el artículo 21 de la Ley 8204, incluyendo, expedientes, bases de datos, comprobantes de transacción, entre otros. La documentación de respaldo de las demás transacciones, debe estar a disposición de las autoridades administrativas y judiciales competentes, conforme lo indicado en los incisos anteriores, la cual puede obtenerse de los expedientes, bases de datos, comprobantes de transacción, entre otros.

Artículo 19 bis. Transferencias electrónicas. [71]

Los sujetos obligados que presten el servicio de transferencias desde o hacia el exterior en moneda local o extranjera, que igualen o superen los US$1,000.00 (mil dólares en la moneda de los Estados Unidos de América) o su equivalente en colones u otra moneda extranjera, deben registrar electrónicamente la información que se detalla seguidamente:

a) Datos de la persona a cuyo nombre se realiza la transacción (cliente): nombre completo o razón social (para persona jurídica), número de identificación.

b) Descripción de la Transacción: tipo de transacción (ingreso o egreso), número de la operación, fecha y hora de la transacción, monto y moneda original transada.

21

Figura 42. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

Respecto a la contraparte en el exterior, toda transferencia debe estar acompañada de lo siguiente:
a) Información requerida sobre el originador.
(i) el nombre del originador;
(ii) el número de cuenta del originador cuando la cuenta se utilice para procesar la transacción o, de no haber una cuenta, un único número de referencia de la transacción que permita rastrearla; y
(iii) la dirección del originador o su número de identidad nacional o el número de identificación del cliente o la fecha y lugar de nacimiento, si se cuenta con dicha información.
b) Información requerida sobre el beneficiario.
(i) el nombre del beneficiario; y
(ii) el número de cuenta del beneficiario cuando la cuenta se utilice para procesar la transacción o, de no haber una cuenta, un único número de referencia de la transacción que permita rastrearla.

En el caso de las transferencias electrónicas nacionales, es exigido a la institución financiera originadora que la información que acompañe a las transferencias incluya la información del originador tal y como se indica para las transferencias electrónicas desde y hacia el exterior.

Para los casos de las transferencias electrónicas que estén por debajo del umbral señalado en el párrafo primero de este artículo, las personas físicas o jurídicas sujetas al cumplimiento de la Ley 8204 deben asegurarse que contengan el nombre del originador y el nombre del beneficiario, además de un número de cuenta para cada uno o un número único de referencia de la transacción.

La institución financiera que hace la orden no podrá ejecutar la transferencia electrónica si no cumple con los requisitos establecidos anteriormente.

Las instituciones financieras intermediarias y beneficiarias de las transacciones electrónicas, deben contar con políticas y procedimientos eficaces basados en el riesgo para determinar: i) cuando ejecutar, rechazar o suspender una transferencia electrónica que carezca de la información requerida sobre el beneficiario; y (ii) la acción de seguimiento apropiada.

Artículo 20. Operaciones múltiples [4]

Las personas físicas o jurídicas sujetas al cumplimiento de la Ley 8204, deben registrar el ingreso o egreso (de manera separada) de las transacciones múltiples, entendiendo estas como, todas aquellas operaciones realizadas en efectivo y mediante transferencias desde o hacia el exterior; que durante un mes calendario, en conjunto igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otra moneda. El detalle de las transacciones que componen la operación múltiple debe estar a disposición de la Superintendencia respectiva.

El registro de las transacciones múltiples podrá ser físico o electrónico y debe contener como mínimo: Nombre completo o razón social, teléfono, fecha de nacimiento o de constitución, número de identificación, tipo de identificación (cédula, pasaporte, cédula de residencia o cédula jurídica) descripción de la transacción, indicando si corresponde a ingresos o egresos.

22

Figura 43. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

Asimismo para cada una de estas transacciones deberá quedar constancia de la fecha, tipo (por ejemplo: depósito a cuenta número…, cambio de cheque número…, de la cuenta número…) medio de pago utilizado (efectivo, cheques, transferencias, valores, entre otros) número de operación, moneda, monto individual, monto total.

En caso de que las transacciones se realicen en diferentes tipos de moneda, el monto total deberá ser convertido a US dólares, al tipo de cambio de compra establecido por el Banco Central de Costa Rica al último día de mes.

La documentación de respaldo de las demás transacciones múltiples, debe estar a disposición de las autoridades administrativas y judiciales competentes, conforme lo indicado en los incisos anteriores, la cual puede obtenerse de los expedientes, bases de datos, comprobantes de transacción, entre otros.

Artículo 21. Remisión de información a las Superintendencias

Los sujetos fiscalizados deben reportar a la Superintendencia respectiva, las transacciones realizadas por sus clientes en efectivo o mediante transferencias desde o hacia el exterior durante el mes calendario, ya sean únicas o múltiples, que igualen o superen los US$10,000.00 (diez mil dólares en la moneda de los Estados Unidos de América) o su equivalente en otra moneda. Dicho reporte debe ser remitido dentro de los 20 días naturales posteriores al cierre de cada mes, por el medio y forma que indique cada Superintendencia y debe incluir la siguiente información: nombre completo o razón social del cliente, número de identificación, monto del ingreso o egreso en colones o dólares según corresponda, tipo de operación, fecha, detalle de la transacción, origen de los recursos y nombre o código de la entidad.

En el caso particular de las transferencias, la SUGEF mediante Acuerdo del Superintendente definirá el contenido del reporte y el medio de remisión de la información.

Los sujetos fiscalizados por SUGEVAL, SUPEN y SUGESE que mantengan cuentas corrientes para recibir recursos de sus clientes en las entidades fiscalizadas por SUGEF, a través de su oficial de cumplimiento podrán requerir a su homólogo en dichas entidades, la información respecto de aquellas transacciones realizadas en efectivo por sumas iguales o superiores a los US$10,000.00 o su equivalente en otras monedas, en un plazo de 10 días naturales, a efectos de que dichas entidades puedan cumplir con las obligaciones de reporte que les impone el ordenamiento jurídico.

Las entidades o sujetos obligados por el artículo 15 de la Ley 8204, deben reportar las transacciones según los lineamientos que determinen la Superintendencia General de Entidades Financieras, en los términos y condiciones que ésta establezca.

En todos los casos, la información que no cumpla con las condiciones establecidas por la Superintendencia respectiva, que presente errores o sea incompleta, se considerará como no presentada.

23

Figura 44. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)

CONASSIF CONSEJO NACIONAL DE SUPERVISIÓN DEL SISTEMA FINANCIERO

SUGEF

Para la preparación y elaboración de este informe, los Auditores Externos no pueden tener acceso a la identidad de los clientes de los casos que se investiguen, o que hayan sido reportados a las autoridades como actividades sospechosas.

Aquellas operaciones detectadas durante las revisiones de los Auditores Externos, que a su criterio constituyen actividades inusuales, deben ser informadas al Oficial de Cumplimiento, quien las evaluará y decidirá si deben ser reportadas a la Unidad de Inteligencia Financiera.

El informe anual sobre prevención y control de legitimación de capitales y financiamiento al terrorismo, se considera confidencial, debe ser presentado al sujeto fiscalizado en el plazo máximo del 31 de marzo de cada año con corte a diciembre y debe estar a disposición de la Superintendencia respectiva para efectos de supervisión.

Artículo 38 Apartados mínimos del informe anual

El informe debe referirse a los siguientes apartados:

a) Elaboración y mantenimiento del manual de cumplimiento.
b) Metodología para la clasificación del riesgo del cliente. Incluyendo la revisión de las políticas y procedimientos para tal fin.
c) Perfiles de riesgo de los clientes.
d) Procedimientos de identificación de clientes (Política conozca a su cliente).
e) Procedimientos para asegurar una debida diligencia más exhaustiva para las categorías de clientes de alto riesgo.
f) Políticas establecidas y procedimientos de control para abordar todo riesgo específico asociado con el uso indebido de los avances tecnológicos, especialmente en las relaciones o transacciones comerciales que no son cara a cara, tales como, servicios y transacciones por Internet, uso de cajeros automáticos, banca por teléfono, transmisión de instrucciones o solicitudes por fax o medios similares, uso de tarjetas prepagadas.
g) Servicios de transacciones electrónicas.
h) Procedimientos para el monitoreo de cuentas.
i) Medidas establecidas para el registro y notificación de las transacciones en efectivo únicas y múltiples, así como, de las transferencias realizadas desde y hacia el exterior.
j) Políticas y procedimientos de los reportes de las operaciones inusuales y sospechosas.
k) Desarrollo e implementación de programas de inducción y capacitación anual al personal.
l) Responsabilidades y funciones relacionadas con la Oficialía de Cumplimiento y sus funcionarios.
m) Responsabilidades y funciones relacionadas con el Comité de Cumplimiento.
n) Políticas de reclutamiento y selección de personal.
o) Deberes de la Auditoría Interna, Gerencia General y Junta Directiva u órgano equivalente.
p) Políticas sobre las relaciones comerciales con entidades extranjeras.
q) Descripción de las limitantes encontradas, que impiden que el Oficial de Cumplimiento desarrolle eficazmente sus funciones.
r) Resultados del seguimiento de hallazgos de informes anteriores.

Cuando no proceda la evaluación de algún apartado, debe señalarse expresamente en el informe, indicando los motivos. Adicionalmente, en el informe debe añadirse cualquier otro aspecto relativo a los procedimientos y órganos de control interno y comunicación que, atendiendo a las peculiaridades

34

Figura 45. Acuerdo 12-10 (Extracto)

Fuente: (SUGEF, 2017)