ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: “EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA INFORMÁTICA BASADO EN SU RIESGO INHERENTE”

AUTORES: CAJAS SINCHIGUANO, FREDDY ALEXANDER
LUJE MISACANGO, ROGER ANDRES

DIRECTOR: ING. PÁLIZ OSORIO, VÍCTOR MANUEL

SANGOLQUÍ

2020

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA INFORMÁTICA BASADO EN SU RIESGO INHERENTE***" realizado por los señores ***Cajas Sinchiguano, Freddy Alexander*** y ***Luje Misacango, Roger Andres***, ha sido revisado y analizado en su totalidad por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de Fuerzas Armadas ESPE, para que lo sustente públicamente.

Sangolquí, 05 de febrero del 2020.

Ing. Páliz Osorio, Víctor Manuel
C.C.: 1708034622
DIRECTOR

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***Cajas Sinchiguano, Freddy Alexander*** con cédula de ciudadanía n° **050343175-1**, y ***Luje Misacango, Roger Andres*** con cédula de ciudadanía n° **172096384-0,** declaramos que el contenido, ideas y criterios del trabajo de titulación "***EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA INFORMÁTICA BASADO EN SU RIESGO INHERENTE"*** es de nuestra autoría y responsabilidad, cumpliendo con los requisitos legales, teóricos, científicos, técnicos y metodológicos establecidos por la Universidad de las Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Sangolquí, 05 de febrero del 2020.

Cajas Sinchiguano, Freddy Alexander
C.C. 0503431751

Luje Misacango, Roger Andres
C.C. 1720963840

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, ***Cajas Sinchiguano, Freddy Alexander*** y ***Luje Misacango, Roger Andres***, autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: **"*EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA INFORMÁTICA BASADO EN SU RIESGO INHERENTE*"** en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.

Sangolquí, 05 de febrero del 2020.

Cajas Sinchiguano, Freddy Alexander
C.C. 0503431751

Luje Misacango, Roger Andres
C.C. 1720963840

DEDICATORIA

Quiero dedicar mi tesis a todos quienes formaron parte de este proceso, para Uds.:

A Dios, por haberme regalado la salud y la vida para poder cumplir con uno de mis sueños, culminar mi carrera. Siempre estaré inmensamente agradecido.

A mis padres Fredy y Norma, quienes me han sabido guiar por el camino del bien con sus concejos y enseñanzas, su ayuda me ha permitido llegar a cumplir un sueño más, para Uds. todo mi cariño y agradecimiento por haber confiado en mí en todo momento, por haberme brindado todo su apoyo y por haberme forjado como la persona que soy. Este logro no es solo mío sino también de Uds. Gracias padre y madre.

A mis abuelitos Carlos y Abigail, mis segundos padres, les agradezco con todo mi cariño por toda su ayuda, por la preocupación y cariño que me han sabido regalar, todo ello ha hecho de mí una mejor persona.

A mis hermanos Christian y Abigail, quiero que esto sirva como precedente para que Uds. también cumplan con sus sueños y se den cuenta que todo es posible si uno se lo propone y lucha por conseguirlo.

A mi enamorada Emily, por todo su apoyo y preocupación, por estar en los buenos y los malos momentos siempre apoyándome. Me ayudaste hasta donde se te hacía posible, incluso más que eso.

AGRADECIMIENTO

¿Cómo decir "gracias", cuando hay tantas personas a las que agradecer? Este proyecto es una forma de agradecimiento a mis padres, que fueron ejemplo de responsabilidad y sacrificio. Mis amigos, con quienes a lo largo de la carrera compartí experiencias, alegrías y frustraciones. Aquellos docentes, que con sus conocimientos, exigencias y virtudes fueron cada día una fuente de inspiración.

En fin, gracias a la vida, por permitirme alcanzar esta meta, que no fue fácil, pero que forjó mi carácter y me dio la confianza para afrontar cualquier reto futuro.

Luje Misacango Roger Andres

PER ASPERA AD ASTRA!

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La auditoría informática se ha convertido en una pieza fundamental para asegurar el éxito y el uso de sistemas informáticos en las organizaciones. El éxito o fracaso de una auditoría depende de varios factores: experticia, herramientas, metodologías, etc., cada uno de estos elementos son elegidos por el auditor informático, basado en su conocimiento y experiencia. La selección incorrecta de estos componentes puede desencadenar resultados de auditoría subjetivos, imprecisos y perjuicios para la organización. Mediante un análisis de metodologías de auditoría informática se determinará el nivel de riesgo inherente de cada una, obteniendo así el nivel de impacto de su aplicación. Para el desarrollo de este análisis se trabajará con una metodología de investigación propia de tipo exploratoria cuantitativa, basada en el método deductivo para la selección de parámetros relacionados al riesgo inherente, con perspectiva crítica para la cuantificación e interpretación de datos estadísticos. La investigación será validada con el método Delphi, mediante encuestas aplicadas a auditores expertos utilizando escalas no comparativas para confirmar la objetividad e imparcialidad del modelo de evaluación. Los procedimientos a realizarse demostrarán que es posible cuantificar el nivel de riesgo inherente, mediante tablas de ocurrencia, cumplimiento y priorización.

PALABRAS CLAVE:

- **AUDITORÍA INFORMÁTICA**
- **METODOLOGÍAS AUDITORÍA INFORMATICA**
- **RIESGO INHERENTE**
- **ENCUESTAS ESCALAS NO COMPARATIVAS**

ABSTRACT

Computer auditing has become a fundamental piece to guarantee the success and use of computer systems in organizations. The success or failure of an audit depends on several factors: expertise, tools, methodologies, etc., each of these elements are chosen by the IT auditor, based on their knowledge and experience. Incorrect selection of these components may result in subjective audit results and financial loss for the organization. Following this, an analysis of computer audit methodologies was proposed, to determine the level of inherent risk that its application would imply. Work with an own research methodology of quantitative exploratory type, based on the deductive method for the selection of parameters related to inherent risk, with a critical perspective for the quantification and interpretation of statistical data. The investigation will be validated with the Delphi method, through evaluations with non-comparative scales, applied to expert auditors to confirm the objectivity and impartiality of the evaluation model. The procedures to be carried out will demonstrate that it is possible to quantify the level of inherent risk, by means of occurrence, compliance and prioritization tables.

KEYWORDS:

- **COMPUTER AUDIT**
- **INFORMATIC AUDIT METHODOLOGIES**
- **INHERENT RISK**
- **NON-COMPARATIVE SCALE SURVEYS**

CAPÍTULO I

INTRODUCCIÓN

El presente trabajo de investigación tiene como finalidad conceder a las organizaciones e investigadores, un modelo base, para la selección de metodologías de auditoría informática con el menor grado de riesgo inherente. Mediante la generación de parámetros asociados al riesgo inherente y la aplicación del método Delphi, será posible validar y sustentar los resultados obtenidos. El desarrollo de esta investigación estará compuesto por las siguientes etapas: análisis e identificación de metodologías de auditoría de TI, definición de parámetros basados en el análisis, tablas de priorización, cumplimiento, ocurrencia, clasificación en rangos de valores y gráficos estadísticos que permitan visualizar y servir de apoyo en la selección de una metodología de auditoría de TI acorde a las necesidades de la organización.

1.1 Antecedentes

Se ha analizado e identificado que para las organizaciones hoy en día la información se ha convertido en el elemento intangible con mayor valor, además, si se considera aspectos como el aumento considerable de sistemas informáticos, que permiten gestionar la información para la toma de decisiones y con ello fomentan el crecimiento organizacional; la información puede ser considerada como uno de los activos fundamentales que posee una organización.

Dicha información es administrada por sistemas informáticos que han sido desarrollados para cumplir objetivos específicos, de ahí surge la necesidad de

garantizar y asegurar el funcionamiento adecuado y cumplimiento de objetivos de dichos sistemas informáticos mediante la aplicación de la auditoría de sistemas informáticos o auditorías de TI.

Tal como mencionan (Guitián & Dante, 2014), la auditoría de sistemas de información permite conocer la realidad de una organización en todos sus niveles en lo referente a los sistemas establecidos para gestionar la información, ya sea del ámbito empresarial o también en organizaciones de servicios. El autor (Soy Aumatell, 2003) indica que la auditoría de la información, a diferencia de las auditorías contables u otras modalidades que están bastante normalizadas, no dispone de una metodología estándar y consensuada, ni tampoco de directrices o normas que permitan contrastar los resultados obtenidos.

Por otra parte, el autor (Guitián & Dante, 2014) indica que existe una tendencia a realizar auditorías de enfoque híbrido-holístico, es decir, guías genéricas que se adapten a las necesidades de la organización. Con la misma propensión se encuentra la Asociación internacional que da apoyo a los controles de sistemas de información, (ISACA, 2019), señala que son varias las metodologías o marcos de referencia que requieren una gran cantidad de esfuerzo, tiempo, recursos financieros y tienden a ser complejos; al final la calidad de los resultados de auditoría son propensos a ser subjetivos debido a que no se ha considerado el riesgo inherente propio de la metodología seleccionada para el desarrollo del proceso de auditaría en la organización.

Basados en los aspectos que disminuyen la credibilidad de los resultados de una auditoría se encuentra la necesidad de acometer un proceso de evaluación a

metodologías de auditoría de la información, para su correcta selección y aplicación, tomando en consideración parámetros basados en su riesgo inherente.

1.2 Problemática

1.2.1 Contextualización del problema

Las metodologías de auditoría tradicionales se han vuelto ineficientes ante la gran cantidad de información y complejidad de los sistemas informáticos modernos, según un estudio realizado por la revista Forbes, el autor (Bernard, 2018) menciona que la cantidad de datos producidos diariamente a nivel mundial es de 2.5 quintillones de bytes, cuantía que exclusivamente debería ser manipulada mediante técnicas de Minería de datos. Llevar a cabo un proceso de auditoría holístico y eficiente con esta inmensa nube de datos es inimaginable, es por ello que actualmente se emplean técnicas avanzadas de manejo de datos para priorizar información trascendental para el auditor.

La función de un auditor es emitir recomendaciones para mejorar los procesos de una organización, empresas expertas en auditoría han desarrollado herramientas que automatizan el proceso de verificación de cumplimiento de indicadores propuestos en cada marco de gestión como COBIT, MAGERIT, OCTAVE, ISO, etc., mediante los cuales las organizaciones puedan certificarse en parámetros como: seguridad, riesgos, calidad, procesos de negocio, etc. No obstante, el auditor más que una herramienta de automatización, requiere de guías y escalas que le permitan conocer la efectividad de las herramientas con las que efectúa programas de auditoría y al mismo tiempo emitir resultados precisos en pro del desarrollo de la organización.

A nivel general, se puede apreciar brechas importantes en la aplicación de programas de auditoría informática debido al desconocimiento, inexperiencia, uso inadecuado de metodologías por parte del auditor y por falta de investigación. Un escenario específico de esta problemática es el sistema escolástico de Instituciones de Educación Superior en el Ecuador, las cuales cuentan con indicadores de acreditación, más no, con marcos de referencia regulatorios, peor aún metodologías que permitan a los auditores emitir criterios imparciales.

La calidad de los resultados de una auditoría informática, depende de varios factores como: experticia del auditor, metodologías a utilizar, tamaño de la organización, etc., por esta razón, es necesario definir parámetros, rangos y categorías asociados al riesgo inherente para aplicarlos a las principales metodologías de auditoría y con ello facultar así al auditor una herramienta que permita la selección de la mejor auditoría, para que continúe con la ejecución y la obtención de resultados objetivos.

1.3 Formulación del problema

¿Cómo desarrollar un análisis de metodologías de auditoría de sistemas de información, basado en cuantificadores asociados al riesgo inherente, para evaluar la efectividad de las metodologías y el nivel de riesgo inherente que implicaría su aplicación?

1.4 Justificación

La información generada por organizaciones ha crecido en volúmenes importantes, lo que obliga el uso de herramientas aptas para el tratamiento de

información, tomando en cuenta criterios de confidencialidad, integridad, disponibilidad, autenticidad, trazabilidad y los riesgos que estas características conllevarían durante una auditoría, sin embargo, un auditor informático necesita de escalas y guías de contraste para calcular el riesgo inherente existente en las metodologías de auditoría que él cree necesario utilizar.

El tamaño de la organización no es importante, cuando se trata de mitigar el riesgo inherente de una auditoría informática, los auditores y las partes interesadas en general deben estar conscientes de la calidad, confiabilidad de las herramientas y técnicas empleadas para llevar a cabo este proceso crítico. Si el criterio del auditor falla por no tomar en cuenta estos factores, el impacto generado puede ocasionar pérdidas millonarias en cualquier organización.

Por esta razón, es importante establecer parámetros asociados al riesgo inherente que permitan contrastar la subjetividad y que facultarán al auditor la emisión de criterios objetivos y adecuados a la realidad de las organizaciones.

1.5 Objetivos

1.5.1 Objetivo general

Determinar el nivel de riesgo inherente en metodologías de auditoría informática usando escalas no comparativas.

1.5.2 Objetivos Específicos

- Realizar una revisión de literatura para conocer los factores que influyen en la subjetividad de resultados de las metodologías de auditoría informática.

- Establecer características y niveles de acuerdo, tomando en consideración criterios de auditores informáticos expertos, fundamentado en escalas no comparativas para la determinación del riesgo inherente existente en las metodologías de auditoría informática.
- Comparar los resultados obtenidos en la evaluación de cada metodología usando técnicas de tabulación cuantitativa para determinar la metodología informática que posee un grado de subjetividad menor.
- Validar el método de evaluación elaborado, usando la técnica Delphi con la finalidad de rectificar, en caso de existir consideraciones hechas por los expertos.

1.6 Alcance

La presente investigación contempla la definición, análisis y validación de un modelo comparativo de metodologías de auditoría informática mediante el establecimiento de parámetros, rangos y categorías asociados al riesgo inherente.

Para el pre análisis de los parámetros asociados al riesgo y su post validación se hace uso de la matriz de priorización de Holmes y se aplican escalas Likert para medir el nivel de riesgo, probabilidad e impacto de cada uno de ellos.

El alcance cubre la validación del modelo por auditores expertos en el área de TI utilizando el método Delphi, con el propósito de ofrecer resultados legítimos que sirvan de guía para entidades y profesionales comprometidos con la validez y calidad de los resultados que una auditoría de cualquier magnitud precisa.

En función de la validación del modelo propuesto, se depura y se redefine en caso de ser necesario, cabe resaltar que este modelo es específico para conocer el

riesgo inherente de metodologías de auditoría informática. En caso de requerir aplicación en un ámbito diferente es necesario llevar a cabo el mismo proceso para la definición de un nuevo modelo que se ajuste a los requerimientos del auditor.

CAPÍTULO II

MARCO TEÓRICO

2.1 Señalamiento de variables

- **Variable independiente:** Parámetros asociados al riesgo inherente
- **Variable dependiente:** Metodologías de auditoría informática

2.1.1 Red de Categorías

Para fundamentar el marco teórico de investigación, se estructuró una red de categorías, que facilitan la percepción del objeto de estudio, el esquema de red se presenta en la figura 1.

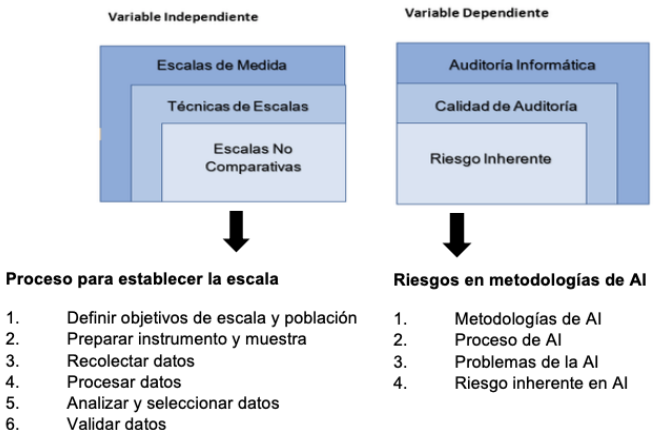

Figura 1. Red de categorías para las variables de investigación

2.2 Escalas de medida

El uso y procedencia de la escala como instrumento para la recolección de información, se relaciona con el enfoque cuantitativo dentro de una investigación. Es importante conocer el tipo de escala que se va a utilizar dependiendo de las características de los datos a comparar, puesto que de esto dependerá la confiabilidad de los resultados.

2.2.1 Técnicas de Escalas

Según el estudio realizado por (Baldeón Garzón & Coronel Guerrero, 2012) comentan que en el mundo de la investigación se han desarrollado una gran cantidad de escalas de medición, donde la mayoría de investigadores las han clasificado en dos grandes grupos que son escalas comparativas y no comparativas. Debido a la naturaleza del tema de investigación del presente trabajo se ve necesario únicamente incluir el análisis de las escalas no comparativas.

2.2.2 Escalas No Comparativas

De acuerdo a (Cárdenas, 2010) consiste en un tipo de técnica de escala, donde cada objeto de estímulo se evalúa de manera independiente con relación a los otros objetos en el conjunto de estímulos, por otra parte, el autor (Mario, 2012) indica que las escalas no comparativas pueden emplear cualquier tipo de calificación. Se subdivide en las siguientes escalas de clasificación:

2.2.3 Escala de Clasificación Continua

Este tipo de escala es fácil de construir es gráfica, simplemente traza una línea horizontal numerada y se establece un criterio, por ejemplo, malo y bueno a cada extremo de la línea, luego se les solicita a los entrevistados que califiquen escribiendo una marca en la posición correspondiente de la línea. Una de las desventajas de esta clasificación es que la puntuación puede ser poco confiable.

2.2.4 Escala de clasificación por reactivos

Es una escala por categorías que posee números o descripciones breves relacionadas con cada una. Las categorías van ordenadas de acuerdo a su posición y se solicita a los participantes que seleccionen la categoría específica que mejor define al objeto que se busca calificar.

2.2.5 Escala de Likert

El autor (Cárdenas, 2013) lo define como una escala de medición que posee cinco categorías con respuestas que van desde “completo desacuerdo” a “completo acuerdo”, por otra parte, el autor (Hernández, 2013) completa la definición cuando menciona que esta escala indica el nivel de acuerdo o desacuerdo con cada una de las series de afirmaciones sobre los objetos de estímulo, a continuación, en la tabla 1 se presenta un ejemplo de la estructura de este tipo de escala.

Tabla 1
Estructura de una Tabla de Likert

Categoría	Completamente de acuerdo	De acuerdo	Ni de acuerdo ni en desacuerdo	En desacuerdo	Completamente en desacuerdo
Tienda X vende productos de alta calidad	X				
Me gusta comprar en Tienda X		X			
Las políticas de crédito en Tienda X son terribles				X	
La atención de Tienda X es muy buena	X				
Los precios de Tienda X son bajos			X		

Fuente (Hernández, 2013)

2.2.6 Escala de Diferencial Semántico

Se lo define como una escala de clasificación que relaciona etiquetas bipolares y que poseen un significado semántico, por ejemplo: vacío - lleno. En el eje horizontal se escribe el rango, por ejemplo, de 1 a 5 y en el eje vertical van las etiquetas. Los participantes deben marcar con una X para cada etiqueta.

2.2.7 Escala de Stapel

Según menciona (Cárdenas, 2010) se considera a esta escala como una versión reducida de la escala de diferencial semántico. El entrevistado debe dar su opinión con respecto a un único adjetivo en medio de un rango de valores de entre [-5, 5].

2.3 Auditoría informática

2.3.1 Antecedentes

El constante y veloz desarrollo tecnológico ha provocado que los sistemas informáticos sean potentes herramientas, aptas para asistir y ser aplicadas en cualquier tipo de organización, tal como indica (E. Gómez, 2015) a partir del siglo XX los sistemas de información se han vuelto necesarios en cualquier organización empresarial. Por otra parte, se ha analizado que la importancia del software empresarial se ha generado por:

- Versatilidad del software.
- Funcionalidades basadas en la razón de ser de las organizaciones.
- Reglas del negocio.
- Sustitución a procesos establecidos.
- Poder de toma de decisiones.

Debido a la trascendencia antes mencionada del software en las organizaciones, ha surgido la necesidad de controlar y regular los Sistemas Informáticos, tal como menciona (Mario, 2012) no existe evidencias comprobables sobre los inicios de la Auditoría de Sistemas, sin embargo, se mencionan ciertos autores tales como Echenique, Lee, Rosalva Escobedo Valenzuela, etc. como sus progenitores ya que realizaron las primeras publicaciones sobre este proceso de evaluación.

El autor (Carrion Haro & Leyton, 2006) indica que la Auditoría Informática surge por la necesidad de evaluar no solo sistemas informáticos, sino la información generada por los mismos, sus componentes y todo lo que esté relacionado con ello.

Acotando al tema (Mario, 2012) en su publicación indica que un programa de Auditoría Informática busca evaluar controles internos que se realizan en un sistema de información, verificando fases y resultados de procesamiento para localizar errores, que deberán ser reducidos a futuro mediante las mejoras recomendadas.

También señala que no es suficiente verificar resultados de los procesos, sino que el auditor debe revisar existan los suficientes controles internos en el sistema informático, clasificando las metodologías de Auditoría en dos notables grupos e indica lo siguiente:

2.3.1.1 Auditoría Externa

Es realizada por auditores externos a la empresa valorada, para permitir que se aplique con toda libertad los métodos, técnicas y herramientas de auditoría, donde se emitirá resultados absolutamente independientes. En la figura 2 se muestran los elementos de la auditoría externa, el auditado es definido como la "organización que es auditada" y cliente es definido como la "organización o persona que solicita la auditoría".

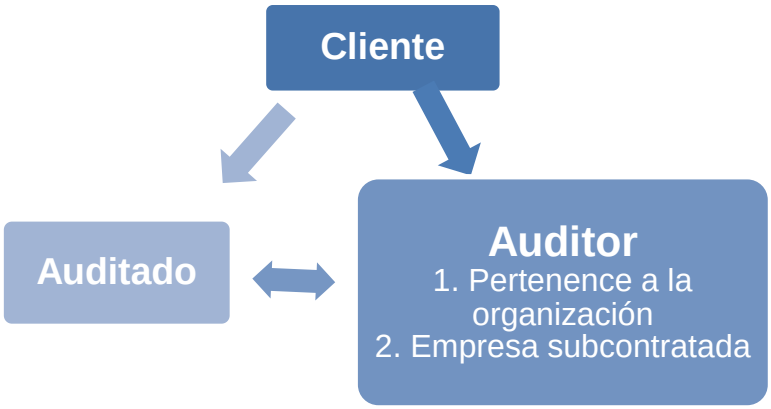

Figura 2. Elementos de la auditoría externa
Fuente: (Mario, 2012)

En este contexto existe un acuerdo contractual de colaboración entre cliente y suministrador (organización auditada) para someterse a una auditoría de evaluación o seguimiento con la finalidad de establecer relaciones comerciales o de alguna otra índole.

2.3.1.2 Auditoría Interna

El auditor a cargo de este proceso de auditoría desempeña sus labores en la empresa donde se realiza la auditoría, está incluido en las actividades y podría llegar a influir en el juicio emitido sobre la evaluación de las áreas de la empresa.

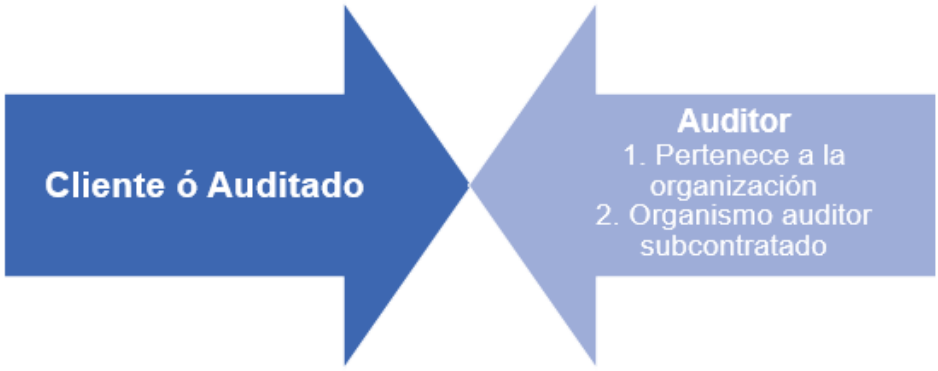

Figura 3. Elementos de la auditoría interna
Fuente: (Mario, 2012)

2.3.2 Auditoría Informática

El término Auditoría Informática por el autor (Guindel Sánchez, 2009) indica que dicho término es mal utilizado al considerar que consiste en una evaluación con el único objetivo de detectar errores y fallas de los Sistemas, sin embargo, este término tiene mayor alcance. De acuerdo a la revisión de literatura, las definiciones difieren, pero todas tratan de describir los procesos y detalles que abarca una

Auditoría Informática, a continuación, se presentan varias definiciones de algunos autores:

Es un proceso formal ejecutado por especialistas del área de Auditoría Informática, que está orientado a la verificación y aseguramiento de las políticas y procedimientos establecidos para el manejo y uso adecuado de las TI para que se lleve a cabo de forma oportuna y eficiente (Guindel Sánchez, 2009).

La auditoría informática comprende el diagnóstico y evaluación del ambiente informático (hardware, software, bases de datos, redes, instalaciones, etc.) sobre la base de estándares internacionales y de modelos de referencia que hacen recomendaciones sobre la forma de administrarlo; es un proceso empresarial, en el cual intervienen de manera conjunta responsables del área de TI, administradores, contadores, auditores y coordinadores del resto de procesos ejecutados en la organización; su participación puede concretarse en las diferentes etapas de la auditoría informática: planificación, ejecución (levantamiento de información), análisis de resultados, hallazgos o evidencias útiles en la elaboración del informe final (Cárdenas, 2010).

Una definición completa es la del autor (Mario, 2012) cuando menciona que una auditoría de TI es “una revisión técnica y especializada realizada a los sistemas informáticos de una organización, así como a sus equipos de comunicaciones, periféricos y otros. Esta revisión se realiza también a la gestión informática, uso de recursos y medidas de seguridad. Tiene como propósito la evaluación del correcto uso de los sistemas para la gestión de datos, procesamiento de información y la emisión adecuada de resultados, incluye también evaluaciones al cumplimiento de

funciones y actividades de funcionarios o usuarios que estén involucrados con los servicios que proporcionan los sistemas informáticos".

Analizando estos conceptos, el grupo de trabajo planteó la definición de auditoría de sistemas de información como un procedimiento técnico de valoración realizado por expertos en AI, quienes basados en técnicas, herramientas, estándares internacionales y modelos de referencia evalúan sistemas informáticos, hardware e información de una organización, proceso que puede o no ser solicitado por la dirección de una organización, con el objetivo de revisar y corregir el rendimiento, seguridad, efectividad y emisión correcta de resultados.

2.3.3 Fases de la Auditoría Informática

Generalmente una auditoría informática está estructurada en tres notables etapas, descritas a continuación, de acuerdo al análisis realizado por (Bonilla, 2015).

2.3.3.1 Primera etapa: planificación de la auditoría

El autor (Bonilla, 2015) considera a esta etapa como fundamental en el proceso de auditoría ya que establece las actividades que serán desarrolladas durante su ejecución, también define procesos, las técnicas y los temarios que se necesiten para continuar con la fase de ejecución. La importancia de esta etapa radica en que aquí se plantea una estrategia general que genere los resultados deseados, la planificación de la auditoría es realizada considerando el tamaño, complejidad de la organización, el nivel de conocimiento y experiencia del auditor en la organización auditada, generalmente implica procedimientos como:

- Identificación de los motivos para ejecutar la auditoría.

- Realizar una visita previa al establecimiento que será auditado.
- Establecimiento de los objetivos de la auditoría.
- Definición de los puntos a evaluarse en la auditoría.
- Generación de planes, temarios, planificación de presupuestos para la auditoría.
- Reconocimiento y elección de métodos, técnicas, instrumentación y procedimientos necesarios para la auditoría.
- Asignación de recursos y equipos para la auditoría.

2.3.3.2 Segunda etapa: ejecución de la auditoría

En esta etapa se ejecuta las pruebas de auditoría, es decir se dedica directamente al trabajo de campo, se debe considerar se podrán realizar pruebas en cualquier momento, el propósito es hallar y salvaguardar las evidencias correspondientes a las actividades que se realicen en la organización, se realizan acciones puntuales como:

- Ejecución de actividades planificadas para la auditoría.
- Uso de herramientas e instrumentos para la auditoría.
- Identificación y registro de las desviaciones o anomalías halladas.
- Elaboración de las conclusiones preliminares para pasarlas a discusión.
- Agrupación de la documentación generada durante la auditoría.

2.3.3.3 Tercera etapa: dictamen de la auditoría informática

La tercera y última etapa del proceso de auditoría implica la generación del reporte de hallazgos, denominado también como informe de auditoría, el cual

contiene las conclusiones y recomendaciones correspondientes a los problemas y falencias que fueron halladas en la ejecución de la auditoría, comprende actividades específicas como:

- Análisis de información y elaboración de informes con las novedades detectadas.
- Elaboración del informe de auditoría.
- Exposición del informe de auditoría.

2.3.4 Tipos y clases de auditorías informáticas

2.3.4.1 Auditoría con la computadora

Según indica (Mario, 2012) es un tipo de auditoría donde mediante un análisis detallado de necesidades por parte del auditor y de competencias de la empresa se hace uso de equipos informáticos para la valoración de las actividades y procesos sean o no computarizados susceptibles de automatización.

2.3.4.2 Auditoría sin la computadora

En este tipo de auditoría indica (Mario, 2012) se valora a los sistemas basados en métodos de valoración tradicionales con la diferencia que no se usa sistemas informáticos, aunque éstos se encuentran involucrados en la evaluación. También señala que este tipo de auditoría está dirigida para temas operativos, financieros, administrativos, también se menciona que es un tipo de auditoría donde sus métodos, técnicas y procedimientos están enfocados específicamente en la evaluación típica de su proceder y también la validez de las transacciones económicas, administrativas y operacionales de un área de cómputo específica, y de

todos los escenarios que afectan a las actividades donde se trabaja con sistemas informáticos, esta evaluación se realiza sin el uso de los sistemas computacionales.

2.3.4.3 Auditoría a la Gestión Informática

El autor (Mario, 2012) menciona que es una auditoría empleada específicamente para la examinación de servicios y actividades administrativas que desempeña un departamento de cómputo, tales como proyección, organización, gestión y verificación de información. Este tipo de auditoría se realiza con el objetivo de revisar la ejecución de funciones y actividades destinadas a los funcionarios y usuarios, así como también controla y valora las operaciones y tareas en las que trabaja el sistema, el uso y protección de la información. Otro uso es la verificación del avance, establecimiento, mantenimiento y uso de los sistemas, sus equipos físicos e instalaciones. El objetivo de esta auditoría es informar a los auditores sobre el estado y calidad de la administración de los sistemas informáticos de una empresa.

2.3.4.4 Auditoría al sistema de cómputo

El autor (Mario, 2012) señala que es un programa de auditoría de tipo técnico, que tiene como fin la valoración de funcionamiento y uso adecuado del hardware, software y periféricos de la organización. Esta auditoría analiza específicamente la arquitectura de las partes físicas y demás elementos del hardware, incluyendo equipos agregados, las instalaciones y comunicaciones externas o internas, también considera el diseño, desarrollo y uso del software de operación, base y aplicación, es decir sistemas operativos, lenguajes de procesamiento y programas de

desarrollo, o grupo de aplicaciones institucionales que son utilizados en la empresa donde trabajan los equipos de cómputo en evaluación.

2.3.4.5 Auditoría Alrededor de la Computadora

En la investigación realizada por (Mario, 2012) se menciona que en este tipo de auditoría se evalúa la actividad de los sistemas informáticos, con el afán de evaluar las actividades vinculadas que se llevan alrededor de éstos, además se indica que es una revisión específica a todo lo que está alrededor de un equipo informático, es decir su software, actividades, realizando una evaluación profunda de sus funciones y procesos de acceso y procesamiento de datos, la generación y posterior almacenamiento de los resultados, las actividades de organización y presupuesto del centro informático, así como también la gestión administrativa, el servicio de atención al usuario, con ello se busca examinar individual y completamente a las figuras que aportan al buen desempeño del área.

2.3.4.6 Auditoría de Seguridad a Sistemas Computacionales

(Mario, 2012), menciona que la seguridad es un parámetro muy importante ya que incluso puede estar relacionado con otras auditorías, por lo cual es muy importante su evaluación individual, en este tipo de auditoría se realiza una revisión exhaustiva, técnica y experta en los temas relacionados a la seguridad de un sistema informático y usuarios, con respecto al sistema se revisa las aplicaciones, funcionalidades y acciones que se toman tanto de forma preventiva, como también correctiva y que contribuyan a resguardar la seguridad de las estaciones de trabajo, redes, bases de datos, establecimiento y usuarios del sistema. Además, se gestiona revisiones de los planes de contingencia y medidas de defensa para el activo más

importante, es decir la información, y para todos los aspectos que contribuyen a la salvaguarda del área, incluyendo la prevención y eliminación de brechas y virus informáticos.

2.3.4.7 Auditoría a los Sistemas de Redes

(Cárdenas, 2010) menciona que para ejecutar una auditoría de redes hay que considerar niveles arquitectónicos, administrativos, funcionales, software, hardware y demás aspectos que repercuten en los sistemas de comunicaciones de la organización. Además, menciona que el objetivo de esta auditoría es proteger el principal recurso de una organización, la información, disminuyendo el riesgo de ser vulnerado a causa de debilidades en la infraestructura tecnológica de la organización.

2.3.4.8 Auditoría Integral a Centros de Cómputo

Debido al uso progresivo de equipos informáticos en las empresas es imprescindible supervisar constantemente el funcionamiento y uso adecuado de estos sistemas. (Mario, 2012) indica que esta auditoría se debe llevar a cabo por un equipo de auditores multidisciplinario, perpetrando, de forma integral el control interno de los sistemas físicos y lógicos y por consiguiente determinar su impacto. Finalmente, (Mario, 2012) menciona que esta auditoría incluye la revisión del sistema administrativo para la adquisición de software y hardware, puesto que, es necesaria una adecuada integración de recursos informáticos cumpliendo con normas, políticas y estándares que regulan la implementación de este tipo de sistemas.

2.3.4.9 Auditoría ISO - 9000 Sistemas Computacionales

ISO-9000 es un conjunto de normas canalizadas para asegurar la calidad de los productos o servicios que brinda una organización. (Cárdenas, 2010) señala que los auditores se deben guiar estrictamente por los lineamientos y procedimientos que dicta la norma, de modo que, la empresa mejore la calidad de sus procesos. Los fundamentos de calidad que mide esta norma son: documentar lo que se hace, realizar lo que se está documentando, revisar lo que se hace con lo documentado (ISO-9000, 2017). Para que la certificación ISO-9000 tenga validez, la auditoría debe ser llevada a cabo por una entidad externa, caso contrario no tendrá efecto.

2.3.4.10Auditoría Outsourcing

Outsourcing se refiere a la transferencia de la propiedad de una o más funciones del negocio que normalmente son ejecutadas por el personal y recursos internos, hacia una entidad externa. (Cárdenas, 2010) menciona que, esta auditoría permite conocer la confiabilidad y eficiencia de los proveedores que ofrecen tercerización de servicios tales como: procesamiento de datos, recurso humano, capacitación, mantenimiento, etc. Esta auditoría puede ser enfocada desde dos puntos de vista: el cliente de outsourcing o el proveedor de outsourcing, de esta manera se hace un análisis exhaustivo de los sistemas computacionales de la calidad del servicio.

2.3.4.11Auditoría Ergonómica de Sistemas Computacionales

El término ergonomía en auditoría de sistemas computacionales, se entiende como el estudio, medición del bienestar, seguridad y repercusiones que tienen los

elementos mobiliarios en el ambiente laboral y la salud de los usuarios, así como también su productividad. (Cárdenas, 2010) indica que el objetivo primordial que tiene esta auditoría es la búsqueda del mejoramiento del desempeño del trabajador, adaptando productos de uso cotidiano como sillas, mesas, apoya-cabezas para la satisfacción, seguridad y salud del trabajador.

2.3.5 Objetivos de la Auditoría Informática

Según el autor (Cárdenas, 2010) los principales objetivos de una Auditoría Informática son:

- Evaluar la eficiencia de un Sistema Informático.
- Verificar el cumplimiento del Estándar o Normativa en ese ámbito.
- Revisar eficazmente la gestión de recursos informáticos.

Por otra parte, el autor (Carrion Haro & Leyton, 2006) indica que los objetivos de una auditoría son de carácter general y pueden ser adecuados al tipo de auditoría que pretenda realizarse, pero es importante primero establecer los objetivos que se quieren cubrir en la auditoría. También hace énfasis en que el objetivo principal de una auditoría informática es la operatividad, considerando que no es admisible detener la maquinaria informática para descubrir fallos, también indica que la auditoría debe comenzar sus actividades mientras los Sistemas Informáticos se encuentran operativos, buscando mantenerlos en ese estado a nivel parcial y global.

2.3.6 Metodologías de Auditoría Informática

Tal como se menciona en (Carrion Haro & Leyton, 2006),la identificación de riesgos de manera anticipada ayuda a implementar de forma oportuna las medidas

de seguridad, esta actividad puede ser facilitada gracias a las metodologías de auditoría. Así mismo (Mario, 2012) establece que el uso de cualquier metodología depende del objeto en revisión o análisis y clasifica en dos grupos específicos a las Metodologías de Auditoría Informática:

2.3.6.1 Cuantitativas

Basadas en un modelo matemático numérico que ayuda a la realización del trabajo, producen una lista de riesgos que se pueden comprar fácilmente ya que poseen valores numéricos. Han sido diseñadas para generar una lista de riesgos con valores que determinan los niveles de ocurrencia de eventos extraídos de los riesgos (Mario, 2012).

2.3.6.2 Cualitativas

Están basadas en el criterio y razonamiento humano, quién es capaz de definir un proceso de trabajo, puede excluir riesgos significantes gracias a la experiencia. Se basa en métodos estadísticos y lógica borrosa (Mario, 2012).

2.3.7 Iso 19000

2.3.7.1 Objeto y campo de uso

Según se indica en (Rey, 2007) el objetivo de la norma internacional ISO 19000 es entregar un marco de referencia o guía sobre las directrices de una auditoría, la administración de un programa de auditoría, la ejecución de auditorías a sistemas de gestión de calidad, entre otros. Con respecto a la aplicación, el mismo autor indica que la implementación está abierta a las organizaciones que deben

efectuar auditorías internas o externas a los sistemas de gestión de la calidad o que deben gestionar programas de auditoría.

2.3.7.2 Contenido De Un Programa De Auditoría

Tal como indica (Rey, 2007) los proyectos de auditoría deberán incorporar los aspectos que se mencionan a continuación:

- Auditorías internas para abarcar el sistema de gestión de calidad en una organización durante el año en curso.
- Auditorías de segunda parte al sistema de gestión de proveedores de productos o servicios críticos.
- Auditorías para entregar y sostener la certificación efectuada por organismos de certificación.
- Implica la planificación, aprovisionamiento de recursos y el decreto de procedimientos acordes que permitan realizar las auditorías dentro del programa.

2.3.7.3 Principios de Auditoría

De acuerdo con (Rey, 2007) las auditorías están caracterizadas por someterse a varios principios, los cuales convierten a la auditoría en una herramienta eficaz y confiable que apoya al cumplimiento de políticas y controles de gestión, de esta forma aporta con información sobre la cual una organización ejerce la mejoría de su desempeño. Principalmente el apego a estos principios es un requisito necesario para otorgar las conclusiones de la auditoría y que ellas sean

adecuadas y capaces, que posibiliten a los auditores trabajar de forma independiente para que se lleguen a conclusiones afines en condiciones similares.

2.3.7.4 Responsabilidades, recursos y procedimientos

En este tema el autor (Rey, 2007) indica que el compromiso de la administración de un programa de auditoría debe asignarse a una o más personas, que tengan conocimientos generales de los principios de la auditoría, de la jurisdicción de los auditores y de la implementación de técnicas de auditoría. Las personas deberán ser habilidosas para la gestión, con conocimientos técnicos y concernientes al negocio considerando las funciones que van a ser auditadas.

2.3.7.5 Recursos del programa de Auditoría

El mismo autor (Rey, 2007) además señala que cuando se identifiquen los procedimientos del programa de auditoría se debería considerar:

- Recursos financieros precisos para desplegar, establecer, guiar y mejorar las acciones de la auditoría.
- Técnicas de auditoría.
- Procedimientos para conseguir, sostener la competencia de los auditores y lograr el mejoramiento del desempeño.
- Disposición de personal experto, así como de auditores que cuenten con la competencia apropiada para cumplir las metas planteadas de la auditoría.
- Extensión y alcance del programa de auditoría.
- Tiempos de movilización, hospedaje y otros gastos que implica el proceso de auditoría.

2.3.7.6 Metodologías para Análisis De Riesgos

Se puede entender a una metodología como una agrupación de prácticas que establecen una investigación. De acuerdo a la literatura existen múltiples metodologías que posibilitan ejecutar el análisis de riesgos que pueden estar presentes en una organización, por ello a continuación se presenta una breve reseña sobre algunos de estos métodos.

2.4 Cobit

El autor (E. Gómez, 2015) la considera como una herramienta para el gobierno de TI, presentada en el año 1996, la misma que vincula a la gestión de tecnología informática con prácticas de control, así mismo establece y aplica estándares internacionales en un recurso crítico para la gerencia, los profesionales de control y auditores. El mismo autor indica que se basa en la filosofía de que los recursos de TI poseen la necesidad de ser gestionados por un conjunto de procesos integrales que provean información pertinente y confiable, para que una organización logre sus objetivos. A continuación, en la figura 4 se muestra la estructura general conceptual de COBIT 5.

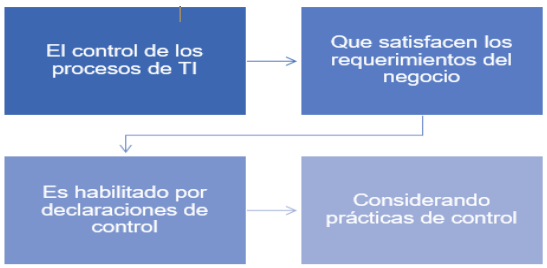

Figura 4. Estructura de COBIT

La herramienta está estructurada de forma que se gestione completamente las tecnologías de información (TI) de la organización, organizada en componentes tal se menciona a continuación:

- **Procesos de TI:** para garantizar mecanismos de control y monitoreo adecuado de los requerimientos de
- **Recursos de TI:** administrados por los encargados del proceso para alcanzar los objetivos de los requerimientos del negocio.
- **Requerimientos de negocio:** basados en las necesidades de la organización.

Fuente: (COBIT 5, 2018)

2.4.1.1 Octave

Son las siglas de Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE) es una metodología para el análisis de riesgos creado por el Software Engineering Institute (SEI) en la Universidad de Carnegie Mellon. Pone a disposición una serie de herramientas, técnicas y métodos para la identificación y gestión de riesgos de seguridad de los sistemas de información (OCTAVE, 2007) .Las fases necesarias para llevar a cabo la examinación de problemas organizacionales y tecnológicos son descritas en la figura 5.

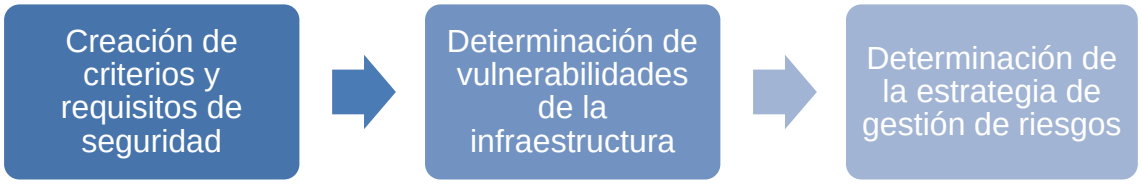

Figura 5. Fases Metodología - OCTAVE
Fuente: (Octave, 2018)

2.4.1.1.1 Creación de Criterios y Requisitos de Seguridad

Los activos de información, sus valores, amenazas y los requisitos de seguridad se identifican utilizando el conocimiento del personal de múltiples niveles dentro de la organización.

2.4.1.1.2 Identifica Vulnerabilidades de Infraestructura

Se hace uso de la información recopilada en la fase uno para identificar los componentes de infraestructura de alta prioridad.

2.4.1.1.3 Determina Estrategias y Planes de Seguridad

Esta etapa comprende un compendio de información de las fases uno y dos con el propósito de identificar mediante el análisis de los activos las amenazas y vulnerabilidades asociadas.

2.4.1.2 Magerit

Es una metodología de gestión y análisis de riesgos desarrollado en España por el Consejo Superior de Administración Electrónica (CSAE), en respuesta a la dependencia masiva de la sociedad a las TI (Syalim, Hori, & Sakurai, 2009) .El proceso de análisis de riesgos utilizando MAGERIT se muestra en la figura 6.

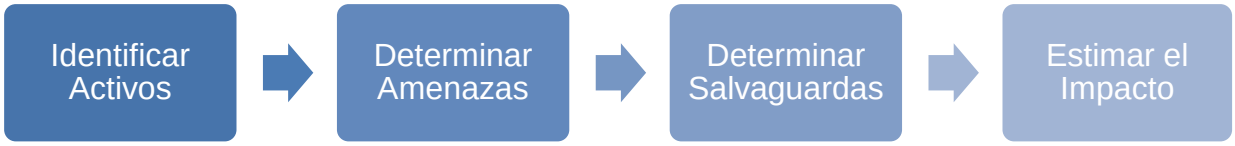

Figura 6. Estructura metodología MAGERIT
Fuente: (Magerit, 2018)

2.4.1.2.1 Identifica activos y relación con perjuicios que provoca la degradación

Los activos corresponden a las atributos y elementos inmersos en las TIC que son necesarios para que la organización funcione adecuadamente y que son susceptibles a ser atacados, estos activos pueden ser información, hardware, software, recurso humano, etc. En este paso es necesario establecer el valor cuantitativo, cualitativo y la interrelación de entre activos, pues cuanto más valioso es un activo, necesitará de mayores medidas de seguridad.

2.4.1.2.2 Determinar amenazas relacionadas a los activos

Las amenazas son cosas que podrían afectar y causar daño a los activos, estas amenazas pueden ser de origen natural como terremotos, de origen industrial como fallos eléctricos, defectos técnicos de las aplicaciones o vulnerabilidades,

causadas por personas de forma accidental y causadas por personas de forma intencionada. Para ello hay que establecer una valoración de cada amenaza y categorizarla de acuerdo al impacto al activo.

2.4.1.2.3 Determinar salvaguardas y su eficacia frente al riesgo

Las salvaguardas son mecanismos que ayudan a disminuir el riesgo o limitar el daño causado, estas salvaguardias son consideradas de acuerdo al tipo de activo a proteger, el grado de seguridad que necesita un activo, cantidad de amenazas a las que se está expuesto.

2.4.1.2.4 Estimación del impacto

El impacto es definido como el daño sobre el activo derivado de la materialización de la amenaza, el riesgo se incrementa proporcionalmente con su impacto y su frecuencia. Según la investigación realizada por (Syalim et al., 2009) se concluye que MAGERIT no proporciona una guía sobre las recomendaciones de control para la fase de análisis de riesgos, sino más bien para la etapa de gestión de la seguridad.

2.5 Calidad de auditoría

2.5.1 Calidad

El concepto “Calidad” es definido según la RAE como la propiedad o conjunto de propiedades inherentes a una cosa que permite apreciarla como igual, mejor o peor que las restantes de su misma clase. En auditoría la calidad no significa utilizar herramientas o metodologías que son tendencia, para que una auditoría informática sea de calidad debe ser tratada como un enfoque sistémico, ubicándola como un

componente de dicho sistema encargado de proteger y mejorar el funcionamiento de la organización auditada.

El objetivo primordial de una auditoría informática es evaluar los sistemas y procesos de información de la organización con el fin de contrastar si se está llevando a cabo un control adecuado de sus actividades, es vital que el auditor garantice una auditoría de calidad, generando confianza y seguridad para el auditado. La calidad no se improvisa, sino que, es fruto del trabajo competente, riguroso y sistemático del equipo de auditoría (Guindel Sánchez, 2009). Considerando que el objetivo principal de la calidad es satisfacer las necesidades del consumidor, existen tres factores determinantes para conseguir un producto o servicio de calidad:

- Dimensión técnica: aspectos metodológicos y tecnológicos que afectan al producto o servicio.
- Dimensión humana: preservar las buenas relaciones entre el cliente.
- Dimensión económica: intentar disminuir costos tanto para el auditado como para la empresa auditada.

2.5.2 Requisitos de calidad de la auditoría informática

Para garantizar que un programa de auditoría informática sea de calidad, debe cumplir al menos tres de los siguientes requisitos:

- **Plan de auditoría:** Donde se detalle en forma general al equipo de auditoría, su misión, sus funciones y las responsabilidades que tienen asignadas.

- **Manual de auditoría:** Donde se detalle específicamente las actividades que se van a realizar en el programa de auditoría, las metodologías y las herramientas que se emplearán.
- **Personal de auditoría:** se debe identificar los involucrados que participarán en el proceso de auditoría, ya que no se puede auditar a toda la organización.

2.5.3 Fases de una auditoría de calidad

En la figura 7 que se presenta a continuación, se expone las fases de una auditoría de calidad, la misma que deberá ser ejecutar por parte del equipo auditor quienes tendrán que respaldar los resultados del programa de auditoría.

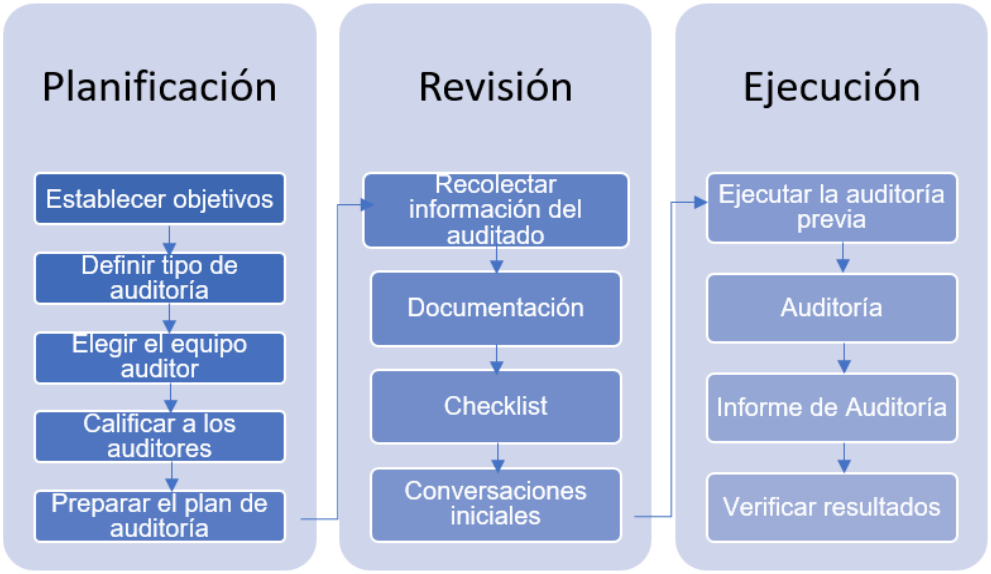

Figura 7. Principios de la seguridad de la información

Fuente: (Mario, 2012)

2.5.3.1 Planificación

El equipo de auditoría debe llevar a cabo las actividades de la figura para asegurar el cumplimiento de un proceso objetivo, sistemático y preciso. En la etapa de planeación se establece el objeto de auditoría, procedimientos, tareas, entidades afectadas y el equipo auditor responsable, esto con el objetivo de proceder de forma estructurada.

2.5.3.2 Revisión

En esta etapa el equipo auditor toma contacto con la filosofía, metas, actividades y procesos de la empresa para posteriormente hacer una lista de verificación, con todos los aspectos que se van a revisar en la auditoría. Es preciso informar con antelación las fechas de auditoría a la organización mediante una reunión con las máximas autoridades de la entidad objeto.

2.5.3.3 Ejecución

Contempla el desarrollo preliminar y final de la auditoría, se pretende identificar problemas y fallos de la entidad, con la finalidad de establecer propuestas y recomendaciones de mejora continua. Es importante aclarar que no todas las fases se presentan cuando se lleva a cabo una auditoría, depende en gran medida de la complejidad y amplitud de la misma (Guindel Sánchez, 2009).

2.6 Riesgo de Auditoría

El riesgo es definido como la probabilidad de que una amenaza afecte en gran medida a las vulnerabilidades de los sistemas de información de las

organizaciones. Los autores (Calderón & Ocaña, 2014) indican que no existe riesgo sin una vulnerabilidad o amenaza presente, también indica que en un programa de auditoría un riesgo puede estar presente en cualquier etapa del proceso, ya sea por inexperiencia, desconocimiento, desorganización del auditor, o por no utilizar las herramientas, metodologías o técnicas adecuadas. Un auditor puede generar informes errados o subjetivos por no haber tomado en cuenta faltas significativas en el proceso de auditoría, es por ello que existen niveles de riesgo para situaciones o hechos particulares.

2.6.1 Riesgo de Auditoría Informática

Se ha definido al riesgo de una auditoría informática como la posibilidad de omitir la detección o el descubrimiento de errores, durante la aplicación de un programa de auditoría debido a que sus procedimientos y controles no son suficientes o no permiten detectar dichas irregularidades significativas.

2.6.2 Riesgo Inherente

Es un componente del riesgo de auditoría, son errores importantes generados por la naturaleza y las características propias de la organización ya que forman parte de ella, tales como usuarios, el tipo y tamaño de la organización, cultura organizacional, estilos de gerencia, comunicación, administración de la organización y resistencia al programa de auditoría. Estos parámetros pueden influir y generar impactos negativos en el cumplimiento de los objetivos durante una auditoría de TI.

Un método preciso para identificar el riesgo inherente es considerar la identificación del riesgo como parte integral durante la indagación de la organización,

es decir que el auditor informático deberá tener total conocimiento sobre las reglas del negocio y las áreas que pueden representar fuentes de riesgo durante el programa de auditoría, tales como:

- Naturaleza de la Organización.
- Políticas Internas.
- Objetivos y Estrategias.
- Control Interno.
- Factores Externos.

2.6.3 Riesgos de Control

Son los riesgos que se suscitan por la estructura, diseño y procedimientos del Sistema de Control Interno implementado en la empresa.

2.6.4 Riesgos de Detección

Está relacionado con la ineficacia de los auditores al llevar a cabo los programas de auditoría, en otras palabras, planificaciones mal elaboradas. Según COSO el riesgo es un factor identificado que podría afectar a la consecución de un objetivo como:

- Efectividad de las operaciones.
- Confiabilidad de la información.
- Cumplimiento de leyes y regulaciones.

2.7 Análisis del riesgo

El primer paso es identificar los procesos críticos de la organización y su impacto en los sistemas de información, luego se procede con el análisis de amenazas y vulnerabilidades que afecten a los objetivos del plan estratégico de la entidad. Los riesgos de negocio pueden ser materializados por amenazas que afecten a los activos de la entidad y están relacionados con la confidencialidad, disponibilidad e integridad de la información (Baldeón Garzón & Coronel Guerrero, 2012).

2.7.1 Objetivos del análisis al riesgo

Los principales objetivos del análisis adecuado del riesgo de un programa de auditoría de TI son:

- Cuantificar el impacto y el costo de los riesgos potenciales.
- Justificar el costo/beneficio de la implementación de medidas de control.

2.7.2 Técnicas de evaluación del riesgo

Una técnica de evaluación del riesgo está relacionada con la identificación de los procesos más críticos del negocio y relacionado con las TI (ISACA, 2018). Esto permite establecer un enfoque holístico de las áreas que serán auditadas por su nivel de complejidad y criticidad, facilitando una gestión adecuada de la función de auditoría. Entre los métodos más relevantes para llevar a cabo este proceso se encuentran los citados por (Calderón & Ocaña, 2014).

- Dificultad técnica.

- Nivel de procedimientos de control.
- Nivel de pérdidas financieras.

2.7.3 Evaluación del riesgo de auditoría

La evaluación del riesgo se la puede interpretar como un proceso donde de acuerdo al análisis de existencia y magnitud de los factores del riesgo, se valora el riesgo presente en cada parámetro (Mario, 2012).En general los niveles de riesgo de auditoría se miden en cuatro probables niveles, estos son:

- Mínimo
- Bajo
- Medio
- Alto

El mismo autor (Mario, 2012) indica que la evaluación de los niveles de riesgo es un proceso completamente subjetivo y está alineado estrictamente al criterio, capacidad y experiencia del auditor. También señala que es la base para la determinación del planteamiento u orientación de la auditoría, por lo tanto, es un proceso cuidadoso que se realiza por quienes son poseedores de la mayor capacidad y experiencia en un equipo de trabajo.

2.7.4 Riesgo en herramientas de auditoría informática

Todas las profesiones cuentan con herramientas, procesos y metodologías para planificar, desarrollar o ejecutar una actividad. Un ingeniero civil necesita de software CAD, equipos de construcción, maquinaria especializada, un doctor posee herramientas de diagnóstico y equipos especializados, un auditor posee

metodologías, procesos, herramientas de verificación y cumplimiento, el uso adecuado de estos artefactos puede decidir el éxito o fracaso de una función. En el caso del ingeniero o del médico, una mala planificación de construcción o un mal diagnóstico puede provocar problemas críticos en proyectos e incluso el deceso de personas inocentes, en el caso específico de la auditoría, se puede comprometer el éxito o fracaso de la entidad auditada, lo cual es igual de grave, ya que, miles de empleos están en juego.

Para la ejecución de una auditoría de TI existen diversas herramientas y metodologías certificadas por organismos internacionales, que han sido usadas por años y cada vez se han hecho más populares por el éxito, seguridad y confianza que han propagado en las organizaciones, sin embargo, muy pocos estudios se han hecho sobre el riesgo inherente que poseen las metodologías, dejando muchas veces ambiguo la razón por la cual un auditor elige una u otra para llevar a cabo el proceso de auditoría. En la investigación realizada por (Guitián & Dante, 2014) se observa una tendencia a realizar auditorías de TI con enfoque híbrido orientadas hacia la identificación y mejora continua de estrategias, recursos y procesos de la organización, y así generar de resultados de calidad sostenibles en el tiempo.

2.8 Método empírico analítico

Para la ejecución del presente proyecto se debe considerar un tipo de investigación, se seleccionó la investigación aplicada debido a que se fundamenta en el empleo y uso de los conocimientos adquiridos, también porque realiza la implementación y esquematiza la práctica basada en la investigación, es decir la

utilización de los conocimientos en la práctica para aplicarlos a favor de los grupos que participan el desarrollo y a la sociedad en general.

2.8.1 Método Delphi

Es un método de información ordenado que se basa en la prospectiva y el presagio, el cual está basado en un panel de especialistas para los asuntos tratados o investigados quienes, en base a su conocimiento o experiencias comprobadas, como resultado se obtiene información cualitativa con gran precisión; forma un intercambio de opiniones o juicios de expertos para proceder a destacar respuestas a las preguntas planteadas en un cuestionario, utiliza elementos como:

- Anonimato de participantes
- Feedback de opiniones
- Respuestas estadísticas

Tiene como objetivo direccionar y permitir la toma de decisiones en el desarrollo de proyectos de investigación, es una secuencia de tareas que comienza por el establecimiento del tema de investigación, se selecciona el panel de expertos, se informa al panel la información que se desea, tal como se detalla en la siguiente figura:

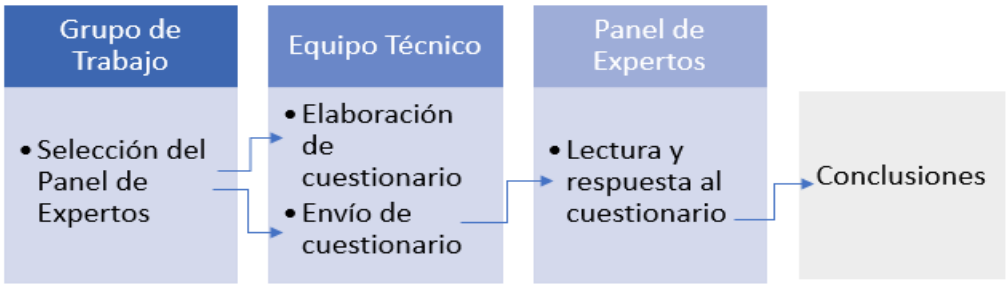

Figura 8. Estructura - Método Delphi
Fuente: (Mario, 2012)

2.9 Priorización de selección de criterios de evaluación

Consiste en el uso de técnicas y herramientas para obtener criterios o resultados cuantitativos que puedan ser analizados y clasificados debido a su puntuación con respecto a todas las métricas a usar en el proyecto de investigación, tomando en cuenta las áreas a las que pertenecen.

2.9.1 Matriz de Priorización de Holmes

También llamado matriz de impacto, está herramienta puede ser utilizada en combinación con diagramas de árbol y diagramas matriciales para la identificación de criterios clave (Murillo, 2010). La priorización del impacto o prioridad se realiza en base a un criterio en particular que es importante o de mayor riesgo para la organización (Murillo, 2010).

El proceso de construcción de esta matriz debe ser en conjunto con el equipo de trabajo mediante una lluvia de ideas para listar criterios o alternativas de comparación, en esta etapa no se toma en cuenta su importancia o impacto (Murillo, 2010).Es importante que la palabra que defina el criterio no sea neutral, debe tratarse de un juicio (Murillo, 2010). Una vez listados los criterios de comparación, estos deben ser filtrados y transcritos en ambos lados de una matriz en L. Posteriormente se utiliza una escala predefinida para comparar la trascendencia relativa de cada criterio respecto del resto de criterios (Murillo, 2010). Finalmente se suman los valores de cada fila y columna de la matriz. La siguiente tabla muestra un ejemplo de la matriz de priorización o matriz de impacto.

Tabla 2
Matriz de priorización de Holmes

Característica	Criterio 1	Criterio 2	Criterio 3	Criterio n	Total	Ponderación del Criterio
Criterio 1	X					%
Criterio 2		X			X	%
Criterio 3			X			%
Criterio n		X				%
TOTALES						1,00

Fuente: (Murillo, 2010).

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Introducción

En este capítulo se plantea el uso de una metodología de investigación propia de tipo exploratoria – cuantitativa, basada en el método deductivo para la selección de métricas o parámetros relacionados al riesgo inherente de metodologías de auditoría informática, además se provee una perspectiva crítica, que estará sustentada en la cuantificación e interpretación de los datos estadísticos hallados. Esta metodología de investigación consta de una serie de actividades que están detallados en la figura 9. La metodología propuesta se compone de 4 fases detalladas a continuación:

- Fase de investigación: [Búsqueda y selección de metodologías – Características y variables comunes]
- Fase de definición: [Definición de criterios de comparación – Desarrollo del modelo comparativo]
- Fase de validación: [Aplicación del método Delphi – Generación de resultados]
- Fase de análisis y conclusiones: [Aplicación del modelo – Análisis comparativo]

Como resultado se espera generar un modelo de evaluación de metodologías de auditoría informática apoyados en el análisis e identificación de parámetros asociados al riesgo inherente, dichos parámetros serán clasificadas en categorías de acuerdo a la estructura de una metodología de auditoría y posteriormente serán

validadas utilizando el Método Delphi, apoyados en un grupo de auditores informáticos expertos usando un cuestionario del cual se obtendrá una retroalimentación, que permitirá generar una versión depurada del modelo de evaluación.

De esta manera se pretende defender la hipótesis planteada y contribuir con la identificación y cuantificación del riesgo inherente que implicaría la aplicación de algún marco de referencia en un programa de auditoría, facultando de esta manera al auditor la emisión de juicios, recomendaciones con mayor legitimidad, así como también el mejoramiento en la credibilidad de los resultados de un programa de auditoría. En la siguiente figura se presenta el modelo de investigación a utilizarse:

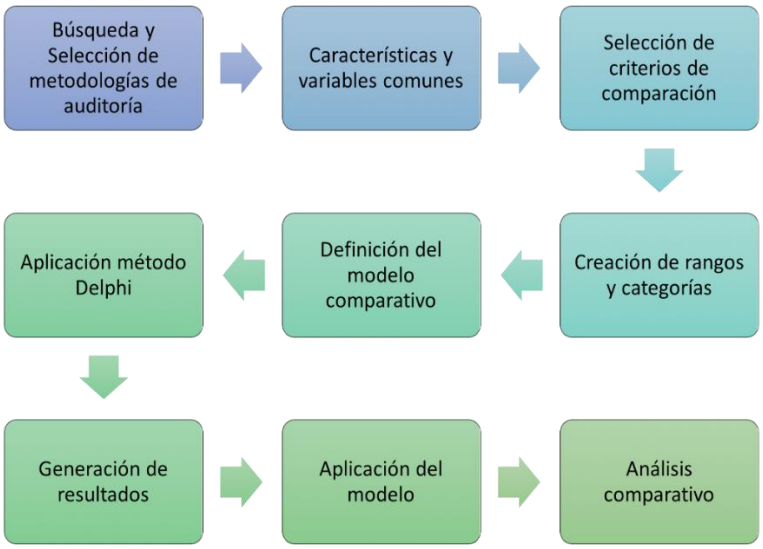

Figura 9. Metodología de la investigación a usarse

3.2 Niveles de investigación

Este estudio comprende desde el nivel exploratorio donde se identifican y seleccionan metodologías de auditoría informática, hasta el nivel explicativo donde se examina y presenta los niveles de riesgo inherente presente en el grupo de

metodologías de auditoría informática del estudio y con ello se llega a la comprobación de la hipótesis.

3.2.1 Población y Muestra

El proceso de análisis se lo realizará a un grupo de cuatro metodologías de auditoría informática, dichas metodologías van a ser seleccionadas considerando el cumplimiento de los siguientes parámetros:

- Cumplimiento con la estructura general de una metodología de auditoría informática.
- La metodología debe ser utilizada con frecuencia en programas de auditoría, basados en una investigación bibliográfica.
- La metodología debe haber sido desarrolladas por organismos internacionales y por expertos en el campo de la auditoría.

La validación del presente trabajo de investigación se la realizará a un grupo de auditores informáticos expertos quienes realizarán la revisión del trabajo de investigación y aportarán con sus observaciones que orientarán orientar la versión final del trabajo de investigación.

3.2.2 Métodos, técnicas e instrumentos

El grupo de trabajo hará uso de los siguientes métodos para realizar la adquisición de conocimiento durante la investigación:

- **Método Deductivo:** Se utilizará este método ya que basados en los procedimientos generales de las auditorías se espera llegar a planteamientos y revisiones puntuales relacionadas al riesgo inherente.

- **Método Analítico:** Para examinar las estructuras de las metodologías de auditoría informática y el cumplimiento de parámetros asociados al riesgo inherente.
- **Método Comparativo:** Para comparar los parámetros asociados al riesgo inherente y las metodologías de auditoría informática, con ello lograr establecer acercamientos que permitan cuantificar el riesgo inherente.

Además, contemplando que se van a trabajar con variables para determinar el riesgo inherente, se utilizará la tabulación para presentar datos generados en la presente investigación. Las técnicas de verificación verbal que se espera utilizar la investigación se presentan a continuación:

- **Indagación:** Se realizarán conversaciones directas con el tutor del proyecto de investigación, para obtener los lineamientos y directrices necesarias.
- **Encuesta:** Para obtener las opiniones de los revisores sobre los avances que se realicen en el proyecto de investigación.
- **Entrevistas:** Se realizarán entrevistas con los revisores del proyecto de investigación con el objetivo de explicar, interpretar o contradecir los puntos de vista recibidos.

CAPÍTULO IV

CASO DE ESTUDIO EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA INFORMÁTICA

4.1 Introducción

En este capítulo se desarrollará el caso de estudio enfocado a la evaluación de metodologías de auditoría informática considerando el riesgo inherente, mediante el análisis de metodologías y alineados al modelo de evaluación que se desarrollará y que permitirá cuantificar el nivel de riesgo que implica la implementación de alguna metodología en un programa de auditoría.

Para construir un modelo de evaluación de marcos de referencia, se iniciará por el estudio y selección de metodologías de auditoría informática desarrolladas por organismos internacionales.

4.2 Búsqueda y selección de metodologías de auditoría

En la primera fase se utilizará mecanismos de recolección de información para identificar varias metodologías de auditoría informática que sean utilizadas y aceptadas a nivel mundial, para ello se realiza una búsqueda y revisión de literatura en bases digitales tomando en consideración a organismos internacionales que se ocupan del control y de las auditorías de sistemas informáticos, tales como: ISACA, ISO, NIST, INCIBE, ENISA.

4.2.1 Selección de palabras clave

La búsqueda de información relacionada a metodologías de auditoría de sistemas de información se realizó en bases digitales utilizando las palabras clave que se presentan a continuación en la Figura 8.

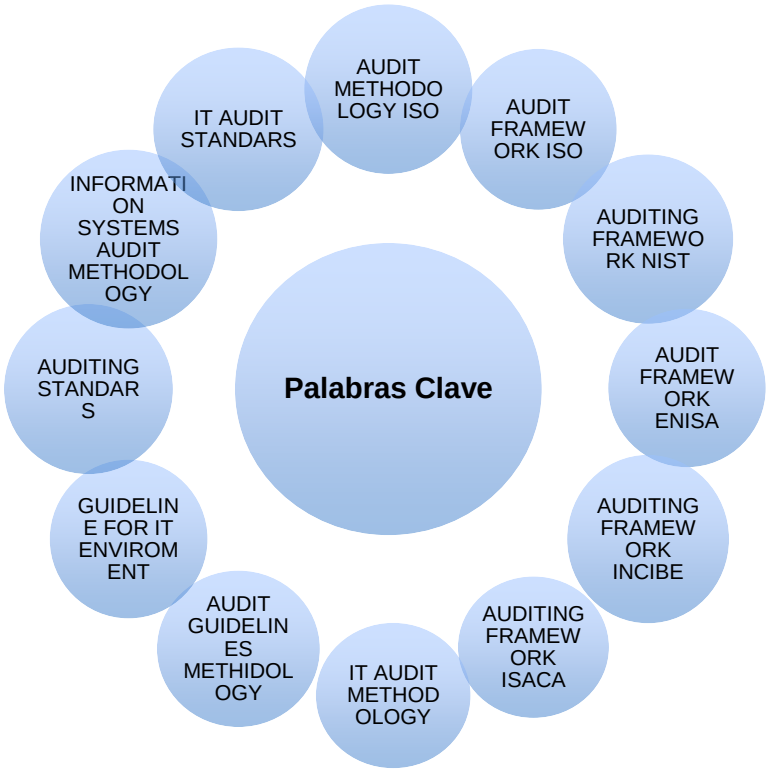

Figura 10. Palabras clave usadas en la búsqueda de metodologías de AI

La búsqueda permitió encontrar gran variedad de marcos de referencia que gestionan las auditorías informáticas y también la ciberseguridad, los resultados de la investigación se presentan a continuación en la tabla 3, clasificados por el organismo normativo internacional que los administra.

Tabla 3
Marcos de referencia hallados en la investigación

Organismo Normativo	Marco de Referencia
ISO	ISO / IEC 27001: 2013 - Information technology - Security techniques - Information security management systems - Requirements
	ISO 19011 - Directrices para la auditoría de Sistemas de Gestión
INCIBE	Instituto Nacional de Ciberseguridad España: Taxonomía de Soluciones de Ciberseguridad.
NIST	National Institute of Standars and Technology: Cybersecurity Framework Audit Program.
ISACA	Systems Audit and Control Association: ITAF - Information Technology Assurance Framework
	COBIT 4.1/COBIT 5
HITRUST CSF	Health Information Trust Alliance: HITRUST Common Security Framework
ENISA	European Union Agency for Network and Information Security: Auditing Framework for TSPs
ECA	European Court of Auditors: Guideline for audit of IT environment
NSW Government	New South Wales Government: Independent Audit Guideline
ISSAI/INTOSAI	International Standars of Supreme Audit Institutions/International Organization of Supreme Audit Institutions: Guidelines on IT Audit ISSAI 5300
PCAOB	Public Company Accounting Oversight Board: Risk Assessment Auditing Standars
Australian Government. Department of Environment	Independent Audit and Audit Report Guidelines
IIA'S	The Institute of Internal Auditors: Global Technology Audit Guidelines

4.3 Selección de marcos de referencia

Durante el levantamiento de información se halló un conjunto de marcos de referencia haciendo uso de la investigación bibliográfica, se procedió a descartar las

metodologías que no tienen relación directa con el ámbito de la auditoría informática, considerando los siguientes puntos:

- Guías de auditoría del gobierno australiano: propone guías de auditoría para la protección del medio ambiente y conservación de la biodiversidad.
- Guías de auditoría del gobierno de Gales: ya que propone pautas de auditoría para proyectos de construcción e infraestructura en agencias gubernamentales del gobierno de Gales.
- PCAOB: Debido a que propone guías relacionadas a la evaluación del auditor y respuesta al riesgo en auditorías contables.
- Marcos de referencia de organizaciones internacionales orientadas a ciberseguridad tales como INCIBE, NIST, HITRUST, ENISA, ISO 27000
- Guías orientadas a la gestión de objetivos, de control de la organización, para minimizar el riesgo de TI como COBIT y las guías de la asociación Europea CEA.

Por otra parte, se incluyó a las guías y marcos de referencia encontrados en bases digitales y que están mencionados en el estudio de (Gartner, 2012) “IT Audit Standars, Frameworks, and Guidelines for Auditees and Auditors”, tales como, ITAF de ISACA y las guías de auditoría de IIA’S, según dicho estudio son marcos vigentes por su alta aceptación a nivel mundial por parte de auditores expertos en TI. En la Tabla 4 se presenta, clasifica y registra los marcos de referencia que cumplen con las características de selección detallados en el punto 3.2.1 y que serán seleccionados para la presente investigación.

Tabla 4
Marcos de referencia seleccionados para el objeto de estudio

Organismo Normativo	Marco de Referencia
ISO	ISO 19011 - Directrices para la auditoría de Sistemas de Gestión
ISACA	ITAF - Information Technology Assurance Framework
ISSAI/INTOSAI	ISSAI 5300 - Guidelines on IT Audit
IIA'S	Global Technology Audit Guidelines (CTAGs) • CTAG 11: Developing the IT Audit Plan • Developing the Internal Audit Strategic Plan • International Professional Practices Framework (IPPF Standars) • Engagement Planning • Evaluating Ethics-related Programs and Activities • Formulating and Expressing Internal Audit Opinions • Independence and Objectivity • Audit Reports

Los marcos de referencia definidos en la Tabla 4 en general tienen como objetivo la minimización del riesgo inherente durante el ciclo de vida de la auditoría informática en sus etapas de Planificación - Ejecución - Reportes. El autor (Marquez, 2015) indica que las metodologías de auditoría informática en general son de tipo cualitativo/subjetivo (subjetivas por excelencia), es decir, desarrolladas por profesionales de gran nivel, experiencia, formación y capacidad necesaria para dictar recomendaciones técnicas, operativas y jurídicas. En (ISO, 2018) se indica que se debe considerar que la credibilidad de un proceso de auditoría depende directamente de la jurisdicción de las personas involucradas.

4.4 Características y variables comunes

Posterior a la definición de metodologías de auditoría informática, se pretende realizar un análisis de características y variables comunes con el objetivo de obtener parámetros de cada metodología que permitan realizar una comparación entre ellas.

Para llevar a cabo la caracterización entre los marcos de referencia seleccionados, es necesario plantear y registrar una taxonomía individual, basados en ello se podrá determinar características que gestionan el riesgo inherente.

4.4.1 Taxonomía Metodologías de Auditoría

4.4.1.1 Iso 19011

Esta norma proporciona directrices para llevar a cabo auditorías sobre los sistemas de gestión y es aplicable a cualquier institución que necesite proyectar y elaborar auditorías internas, externas o gestionar un programa de auditoría (ISO, 2018).

4.4.1.1.1 Principios de auditoría

- Integridad.
- Presentación imparcial.
- Debido cuidado profesional.
- Confidencialidad.
- Imparcialidad.
- Enfoque basado en la evidencia.
- Enfoque basado en riesgo.

4.4.1.1.2 Gestión de un programa de auditoría (PHVA)

- Establecimiento de los objetivos del programa de auditoría.
- Determinación y evaluación de los riesgos y oportunidades del programa de auditoría.
- Establecimiento del programa de auditoría.

- Roles y responsabilidades para la gestión del programa de auditoría.
- Competencias para gestionar el programa de auditoría.
- Establecimiento de la extensión del programa de auditoría.
- Determinación de los recursos del programa de auditoría.

- Implementación del programa de auditoría.
  - Definición de los objetivos, el alcance y los criterios para una auditoría individual.
  - Selección y determinación de los métodos de auditoría.
  - Selección de los miembros del equipo auditor.
  - Asignación de responsabilidades al líder del equipo auditor.
  - Gestión de los resultados del programa de auditoría.
  - Gestión y conservación de registros del programa de auditoría.
- Seguimiento del programa de auditoría.
- Revisión y mejora del programa de auditoría.

4.4.1.1.3 Realización de la auditoría (PHVA)

- Inicio de la auditoría.
  - Establecimiento del contacto con el auditado.
  - Determinación de la viabilidad de la auditoría.
- Preparación de las actividades de auditoría.
  - Revisión de la información documentada.
  - Planificación de la auditoría.
    - Enfoque basado en riesgos para la planificación.
    - Detalles de la planificación de auditoría.

- Asignación de las tareas al equipo auditor.
- Preparación de información documentada para la auditoría.

- Realización de actividades de auditoría.
  - Asignación de roles, responsabilidades, guías y observadores.
  - Realización de la reunión de apertura.
  - Comunicación durante la auditoría.
  - Disponibilidad y acceso de la información de auditoría.
  - Revisión de la información documentada durante la auditoría.
  - Recopilación y verificación de la información.
  - Generación de hallazgos de auditoría.
  - Determinación de las conclusiones de auditoría.
  - Realización de la reunión de cierre.
- Preparación y distribución del informe de auditoría.
- Finalización de la auditoría.
- Realización de las actividades de seguimiento de una auditoría.

4.4.1.1.4 Competencia y evaluación de los auditores

- Generalidades
- Métodos de auditoría.
- Enfoques para la auditoría.
- Juicio profesional.
- Verificación de la información.
- Muestreo.
- Selección de fuentes de información.

4.4.1.2 Isaca - Itaf

ITAF es un marco de referencia completo general que establece directrices de auditoría, buenas prácticas, estándares, define funciones, aseguramiento de roles y responsabilidades profesionales; conocimientos y habilidades para asegurar una auditoría de TI. Tal como indica (ISACA, 2014) define términos y conceptos, proporciona orientación, herramientas y técnicas para la planificación, diseño, ejecución y desarrollo de reportes de auditoría informática.

ITAF está basado en el material de ISACA, se presenta como una única fuente de conocimiento para profesionales de auditoría, auditores informáticos, etc. se pueden encontrar orientación, procedimientos de investigación, políticas y desarrollo de informes para realizar auditorías de TI eficaces. De acuerdo con (ISACA, 2018) ITAF es aplicable a cualquier auditoría de TI formal, se debe considerar que las directrices y técnicas no son obligatorias, pero es muy recomendable estar alineados a ellas. Este marco de referencia está estructurado en tres partes:

- **Normas Generales (serie 1000):** Son los principios que conducen la profesión del aseguramiento de las TI. Es decir, los atributos del auditor tales como independencia, objetividad, conocimiento, competencia y habilidades.
- **Directrices de Rendimiento (serie 1200):** Trata los parámetros de las tareas de auditoría, tales como planificación, supervisión, alcance, riesgo, supervisión y administración de las tareas.
- **Directrices de Informes (serie 1400):** Gestiona los tipos de reportes, medios de comunicación e información.

A continuación, se presenta la estructura de la normativa clasificada en sus fases de ejecución:

4.4.1.2.1 Estándares

- Estándares generales (serie 1000).
  - 1001. Carta de auditoría.
  - 1002. Independencia organizacional.
  - 1003. Independencia profesional.
  - 1004. Expectativa razonable.
  - 1005. Cuidado profesional.
  - 1006. Competencias.
  - 1007. Afirmaciones.
  - 1008. Criterios.
- Estándares de desempeño (serie 1200).
  - 1201. Planificación de la asignación.
  - 1202. Evaluación de riesgo en la planificación.
  - 1203. Desempeño y supervisión.
  - 1204. Materialidad.
  - 1205. Evidencia.
  - 1206. Uso del trabajo de otros expertos.
  - 1207. Irregularidades y actos ilegales.
- Estándares de reportes (serie 1400).
  - 1401. Reportes.
  - 1402. Actividades de seguimiento.

4.4.1.2.2 Lineamientos de aseguramiento de SI

- Estándares generales (serie 2000).
    - 2001. Carta de auditoría.
    - 2002. Independencia organizacional.
    - 2003. Independencia profesional.
    - 2004. Expectativa razonable.
    - 2005. Cuidado profesional.
    - 2006. Competencias.
    - 2007. Afirmaciones.
    - 2008. Criterios.
- Estándares de desempeño (serie 2200)
    - 2201. Planificación de la asignación.
    - 2202. Evaluación de riesgo en la planificación.
    - 2203. Desempeño y supervisión.
    - 2204. Materialidad.
    - 2205. Evidencia.
    - 2206. Uso del trabajo de otros expertos.
    - 2207. Irregularidades y actos ilegales.
    - 2208. Muestreo.
- Estándares de reportes (serie 2400).
    - 2401. Reportes.
    - 2402. Actividades de seguimiento.

4.4.1.2.3 Herramientas y técnicas

- Investigaciones y Programas de auditoría de ISACA

- Familia de productos COBIT 5, IT Risk, IT Audit Basics

4.4.1.3 Issai 5300

Es el primer marco de referencia desarrollado en base a las normas de las ISSAI, posee un alcance global, establece directrices y principios, es decir, define una metodología general para ejecutar auditorías informáticas. Según indica (INTOSAI & ISSAI, 2016) esta normativa puede ser utilizada como una guía para llevar a cabo auditorías, desarrollar la capacidad de la auditoría y para gestionar sus recursos, tiene como objetivo suministrar garantías a las organizaciones auditadas para aumentar la integridad y confiabilidad en los resultados obtenidos. Esta normativa está basada en:

- Normas existentes relacionadas a auditorías de TI
- Normas relativas a los sistemas de información
- Normas internacionales de auditoría
- ISSAI's existentes

El autor (INTOSAI & ISSAI, 2016) indica que el marco de referencia ISSAI 5300 ha sido organizada en dos notables categorías:

- **Requisitos:** Son los elementos fundamentales para la realización de una auditoría informática de buena calidad.
- **Explicaciones:** Para expresar y definir los requisitos en términos generales, con el objetivo de asegurar que la ISSAI conserve su objetivo de proveer orientación y apoyo general.

El marco de referencia ISSAI 5300 está estructurado tal como se presenta en la siguiente ilustración:

Figura 11. Estructura Marco de Referencia – ISSAI 5300

El marco de auditoría ISSAI 5300 es consistente con los principios fundamentales de las normas de auditoría pública sectorial (INTOSAI/ISSAI-100, 2013) principios fundamentales de la auditoría financiera (INTOSAI/ISSAI-200, 2013), principios de auditoría de rendimiento (INTOSAI/ISSAI-300, 2013) principios fundamentales de auditoría de cumplimiento (INTOSAI/ISSAI-400, 2013). A continuación, se presenta los principios, características y composición de la normativa en función de sus fases de ejecución.

4.4.1.3.1 Principios de Auditoría

- Principios generales de auditoría
    - Ética e independencia
    - Juicio profesional, diligencia y escepticismo
    - Control de calidad
    - Gestión y habilidades del equipo de auditoría
    - Riesgo de auditoría
    - Materialidad

- Documentación
- Comunicación

4.4.1.3.2 Fase de Planificación

- Planificación de la auditoría basado en una evaluación de riesgos.
  - Establecimiento de niveles de riesgo: Estratégico, Anual y de Equipo.
- Planificación estratégica de auditoría de TI.
  - Identificación del universo de auditoría.
  - Definición de metas y objetivos de la auditoría.
- Planificación anual de auditoría de TI.
- Planificación a nivel de equipo de auditoría de TI.
  - Conocimiento sobre riesgos inherentes que se enfrentan los sistemas de TI.
- Selección de la muestra apropiada de auditoría de TI.
- Objetivos de la auditoría de TI.
- Alcance de la auditoría de TI.
- Capacidades de la Entidad Fiscalizadora.
  - Asignación de recursos.
  - Contratación de recursos externos.
  - Vinculación con la entidad auditada.
  - Evidencia de auditoría.

4.4.1.3.3 Fase de Ejecución

- Recopilación de evidencia de auditoría
- Supervisión y revisión al proceso de auditoría

- Casos de fraude, corrupción y otras irregularidades.
- Limitaciones
- Seguimiento

4.4.1.3.4 Fase de Informe

- Requisitos de presentación de informes de auditoría de TI.
- Contenidos y formato del informe de auditoría de TI.

4.4.1.3.5 Herramientas y técnicas

- Identificación de las técnicas específicas de auditoría.
- Técnicas de planificación.
- Técnicas de ejecución de auditoría
- Elección de un adecuado sistema de preservación de información.
- Herramientas de auditoría de TI.

4.4.1.4 IIA's - CTAGs

Proporciona guías que orientan a los auditores internos a comprender el entorno de TI en la organización. IIA tiene 16 guías enfocadas en diferentes áreas:

- **Auditoría de áreas de TI:** continuidad del negocio, riesgos de privacidad, riesgos de TI y controles, aplicación de controles, proyectos de TI, gobernanza de TI, outsourcing y gestión de auditorías de TI
- **Auditoría de seguridad de TI:** gobierno de seguridad de TI, detección y prevención de fraudes, gestión de identidades y accesos, vulnerabilidades, administración de parches.

- **Auditoría de TI y conceptos:** tecnologías de análisis de datos, plan de auditoría de TI y auditoría continua.

El conjunto de guías prácticas de IIA's debería ser usado en conjunto con los estándares IIPF (International Professional Practices Framework) y los requerimientos de la organización, ya que de esto depende el éxito de la auditoría (Gartner, 2012). A continuación, se presenta la composición de esta metodología.

4.4.1.4.1 CTAG 11: Desarrollo del Plan de Auditoría de TI

- Entender el negocio.
  - Identificar las estrategias y objetivos de negocio de la organización.
  - Identificar la estructura de las operaciones de negocio de la organización.
  - Entender el modelo de soporte de servicio de TI.
- Definir el universo de las TI.
  - Identificar el modelo de negocio.
  - Identificar aplicaciones importantes que soportan las operaciones del negocio.
  - Identificar la infraestructura crítica para las aplicaciones importantes.
  - Identificar el rol de las tecnologías de apoyo.
  - Identificar proyectos de gran envergadura.
  - Determinar temas de auditoría objetivos.
- Realizar una evaluación de riesgos.
  - Definir un proceso para la identificación de riesgos.

- Asegurar la evaluación del riesgo de auditoría de TI.
- Asegurar la evaluación del riesgo de auditoría del negocio.

- Formalizar el Plan de auditoría.
  - Seleccionar y clasificar las actividades de auditoría.
  - Determinar el ciclo y la frecuencia de auditoría.
  - Agregar actividades de auditoría basándose en requerimientos.
  - Validar el plan con la gestión del negocio.

4.4.1.4.2 IPPF Guía de Desarrollo Plan Estratégico de Auditoría Interna

- Entender los objetivos y estrategias de la organización.
- Utilizar estándares IPPF definidos por IIA's.
- Entender las necesidades de los stakeholders.
- Establecer la misión y visión para las actividades de auditoría interna.
- Identificar los factores de éxito críticos.
- Determinar el estado actual de las actividades de auditoría mediante un análisis SWOT(FODA) para la misión, visión y factores de éxito.
- Identificar y priorizar actividades clave para el éxito de la auditoría interna.

4.4.1.4.3 IPPF Estándares

- Estándares generales.
  - 1000. Propósito, Autoridad y Responsabilidad.
  - 1010. Reconocer guías mandatarias del estatuto de auditoría interna.
  - 1100. Independencia y objetividad.
  - 1110. Independencia organizacional.

- 1111. Interacción directa con la junta.
- 1112. Roles del Jefe de auditoría fuera del ámbito de auditoría interna.
- 1120. Objetividad individual.
- 1130. Faltas a la independencia u objetividad.
- 1200. Competencia y debido cuidado profesional.
- 1210. Competencia.
- 1220. Debido cuidado profesional.
- 1230. Continuo desarrollo profesional.
- 1300. Programa de aseguramiento y mejora de la calidad.
- 1310. Requisitos del programa de mejora y aseguramiento de la calidad.
- 1311. Evaluaciones internas.
- 1312. Evaluaciones externas.
- 1320. Informe sobre el programa de mejora y aseguramiento de la calidad.
- 1321. Declaración de conformidad con los estándares IPPF.
- 1322. Divulgación de no conformidad.

- Estándares de rendimiento.
  - 2000. Gestión de las actividades de auditoría interna.
  - 2010. Planificación.
  - 2020. Comunicación y aprobación.
  - 2030. Gestión de recursos.
  - 2040. Políticas y procedimientos.
  - 2050. Coordinación y confianza.

- 2060. Reportes a la alta gerencia y al directorio.
- 2070. Outsourcing y responsabilidad de la organización en la auditoría interna.
- 2100. Naturaleza del trabajo.
- 2110. Gobernación.
- 2120. Gestión del riesgo.
- 2130. Control.
- 2200. Planificación de actividades.
- 2201. Consideraciones de la planificación.
- 2210. Objetivos de las actividades.
- 2220. Ámbito de las actividades.
- 2230. Asignación de recursos a las actividades.
- 2240. Programa de trabajo para las actividades.
- 2300. Ejecución de las actividades.
- 2310. Identificar información.
- 2320. Análisis y evaluación.
- 2330. Documentación de información.
- 2340. Supervisión de información.
- 2400. Comunicación de resultados.
- 2410. Criterios de comunicación.
- 2420. Calidad de la comunicación.
- 2421. Errores y omisiones.
- 2430. Declaración de conformidad con los estándares IPPF.
- 2431. Divulgación de no conformidad.
- 2440. Difusión de resultados.

- 2450. Opiniones generales.
- 2500. Monitoreo del progreso.
- 2600. Comunicación de la aceptación de riesgos.

4.5 Definición y apreciación de variables

Posterior al análisis de estructura y composición realizado individualmente a los marcos de referencia se encontró que las metodologías en estudio poseen características y variables comunes, que permitirán definir algunos parámetros asociados al riesgo inherente, quienes a su vez que permitan evaluar la efectividad, eficiencia y calidad de las metodologías de auditoría informática basados en el riesgo inherente que implicaría el uso de cada una de ellas en un programa de auditoría.

4.5.1 Definición de características

Si bien las metodologías seleccionadas para el presente estudio tienen el mismo objetivo, se ha analizó que no todas cumplen estrictamente con las mismas estructuras y singularidades, por ese motivo se realizará un análisis enfocado únicamente en las características de los marcos de referencia, que estén alineados de alguna forma el riesgo inherente, con ello se busca identificar, redefinir y establecer características generales basados en el riesgo inherente, estas características contarán con su respectiva descripción - justificación que justifique y pruebe su relación con el riesgo inherente, se las clasificará en grupos asociados a la estructura general de una metodología de auditoría, es decir:

- Planeación de la Auditoría de TI.

- Obtención de Información durante el proceso de auditoría.
- Análisis, clasificación y evaluación de información.
- Informe, desarrollo y presentación del informe final.

Las características y su descripción serán definidas de forma general para así evitar su apego a una única metodología de auditoría, adicional se definirá un campo código que permita identificar a las características individualmente, este proceso se lo realizó y se lo presenta en las tablas 5, 6, 7, 8 y 9.

Tabla 5
Etapa de Planeación

Planeación de la Auditoría de TI		
Código	**Característica**	**Descripción**
C-101	Planificación del proceso de auditoría basado en riesgos	La planificación debe considerar los elementos de riesgo que pueden influenciar en la pertinencia de la auditoría y sus conclusiones. Los riesgos presentes durante la auditoría comprenden riesgo inherente, de control y de detección.
C-102	Establecimiento de objetivos para el proceso de auditoría	Los objetivos permiten conocer la organización, el tamaño, su naturaleza e identificar los riesgos propios del auditado.
C-103	Establecimiento de procedimientos para el proceso de auditoría	Establece procedimientos que facilitan la programación y organización de auditorías considerando los riesgos del programa.
C-104	Gestión de recursos para el proceso de auditoría	Identifica recursos financieros necesarios para el programa basado en el alcance del programa de auditoría y sus riesgos.
C-105	Selección de miembros del equipo auditor para el proceso de auditoría	El administrador del programa de auditoría selecciona los miembros del equipo auditor considerando que posea las jurisdicciones necesarias e independencia organizacional.
C-106	Asignación de responsabilidades a los miembros del equipo auditor	El administrador asigna responsabilidades e independencia al líder del equipo y a cada miembro, considerando que usarán información del auditado para evaluar y tratar con riesgos vinculados a los objetivos de auditoría.

Tabla 6
Etapa de Implementación

Implementación del programa de Auditoría de TI		
Código	**Característica**	**Descripción**
C-201	Análisis de aptitudes a los miembros del equipo auditor	Los auditores deben poseer aptitudes que les permitan actuar con ética, imparcialidad, sinceridad y honestidad, deben ser tolerantes, dispuestos a atender ideas y puntos de vista alternos, deben mantener una actitud objetiva para que los hallazgos y conclusiones solo estén basados en evidencias.
C-202	Definición de roles y responsabilidades al administrador del proceso de auditoría	El administrador debe reconocer, valorar riesgos del programa, asegura el despliegue del programa, los criterios de auditoría e informa novedades a la alta gerencia.
C-203	Control de competencias a los miembros del equipo auditor	Controla que el equipo auditor este conformado por personas con jurisdicciones que permitan alcanzar exitosamente los resultados del proceso de auditoría. Los auditores se mantienen constantemente actualizados para ser capaces de identificar factores que afecten la fiabilidad de las evidencias y conclusiones de la auditoría.
C-204	Seguimiento al proceso de auditoría	El administrador debe monitorear la implementación del programa considerando el plan de auditoría, cronogramas, objetivos, desempeño de auditores y los hallazgos de la auditoría considerando el riesgo de auditoría.
C-205	Supervisión de cumplimiento al proceso de auditoría	El administrador debe evaluar el cumplimiento de objetivos del programa, revisa la efectividad de las medidas que direccionan los riesgos asociados al programa de auditoría.
C-206	Gestionar registros del programa de auditoría	El administrador debe asegurar la gestión de registros de auditoría para demostrar la efectividad del programa, considerando los registros relacionados con los riesgos del programa de auditoría.

Tabla 7

Etapa de Obtención de Información

Obtención de Información de la Auditoría		
Código	**Característica**	**Descripción**
C-301	Recolección y comprobación de evidencias del proceso de auditoría	Los auditores deberán obtener los datos, registros, documentos e información suficiente para sacar conclusiones, la misma que debe ser recopilada usando medios de muestreo apropiados, solo la información verificable debe ser aceptada y considerada como evidencia de auditoría. Si aparecen riesgos nuevos deberán ser gestionados por el equipo auditor.
C-302	Materialidad durante el proceso de auditoría	Los auditores deben considerar posibles debilidades o ausencias de controles que pueden provocar debilidad material.
C-303	Toma de acciones frente a riesgos y fraudes relativos a los objetivos.	Los auditores deben considerar el riesgo de irregularidades, casos de fraude, corrupción e irregularidades que pueden encontrarse y que deberán ser reportados oportunamente a las autoridades regulatorias o competentes en caso de ser necesario.
C-304	Monitoreo y seguimiento de actividades	Se verifican los criterios determinados por el auditor, evaluación de pruebas, documentación y gestión de riesgos ya que son parámetros que influyen en la inadecuada o baja credibilidad de las conclusiones de auditoría.

Tabla 8

Etapa de Análisis, Clasificación y Evaluación de Información

Análisis, Clasificación y Evaluación de información		
Código	**Característica**	**Descripción**
C-401	Revisión de documentación en el proceso de auditoría	Los hallazgos deben ser referenciados específicamente al cumplimiento o incumplimiento de regulaciones, ya que permiten comprender la planificación, ejecución de la auditoría y sirven para la posterior elaboración de recomendaciones.
C-402	Gestión de eventos en el proceso de auditoría	El administrador debe asegurar que se gestionen adecuadamente los registros de auditoría, tales como reuniones, entrevistas, observaciones del programa.
C-403	Supervisión y revisión del programa de auditoría	El administrador del programa de auditoría debe garantizar que la auditoría es supervisada y revisada periódicamente.

Tabla 9
Etapa de Informe, Desarrollo y Presentación del Informe Final

Informe, Desarrollo y Presentación del Informe Final		
Código	**Característica**	**Descripción**
C-501	Contenido del informe de auditoría	Los auditores deberán mencionar causas, riesgos asociados, restricciones, limitaciones y preocupaciones que el auditor pueda tener con relación al proceso de auditoría.
C-502	Supervisión de criterios de evaluación del auditor	Los criterios emitidos por el auditor deben ser cualitativos para evidenciar conocimiento y cuantitativos para probar los años de experiencia, número de auditorías y horas de entrenamiento.
C-503	Concertación de conclusiones del proceso de auditoría	El equipo se reunirá para llegar a un acuerdo sobre las conclusiones considerando el riesgo inherente del proceso de auditoría.
C-504	Preparación del reporte del proceso de auditoría	El reporte debe presentar la síntesis del proceso indicando obstáculos hallados y que puedan disminuir la credibilidad en las conclusiones de la auditoría.
C-505	Gestión de resultados del programa de auditoría	El administrador debe asegurar que revisó y aprobó los reportes de auditoría, idoneidad y conveniencia de los hallazgos de auditoría, se revisará la causa y validez de las recomendaciones correctivas o preventivas.
C-506	Revisión y mejora continua del programa de auditoría	El administrador debe revisar si el programa de auditoría alcanzó los objetivos, considerando la efectividad de las medidas consideradas para gestionar los riesgos de la auditoría.

4.5.2 Determinación de características

Las características antes definidas están relacionadas directamente a los riesgos que implican las auditorías informáticas. La evaluación estará clasificada de acuerdo a las etapas de un programa de auditoría informática general, considerando que si están presentes totalmente o si poseen algunas cláusulas que son semejantes a la descripción de la característica, en caso de ser positivo se les marcará con un visto que tiene un valor de 1 punto; al final de cada grupo se

realizará un sumatorio para conocer a la metodología que cumple con la mayor cantidad de características.

Tabla 10

Evaluación de Metodologías - Planeación de la Auditoría

Planeación de la Auditoría de TI					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-101	Planificación de la auditoría basado en riesgos		✓	✓	✓
C-102	Establece objetivos del programa de auditoría	✓	✓	✓	✓
C-103	Establece procedimientos para el programa de auditoría	✓	✓		✓
C-104	Identifica recursos del programa de auditoría	✓		✓	✓
C-105	Elección de miembros del equipo auditor	✓		✓	✓
C-106	Asignación de responsabilidades al líder del equipo auditor	✓	✓		✓
Sumatorio		5	4	4	5

Tabla 11

Evaluación de Metodologías - Implementación de la Auditoría

Implementación del programa de Auditoría de TI					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-201	Consideración aptitudes de los miembros del equipo auditor	✓	✓	✓	✓
C-202	Define roles y responsabilidades de miembros del equipo auditor	✓			✓
C-203	Controla competencias de los miembros del equipo auditor	✓	✓	✓	✓
C-204	Monitoreo del programa de auditoría	✓	✓	✓	✓
C-205	Verificación de cumplimiento del programa de auditoría	✓	✓		✓
C-206	Gestionar registros del programa de auditoría	✓			
Sumatorio		6	4	3	5

Tabla 12
Evaluación de Metodologías - Obtención de información

Obtención de Información					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-301	Recolección y verificación de evidencia de auditoría	✓	✓	✓	✓
C-302	Materialidad durante el proceso de auditoría		✓	✓	
C-303	Toma de acciones frente a riesgos y fraudes relativos a los objetivos	✓	✓	✓	
C-304	Monitoreo y seguimiento de actividades		✓		
Sumatorio		2	4	3	1

Tabla 13
Evaluación de Metodologías - Análisis de información

Análisis, clasificación y evaluación de información					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica/Variable**				
C-401	Revisión de documentación en la auditoría de TI		✓	✓	✓
C-402	Gestión de eventos del programa de auditoría	✓			✓
C-403	Supervisión y revisión del programa de auditoría		✓	✓	✓
Sumatorio		1	2	2	3

Tabla 14
Evaluación de Metodologías - Informe Final

Informe, desarrollo y presentación del informe final					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-501	Contenido del informe de auditoría		✓	✓	
C-502	Gestión de criterios de evaluación del auditor	✓	✓	✓	
C-503	Concertación de conclusiones del proceso de auditoría	✓		✓	✓
C-504	Preparación del reporte del proceso de auditoría	✓	✓	✓	✓
C-505	Gestión de resultados del programa de auditoría	✓			✓
C-506	Revisión y mejora continua del programa de auditoría	✓			
Sumatorio		5	3	4	3

El proceso de evaluación de características, generó cinco grupos de valores, los cuales han sido denominados como sumatorios; y que han sido obtenidos de las tablas 10, 11, 12, 13 y 14; estos valores serán ponderados de forma vertical respetando la metodología a la que pertenece cada valor, el resultado de esta operación se lo presentan en la tabla 15, este valor ha sido interpretado como un sumatorio total de los grupos.

Tabla 15
Evaluación de Metodologías – Sumatorio Total

ISO 19011	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
19	17	16	17

Basados en los resultados del sumatorio total y que constan en la tabla 15, se ha podido analizar que:

- El marco de referencia más completo que cumple con la mayor cantidad de características es **ISO 19011** con un valor total de 19 puntos.
- Se determina que el conjunto de marcos de referencia seleccionados para la presente investigación, cumplen con un promedio de 17,25 características.
- Se verifica que los parámetros asociados al riesgo inherente desarrolladas en la investigación cumplen y son aptos para cuantificar el nivel de riesgo inherente, considerando que su presencia influye en la extensión, integridad y resultados de una metodología de auditoría de TI.

4.6 Selección de criterios de comparación

Las características obtenidas en la etapa de parametrización serán depuradas y filtradas por el equipo de trabajo con la finalidad de clasificar, identificar y priorizar a las que poseen mayor relevancia. La herramienta a utilizar es la matriz de priorización de Holmes, con el objetivo de precisar y cuantificar la presencia de una característica en los marcos de referencia seleccionados para el presente análisis.

El método de comparación a utilizarse en este caso de estudio será de todos contra todos, donde se confronta las características por pares buscando obtener un valor que permita priorizar a las características, para realizar el proceso de comparación se ha establecido que se utilizarán los siguientes criterios de comparación:

- **Valor ‘1’:** Si la primera característica se considera más importante que la segunda característica en relación al riesgo inherente.

- **Valor ‘0.5’:** Si se considera que ambas características poseen la misma importancia con respecto al riesgo inherente.
- **Valor ‘0’:** Si la primera característica se considera menos importante que la segunda característica en relación al riesgo inherente.

Es importante considerar que el proceso de priorización de características es realizado en función de la importancia que implica una característica en relación a otras características, basados en este análisis se deduce que el nivel priorización que posee un parámetro, es equivalente efecto o impacto que implica su presencia en alguna metodología. Cuando se haya efectuado la comparación de características se realizará el siguiente proceso para cuantificar el nivel de impacto que implica su existencia en un marco de referencia.

Cuando se haya concluido la comparación de parámetros, se hace necesario determinar un valor que permita cuantificar el impacto y con el mismo priorizar las características, para conseguir este valor se efectuará el siguiente proceso:

I. En primer lugar, se realizará un sumatorio de los criterios de comparación por cada metodología, a este valor se lo ha denominado como valor horizontal.
II. Se llevará a cabo un sumatorio total obtenido de la suma de los valores horizontales, este valor se lo ha denominado valor vertical, estará ubicado en la parte inferior.
III. Se calculará la proporción entre el valor horizontal y valor vertical multiplicado por cien, logrando determinar de esta manera el nivel de impacto que posee una característica.

La ejecución del proceso detallado en los pasos I, II, III, así como también sus resultados se presentan a continuación en la figura 12.

PRIORIZACIÓN DE PARÁMETROS ASOCIADOS AL RIESGO INHERENTE	Planificación del proceso de auditoría basado en riesgos	Establecimiento de objetivos para el proceso de auditoría	Establecimiento de procedimientos para el proceso de auditoría	Gestión de recursos para el proceso de auditoría	Selección de miembros del equipo auditor para el proceso de auditoría	Asignación de responsabilidades a los miembros del equipo auditor	Análisis de aptitudes a los miembros del equipo auditor	Definición de roles y responsabilidades al administrador del proceso de auditoría	Control de competencias a los miembros del equipo auditor	Seguimiento al proceso de auditoría	Supervisión de cumplimiento al proceso de auditoría	Gestionar registros del programa de auditoría	Recolección y comprobación de evidencias del proceso de auditoría	Materialidad durante el proceso de auditoría	Toma de acciones frente a riesgos y fraudes relativos a los objetivos.	Monitoreo y seguimiento de actividades	Revisión de documentación en el proceso de auditoría	Gestión de eventos en el proceso de auditoría	Supervisión y revisión del programa de auditoría	Contenido del informe de auditoría	Supervisión de criterios de evaluación del auditor	Concertación de conclusiones del proceso de auditoría	Preparación del reporte del proceso de auditoría	Gestión de resultados del programa de auditoría	Revisión y mejora continua del programa de auditoría	Valor Horizontal	Impacto (I)
Planificación del proceso de auditoría basado en riesgos		1	0	1	0	0	0	0	0	0	0	0,5	0	0	0	0	0,5	0	0	0	0	0	0	0	0,5	3	1,04
Establecimiento de objetivos para el proceso de auditoría	1		0,5	0,5	0	1	0	0	0	1	0	0,5	0	0	0	0	0	0	0	0	0	0	0	0	0	0,5	5	1,73
Establecimiento de procedimientos para el proceso de auditoría	0,5	1		1	1	0,5	1	0	1	1	0	1	1	0	0,5	0,5	0,5	1	0,5	0,5	0,5	0,5	0	0.5	0,5	14	4,84
Gestión de recursos para el proceso de auditoría	0,5	0,5	0,5		1	0,5	0	0	0	0	0	1	0	0	0	0,5	0	0.5	0	0	0	0	0	0	0	0,5	5	1,73
Selección de miembros del equipo auditor para el proceso de auditoría	0	0,5	0	0,5		0	0	0	0,5	0	0	1	0,5	0	0,5	0,5	0,5	0,5	0	0,5	0	0	0,5	0	0,5	6,5	2,25
Asignación de responsabilidades a los miembros del equipo auditor	0,5	0,5	0,5	0,5	0,5		0,5	0,5	0,5	0,5	0	0,5	0,5	0,5	0	1	0,5	0,5	0	0	0	0	0	0	0	0,5	8	2,76
Análisis de aptitudes a los miembros del equipo auditor	0,5	1	0,5	1	0,5	1		1	0,5	1	0,5	0,5	0,5	0,5	0,5	1	0,50	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	15,5	5,35
Definición de roles y responsabilidades al administrador del proceso de auditoría	0	0	0,5	0,5	0	0,5	0		0	0,5	0,5	1	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0	0,5	0,5	10	3,45
Control de competencias a los miembros del equipo auditor	0	0	0	0,5	0,5	0,5	0,5	0,5		0,5	0	1	0	0,5	0,5	1	0,5	0,5	0	0	0,5	0,5	0,5	0,5	0,5	9,5	3,28
Seguimiento al proceso de auditoría	0	0	0,5	0,5	1	1	1	0,5	1		0,5	1	0,5	0,5	0	0,5	0,5	0,5	0,5	0,5	0	0	0	0	0,5	11	3,80
Supervisión de cumplimiento al proceso de auditoría	0	0	0	0,5	0,5	0	0,5	0	0	0,5		0,5	0,5	0,5	0,5	0,5	0	0,5	0	0,5	0,5	0,5	0,5	0,5	0,5	7,5	2,59
Gestionar registros del programa de auditoría	0	0	0	0,5	0	0	0	0	0	0,5	0,5		0	0	0	0,5	0	0,5	0	0	0	0,5	0	0	0	3,5	1,21
Recolección y comprobación de evidencias del proceso de auditoría	1	1	0,5	1	0,5	1	0,5	0,5	0,5	0,5	0,5	1		0,5	0,5	0,5	0,5	1	0,5	0,5	0,5	0	0,5	0	1	14,5	5,01
Materialidad durante el proceso de auditoría	0,5	1	1	1	1	1	0,5	1	0,5	1	1	1	0,5		0,5	1	0,5	1	1	0,5	0,5	0,5	0,5	0,5	1	18,5	6,39
Toma de acciones frente a riesgos y fraudes relativos a los objetivos	0,5	0,5	1	1	1	1	0,5	0,5	0,5	0,5	0,5	1	1	0,5		1	0,5	1	1	1	1	0,5	0,5	0,5	0,5	17,5	6,04
Monitoreo y seguimiento de actividades	0,5	0,5	1	1	0,5	0,5	0,5	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5		0	0	0	0	0	0	0	0	0,5	9,5	3,28
Revisión de documentación en el proceso de auditoría	0,5	1	1	1	1	1	0,5	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5		1	0,5	0,5	1	0,5	0,5	0,5	0,5	16	5,53
Gestión de eventos en el proceso de auditoría	0	0,5	0,5	0,5	0	0	0	0	0,5	0,5	0,5	0,5	0	0,5	0,5	0,5	0		0	0	0	0	0,5	0	0	5,5	1,90
Supervisión y revisión del programa de auditoría	0,5	0,5	0,5	1	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0,5	0	0	0,5	0,5	1		0	0	0	0	0	0,5	9,5	3,28
Contenido del informe de auditoría	0,5	0,5	1	1	1	1	0,5	0,5	1	0,5	0,5	1	0,5	0,5	1	1	0,5	1	1		0,5	0,5	0,5	0,5	1	17,5	6,04
Supervisión de criterios de evaluación del auditor	0,5	1	0,5	1	1	1	0,5	0,5	0,5	1	1	1	0,5	0,5	0,5	0,5	0,5	1	1	0,5		0,5	0,5	0	1	16,5	5,70
Concertación de conclusiones del proceso de auditoría	1	1	1	1	1	1	0,5	1	0,5	1	1	1	0,5	1	0,5	1	0,5	1	1	1	1		0,5	0,5	1	20,5	7,08
Preparación del reporte del proceso de auditoría	1	1	0,5	1	1	1	0,5	1	0,5	0,5	0,5	1	0,5	0,5	1	1	1	1	0,5	0,5	0,5	0,5		0,5	1	18	6,22
Gestión de resultados del programa de auditoría	1	1	0,5	1	1	1	1	1	1	0,5	0,5	1	1	0,5	1	1	0,5	1	1	0,5	0,5	0,5	0,5		1	19,5	6,74
Revisión y mejora continua del programa de auditoría	0,5	0	0,5	1	0,5	0,5	0	0	0	0,5	0,5	0,5	0,5	0,5	1	0,5	0	0	0,5	0	0	0	0	0,5		8	2,76
																						Valor Vertical				289,5	100,00

Figura 12. Matriz de holmes - Características basadas en el riesgo inherente

Del análisis realizado en la figura 12, se observa en la columna Impacto (I) la ponderación obtenida por cada característica, este valor representa un nivel de impacto que implica la presencia del parámetro en alguno de los marcos de referencia del análisis, a continuación, en la tabla 16, se presenta las características priorizadas de mayor a menor, considerando el nivel de impacto.

Tabla 16
Características basadas en el riesgo inherente - impacto

Niveles de impacto de las características		
Código	**Característica**	**Impacto (I)**
C-503	Concertación de conclusiones del proceso de auditoría	7,08
C-505	Gestión de resultados del programa de auditoría	6,74
C-302	Materialidad durante el proceso de auditoría	6,39
C-504	Preparación del reporte del proceso de auditoría	6,22
C-303	Toma de acciones frente a riesgos y fraudes relativos a los objetivos	6,04
C-501	Contenido del informe de auditoría	6,04
C-502	Supervisión de criterios de evaluación del auditor	5,7
C-401	Revisión de documentación en el proceso de auditoría	5,53
C-201	Análisis de aptitudes a los miembros del equipo auditor	5,35
C-301	Recolección y comprobación de evidencias del proceso de auditoría	5,01
C-103	Establecimiento de procedimientos para el proceso de auditoría	4,84
C-204	Seguimiento al proceso de auditoría	3,8
C-202	Definición de roles y responsabilidades al administrador del proceso de auditoría	3,45
C-203	Control de competencias a los miembros del equipo auditor	3,28
C-304	Monitoreo y seguimiento de actividades	3,28

CONTINÚA

C-403	Supervisión y revisión del programa de auditoría	3,28
C-106	Asignación de responsabilidades a los miembros del equipo auditor	2,76
C-506	Revisión y mejora continua del programa de auditoría	2,76
C-205	Supervisión de cumplimiento al proceso de auditoría	2,59
C-105	Selección de miembros del equipo auditor para el proceso de auditoría	2,25
C-402	Gestión de eventos en el proceso de auditoría	1,9
C-102	Establecimiento de objetivos para el proceso de auditoría	1,73
C-104	Gestión de recursos para el proceso de auditoría	1,73
C-206	Gestionar registros del programa de auditoría	1,21
C-101	Planificación del proceso de auditoría basado en riesgos	1,04

Basados en la priorización de parámetros detallado en la tabla 17, se ha encontrado que la característica con mayor nivel de impacto es la C-503 correspondiente a “Concertación de conclusiones del proceso de auditoría” la misma que tiene un nivel de impacto de 7.08 puntos, lo cual permite entender que la reunión que realiza el equipo auditor posterior al programa de auditoría donde se acuerda las conclusiones del proceso, juega un papel importante disminuyendo el nivel de riesgo inherente que tendrán los resultados de auditoría y además permite deducir que es necesario que las metodologías deberían contemplar y considerar esta característica en su estructura para sus nuevas versiones en caso de no tenerla.

Por otra parte, se encontró que la característica menos relevante es la C-101 “Planificación del proceso de auditoría basado en riesgos” con un puntaje de 1,04 haciendo entender que, si bien se debe considerar los elementos de riesgo de la auditoría en la planificación, la presencia de esta característica no generará un nivel alto de impacto durante el uso del marco de referencia que la posea, sin embargo, se recomienda no ser omitida.

Luego de analizar los resultados de la matriz, en la siguiente figura se presentan los porcentajes de ponderación agrupados por fases.

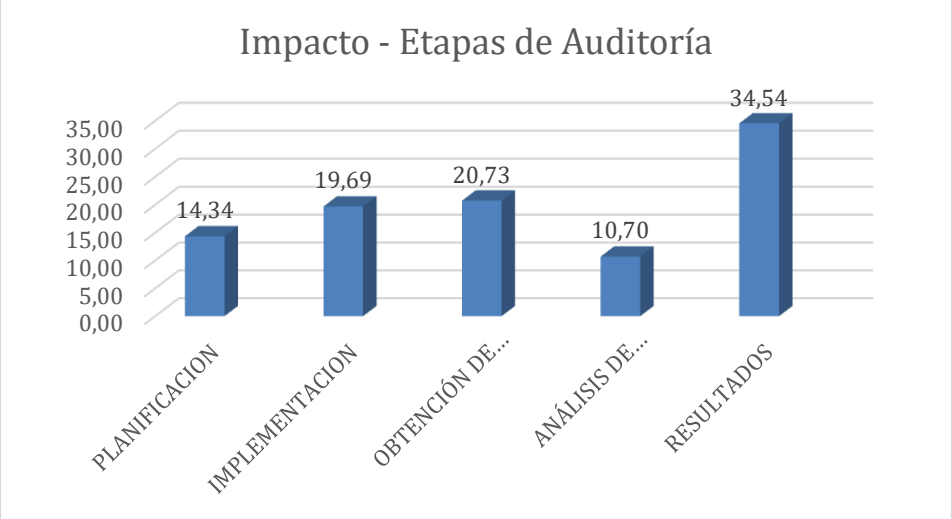

Figura 13. Nivel de impacto por fases de una auditoría de TI

CAPITULO V

DEFINICIÓN Y APLICACIÓN DEL MODELO COMPARATIVO

5.1 Definición Del Modelo Comparativo

Durante el análisis de características se observó que la inexistencia de una característica puede implicar un riesgo para la metodología, considerando que mientras más características posea esa metodología puede ser estimada como un marco de referencia con mayor completitud, integridad y exactitud, obviamente considerando al riesgo inherente.

Por tal motivo y basados en la literatura relacionada al análisis de impacto y probabilidad del riesgo, se pretende utilizar la siguiente fórmula para determinar y cuantificar el nivel de riesgo inherente que implica el uso de una metodología de auditoría informática.

$$R = P * I$$

Dónde:

$$\boldsymbol{R}: Riesgo \quad \boldsymbol{P}: Probabilidad \; \boldsymbol{I}: Impacto$$

Analizando la estructura de la ecuación (1), se determinó que sus variables pueden ser utilizadas para cuantificar el nivel de riesgo inherente de las características desarrolladas en las tablas 10, 11, 12, 13 y 14, el grupo de trabajo está enfocado únicamente en este tipo de riesgo debido a que es el corazón de la presente investigación, por ello la estructura de la ecuación (1) será relacionada y usada en este proyecto de la siguiente forma:

- **Probabilidad:** Para calcular la ocurrencia o presencia de las características, aplicado al grupo de metodologías de auditoría informática de presente estudio.
- **Impacto:** Evaluado en función de la priorización de características del estudio, este valor fue calculado y detallado en la tabla 16, donde se utilizó la matriz de Holmes.

5.2 Análisis de características

El análisis individual de características permitirá calcular dos tipos de riesgo, el primero está asociado a la presencia de características, en el grupo metodologías de la presente investigación, mediante un análisis de proporcionalidad utilizando regla de tres y tomando en cuenta que una característica puede estar presente en una o varias metodologías de auditoría, los valores de probabilidad serán determinados de la siguiente forma:

- Si una característica está presente en todas las metodologías seleccionadas para el análisis, se le asigna un valor de probabilidad de 1 o del 100%,
- Si una característica está presente en tres metodologías tendría un valor de probabilidad de 0,75 o del 75% y así sucesivamente.

El resultado de este análisis se presenta en la tabla 17 ordenados considerando la priorización de la tabla 16, donde el campo Probabilidad (P) corresponde a la probabilidad de presencia de una característica en el grupo de metodologías de la presente investigación.

Tabla 17
Probabilidad de presencia de las características

Probabilidades de ocurrencia

Código	Característica	Probabilidad (I)
C-503	Concertación de conclusiones del proceso de auditoría	0,75
C-505	Gestión de resultados del programa de auditoría	0,50
C-302	Materialidad durante el proceso de auditoría	0,50
C-504	Preparación del reporte del proceso de auditoría	1
C-303	Toma de acciones frente a riesgos y fraudes relativos a los objetivos	0,75
C-501	Contenido del informe de auditoría	0,50
C-502	Supervisión de criterios de evaluación del auditor	0,75
C-401	Revisión de documentación en el proceso de auditoría	0,75
C-201	Análisis de aptitudes a los miembros del equipo auditor	1
C-301	Recolección y comprobación de evidencias del proceso de auditoría	1
C-103	Establecimiento de procedimientos para el proceso de auditoría	0,75
C-204	Seguimiento al proceso de auditoría	1
C-202	Definición de roles y responsabilidades al administrador del proceso de auditoría	0,50
C-203	Control de competencias a los miembros del equipo auditor	1
C-304	Monitoreo y seguimiento de actividades	0,25
C-403	Supervisión y revisión del programa de auditoría	0,75

CONTINÚA

C-106	Asignación de responsabilidades a los miembros del equipo auditor	0,75
C-506	Revisión y mejora continua del programa de auditoría	0,25
C-205	Supervisión de cumplimiento al proceso de auditoría	0,75
C-105	Selección de miembros del equipo auditor para el proceso de auditoría	0,75
C-402	Gestión de eventos en el proceso de auditoría	0,50
C-102	Establecimiento de objetivos para el proceso de auditoría	1
C-104	Gestión de recursos para el proceso de auditoría	0,75
C-206	Gestionar registros del programa de auditoría	0,25
C-101	Planificación del proceso de auditoría basado en riesgos	0,75

Una vez obtenidos para cada característica los valores de probabilidad e impacto, se continúa con la determinación del riesgo también para cada característica, realizando el producto entre las variables Impacto (I) y Probabilidad (P), que fueron halladas en el proceso y están detallados en las tablas 17 y 18 respectivamente; los resultados de la cuantificación del riesgo son presentados a continuación en la tabla 19, manteniendo el orden de priorización de características.

Tabla 18

Valores de riesgo en las características del análisis

Cuantificación del Riesgo				
N°	**Código**	**Impacto (I)**	**Probabilidad (P)**	**Riesgo (R)**
1	C-503	7,08	0,75	5,31
2	C-505	6,74	0,5	3,37
3	C-302	6,39	0,5	3,195
4	C-504	6,22	1	6,22
5	C-303	6,04	0,75	4,53
6	C-501	6,04	0,5	3,02
7	C-502	5,7	0,75	4,275
8	C-401	5,53	0,75	4,1475
9	C-201	5,35	1	5,35
10	C-301	5,01	1	5,01
11	C-103	4,84	0,75	3,63
12	C-204	3,8	1	3,8
13	C-202	3,45	0,5	1,725
14	C-203	3,28	1	3,28
15	C-304	3,28	0,25	0,82
16	C-403	3,28	0,75	2,46
17	C-106	2,76	0,75	2,07
18	C-506	2,76	0,25	0,69
19	C-205	2,59	0,75	1,9425
20	C-105	2,25	0,75	1,6875
21	C-402	1,9	0,5	0,95
22	C-102	1,73	1	1,73
23	C-104	1,73	0,75	1,2975
24	C-206	1,21	0,25	0,3025
25	C-101	1,04	0,75	0,78

Los valores resultados de la variable Riesgo (R) detallados en la tabla 22, permiten conocer el nivel de riesgo inherente que implica la inexistencia individual de

las características en las metodologías de auditoría de la investigación; estas metodologías en estudio son detallados en la tabla 4. A continuación, las figuras 14, 15 y 16 se muestran gráficamente las variables de impacto, probabilidad y riesgo.

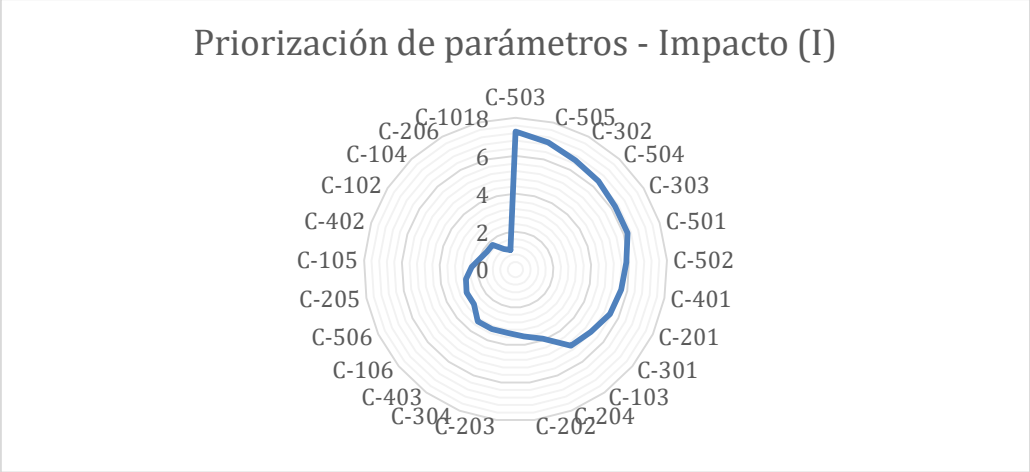

Figura 14. Cuantificación de la variable impacto

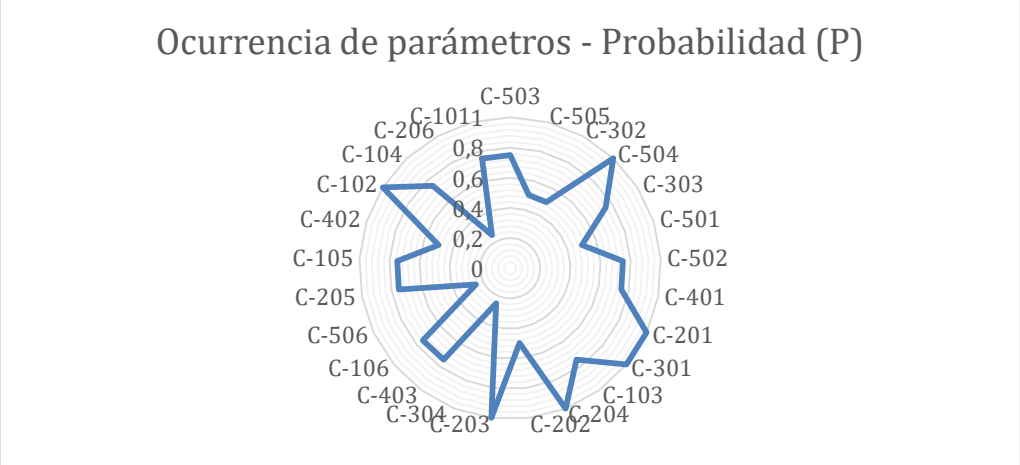

Figura 15. Cuantificación de la variable probabilidad

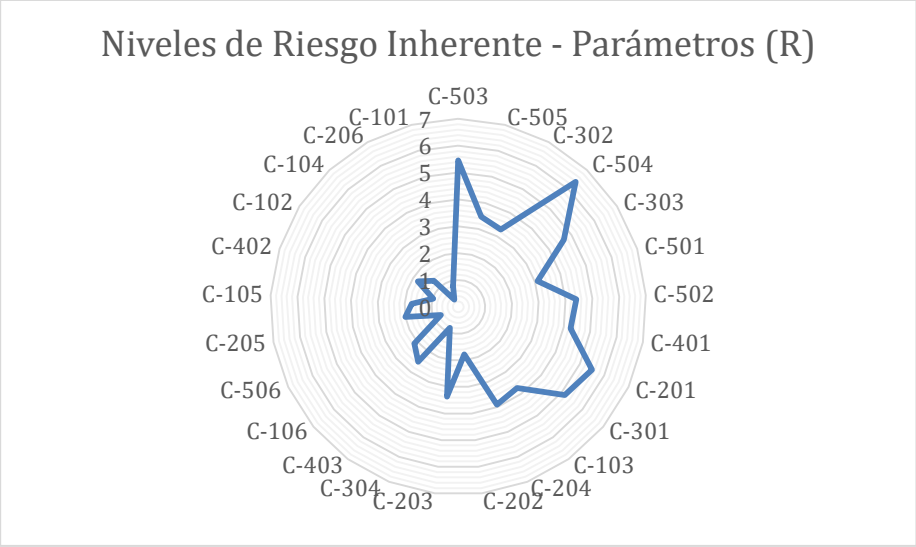

Figura 16. Cuantificación del riesgo por parámetro

Basados en los valores obtenidos en la tabla 18, se plantea la siguiente figura para representar gráficamente los valores del riesgo que provocan las métricas, de acuerdo a las fases de una auditoría de TI.

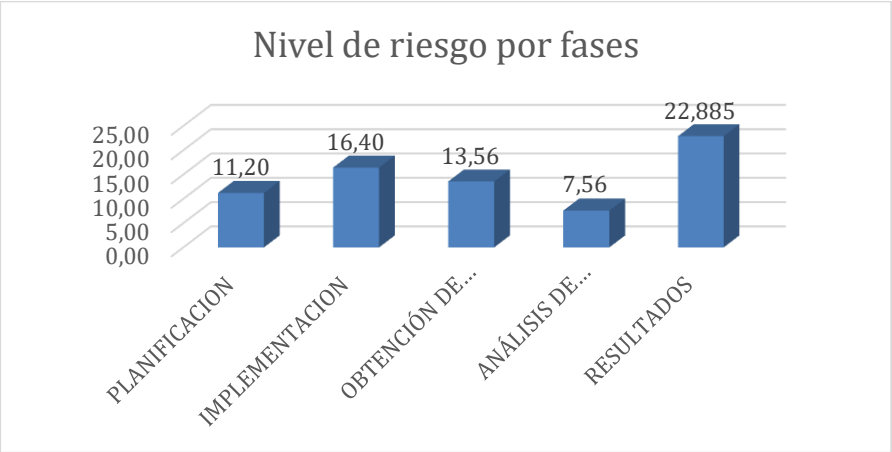

Figura 17. Nivel de riesgo agrupado por fases

5.3 Rangos y categorías

El proceso de análisis generó datos correspondientes a la cuantificación del riesgo inherente, por ello se hace necesario la definición de criterios que permitan clasificar en categorías dichos valores. Los criterios de probabilidad e impacto serán establecidos considerando los valores máximos o mínimos que pueden tomar basados en la tabla 17 y para el riesgo se estableció un análisis de acuerdo al punto 4.3.2 de ocurrencia de características y también se consideró a la tabla 18. En las siguientes tablas se presentan los criterios definidos y que serán utilizados para categorizar los valores correspondientes a las variables de probabilidad, impacto y riesgo.

Tabla 19
Rangos y valores del parámetro 'Probabilidad'

Probabilidad	
1	Alta
0.75	Media
0.5	Baja

Tabla 20
Rangos y valores del parámetro 'Impacto'

Impacto	
8,1 - 10	Muy Alta
6,1 – 8	Alta
4,1 – 6	Media
2,1 – 4	Baja
0 – 2	Muy Baja

Tabla 21
Rangos y valores del parámetro 'Riesgo'

Riesgo	
17,1 – 22,6	Riesgo Crítico
11,4 – 17	Riesgo Alto
5,7 – 11,3	Riesgo Medio
0 – 5,6	Riesgo Bajo

5.4 Aplicación del modelo comparativo

Los resultados del cálculo de las variables probabilidad, impacto y riesgo de cada característica definida en la tabla 5, permiten definir un modelo para la medición del riesgo inherente reproducible a cualquier grupo de metodologías o marcos de referencia de auditoría informática. A continuación, se detalla el procedimiento utilizado para la determinación de los niveles de riesgo inherente en los marcos de auditoría informática seleccionados en este estudio:

I. Se empieza con la definición de un grupo de veinte y cinco características seleccionadas por el equipo de trabajo mediante una clasificación taxonómica de las metodologías seleccionadas en la etapa de investigación, esta cantidad ha sido denominada como universo de características.

II. Se elabora una tabla de existencia o inexistencia de cada una de las características encontradas vs el grupo de metodologías de auditoría seleccionadas, este proceso se lo realiza en las tablas 10,11,12,13,14 y se va mantienen las estructuras que organizan a las características de

acuerdo a las etapas de un programa de auditoría (Planificación, Implementación, Obtención de información, Análisis de información, Informe final y Retroalimentación).

III. Basados en el análisis de riesgos individuales realizado en la tabla 18, se establecen dichos valores de riesgo inherente en los campos de evaluación donde no existió la presencia de alguna característica, es decir se cuantificará la inexistencia de características en las metodologías.

IV. En cada etapa se obtendrá un sumatorio parcial del riesgo, valor que será el resultado de la suma de vertical de riesgos por cada marco de referencia.

V. Se realizará un sumado total de los valores parciales del riesgo, este valor es interpretado como el nivel de riesgo inherente que poseen las metodologías de auditoría.

La ejecución del proceso relacionado a la cuantificación del riesgo que se explicó en los pasos I, II, III, IV y V, se presentan a continuación en las tablas 23,24,25,26 y 27.

Tabla 22

Cuantificación del Riesgo - Etapa de Planeación de la Auditoría

Planeación de la Auditoría de TI					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-101	Planificación de la auditoría basado en riesgos	0,78	✓	✓	✓
C-102	Establece objetivos del programa de auditoría	✓	✓	✓	✓
C-103	Establece procedimientos para el programa de auditoría	✓	✓	3,63	✓
C-104	Identifica recursos del programa de auditoría	✓	1,3	✓	✓
C-105	Elección de miembros del equipo auditor	✓	1,69	✓	✓
C-106	Asignación de responsabilidades al líder del equipo auditor	✓	✓	2,07	✓
Sumatorio Parcial del Riesgo		**0,78**	**3**	**5,07**	**0**

Tabla 23

Cuantificación del Riesgo - Etapa de Implementación de la Auditoría

Implementación del programa de Auditoría de TI					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-201	Consideración aptitudes de los miembros del equipo auditor	✓	✓	✓	✓
C-202	Define roles y responsabilidades de miembros del equipo auditor	✓	1,73	1,73	✓
C-203	Controla competencias de los miembros del equipo auditor	✓	✓	✓	✓
C-204	Monitoreo del programa de auditoría	✓	✓	✓	✓
C-205	Verificación de cumplimiento del programa de auditoría	✓	✓	2	✓
C-206	Gestionar registros del programa de auditoría	✓	0,31	0,31	0,31
Sumatorio Parcial del Riesgo		**0**	**2,03**	**4,03**	**0,31**

Tabla 24

Cuantificación del Riesgo - Etapa de Análisis de información

Análisis, clasificación y evaluación de información					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica/Variable**				
C-401	Revisión de documentación en la auditoría de TI	4,15	✓	✓	✓
C-402	Gestión de eventos del programa de auditoría	✓	0,95	0,95	✓
C-403	Supervisión y revisión del programa de auditoría	2,46	✓	✓	✓
Sumatorio Parcial del Riesgo		**6,61**	**0,95**	**0,95**	**0**

Tabla 25

Cuantificación del Riesgo - Obtención de información

Obtención de Información					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-301	Recolección y verificación de evidencia de auditoría	✓	✓	✓	✓
C-302	Materialidad durante el proceso de auditoría	3,2	✓	✓	3,2
C-303	Toma de acciones frente a riesgos y fraudes relativos a los objetivos	✓	✓	✓	4,53
C-304	Monitoreo y seguimiento de actividades	0,82	✓	0,82	0,82
Sumatorio Parcial del Riesgo		**4,02**	**0**	**0,82**	**8,55**

Tabla 26
Cuantificación del Riesgo - Etapa de Informe Final

Informe, desarrollo y presentación del informe final					
Metodología		**ISO 19011**	**ISACA - ITAF**	**ISSAI 5300**	**IIA's Audit Guides**
Código	**Característica**				
C-501	Contenido del informe de auditoría	3,02	✓	✓	3,02
C-502	Gestión de criterios de evaluación del auditor	✓	✓	✓	4,28
C-503	Concertación de conclusiones del proceso de auditoría	✓	5,31	✓	✓
C-504	Preparación del reporte del proceso de auditoría	✓	✓	✓	✓
C-505	Gestión de resultados del programa de auditoría	✓	3,37	3,37	✓
C-506	Revisión y mejora continua del programa de auditoría	✓	0,69	0,69	0,69
Sumatorio Parcial del Riesgo		**3,02**	**9,37**	**4,06**	**8**

Los valores parciales del riesgo son sumados, sus resultados se presentan a continuación en la tabla 28.

Tabla 27
Niveles totales de riesgo inherente

ISO 19011	ISACA - ITAF	ISSAI 5300	IIA's Audit Guides
14,43	15,35	14.93	16,86

5.5 Análisis comparativo

Se ha encontrado la información suficiente para realizar un análisis considerando los resultados del modelo comparativo, los niveles totales de riesgo inherente son considerados como parte fundamental de la presente investigación; por tal motivo y apoyados en los valores de la tabla 27, se puede afirmar que la

metodología con el mayor nivel de riesgo inherente es **IIA's Audit Guides** con un valor de **16,86** puntos de riesgo inherente, es decir que esta metodología cumple con la estructura general de un marco de referencia pero las características que la componen no gestionan adecuadamente el riesgo inherente y posee un rango de Riesgo Crítico; provocando de esta manera una implementación aparentemente normal en un programa de auditoría, pero en la etapa de resultados se tendría un nivel alto de subjetividad valga la redundancia, donde el equipo auditor puede haber influenciado en la definición de conclusiones, ya sea por su falta de competencias o su imparcialidad, y por lo tanto generar conclusiones y recomendaciones alejadas de la realidad con baja credibilidad y objetividad, motivo por el cual se sugiere evitar la aplicación de esta metodología en un programa de auditoría de Ti.

Siguiendo el análisis de los niveles de riesgo inherente, la metodología **ISSAI 5300**, si bien es un marco de referencia que cumple con una buena parte de los parámetros asociados al riesgo inherente, en el análisis de presencia de parámetros la inexistencia de características clave para la presente investigación, provocó que su nivel total de riesgo inherente se eleve a **14.93** puntos, con este valor estaría clasificado en el rango de Riesgo Alto y por tal motivo no se recomendaría la implementación de este marco de referencia debido a que la etapa de resultados contaría con juicios alejados de la realidad debido al nivel de distorsión que existiría y que terminaría comprometerían las conclusiones y recomendaciones del programa de auditoría.

Continuando con el análisis, los resultados del análisis permiten observar que la metodología de auditoría **ITAF** de ISACA es la que posee el segundo lugar en nivel de riesgo inherente con un puntaje de **15.35** puntos, clasificándolo en un rango

de Riesgo Alto este marco de referencia podría ser implementado en un programa de auditoría, siempre y cuando se consideren los parámetros que le hacen falta en el proceso de análisis del riesgo del programa de auditoría, con el objetivo de minimizar el nivel de riesgo y con ello obtener conclusiones y recomendaciones que generan un alto nivel de objetividad y credibilidad en la etapa de resultados.

La metodología de auditoría informática que posee el menor nivel de riesgo inherente de acuerdo al análisis realizado, es la **ISO 19011** con una ponderación de **14,43** puntos, clasificándolo así en un rango de Riesgo Alto; considerando basado que es el marco de referencia con menor nivel de riesgo inherente en comparación de los otros marcos de referencia, se sugiere considerar su implementación de esta metodología al ser considerada como la más extensa, que cumple con la mayor cantidad de parámetros asociados al riesgo inherente y que realiza una gestión completa de riesgos en todas sus etapas, la integridad de su estructura establece controles y características que buscan minimizar con mayor detalle los riesgos y entre ellos el riesgo inherente, motivo por el cual permitirá obtener los mejores resultados del programa de auditoría y específicamente la etapa de resultados tendría un alto nivel de credibilidad, baja subjetividad por parte del equipo auditor y los mejores resultados y recomendaciones para el auditado.

En la figura 18, se representa gráficamente el nivel de riesgo inherente que poseen las metodologías de auditoría de TI de acuerdo al análisis.

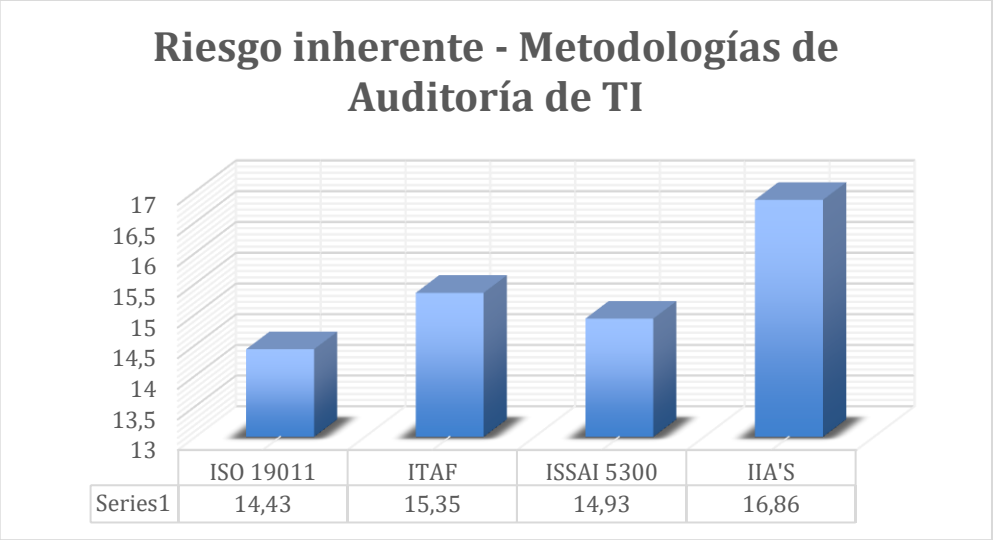

Figura 18. Niveles de riesgo inherente – Metodologías de Auditoría de TI

5.6 Observaciones

Considerando el nivel de riesgo inherente que generaría la implementación de cada metodología, se puede observar que la cuantificación del riesgo inherente permite evaluar a detalle el cumplimiento de estos parámetros.

Considerando la tabla 15, se puede apreciar que el cumplimiento de los parámetros es el mismo para los marcos de referencia ITAF & IIA's Audit Guides, dando a entender que poseen el mismo nivel de riesgo inherente, pero mediante la cuantificación del riesgo se pudo determinar que la metodología ITAF posee un menor nivel de riesgo inherente, con 15.35 puntos, a diferencia de IIA's Audit Guides, con 16.86 puntos de riesgo inherente.

Analizando los datos generados en este estudio, se ha encontrado que el incumplimiento total de los parámetros en una metodología de auditoría produciría un riesgo inherente máximo de 73,62 puntos, valor que sobrepasan el umbral de

riesgo permitidas y establecidas en el presente análisis, y que obviamente sugieren provocarían evitar la implementación de alguna metodología, pero son presentados como referencia para tener una idea de lo que provocaría su omisión

Basados en la tabla 22, en la figura 19 se representa gráficamente los niveles de riesgo que implica la inexistencia de parámetros asociados al riesgo inherente clasificado en etapas de una auditoría de TI.

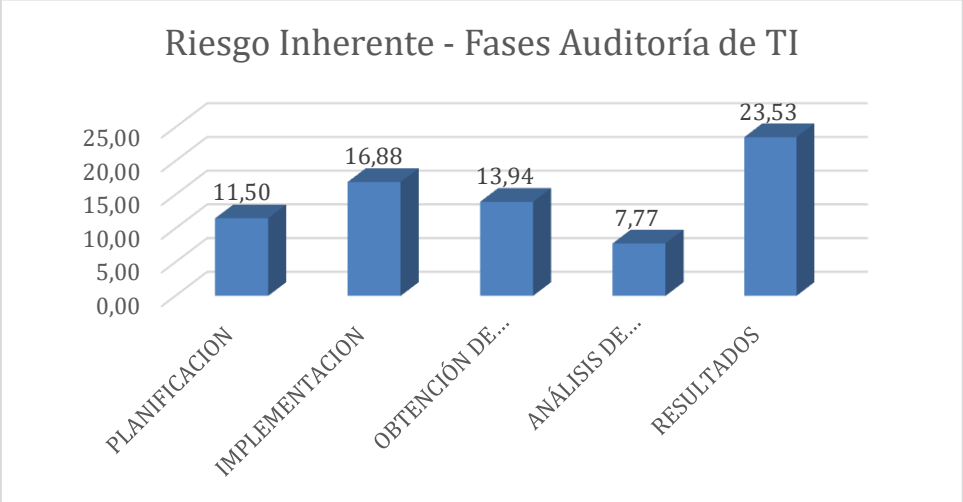

Figura 19. Niveles de riesgo inherente - Fases Auditoría

De los valores presentados en la figura 18, se puede entender que la etapa de un marco de referencia que genera mayor nivel de riesgo inherente es la de generación de resultados, por ese motivo se debería prestar especial atención a etapa si se desea disminuir el nivel de riesgo inherente del programa de auditoría.

5.7 Aplicación del método Delphi

El presente análisis y modelo de evaluación de metodologías de auditoría informática, será evaluado y validado usando la técnica Delphi, es decir, que estará sometido al juicio de auditores informáticos expertos con el objetivo de validar la

objetividad e imparcialidad del modelo propuesto y perfeccionarlo en caso de existir recomendaciones.

A continuación, se presenta información de los docentes que participaron como evaluadores del modelo, los mismos que cuentan con la formación y experiencia necesaria para poder evaluar el presente proyecto:

- Ing. Mario Bernabé Ron Egas Msc.
    - Docente Universidad de las Fuerzas Armadas – ESPE
    - Auditor CISA Certification
    - Master Sistemas e Informática
- Ing. Geovanni Ninahualpa Quiña Msc.
    - Docente Universidad de las Fuerzas Armadas – ESPE
    - Master en Auditoría Informática
- Ing. Daysi Imbaquingo Msc.
    - Docente Universidad Técnica del Norte - UTN
    - Master en Evaluación y Auditoría de Sistemas

La aplicación del método Delphi, ha permitido tabular los resultados que se presentan a continuación en las tablas 29, 30, 31, 32, 33, 34, 35 y 36 donde se va a presentar las calificaciones realizadas por cada auditor.

Sección 1.-Grado de consistencia de las etapas del modelo

Tabla 28

Delphi. Etapas del modelo

Etapas del modelo de selección de metodologías de Auditoría Informática	Calificaciones			Total
	MR	GN	DI	
Fase de investigación	5	5	5	5
Fase de definición de parámetros	5	5	5	5
Fase de validación	5	5	5	5
Fase de análisis y conclusiones	5	5	5	5
		Promedio		**5**

Sección 2.-Grado de relevancia de las normas y técnicas utilizadas

Tabla 29

Delphi. Relevancia de las normas

Etapas del modelo de selección de metodologías de auditoría	Normas y técnicas	Calificaciones			Total
		MR	GN	DI	
Fase de investigación	Revisión y Análisis de Literatura	4	4	4	4
Fase de definición de parámetros	Matriz de priorización de Holmes	4	4	5	4.33
Fase de validación	Método Delphi	4	4	4	4
Fase de análisis y conclusiones	Validación propia	3	4	3	3.33
			Promedio	**3.91**	

Sección 3.-Relevancia de las metodologías de auditoría seleccionadas:

Tabla 30
Delphi. Relevancia de las metodologías

Características	Calificaciones			Total
	MR	GN	DI	
ITAF	5	5	5	5
ISO 19011	5	5	5	5
ISSAI 5300	4	5	4	4.33
IIA'S	4	4	4	4
		Promedio		**4.58**

Sección 4.-Relevancia del análisis de metodologías de auditoría informática en relación al riesgo inherente:

Tabla 31
Delphi. Relevancia del análisis de las metodologías

Características	Calificaciones			Total
	MR	GN	DI	
Consistente	4	5	5	4.66
Reproducible	4	5	5	4.66
Imparcial	4	5	5	4.66
Objetivo	4	5	5	4.66
		Promedio		**4.66**

Sección 5.-Grado de coherencia en la ponderación y priorización de métricas utilizando la Matriz de Holmes

Tabla 32

Delphi. Coherencia y ponderación de métricas

Características	Ponderación en la investigación	Calificaciones			Total
		MR	GN	DI	
Planificación de la Auditoría de TI	14,33%	5	4	5	4.66
Implementación del programa de Auditoría de TI	19,69%	5	4	5	4.66
Obtención de información y evidencia	20,73%	5	4	5	4.66
Análisis, clasificación y evaluación de la información	10,71%	4	4	5	4.33
			Promedio		4.59

Sección 6.-Grado de coherencia en la ponderación del riesgo clasificado de acuerdo a las fases de una auditoría general

Tabla 33

Delphi. Coherencia y ponderación del riesgo en fases

Características	Ponderación en la investigación	Calificaciones			Total
		MR	GN	DI	
Planificación de la Auditoría de TI	11,24%	5	4	5	4.66
Implementación del programa de Auditoría de TI	16,41%	4	4	4	4
Obtención de información y evidencia	13,93%	4	4	4	4
Análisis, clasificación y evaluación de la información	8,60%	4	4	4	4
Desarrollo y presentación de resultados	17,59%	4	4	4	4
			Promedio		4.13

Sección 7.-Grado de cumplimiento de las características generales de un proceso de valoración, en el modelo de evaluación de metodologías de auditoría informática

Tabla 34

Delphi. Grado de cumplimiento de las métricas

Características	Calificaciones			Total
	MR	GN	DI	
Consistente	4	5	4	4.33
Reproducible	5	5	5	5
Imparcial	5	5	5	5
Objetivo	4	5	4	4.33
		Promedio		**4.67**

Sección 8.-Grado de coherencia del método de evaluación, usando parámetros asociados al riesgo inherente

Tabla 35

Delphi. Coherencia del método de evaluación

Características	Calificaciones			Total
	MR	GN	DI	
Planificación de la Auditoría de TI	5	4	5	4.66
Implementación del programa de Auditoría de TI	4	4	5	4.33
Obtención de información y evidencia	5	4	5	4.66
Análisis, clasificación y evaluación de la información	4	4	4	4
		Promedio		**4.41**

Los promedios o resultados parciales de cada sección han permitido realizar un promedio general para el presente proyecto de investigación, dando como resultado las calificaciones que se presenta a continuación.

Tabla 36
Delphi. Resultados Delphi parciales.

Número de Sección	**Calificación Promedio**
Sección 1	5.00
Sección 2	3.91
Sección 3	4.58
Sección 4	4.66
Sección 5	4.59
Sección 6	4.13
Sección 7	4.67
Sección 8	4.41
Calificación Total	**4.49**

La calificación de cuatro puntos cuarenta y nueve sobre cinco (4.49 / 5) transformado a la escala de calificaciones sobre veinte puntos, da una nota de diecisiete puntos con noventa y siete cinco sobre veinte (17.975 / 20). Valor que por aproximaciones decimales es semejante a diecisiete puntos con noventa y ocho sobre veinte (17.98 / 20). Por lo tanto, se puede entender que este valor es la calificación final al proyecto de investigación por parte de los auditores.

El método de evaluación también permitió generar recomendaciones por parte de los expertos auditores con el objetivo de refinar el modelo de evaluación desarrollado, a continuación, se presentan dichas observaciones individuales.

Tabla 37
Delphi. Opiniones de los expertos

Auditor Experto	Observaciones
Ing. Mario Ron Msc.	Es un modelo aplicable y que presenta considerar un aspecto muy importante y que a veces no se toma en cuenta que es el riesgo inherente de la auditoría. El proceso aplicado es muy coherente y pertinente al caso estudiado. Es necesario mejorar o profundizar algunos aspectos conceptuales que se traducen más adelante en conclusiones que podrían ser importantes.
Ing. Geovanni Ninahualpa Msc.	Modelo acorde a requerimiento, sugiero realizar bitácora de eventos con el objetivo de fortalecer en función de ejecución en distintas fases.
Ing. Daysi Imbaquingo Msc.	Es un modelo aplicado que se encuentra bien contextualizado, relacionado y acertado para el caso de estudio planteado, se recomienda ser más explícito en aspectos conceptuales que permitan determinar consideraciones finales. Es un modelo que considera el riesgo inherente de la auditoría que es un aspecto que muchas veces se pasa por alto, de forma general se puede concluir que es un modelo totalmente aplicable.

De acuerdo a las observaciones y los resultados cuantitativos obtenidos en la aplicación del método Delphi, se puede interpretar que el modelo de evaluación de metodologías de auditoría informática propuesto por el grupo de trabajo, es un modelo válido, apto para su aplicación.

Este modelo permite determinar los de niveles de riesgo inherente que pueden existir en marcos de referencia de forma objetiva e imparcial, y al mismo tiempo es un modelo flexible ya que se pueden añadir, eliminar o agregar metodologías para su respectivo análisis.

Basados en las observaciones del Ing. Geovanni Ninahualpa, se genera una bitácora de cumplimiento de eventos para fortalecer la ejecución del modelo, cuando

la implementación sea realizada en distintas fases. Dicha bitácora se presenta en la siguiente tabla.

Tabla 38
Bitácora de cumplimiento

BITACORA DE SEGUIMIENTO AL PROCESO DE EVALUACIÓN DE METODOLOGÍAS DE AUDITORÍA BASADOS EN EL RIESGO INHERENTE		
FECHA DE RECIBIDO:	FECHA DE EJECUCIÓN:	N° DE REPORTE: _ _ _ _ _ _ _ _ _
DATOS DEL IMPLEMENTADOR		
NOMBRES:		CÉDULA:
TELÉFONO:		FIRMA : _ _ _ _ _ _ _ _ _ _ _ _ _ _ _
CORREO ELECTRÓNICO:		
FASE	**CUMPLIMIENTO / AVANCE** **1 2 3 4 5**	**OBSERVACIONES/NOVEDADES**
ESTUDIO DE METODOLOGÍAS DE AUDITORÍA		
ANÁLISIS Y SELECCIÓN DE METODOLOGÍAS DE AUDITORÍA		
REVISIÓN DE CUMPLIMIENTO DE PARÁMETROS		
PLANIFICACIÓN		
IMPLEMENTACIÓN		
OBTENCIÓN DE RESULTADOS		
ANÁLISIS DE EVIDENCIA		
RESULTADOS		
PRIORIZACIÓN DE PARÁMETROS		
ELABORACIÓN DE MATRIZ DE PRIORIZACIÓN DE HOLMES		
CUANTIFICACIÓN DEL RIESGO EN PARÁMETROS		

CONTINÚA

EVALUACIÓN/CUANTIFICACIÓN DEL RIESGO INHERENTE EN METODOLOGÍAS

PLANIFICACIÓN

IMPLEMENTACIÓN

OBTENCIÓN DE RESULTADOS

ANÁLISIS DE EVIDENCIA

RESULTADOS

OBSERVACIONES GENERALES

SUGERENCIAS/ RECOMENDACIONES DEL SUPERVISOR

RESPONSABLE	**SUPERVISOR**
FIRMA:	FIRMA:
CI:	CI:

La bitácora presentada en la tabla anterior permitirá llevar un registro del avance e implementación del modelo de evaluación de metodologías de auditoría, basado en una escala de cumplimiento con diferentes puntajes, cuando el evento ha sido completado en su totalidad se deberá marcar cinco puntos y cuando el evento se encuentra en la etapa inicial o en proceso de cumplimiento se deberá marcar los puntos del uno al cuatro de acuerdo al avance del evento. Las personas que deben intervenir son el responsable de la evaluación de metodologías y el supervisor del proceso, quienes deberán firmar al pie de la bitácora.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Introducción

En esta sección se pretende detallar las conclusiones y recomendaciones, resultado del trabajo de investigación que se desarrolló en los capítulos anteriores, resaltando la importancia que genera realizar un análisis de metodologías de auditoría informática basados en su riesgo inherente, guiados por la selección y análisis de marcos de referencia, aportando al desarrollo de métodos que permiten la cuantificación del riesgo inherente y fortaleciendo el uso de la metodología con el menor nivel de riesgo inherente y por lo tanto definición de resultados de un programa de auditoría con alta credibilidad.

6.2 Conclusiones

- Las evidencias demuestran que es posible cuantificar el nivel de riesgo inherente, en el presente trabajo de investigación se hallaron los niveles de riesgo inherente del grupo de metodologías de auditoría seleccionadas; mediante el uso de tablas de priorización, cumplimiento, ocurrencia y gráficos estadísticos.
- Se ha encontrado que varios factores asociados al riesgo inherente que influyen en la subjetividad de resultados ya están inmersos en la estructura de las metodologías de auditoría informática, en caso de no estar seguros de su presencia pueden ser incluidos en el análisis y planificación de riesgos previo

al programa de auditoría, con el objetivo de minimizar el nivel de riesgo inherente.

- Los parámetros asociados al riesgo inherente pueden ser considerados como características relevantes de una metodología de auditoría informática, debido a que su ausencia genera mayores niveles de riesgo inherente, especialmente en la etapa de resultados del programa de auditoría.
- Los niveles de riesgo inherente pueden ser influenciados por la cantidad de parámetros asociados al riesgo inherente que sean utilizados en el análisis de una metodología, es decir a mayores niveles de riesgo inherente, mayor deberá ser la cantidad de parámetros que gestionen el riesgo.
- La auditoría de sistemas de información es una actividad que atraviesa transversalmente las jurisdicciones de otras auditorías, por ello el riesgo inherente debe tener los controles suficientes para evitar la afectación de los resultados.
- Los parámetros asociados al riesgo inherente que fueron desarrollados en la investigación para evaluar metodologías de auditoría de TI, sirven como base de conocimiento. El modelo de evaluación permite encontrar y adicionar parámetros de evaluación, que retroalimenten el modelo propuesto siguiendo una metodología similar.

6.3 Recomendaciones

- Generar reuniones recurrentes donde el equipo analice individualmente la metodología de auditoría informática en relación a su composición y características asociadas al riesgo inherente, logrando mantener la imparcialidad de la investigación.

- Se recomienda que los procesos de análisis de ocurrencia de parámetros asociados al riesgo inherente, deben ser transparentes e imparciales para garantizar el proceso de cumplimiento de características, sin omitir características de alguna metodología del grupo seleccionado, logrando mantener así la integridad y objetividad del estudio.
- La omisión de irregularidades significativas de un programa de auditoría modifica especialmente el sentido de las opiniones generadas en la etapa de resultados, si el nivel de riesgo inherente a pesar de los controles efectuados se mantiene elevado en un nivel crítico, se recomienda recolectar mayor cantidad de evidencias de auditoría.
- Para la validación del proyecto de investigación se puede contar con criterios de expertos en auditoría informática, quienes evaluaran y generaran recomendaciones sustanciales que permitan orientar el modelo de evaluación de metodologías de auditoría informática.
- Se recomienda que en cada etapa de un programa de auditoría se lleve a cabo una retroalimentación de riesgos, esto ayudaría sustancialmente con la minimización del riesgo inherente en la etapa de resultados y por lo tanto mejoraría el beneficio del auditor y del auditado.
- Se debe considerar el uso de bitácoras de cumplimento a efectos de fortalecer la implementación del modelo cuando la implementación sea realizada en distintas fases.

BIBLIOGRAFÍA

Baldeón Garzón, M. J., & Coronel Guerrero, C. A. (2012). Plan maestro de Seguridad Informática para la UTIC de la ESPE con lineamientos de la Norma ISO/IEC 27002. Retrieved from https://repositorio.espe.edu.ec/handle/21000/6025

Bernard, M. (2018). How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Retrieved August 12, 2019, from https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#198b25a60ba9

Calderón, J., & Ocaña, D. (2014). Auditoría informática basada en el análisis de riesgos a la empresa Tecniseguros S.A. Retrieved from http://repositorio.espe.edu.ec/xmlui/handle/21000/9032?show=full

Cárdenas, A. (2010). Técnicas de escala. Retrieved August 12, 2019, from https://es.slideshare.net/aejamett/tcnicas-de-escala

Carrion Haro, A. J., & Leyton, E. (2006). Análisis y elaboración de un informe de auditoría de servicios de telecomunicación para la empresa de prati. Retrieved from https://www.dspace.espol.edu.ec/handle/123456789/3145

E. Gómez, G. (2015). Asociación Española de Contabilidad y Administración de Empresas Servicio Infoaeca Titulo : Limitaciones del sistema contable. Asociación Española de Contabilidad y Administración de Empresas. https://doi.org/10.1029/2004JB003208

Gartner. (2012). IT Audit Standards , Frameworks , and Guidelines for Auditees and

Auditors. (September).

Guindel Sánchez, E. (2009). Calidad y seguridad de la información y auditoría informática. Retrieved from https://e-archivo.uc3m.es/handle/10016/8510

Guitián, M. V. G., & Dante, G. P. (2014). Metodologías y modelos para auditar la información. Análisis reflexivo. Revista General de Información y Documentación, 24(2 SE-Artículos). https://doi.org/10.5209/rev_RGID.2014.v24.n2.47402

INTOSAI/ISSAI-100. (2013). INTOSAI 100 Principios Funadamentales de Auditoría delSector Público. 5.

INTOSAI/ISSAI-200. (2013). Principios Fundamentales de la Auditoría de Desempeño. 1–46. Retrieved from http://www.intosai.org/es/issai-executive-summaries/detail/article/issai-200-fundamental-principles-of-financial-auditing.html

INTOSAI/ISSAI-300. (2013). ISSAI 300 Principios Fundamentales de la Auditoría de Desempeño. INTOSAI (Organizacion Internacional de Las Entidades Fiscalizadoras Superiores).

INTOSAI/ISSAI-400. (2013). ISAAI 400 Principios fundamentales de la auditoría de cumplimiento. 20. Retrieved from http://es.issai.org/media/79470/issai-400-s-new.pdf

INTOSAI, & ISSAI. (2016). Directrices sobre Auditoría de TI.

ISACA. (2018). COBIT 5. Retrieved August 12, 2019, from http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

ISACA. (2019). ISACA. Retrieved from https://www.isaca.org/

ISO. (2018). ISO 19011. 2018.

Mario. (2012). Auditoría en Informatica CUN. Retrieved August 12, 2019, from https://sites.google.com/site/auditoriaeninformaticacun/concepto-de-auditoria

Marquez, D. (2015). calidad de la auditorías de sistemas de información. Retrieved August 13, 2019, from https://es.slideshare.net/danielmarquez77/calidad-de-la-auditorias-de-sistemas-de-informacin

Murillo, V. (2010). Matrices De Priorización. Julio, 12. Retrieved from https://carlosalbertonavatornel.weebly.com/uploads/2/6/1/8/26186377/matrices_de_priorizacin.pdf%0Ahttp://www.vingest.com/pdf/Herramientas/HerrPriorizacion.pdf

OCTAVE. (2007). Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process. Retrieved August 13, 2019, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419

Rey, C. (2007). Auditorías de Sistema de Gestión Ambiental. Master En Ingeniería y Gestión Medioambiental, 5. Retrieved from https://static.eoi.es/savia/documents/componente45576.pdf%0A

Soy Aumatell, C. (2003). Auditoría de la información : análisis de la información generada en la empresa. Retrieved from http://eprints.rclis.org/15630/

Syalim, A., Hori, Y., & Sakurai, K. (2009). Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide. 2009 International Conference on Availability, Reliability and Security, 726–731. https://doi.org/10.1109/ARES.2009.75