UNIVERSIDAD DE COSTA RICA
SISTEMA DE ESTUDIOS DE POSGRADO

PROPUESTA DE UNA METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS DERIVADOS DE LAS TECNOLOGÍAS DE INFORMACIÓN EN LAS AUDITORIAS DE ESTADOS FINANCIEROS EJECUTADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA DE COSTA RICA

Trabajo final de graduación sometido a la consideración de la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas para optar al grado y título de Maestría Profesional en Auditoria de Tecnologías de la Información

MILENA BULGARELLI FUENTES

Ciudad Universitaria Rodrigo Facio, Costa Rica
2018

DEDICATORIA

A mi esposo, Gabriel,

por su apoyo, amor y dedicación.

A mis hijos, Gabriel y Benjamín,

por prestarme de su tiempo y amor.

AGRADECIMIENTOS

A Dios,

quien ha permitido que finalice con éxito este proyecto.

A Arnoldo Sanabria Villalobos, Gino Ramírez Solís y Mario Pérez Fonseca,

por su apoyo en este proyecto.

A André, Javier y Gonzalo,

por su contribución en el logro de las metas parciales que permitieron que llegara a la elaboración de este trabajo.

A Carlos, Carmen, Esteban, Leía, Ricardo, Roy, Ricardo, José,

quienes enriquecieron mi aprendizaje con sus experiencias.

Este Trabajo final de investigación aplicada fue aceptado por la Comisión del Programa de Estudios de Posgrado en Administración y Dirección de Empresas de la Universidad de Costa Rica, como requisito parcial para optar al grado y título de Maestría Profesional en Auditoría de Tecnologías de Información.

_____

M.B.A. Gino Ramírez Solís
Profesor Guía

_____

M.B.A. Mario Pérez Fonseca
Lector

_____

M.B.A. Daniel Sáenz Quesada
Lector de la Empresa

_____

M.Sc. Ridiguer Artavia Barboza
Director Programa de Posgrado en Administración y Dirección de Empresas

_____

Milena Bulgarelli Fuentes
Sustentante

RESUMEN

El objetivo principal de esta propuesta fue elaborar una metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros ejecutadas por la Contraloría General de la República de Costa Rica (CGR), con el fin de que el fiscalizador comprenda y considere las características del ambiente de tecnologías de información al determinar el alcance de la auditoria.

Para lograr lo anterior, se definió un marco teórico, se investigaron aspectos esenciales para conocer el devenir de la Contraloría General de la República (CGR) y normativa aplicable y se analizaron prácticas y procedimientos sobre evaluación de riesgos que al momento de la investigación, aplicaba la División de Fiscalización Operativa y Evaluativa (DFOE) de la CGR en las auditorías financieras.

La principal conclusión, es que la DFOE de la CGR no cuenta con una metodología de evaluación de riesgos derivados de las TI para las auditorías financieras, tal como lo sugieren las mejores prácticas.

ABSTRACT

The main objective of this proposal was to develop a methodology for the evaluation of risks derived from information technologies in the audits of financial statements executed by the Contraloría General de la República Costa Rica (CGR), so that the auditor understands and consider the characteristics of information technology environment when determining the scope of the audit.

To achieve the above, a theoretical framework was defined, essential aspects were investigated to know the Comptroller General of the Republic (CGR) and applicable regulations; practices and procedures were analyzed on risk assessment that at the time of the investigation applied the División de Fiscalización Operativa y Evaluativa (DFOE) of the CGR in financial audits.

The main conclusion is that the DFOE does not have a risk assessment methodology derived from IT for financial audits, as suggested by best practices.

TABLA DE CONTENIDO

LISTA DE CUADROS

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

CGR	Contraloría General de la República de Costa Rica
COBIT	*Control Objectives for Information and related Technology*
COSO ERM	Marco de Referencia Integrado del *Committee of Sponsoring Organizations of the Treadway Commsission*
DFOE	División de Fiscalización Operativa y Evaluativa
IFAC	Federación Internacional de Contadores
INN	Instituto Nacional de Normalización
INTOSAI	Organización Internacional de Entidades Fiscalizadoras Superiores
ISACA	*Information Systems Audit and Control Association*
ISO	*International Organization for Standardization*
ISSAI	Normas Internacionales de las Entidades Fiscalizadoras Superiores
MERTI	Metodología para la Evaluación de Riesgos relacionados con TI
NGASP	Normas Generales de Auditoría para el Sector Público
NIA	Normas Internacionales de Auditoría
OLACEFS	Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores
SEVRI	Sistema Específico de Evaluación del Riesgo Institucional
TI	Tecnologías de Información

INTRODUCCIÓN

El objetivo principal de esta propuesta es elaborar una metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros ejecutadas por la Contraloría General de la República de Costa Rica (CGR), con el fin de que el fiscalizador comprenda y considere las características del ambiente de tecnologías de información al determinar el alcance de la auditoria, mediante la aplicación de las mejores prácticas de evaluación de riesgos.

Este trabajo está organizado en seis capítulos. El primero presenta aspectos generales relacionados con el planteamiento de la propuesta, a saber; objetivos de la investigación, el alcance, la justificación y finalmente se presenta el marco metodológico.

El segundo, presenta el marco teórico, proporcionando a la investigación, un compendio coherente de conceptos y proposiciones.

El tercer apartado, expone la reseña histórica, marco y objetivos estratégico, funciones, estructura orgánica de la Contraloría General de la República (CGR) y normativa y procedimientos aplicables al proceso de auditoría.

El cuarto presenta el diagnóstico sobre la metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros, que al momento de la investigación aplica, la División de Fiscalización Operativa y Evaluativa (DFOE) de la CGR.

El quinto capítulo presenta una propuesta de Metodología de evaluación de riesgos relacionados con TI, que proporcione los lineamientos mínimos que debe seguir la DFOE. Finalmente, en el sexto capítulo se exponen las conclusiones y se plantean las recomendaciones pertinentes.

Capítulo I

Aspectos Introductorios

CAPÍTULO I: ASPECTOS GENERALES

Este capítulo expone aspectos generales relacionados con el planteamiento de la propuesta, a saber; objetivos de la investigación, el alcance, la justificación y finalmente se presenta el marco metodológico.

1.1 OBJETIVOS DE LA INVESTIGACIÓN

1.1.1 Objetivo general

Elaborar una metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros ejecutadas por la Contraloría General de la República de Costa Rica (CGR), con el fin de que el fiscalizador comprenda y considere las características del ambiente de tecnologías de información al determinar el alcance de la auditoria.

1.1.2 Objetivos específicos

1. Identificar la metodología que aplica la División de Fiscalización Operativa y Evaluativa (DFOE) de la Contraloría General de la República para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros.

2. Analizar la metodología aplicada para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros por la DFOE.

3. Determinar los aspectos sujetos a mejora y emitir las recomendaciones pertinentes.

4. Diseñar la propuesta de la metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros.

1.2 ALCANCE

La investigación se fundamentará en la información suministrada por los funcionarios de la DFOE, de la GGR, además se revisará la metodología implementada y documentación del periodo 2017.

El trabajo se enfocará en proponer una metodología para la evaluación de riesgos derivados de las TI en las auditorías de estados financieros que incorpore los aspectos que las mejores prácticas consideren como mínimos.

1.3 JUSTIFICACIÓN

Las tecnologías de información (TI) forman parte esencial de las operaciones de las instituciones, sin duda, han impactando sorprendentemente la forma en que es procesada la información y producidos los informes financieros. La pregunta que nace ante esa realidad es, si las organizaciones han gestionado los riesgos relacionados con las tecnologías de información y consecuentemente se tienen implementados y en operación controles efectivos que mitiguen esos riesgos.

La respuesta a la interrogante anterior, es una actividad fundamental para el trabajo de auditoria, ya que constituye un elemento para establecer el

alcance de la auditoria, así como la naturaleza, y la oportunidad de los procedimientos a aplicar.

En concordancia con lo anterior, la metodología que se pretende desarrollar, permitirá a la CGR, lograr una mejor comprensión del impacto de los riesgos derivados de las TI en las auditorías financieras que realice, conocer la forma en que se mitigan los riesgos originados por el uso de la tecnología, y consecuentemente, determinar el grado de confidencialidad, integridad y disponibilidad de la información.

1.4 MARCO METODOLÓGICO

A continuación, se describe el encuadre paradigmático, enfoque, tipo de investigación, sujetos y fuentes de información y por último las técnicas e instrumentos para la recolección de la información.

1.4.1 Encuadre paradigmático

El encuadre paradigmático a utilizar es naturalista. Este tipo de investigación “trata de comprender la situación o fenómeno tal como se presenta” (Gurdián, 2007, p. 159), por ello, se centra en la realidad que se analiza, la que se trata de comprender e interpretar de forma holística.

1.4.2 Enfoque

El enfoque será cualitativo, lo que se busca es obtener datos sobre la metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorías de estados financieros que realiza la División

de Fiscalización Operativa y Evaluativa (DFOE) de la Contraloría General de la República. Tal como lo indican Hernández, Fernández, & Baptista (2010), “se recolectan con la finalidad de analizarlos y comprenderlos, y así responder a las preguntas de investigación y generar conocimiento”. (p. 409)

El enfoque cualitativo, es útil tanto para conocer el entorno como para capturar esa realidad, de manera que se pueda entender integralmente.

1.4.3 Tipo de investigación

El objetivo principal de esta propuesta es proponer una metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorías de estados financieros, a partir de la información recabada, propósito que comparte con la investigación-acción.

Por lo anterior, esta investigación se llevará a cabo tomando como referente el diseño de investigación-acción. La investigación-acción tiene como finalidad, resolver problemas cotidianos y mejorar prácticas concretas. (Hernández, Fernández, & Baptista, 2010, p. 509)

1.4.4 Sujetos y fuentes de información

1.4.4.1 Fuentes primarias

Para esta investigación los sujetos de información primaria son los funcionarios de la División de Fiscalización Operativa y Evaluativa de la Contraloría General de la República.

Por su parte, como fuentes primarias, o directas, información original que esté disponible en la Contraloría; entre las cuales se citan:

políticas, procedimientos para la identificación de riesgos en las auditorias de estados financieros, informes, entre otros.

1.4.4.2 Fuentes secundarias

Como fuente de segunda mano, se mencionan los documentos que contienen información sobre las fuentes primarias. Entre las fuentes de segunda mano se encuentran: textos bibliográficos, artículos, proyectos de graduación, regulaciones, y demás información publicada oficialmente.

1.4.5 Técnicas e instrumentos para la recolección de información

Para recolectar la información se utilizarán dos herramientas, a saber; documentos, registros y sistema de información y entrevistas.

1.4.5.1 Documentos, registros y sistema de información

Se realizará la inspección del “Procedimiento de Auditoría y los criterios de calidad que se han elaborado para cada una de las tareas que conforman las actividades de planificación, examen y comunicación de resultados” versiones V4 y V5 y de una muestra de papeles de trabajo que soporten informes emitidos por la DFOE durante el 2017.

1.4.5.2 Entrevistas

Se llevarán a cabo entrevistas abiertas, bajo el formato pregunta-respuesta con personal clave de la DFOE. Estas entrevistas, tal como lo dicen Hernández, Fernández, & Baptista (2010) se fundamentan en “una guía general de contenido y el entrevistador posee toda la

flexibilidad para manejarla" (p. 418). De esa manera, es posible manejar su ritmo, estructura y contenido.

Capítulo II

Marco Teórico

CAPÍTULO II: MARCO TEÓRICO

Esta sección proporciona a la investigación, un compendio coordinado y coherente de conceptos y proposiciones relacionados con el objetivo planteado.

2.1 AUDITORÍA, RIESGO Y TECNOLOGÍAS DE INFORMACIÓN

La auditoría se define como una "revisión sistemática de una actividad o de una situación para evaluar el cumplimiento de las reglas o criterios objetivos a que aquellas deben someterse". (RAE, 2018)

Asimismo, puede definirse como "un proceso sistemático en el que de manera objetiva se obtiene y se evalúa la evidencia para determinar si la información o las condiciones reales están de acuerdo con los criterios establecidos" (INTOSAI, 2008, p. 4)

Del análisis de las definiciones anteriores, para esta propuesta, se entenderá auditoría como un proceso sistemático para obtener y evaluar, objetivamente, evidencia, en relación con hechos y eventos de diversa naturaleza; con el fin de comprobar su grado de correspondencia con los criterios establecidos.

En general, las auditorías se pueden clasificar de acuerdo con el objetivo que persiguen, en: de cumplimiento, financiera, operativa, integrada, administrativa, de sistemas de información, forense, entre otras. (ISACA, 2015) Los objetivos de una auditoría determinarán las normas, los principios y los lineamientos que se deberán aplicar.

De seguido, se describirá la auditoría financiera, por ser de interés para cumplir los objetivos de esta investigación, cabe señalar que para fines de esta

propuesta, el término “auditoría financiera” y “auditoría de estados financieros” se utilizan indistintamente.

La auditoría financiera es definida por la INTOSAI (2008) como “la evaluación independiente, reflejada en una opinión de garantías razonables, de que la situación financiera presentada por una entidad, así como los resultados y la utilización de los recursos, se presentan fielmente de acuerdo con el marco de información financiera”.

Asimismo, la auditoría financiera se enfoca en “determinar si la información financiera de una entidad se presenta en conformidad con el marco de referencia de emisión de información financiera y regulatorio aplicable. Esto se logra obteniendo evidencia de auditoría suficiente y apropiada que le permita al auditor expresar una opinión acerca de si la información financiera está libre de representaciones erróneas de importancia relativa debido a fraude o error.” (INTOSAI, 2008, p. 5)

Los principios y procedimientos básicos y esenciales, que se deberán aplicar en las auditorías financieras, están contenidos en las Normas Internacionales de Auditoría (NIA o ISAs, por sus siglas en inglés) emitidas por la Federación Internacional de Contadores (IFAC, por sus siglas en inglés).

En la auditoría del sector público se aplican los principios que establecen las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI, por sus siglas en inglés). Cabe destacar, que los principios de auditoría financiera de las ISAs están incorporadas en las directrices de las ISSAI (1000-2999), proporcionando una guía adicional, por lo que en las auditorías financieras del sector público se puede hacer referencia tanto a las ISSAIs como a las ISAs. (INTOSAI, 2008, p. 3)

Los principios relacionados con el proceso de auditoría financiera, que establecen las normas citadas, se pueden resumir, en tres etapas, a saber;

planeación, realización y elaboración de informes y seguimiento (INTOSAI, 2008, p. 9). La Figura 1 presenta el resumen del proceso de auditoría.

Figura 1 Proceso de auditoría financiera

Fuente: elaboración propia con información de las *ISSAI* 100 y 200. (INTOSAI, 2008)

El cumplimiento del proceso de auditoría, tal como lo describen las Normas, permite reunir evidencia suficiente y apropiada para sustentar el resultado de la auditoría. Todas los principios, que se detallan en la Figura 1 son esenciales, no obstante, de acuerdo con los objetivos de ésta investigación, de seguido, se desarrollarán de la etapa de planeación, los principios "Comprender la entidad", "Identificar y evaluar los riesgos" y "Respuesta del auditor al riesgo", según lo describen las *ISSAIs*.

Comprender la entidad

Para comprender la entidad, las Normas indican que se debe lograr un adecuado conocimiento de los objetivos, las operaciones, el entorno regulatorio, los controles internos, los sistemas financieros, entre otros, que sean relevantes para la auditoría.

Además, se debe tener un claro conocimiento de que la "entidad auditada cuenta con un procedimiento para identificar los riesgos relevantes para los objetivos de los informes financieros y sí estima además la importancia de dichos riesgos evaluando la posibilidad de que ocurran". (INTOSAI, 2008, p. 21)

En cuanto a los controles internos relevantes, como parte del proceso de entendimiento, podrá incluir también:

> "las clases de transacciones de la entidad auditada que sean significativas para los estados financieros;
>
> los procedimientos, tanto manuales como informáticos, por medio de los cuales dichas transacciones se ingresan, registran, procesan, corrigen en caso necesario, transfieren al libro mayor y reportan en los estados financieros;
>
> los registros contables, la información de soporte y las cuentas específicas contenidas en los estados financieros que se usan para ingresar, registrar, procesar y reportar las transacciones; esto incluye los procedimientos para corregir los datos incorrectos y transferir la información al libro mayor;
>
> la forma en que el sistema de información captura eventos y situaciones diferentes a las transacciones que sean significativos para los estados financieros;

el proceso de elaboración y presentación de información financiera usado para preparar los estados financieros;

los controles en torno a los asientos de diario, incluyendo las entradas excepcionales usadas para registrar ajustes u transacciones inusuales no recurrentes."

(INTOSAI, 2008, p. 21)

Identificar y evaluar los riesgos

En la auditoría se debe identificar y evaluar el riesgo de un error producto de deficiencias, desviaciones o representaciones erróneas, que pudieran afectar la información financiera a nivel de aseveraciones para las clases de transacciones, saldos de cuenta y divulgación de datos. Asimismo, se debe evaluar la respuesta de la administración ante los riesgos identificados, incluyendo la implementación y diseño de controles internos para enfrentarlos.

Con ese fin, en la auditoría se necesita:

"identificar los riesgos a lo largo de todo el proceso seguido para obtener un mejor conocimiento de la entidad auditada y de su entorno, examinando los controles relevantes que se relacionan con los riesgos y considerando las clases de transacciones, saldos de cuenta y divulgación de datos que aparecen en los estados financieros;

evaluar los riesgos identificados y valorar si se relacionan de una manera más generalizada con los estados financieros en su conjunto pudiendo afectar potencialmente varias aseveraciones;

relacionar los riesgos identificados con lo que pudiera salir mal a nivel de aseveración, tomando en cuenta los controles relevantes que el auditor pretende examinar; y

considerar la posibilidad de error, incluyendo la posibilidad de varios errores y si el potencial de las mismas es tal como para hacer que sean de significancia."

(INTOSAI, 2008, p. 22)

La identificación y evaluación de los riesgos de los errores significativos deben estar suficientemente documentados.

Respuesta del auditor al riesgo

De acuerdo con los riesgos identificados y evaluados, se deben diseñar procedimientos de auditoría que aborden dichos riesgos, como procedimientos sustantivos y la revisión de controles.

Al diseñar los procedimientos, el auditor deberá considerar el riesgo inherente a las transacciones y el riesgo de control.

La revisión del riesgo de control requiere que se obtenga evidencia de que los controles están operando de manera eficaz. Asimismo, en cuanto a pruebas sustantivas, sin importar si los controles han sido probados, el auditor debe realizar algunas pruebas; si el acercamiento a un riesgo significativo consiste únicamente de procedimientos sustantivos, dichos procedimientos deberán incluir pruebas de detalle. (INTOSAI, 2008, p. 24)

Al llevar a cabo los procedimientos descritos, se debe obtener evidencia suficiente y adecuada que sustente las conclusiones de la auditoría. De forma general, la evidencia proviene de la información

contenida en los registros contables que sirven de base para los estados financieros. Se debe considerar la confiabilidad de la información y tomar en cuenta los controles que existan para su preparación y mantenimiento.

Los principios del proceso de auditoría, abordados anteriormente, resultan fundamentales en el enfoque de auditoría basado en el riesgo[1] de la actividad o negocio que las NIA[2] describen. Al respecto, la NIA 315 define el riesgo de negocio como un "riesgo derivado de condiciones, hechos, circunstancias, acciones u omisiones significativas que podrían afectar negativamente a la capacidad de la entidad para conseguir sus objetivos y ejecutar sus estrategias o derivado del establecimiento de objetivos y estrategias inadecuadas." El riesgo de negocio es más amplio que el riesgo de incorrecciones materiales en los estados financieros" (INTOSAI, 2008)

En concordancia con lo indicado en la NIA 315, los riesgos del negocio podrían afectar negativamente los activos, procesos o la capacidad de una institución para conseguir sus objetivos; por lo que debe ser analizado en las auditorías financieras, en el contexto descrito anteriormente, y con mayor profundidad en las auditorías del sector público, tanto por las exigencias y la orientación contenidas en las normas (NIA, ISSAI) como por lo amplio de su mandato; por lo que no se limita al riesgo de incorrección material en los estados financieros por error o fraude. La definición de riesgo de negocio tiene un amplio alcance, y para fines de esta propuesta se abordará el relacionado con las tecnologías de información (TI).

COBIT 5 para Riesgos, define el riesgo de TI como "el riesgo de negocio asociado con el uso, la propiedad, operación, involucramiento,

---

[1] Se centra en la valoración que el auditor realiza sobre los riesgos para definir el alcance, la naturaleza y la oportunidad de los procedimientos de auditoría.

[2] NIA 315 – "Identificación y evaluación de los riesgos de incorrecciones materiales mediante la comprensión de la entidad y su entorno", NIA 330- "Respuesta del auditor ante los riesgos evaluados" y NIA 500- "Evidencia de auditoría".

influencia y adopción de las TI en una empresa. El riesgo de TI consiste de eventos relacionados a TI que potencialmente podrían impactar al negocio. El riesgo de TI puede darse con una frecuencia e impacto inciertos, generando desafíos en el logro de las metas y los objetivos estratégicos." (ISACA, 2013) Este definición de riesgo de TI, se utilizará a lo largo de esta propuesta.

La adopción de las TI y su dependencia en las instituciones, influye en la forma en que es procesada la información y producidos los informes financieros; por lo que es importante evaluar que se han gestionado los riesgos relacionados con las TI y que se tienen implementados y en operación controles efectivos que mitiguen esos riesgos.

La evaluación de los riesgos relacionados con TI, en la auditoría financiera, se centrará en aspectos de alto riesgo asociados a la integridad, confidencialidad o la disponibilidad de información sensible y crítica, y a los sistemas y procesos subyacentes de información, que generan, almacenan y manipulan dicha información. (ISACA, 2015).

En cuanto a TI, Cardona (2009) de manera amplia, la define tal como sigue: "las TI corresponden al conjunto de actividades que facilitan por medios electrónicos el archivo, procesamiento, transmisión y despliegue interactivo de información" (p. 58).

ISACA (2015) define TI como el "hardware, software, comunicación y otras instalaciones utilizadas para la entrada; el almacenamiento, el proceso, la transmisión y la salida de datos en cualquier de sus formas".

Por su parte, Cobo define TI indicando que son, "dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información que cuentan con protocolos comunes." (Cobo R., 2009, p. 312)

De acuerdo con las definiciones anteriores, para el fin de esta propuesta se entenderá TI como: dispositivos tecnológicos, integrados en medios de informática, telecomunicaciones y redes, que cuentan con protocolos comunes, que posibilitan la comunicación; utilizados para la entrada, el almacenamiento, el proceso, el intercambio, la transmisión y la salida de datos.

2.2 ESTÁNDARES PARA LA GESTIÓN DEL RIESGO

Existen diferentes estándares y mejores prácticas relacionados con la gestión del riesgo, a saber, la serie de ISO[3] 31000, ISO/IEC 27005, COSO ERM y COBIT 5 Riesgos. La gestión del riesgo se define como las acciones coordinadas para dirigir y controlar lo relacionado al riesgo, es la arquitectura (principios, marco de trabajo y proceso) para gestionar los riesgos. (INN, 2009)

La gestión del riesgo, en términos generales, busca identificar vulnerabilidades y amenazas que podrían afectar negativamente los activos, procesos o la capacidad de la organización de conseguir sus objetivos, y en el contexto de TI, las asociadas con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en la organización; y decidir qué controles o contramedidas aplicar; si hubiera alguna, que reduzca el riesgo a nivel aceptable.

A continuación, se describirán cada uno de los estándares mencionados.

2.2.1 ISO 31000

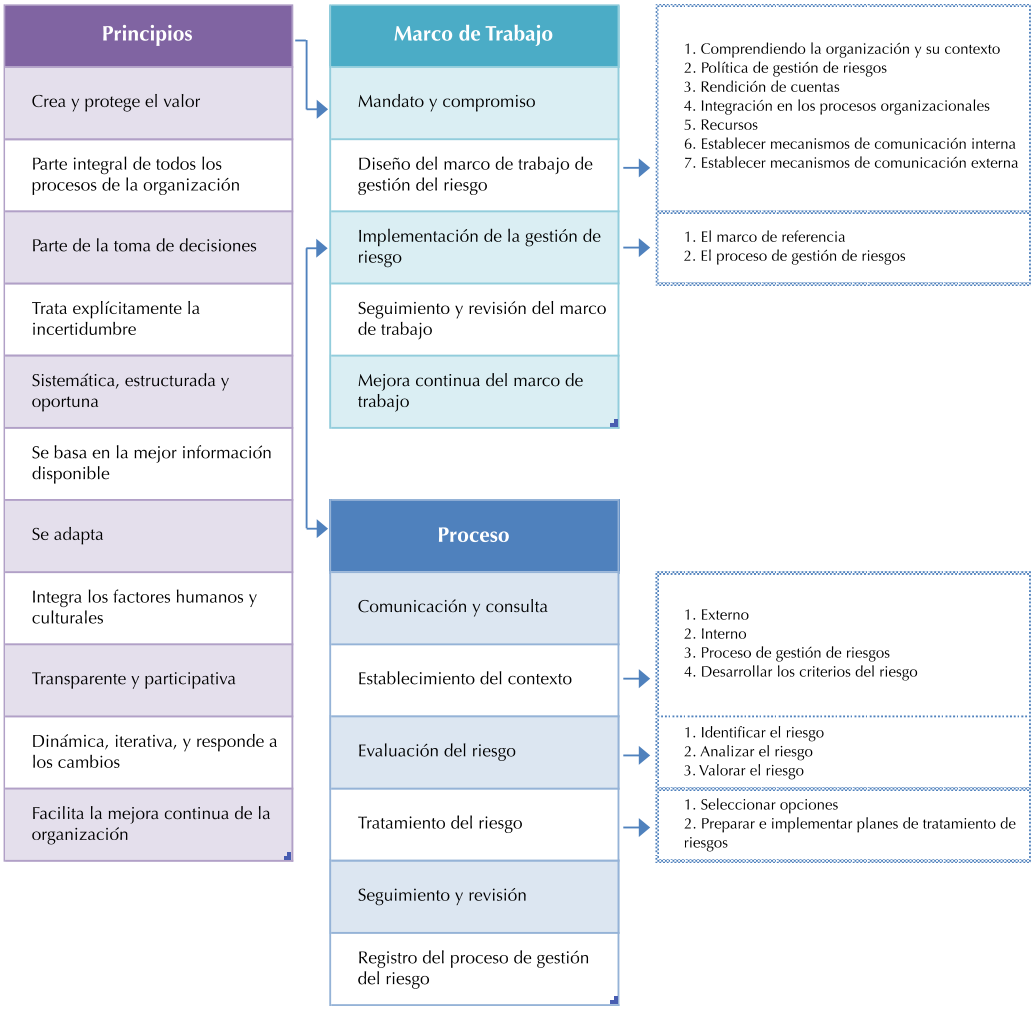
[3] *International Organization for Standardization (ISO)*

La NCh-ISO 31000[4] Gestión del riesgo - Principios y orientaciones, establece una serie de principios y directrices genéricas sobre la gestión de riesgos. La norma puede utilizarse en cualquier organización pública o privada, para gestionar cualquier tipo de riesgo y proporciona un enfoque común en apoyo de las normas que tratan riesgo. (INN, 2009)

Este estándar contiene tres apartados principales, a saber; principios, marco de trabajo y proceso. La Figura 2 presenta la relación entre los principios, el marco de trabajo y el proceso de gestión de riesgos, así como las actividades descritas en la norma.

[4] Esta norma es idéntica a la versión en inglés de la Norma Internacional ISO 31000:2009 *Risk management – Principles and guidelines*.

Figura 2 Relación entre los principios, el marco de trabajo y el proceso de gestión de riesgos



Fuente: elaboración propia con información de la NCh-ISO 31000 (INN, 2009)

La norma indica que para una eficaz gestión del riesgo se deberían cumplir cada uno de los principios, detallados en la Figura 2. Asimismo, destaca que el éxito de la gestión del riesgo dependerá de la eficacia del marco de trabajo, de modo que, proporcione las bases que permitan la integración de todos los niveles de la organización y facilite la gestión eficaz del riesgo mediante la aplicación del proceso de gestión del riesgo. (INN, 2009)

El proceso de gestión del riesgo, descrito por la norma, incluye la aplicación de métodos sistemáticos para: comunicar y consultar a lo largo del proceso; establecer el contexto (interno y externo) para la identificación, análisis, evaluación, tratamiento del riesgo relacionado con cualquier proceso en la organización; realizar seguimiento y revisar los objetivos; e informar y registrar los resultados de las actividades de gestión como base para mejorar el proceso en conjunto.

La evaluación del riesgo busca identificar la manera en que los objetivos de la organización pueden ser afectados y analiza el riesgo relacionándolo con las consecuencias y sus probabilidades antes de decidir si se necesita un tratamiento adicional. Esta evaluación intenta dar respuesta a las siguientes preguntas: ¿qué puede suceder y por qué?, ¿cuáles son las consecuencias?, ¿cuál es la probabilidad de que ocurra?, ¿existen factores que mitiguen las consecuencias del riesgo o que reduzcan la probabilidad del riesgo?

La evaluación del riesgo contempla identificar, analizar y valorar el riesgo, tal como se muestra en la Figura 2. A continuación, se presenta la descripción de cada aspecto.

Identificación el riesgo, el objetivo de esta etapa es generar una lista pormenorizada de eventos que podrían impactar negativamente el logro de los objetivos de la organización, considerando las posibles causas y escenarios que muestran las consecuencias que se podrían producir.

Análisis del riesgo, esta etapa implica desarrollar una comprensión del riesgo, considerando las causas y las fuentes del riesgo, sus consecuencias positivas y negativas, y la probabilidad de que las consecuencias se materialicen. Con ese fin, se identifican los factores que afectan las consecuencias y a la probabilidad y los controles existentes, así con su eficacia y su eficiencia.

De acuerdo con el objetivo para el que se utilizará el resultado del análisis de riesgos, la información disponible y el tipo de riesgo, se formularán las consecuencias y la probabilidad, así como la manera en que éstas se combinan para determinar el nivel de riesgo; esos elementos deberán ser coherentes con los criterios de riesgo y considerar la interdependencia de los diferentes riesgos y sus fuentes.

Se considera en el análisis del riesgo y se comunica a los interesados, la confianza en la determinación del nivel de riesgo, su sensibilidad a las condiciones previas y las hipótesis consideradas.

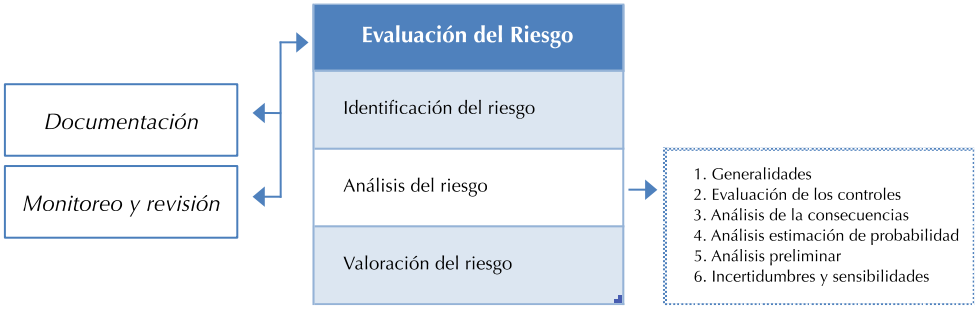
Valoración del riesgo, la finalidad de esta etapa es determinar los riesgos a tratar y la prioridad para implementar una respuesta adecuada, de acuerdo con los resultados del análisis de riesgos. Implica comparar el nivel de riesgo encontrado con criterios previamente establecidos, considerando el contexto amplio del riesgo y la tolerancia definida.

La NCh-ISO 31010[5] Gestión del riesgo – Técnicas de evaluación del riesgo, es una norma soporte a la 31000 y proporciona directrices para la selección y aplicación de técnicas sistemáticas para la evaluación del riesgo. Indica que la finalidad de la evaluación del riesgo es "proporcionar evidencias basadas en información y análisis para tomar decisiones informadas sobre cómo tratar riesgos particulares y cómo hacer la selección entre distintas opciones". (INN, 2013)

Esta norma presenta con mayor detalle el proceso de gestión de riesgos, así como explica, la importancia de la documentación, y el monitoreo y revisión, para la evaluación del riesgo. La Figura 3 presenta las etapas de la evaluación del riesgo y su relación con los otros elementos.

[5] Esta norma es idéntica a la versión en inglés de la Norma Internacional ISO/IEC 31010:2009 *Risk management – Risk assessment techniques*.

Figura 3 Evaluación del Riesgo según la NCh-ISO 31010



Fuente: elaboración propia con información de la NCh-ISO 31010 (INN, 2009)

De seguido, se describirán aspectos de cada una de las etapas de la evaluación del riesgo.

Identificación del riesgo, es la etapa del proceso con el que se descubre, reconocen y registran los riesgos; de seguido se identifican los controles existentes como sus características de diseño, personas que intervienen, procesos y activos. Incluye la identificación de las causas y origen del riesgo y la naturaleza del impacto que podría tener en los objetivos de la organización.

Análisis del riesgo, esta etapa consiste en determinar las consecuencias y sus probabilidades para eventos de riesgo identificados, y la eficacia de los controles existentes. Las consecuencias y sus probabilidades se combinan para determinar el nivel de riesgo. Involucra la consideración de las causas y las fuentes de riesgo, sus consecuencias y la probabilidad de que estas consecuencias puedan ocurrir. Se deben identificar los factores que afectan a las consecuencias y a la probabilidad.

El análisis de riesgos se centrará en la importancia y vulnerabilidad de los componentes del sistema, cuando una consecuencia pueda producir

como resultado una serie de eventos, o no se pueda identificar un evento en concreto.

A continuación se describe cada actividad de la etapa de análisis de riesgos:

Evaluación de controles: el nivel de riesgo depende de la idoneidad y eficacia de los controles. Los aspectos a considerar son ¿cuáles son los controles existentes? ¿son capaces de trata adecuadamente el adecuadamente el riesgo, hasta un nivel tolerable? ¿en la práctica, funcionan los controles de la manera prevista y son eficaces cuando se aplican?.

Análisis de las consecuencias: determina la naturaleza y el tipo de impacto que podría ocurrir al materializarse un evento. Las consecuencias a analizar y los afectados deberían estar definidos de previo cuándo se estableció el contexto. El análisis puede implicar, tener en consideración los controles existentes para tratar las consecuencias; relacionarlas con los objetivos iniciales; hay que tener en consideraciones inmediatas y las que pueden aparecer después; y considerar las consecuencias secundarias.

Análisis y estimación de la probabilidad: para estimar la probabilidad se pueden utilizar datos históricos, utilizar técnicas de predicción o utilizar la opinión de un experto.

Análisis preliminar: busca excluir riesgos que se consideren poco significativos. Los criterios para realizarlo deben ser definidos de previo. Se deben documentar las hipótesis y los resultados.

Incertidumbres y sensibilidades: un análisis de incertidumbres implica determinar variaciones o imprecisiones en los resultados, originadas por la variación de parámetros e hipótesis que se hayan utilizado. Un análisis de sensibilidad involucra la determinación del tamaño y la importancia de la magnitud de riesgo a cambio de un parámetro.

Valoración del riesgo, implica la comparación de niveles estimados de riesgo con los criterios de riesgo definidos, para determinar la importancia del nivel y tipo de riesgo. Un enfoque de valoración, consiste en dividir los riesgos en tres, a saber; una banda superior, donde el nivel de riesgo es intolerable y es esencial tratar el riesgo; una banda media, en la cual costos y beneficios se tienen en cuenta y las oportunidades se compensan con respecto a las consecuencias potenciales; y una banda inferior, donde el riesgo se considera insignificante de manera que no es necesario medidas adicionales.

Los resultados del proceso de evaluación del riesgo se debe documentar, expresando los riesgos en términos inteligibles. Entre los aspectos que se pueden incluir están: los objetivo, descripción de las partes pertinentes del sistema y sus funciones; un resumen del contexto y como se relaciona la situación; los criterios del riesgo aplicados y su justificación; las limitaciones, los supuestos y la justificación de las hipótesis; la metodología aplicada en la evaluación; los resultados de la identificación del riesgo; los datos, los supuestos y sus orígenes y validación; los resultados del análisis del riesgo y su evaluación; los análisis de sensibilidad y de incertidumbre; los supuestos críticos y otros factores sobre los que se necesita seguimiento; la discusión de los resultados; las conclusiones y recomendaciones; y las referencias.

2.2.2 ISO/IEC 27005

La ISO/IEC 27005 Tecnología de Información - Técnicas de seguridad - Gestión de riesgos de seguridad de Información, provee directrices para la gestión del riesgo en la seguridad de la información.

La ISO/IEC 27005 se enfoca en el riesgo de la seguridad de la información, el cual define como “el potencial de que una amenaza explote

las vulnerabilidades de los activos o grupos de activos de información, y por lo tanto, causar daño a la organización”

El proceso de gestión del riesgo de la seguridad de la información descrito por el estándar ISO/IEC 27005, contiene las seis etapa descritas en la ISO 31000. A continuación se detalla la etapa de establecimiento del contexto y la de evaluación del riesgo del proceso.

El establecimiento del contexto incluye definir los criterios básicos para la gestión de riesgos de seguridad de la información, definir el alcances y los límites.

En la evaluación del riesgo se determina el valor de los activos de información, se identifican amenazas, vulnerabilidades, controles existentes y su efecto en los riesgos identificados, así como determinar las consecuencias potenciales, y finalmente, prioriza los riesgos identificados y los clasifica de acuerdo a los criterios definidos. Esta etapa consta de tres actividades, a saber; la identificación, el análisis y la valoración de riesgos.

En la identificación de los riesgos se identifican activos, amenazas, vulnerabilidades, controles existentes y consecuencias. El resultado de esta actividad es una lista de escenarios de incidentes y sus consecuencias.

La actividad de análisis de riesgos incluye la evaluación de las consecuencias y la probabilidad de incidentes, así como la determinación del nivel de riesgo.

En la valoración de riesgos, los niveles de riesgo determinados en el análisis de riesgos se comparan con los criterios de valoración y aceptación de los riesgos definido inicialmente. El resultado de esta actividad es una lista priorizada de los elementos de riesgo y de los escenarios de riesgos que conducen a los elementos identificados de riesgo.

2.2.3 COSO ERM

COSO ERM - Marco de Referencia Integrado del Committee of Sponsoring Organizations of the Treadway Commsission (COSO), es un marco de implementación y gestión del control interno y evaluación de su efectividad. Este Marco define ocho componentes, a saber: ambiente interno, establecimiento de objetivos, identificación de eventos, evaluación del riesgo, respuesta al riesgo, actividades de control, información y comunicación y supervisión.

En el ambiente interno se incluye la filosofía de la gestión de riesgos de la entidad, su apetito de riesgo, y la supervisión.

El establecimiento de objetivos es una precondición para la identificación de eventos, evaluación de riesgo y respuesta al riesgo. Los objetivos se alinean con el apetito de riesgo de la entidad, lo que define los niveles de tolerancia al riesgo de la entidad.

Para la identificación de eventos se considera los factores internos y externos, que pueden potenciar las oportunidades y el riesgo, en el contexto de la entidad.

COSO ERM define evaluación del riesgo como “lo que permite que una entidad considere la medida en que un potencial evento tiene un impacto en el logro de los objetivos”. Se evalúan los eventos desde dos perspectivas, probabilidad e impacto.

Una vez evaluado el riesgo se determina la forma de respuesta. Las posibles respuestas son evitar, reducir, compartir y aceptar el riesgo. Para determinar la respuesta adecuada, se evalúa los efectos en la probabilidad e impacto del riesgo, así como los costos y beneficios.

Las actividades de control son diversas, en este contexto, las de interés, son los tipos de actividades, políticas y procedimientos y controles sobre los sistemas de información.

Los sistemas de información transforman datos en información que apoya el proceso de toma de decisiones, así como suministrar información para gestionar el riesgo.

Finalmente, la supervisión en el COSO ERM se ocupa de la gestión de riesgos, evaluando la presencia y el funcionamiento de sus componentes a través del tiempo.

2.2.4 COBIT 5 Riesgos

COBIT 5 Riesgos proporciona una guía para analizar los riesgos relacionados con TI, aplicables para cualquier tipo de organización. Se basa en COBIT 5. (ISACA, 2013)

Este marco, presenta en dos perspectivas sobre la forma de utilizar COBIT 5 con respecto a riesgos, la perspectiva de la función de riesgos y la perspectiva de la gestión de riesgos.

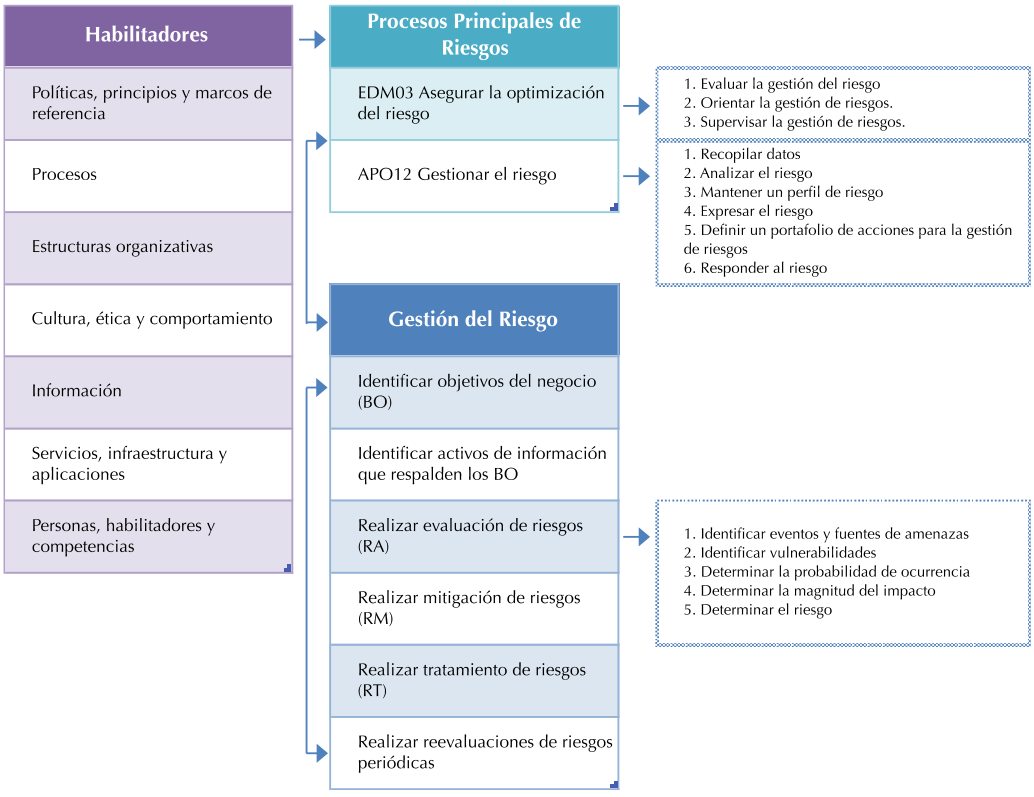
La perspectiva de la función de riesgo, describe lo que se necesita para construir y sostener actividades principales de gobierno y gestión del riesgo en forma efectiva y eficiente. Para cada habilitador describe cómo contribuye a la función global de gobierno y gestión del riesgo. (ISACA, 2013)

Un habilitador es cualquier elemento que ayude a conseguir las metas de la organización, COBIT define siete categorías, a saber; principios, políticas y marcos de trabajo; procesos; estructuras organizativas; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones; y finalmente, personas, habilidades y competencias.

Por su parte, la perspectiva de la gestión de riesgos, describe cómo el proceso principal de gestión de riesgos, para la identificación, análisis, respuesta y reporte sobre los riesgos puede ser apoyado por los habilitadores de COBIT 5. Esta perspectiva requiere implementar los procesos EDM03 Asegurar la optimización del riesgo y APO12 Gestionar el riesgo. El riesgo es presentado en escenarios de riesgo. (ISACA, 2013)

La Figura 4 presenta la relación entre habilitadores, procesos principales de riesgos y la gestión del riesgo, así como las actividades descritas en el marco. Las perspectivas descritas anteriormente, están implícitas en la relación que presenta la Figura 4.

Figura 4 Relación entre habilitadores, procesos principales y gestión del riesgo



Fuente: elaboración propia con información ISACA (2013)

Los habilitadores, que se presentan en la Figura 4, apoyan la implementación de los procesos principales de la gestión de riesgos.

Por su parte, los proceso (EDM03 y APO12), comprenden las actividades principales de la función de riesgos, de manera que brindan soporte a la organización, optimizando recursos y los riesgos. El EDM03, abarca el entendimiento, la articulación y la comunicación del apetito y tolerancia al riesgo, la identificación y gestión del riesgo asociado. El APO12, incluye la continua identificación, evaluación y reducción del riesgo relacionado con TI dentro de los niveles de tolerancia establecidos por la gerencia. (ISACA, 2013)

La instrumentalización de las actividades de los procesos principales, comentados en el párrafo anterior, se realiza con la ejecución del proceso de la gestión del riesgo.

A continuación se describe cada una de las etapa de la gestión del riesgo, como lo indica ISACA (2015).

La gestión del riesgo, inicia con la identificando de los objetivos del negocio, los activos de información y los sistemas o recursos de información subyacentes que generan/almacenan, usan o manipulan los activos clave (hardware, software, bases de datos, redes, instalaciones, personas, etc.) para lograr esos objetivos.

De seguido se clasifican los sistemas o recursos de información en términos de criticidad y sensibilidad.

Después de la identificación de activos de información sensible o crítica, se realiza una evaluación de riesgos, de manera que se identifiquen eventos y fuentes de amenazas y vulnerabilidades, se determina la probabilidad de ocurrencia y la magnitud del impacto en caso de materializarse la amenaza. Además, se determinan las medidas adicionales

que mitigarían el impacto a un nivel aceptable. La evaluación del riesgo finaliza, con la determinación de la visión general del riesgo (cálculo del riesgo), combinando la probabilidad de ocurrencia por la magnitud del impacto.

Seguidamente, durante las etapa de mitigación de riesgos, se evalúan los controles existentes en cuanto a diseño y efectividad. Se debe considerar si los controles son preventivos, detectivos o correctivos, manuales o automatizados, y formales o ad hoc.

Para tratar los riesgos no mitigados por los controles, se deben evaluar contramedidas, de manera que se logre prevenir o reducir la probabilidad de que ocurra un evento de riesgo, detectar la ocurrencia del mismo, o minimizar el impacto transfiriendo el riesgo a otra organización, de acuerdo a un nivel de riesgo aceptado por la gerencia.

La etapa final se relaciona con la reevaluación de los riesgos cuando se identifiquen cambios significativos en el ambiente, ya que la gestión de riesgos es un proceso continuo que busca identificar y evaluar los riesgos a medida que éstos surgen y evolucionan.

El APO12, requiere que los riesgos sean identificados, analizados y que se dé una respuesta de acuerdo con el nivel de riesgo aceptado por la organización, para lo cual, en COBIT se utiliza la técnica de escenarios de riesgos como componente clave.

Un escenario de riesgo es la descripción de un posible evento que puede derivar un impacto cuando y si ocurre. Su análisis, es una técnica que ayuda a describir el riesgo de forma tangible y evaluable.

Los escenarios de riesgo pueden abordarse desde dos enfoques, descendente y ascendente, son complementarios. El enfoque descendente, parte de los objetivos globales de la organización y realiza un análisis de los

escenarios de riesgo de TI más relevantes y probables que impacten los objetivos empresariales. El enfoque ascendente, utiliza una lista de escenarios genéricos para definir los escenarios de riesgos relevantes y los aplica a la situación individual de la organización.

Un escenario de riesgo tiene los siguientes componentes: agente, es quién genera la amenaza; tipo de amenaza, se refiere a la naturaleza del evento (maliciosa, accidental, natural); evento, la divulgación de información, interrupción de un sistema, robo, destrucción; activo/recurso, dónde se presenta el escenarios, cualquier elemento de valor que puede ser afectado por el evento y dar lugar a un impacto; y tiempo, duración del evento, el momento, detección, tiempo transcurrido entre el evento y la consecuencia.

2.3 TÉCNICAS DE EVALUACIÓN DEL RIESGO

La evaluación del riesgo se puede realizar con diferentes grados de detalle y utilizando una o diferentes técnicas. Lo anterior, dependerá del tipo de evaluación y de los resultados esperados, así como, de los criterios de riesgo establecidos como parte del contexto y de la disponibilidad de datos.

La NCh-ISO 31010[6], indica que una técnica es adecuadas para la gestión de riesgos, si cumple con las características siguientes: que la técnica sea justificable y apropiadas para la situación que se está considerando; que proporcione resultados que mejoren la comprensión de la naturaleza del riesgo; y se pueda utilizar de una manera trazable, reproducible y verificable.

Asimismo, la Norma en mención, establece que las técnicas se deben seleccionar con base a los siguientes factores: los objetivos del estudio, las

[6] Esta norma es idéntica a la versión en inglés de la Norma Internacional ISO/IEC 31010:2009 *Risk management – Risk assessment techniques*.

necesidades de las personas que tomen las decisiones, el tipo y gama de riesgos que se analizan, la posible magnitud de las consecuencias, el grado de conocimiento técnico que se necesite, la disponibilidad de información y de datos, la necesidad de actualización de la evaluación de riesgos y finalmente, cualquier requisito contractual y reglamentario.

Existen diferentes técnicas que se pueden aplicar para la evaluación de riesgos, la NCh-ISO 31010 [7] presenta para cada etapa del proceso de evaluación del riesgo una selección de técnicas aplicables, para el detalle refiérase al Anexo 1.

Asimismo, los estándares citados en el apartado 2.2, describen los modelos cualitativos, semi-cuantitativos o cuantitativos como base para el análisis de riesgos, tal como se describe a continuación.

El análisis cualitativo define las consecuencias, la probabilidad y el nivel de riesgo, como alto, medio y bajo, en función de criterios cualitativos.

El método semi-cuantitativo, utiliza escalas numéricas para la evaluación de consecuencias y la probabilidad, y para determinar el nivel de riesgo se combinan esos elementos aplicando una fórmula.

El análisis cuantitativo estima valores para consecuencias y sus probabilidades; y obtienen valores del nivel de riesgo en unidades específicas previamente definidas.

[7] Esta norma es idéntica a la versión en inglés de la Norma Internacional ISO/IEC 31010:2009 *Risk management – Risk assessment techniques*.

2.4 METODOLOGÍA PARA LA EVALUACIÓN DE LOS RIESGOS

A lo largo de este marco teórico se han discutido temas como: la auditoría financiera y su relación con riesgo y las tecnologías de información; seguido de la definición de gestión de riesgo y diversos estándares para la gestión del riesgo; y en el apartado anterior, técnicas utilizados para la evaluación del riesgo.

Todos esos elementos, son esenciales para definir una metodología para la evaluación de riesgos derivados de TI. Para fines de esta propuesta se entenderá como metodología para la evaluación de riesgos, los procedimientos para identificar, analizar y valorar el riesgo, instrumentalizados por medio de la aplicación de las mejores prácticas. De tal manera, que le permita al auditor, lograr una mejor comprensión del impacto de las TI en la institución fiscalizada, conocer la forma en que se mitigan los riesgos originados por el uso de la tecnología, y consecuentemente, determinar el grado de confidencialidad, integridad y disponibilidad de la información.

La metodología para la evaluación de riesgos deberá establecer claramente los siguientes aspectos:

- Establecimiento del contexto: con el fin de cumplir con esta etapa es necesario conocimiento de:
    - Los objetivos, las operaciones, el entorno regulatorio, los controles internos, los sistemas financieros, entre otros, que sean relevantes para la auditoría.
    - Si la entidad auditada cuenta con un procedimiento para identificar los riesgos relevantes para los objetivos de los informes financieros y si estima además la importancia de dichos riesgos evaluando la posibilidad de que ocurran.

- Controles internos relevantes.
- Criterios básicos para la gestión de riesgos, definir el alcance y los límites.

- Identificación de riesgos: se refiere a la etapa de la evaluación de riesgos que permite, descubrir, reconocer y registrar riesgos, identificando las causas y su posible efecto; como resultado de esta etapa se genera es una lista de escenarios de riesgos. Para fines prácticos se identificarán los siguientes elementos para construir los escenarios de riesgos:
  - Eventos.
  - Activos de información y los sistemas o recursos de información subyacentes que generan/almacenan, usan o manipulan los activos clave (hardware, software, bases de datos, redes, instalaciones, personas, etc.), indicando su criticidad y sensibilidad.
  - Vulnerabilidades.
  - Amenazas.
  - Controles existentes describiendo sus características de diseño, tipo de control, (preventivo, detectivo o correctivo, manual o automatizado, formales o ad hoc) personas que intervienen, procesos y activos. Considerando las clases de transacciones, saldos de cuenta y divulgación de datos que aparecen en los estados financieros
  - Naturaleza de las consecuencias.
- Análisis de riesgos: en esta etapa se desarrolla la comprensión del riesgo, considerando los aspectos identificados en la etapa anterior, se evalúa la efectividad de los controles y se determina la probabilidad de ocurrencia, la magnitud del impacto y la visión general del riesgo (Cálculo del riesgo). A continuación se lista cada aspecto a analizar:

- Riesgos no significativos.
- Efectividad de los controles, como lo que pudiera salir mal a nivel de aseveración.
- Estimación del impacto de las consecuencias.
- Estimación de la probabilidad.
- Incertidumbres y sensibilidades.

- Valoración de riesgos: la finalidad de esta etapa es determinar los riesgos a tratar y la prioridad para implementar una respuesta adecuada. Implica comparar el nivel de riesgo estimado con los criterios de riesgos definidos, en el contexto. El resultado de esta etapa es una matriz priorizada de los elementos de riesgo.
- Documentación: los resultados del proceso de evaluación del riesgo se deben documentar. Entre los aspectos que se pueden incluir están:
  - Objetivo y la descripción de las partes pertinentes del sistema y sus funciones.
  - Resumen del contexto y como se relaciona la situación.
  - Criterios del riesgo aplicados y la justificación de los mismos.
  - Limitaciones, los supuestos y la justificación de las hipótesis.
  - Metodología aplicada en la evaluación.
  - Resultados de la identificación del riesgo.
  - Datos, los supuestos y sus orígenes y validación.
  - Resultados del análisis y valoración de los riesgos.
  - Supuestos críticos y otros factores sobre los que se necesita hacer monitoreo.
  - Discusión de los resultados.
  - Conclusiones y recomendaciones.

Una vez explicado el marco teórico coherente de conceptos y proposiciones, en el siguiente capítulo se describirán aspectos esenciales para conocer el devenir de la Contraloría General de la República de Costa Rica.

.

Capítulo III

Contraloría General de la República

CAPÍTULO III: CONTRALORÍA GENERAL DE LA REPÚBLICA

Este capítulo expone aspectos esenciales para conocer el devenir de la Contraloría General de la República (CGR) y normativa aplicable. En el primer apartado se presenta la reseña histórica, seguido del marco estratégico que contempla la misión, visión, y valores, objetivos estratégicos, funciones y la estructura orgánica. En el segundo apartado, se lista la normativa aplicable a los procesos de fiscalización.

3.1 CONTRALORÍA GENERAL DE LA REPÚBLICA

La Contraloría General de la República fue creada en 1949, como la institución encargada de vigilar el uso de los recursos públicos que utilizan las instituciones del Estado. A continuación, se describe el contexto en el que nació la CGR.

3.1.1 Reseña histórica

En el año 1825, al promulgar la 1º Ley Fundamental de Costa Rica, el Pacto de Concordia, se creó un Tribunal de Cuentas, cuya función principal era ejercer un control financiero de orden político, examinando los resultados de las principales rentas que debían rendir los Jefes de Estado. (CGR, 2017)

Posteriormente, se definió un “tribunal superior de cuentas que examinaba, glosaba y fenecía las cuentas que debían rendir los administradores, tesoreros y recaudadores de fondos públicos”. (CGR, 2017)

La Oficina de Control se creó en 1922, al suprimirse el tribunal superior de cuentas, “la cual asumió las funciones de la Contaduría Mayor, además, debía aprobar anticipadamente el presupuesto del año siguiente y ejercer el

control presupuestario". En 1945, se creó el Centro de Control, que era una institución auxiliar del Poder Legislativo, con independencia de los demás poderes y fue denominado "Centro de Control" (CGR, 2017)

En 1949, la Asamblea Constituyente, "evaluó las funciones del Centro de Control y determinó la necesidad de que existiera un órgano que vigilara permanentemente la inversión, procedencia, manejo financiero, económico y legal de los fondos públicos. Es así como se incluyó en la Constitución Política actual un capítulo que creó a la Contraloría General de la República". (CGR, 2017)

En 1950, "se emite la Ley Orgánica de la Contraloría General de la República, la cual señala los objetivos, funciones, atribuciones, procedimientos y organización de la CGR". (CGR, 2017)

Ya para 1951, comienza sus funciones con un presupuesto de ¢300.000 y bajo la dirección de los señores Amadeo Quirós Blanco y Rodolfo Castaing Castro, Contralor General y Subcontralor General de la República, respectivamente. (CGR, 2017)

La Ley Orgánica de la CGR de setiembre de 1994 y sus reformas, en el artículo 12, designa a la Contraloría como órgano rector del ordenamiento de control y fiscalización de la Hacienda Pública. Asimismo en el artículo 21 de la ley citada, se le confiere la potestad de realizar auditorías financieras, operativas y de carácter especial. (CGR, 2006)

Finalmente, para el 2017 la CGR ha realizado xxxxx estudios como órgano rector de control y fiscalización, sumando a la fecha 147 auditorías a los estados financieros en 34 instituciones del sector público. (CGR, 2017)

3.1.2 Marco estratégico de la CGR

Tal como se indicó en el apartado anterior, la Contraloría General de la República es el órgano rector del ordenamiento de control y fiscalización superior; ejerce su competencia sobre los entes y órganos que integran la Hacienda Pública. (Asamblea Legislativa, 1994)

3.1.2.1 Misión y Visión

La misión destaca el propósito por el cual existe la Contraloría General de la República, es un órgano que fiscaliza el uso de los fondos públicos.

Misión

> "Somos el órgano constitucional, auxiliar de la Asamblea Legislativa que fiscaliza el uso de los fondos públicos para mejorar la gestión de la Hacienda Pública y contribuir al control político y ciudadano." (CGR, 2011)

La Contraloría General de la República pretende garantizar la vigilancia efectiva de la Hacienda Pública.

Visión:

> "Garantizaremos a la sociedad costarricense, la vigilancia efectiva de la Hacienda Pública." (CGR, 2011)

3.1.2.2 Valores

Los valores de la CGR expresan las características y normas conductuales que se espera de los funcionarios y funcionarias, con el fin de lograr su misión y con ello la visión. A continuación, los valores de la CGR:

> "Excelencia, búsqueda de la máxima calidad y desempeño en el trabajo diario.
>
> Respeto, valorar los derechos y formas de pensar de los demás.
>
> Justicia, dar a los demás lo que les corresponde de acuerdo con sus derechos y deberes.
>
> Integridad, es realizar todas las acciones con rectitud.
>
> Compromiso, es sentirse identificado con la Contraloría General y así dar el máximo esfuerzo." (CGR, 2011)

3.1.3 Objetivos estratégicos

Los objetivos estratégicos que permitirán a la CGR lograr su misión, son los siguientes, según el Plan Estratégico Institucional (2016):

1. Impactar la eficiencia en la gestión pública priorizando acciones de fiscalización integral dirigidas a mejorar la gestión del servicio público, para una mejor satisfacción del interés colectivo.
2. Incrementar la transparencia propiciando el conocimiento ciudadano sobre la administración de la Hacienda Pública para favorecer el control y la rendición de cuentas.
3. Fortalecer la prevención de la corrupción mediante acciones novedosas de fiscalización integral.
4. Desarrollar una gestión del potencial humano orientada al crecimiento integral del personal y al fomento de una cultura institucional de integración, proclive a la eficiencia, para responder a las necesidades institucionales.

5. Transformar el proceso de fiscalización integral sustentándolo en tecnologías de información para incrementar su confiabilidad y oportunidad.

3.1.4 Funciones

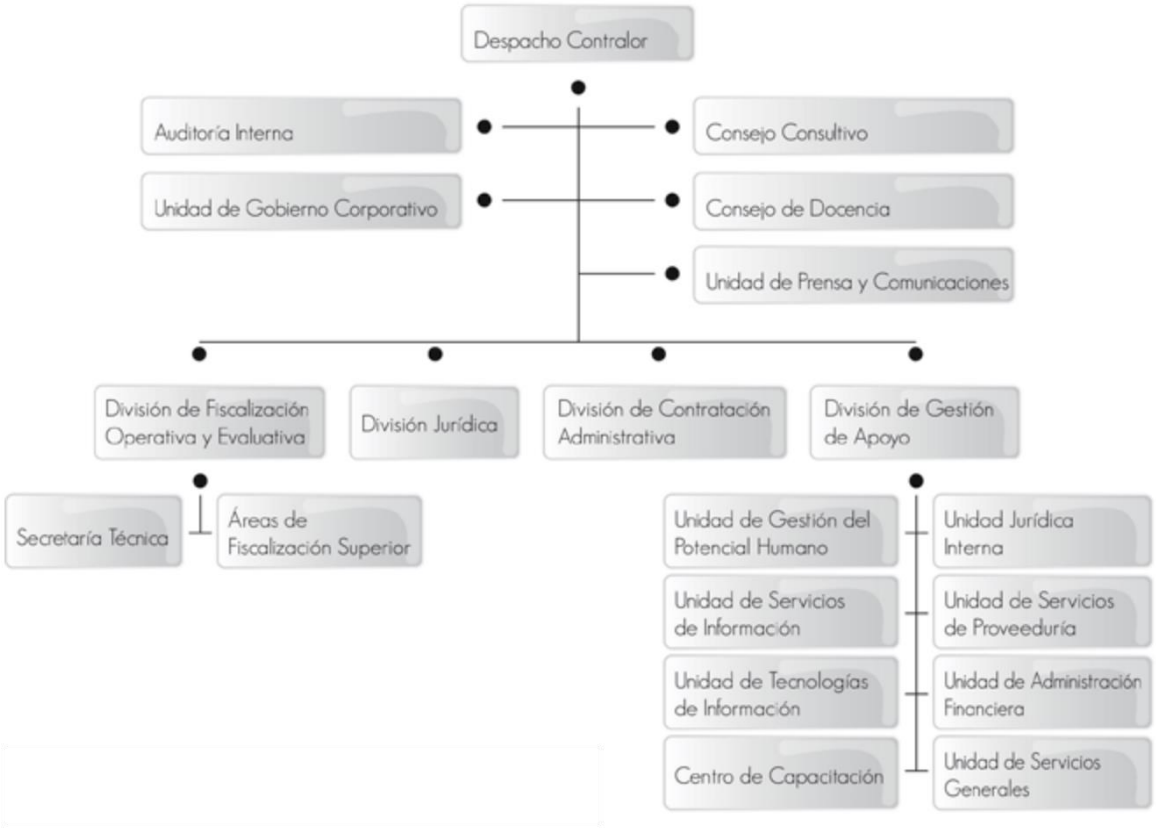
Algunas de las funciones que tiene la Contraloría General de la República son las siguientes, según el Capitulo II de la Ley N.º 7428:

- ***Fiscalización presupuestaria***, examina para su aprobación o improbación, total o parcial, los presupuestos.
- ***Aprobación de actos y contratos***, aprueba los contratos que celebre el Estado y los que por ley especial deben cumplir con este requisito.
- ***Realizar auditorías***, puede realizar auditorías financieras, operativas y de carácter especial en los sujetos pasivos.
- ***Investigación***, puede instruir sumarios administrativos o realizar investigaciones especiales de oficio.
- ***Reglamentaria***, potestad para dictar los reglamentos autónomos de servicio y de organización.
- ***Dirección en materia de fiscalización***, puede dictar planes y programas de su función fiscalizadora, así como las políticas, los manuales técnicos y las directrices.

3.1.5 Estructura orgánica

La Contraloría General de la República, de conformidad con su Ley Orgánica “goza de absoluta independencia funcional y administrativa” (Asamblea Legislativa, 1994); y con fundamento en esa facultad tiene establecida su estructura orgánica, la cual se describe en la Figura 1; junto con aspectos relevantes de sus principales dependencias.

Figura 5 Estructura Organizacional de la Contraloría General de la República



Fuente: Tomado de CGR (2017)

3.2.5.1 Despacho Contralor

El Despacho Contralor "es la dependencia encargada de dirigir, organizar y controlar el quehacer institucional, por lo que está llamado a definir la dirección estratégica de la fiscalización". (CGR, 2011, p. 5) Está integrado "por un Contralor, quien es la máxima autoridad de la institución, de la que ejerce la representación judicial y extrajudicial; un Subcontralor quien sustituye al primero en sus ausencias temporales, lo asiste en el ejercicio de sus atribuciones." (CGR, 2011, p. 5)

El Despacho Contralor tiene cinco unidades de asesoría y apoyo: Consejo Consultivo, Consejo de Docencia, Auditoría Interna, Unidad de Gobierno Corporativo y Unidad de Prensa y Comunicaciones. (CGR, 2011, p. 5)

3.2.5.2 División de Fiscalización Operativa y Evaluativa

La División de Fiscalización Operativa y Evaluativa (DFOE), depende del Despacho Contralor y está a cargo de una Gerencia de División. (CGR, 2011, p. 8) Está División realiza las funciones de fiscalización de la Hacienda Pública en materia de su competencia. Está integrada por una Secretaría Técnica, unidad asesora y de apoyo a la Gerencia de la DFOE y por Áreas de Fiscalización Superior, unidades que ejecutan las labores de fiscalización. (CGR, 2011, p. 9)

Las Áreas de Fiscalización superior son las siguientes: Denuncias e Investigaciones, Seguimiento de Disposiciones, Servicios Ambientales y Energía, Servicios de Infraestructura, Servicios Económicos, Servicios para el Desarrollo Local, Servicios Públicos Generales, Servicios Sociales y Sistema de Administración Financiera de la República. (CGR, 2010)

3.2.5.3 División Jurídica

La División Jurídica, depende del Despacho Contralor y está a cargo de una Gerencia de División. (CGR, 2011, p. 10) Está División "dirige, gestiona y asesora jurídicamente en los procesos institucionales, con el propósito de que toda la actividad que ejerce la institución se desarrolle de conformidad con el ordenamiento jurídico". (CGR, 2011, p. 10)

3.2.5.4 División de Contratación Administrativa

La División de Contratación Administrativa, depende del Despacho Contralor y está a cargo de una Gerencia de División. Está División lidera procesos de fiscalización previa en materia de contratación administrativa, rectoría y asesoría sobre Hacienda Pública en materia de su competencia. (CGR, 2011, p. 12)

3.2.5.5 División de Gestión de Apoyo

La División de Gestión de Apoyo, depende del Despacho Contralor y está a cargo de una Gerencia de División. Está División "agrupa las unidades encargadas de adquirir, generar, transferir y potenciar la información y el conocimiento sobre la base en el aprendizaje individual y colectivo". (CGR, 2011, p. 13)

Está integrada por la Unidad Jurídica Interna, la Unidad de Gestión de Potencial Humano, la Unidad de Servicios de Información, la Unidad de Tecnologías de Información, la Unidad de Servicios Generales, la Unidad de Administración Financiera, el Centro de Capacitación y la Unidad de Servicios de Proveeduría. (CGR, 2011, p. 14)

3.2 NORMATIVA APLICABLE

La Contraloría General de la República de Costa Rica, tiene un amplio grupo de normativa y procedimientos relacionados con el proceso de auditoría, de seguido se presenta una lista que no pretende ser exhaustiva.

- Normas Generales de Auditoría para el Sector Público (NGASP), publicadas mediante la resolución R-DC-064-2014) en La Gaceta N°.

184, del 25 de setiembre 2014. Establecen una base normativa común para el ejercicio de la auditoria en el sector público costarricense. (CGR, 2014)

- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), emitidas mediante resolución R-CO-9-2009 del 26 de enero de 2009, publicada en el Diario Oficial "La Gaceta" N.º 26 del 6 de febrero de 2009.
- Manual General de Fiscalización Integral, R-DC-13-2012, es el instrumento normativo de mayor jerarquía en lo relativo a la regulación y descripción, de forma general, de los procesos desarrollados por la CGR para cumplir con sus objetivos de fiscalización superior de la Hacienda Pública. (CGR, 2012)
- Procedimiento de Auditoría Versión V.4, actualización según el DFOE-ST-0030 de fecha 25 de mayo de 2015.
- Manual Técnico de Auditoría Financiera, diciembre 2013. Es un instrumento para la ejecución de auditorías financieras, el cual contiene herramientas, programas, entre otros. (CGR, 2013)
- Las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI), son un punto de referencia para auditar entidades públicas; emitidas por la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI).
- Normas Internacionales de Auditoría (NIA). Estas Normas contienen objetivos, requerimientos y una guía de aplicación, que constituyen principios básicos y procedimientos esenciales que debe aplicar el auditor en las auditorías de los estados financieros, con la finalidad de alcanzar una seguridad razonable.

Capítulo III

Diagnóstico

CAPÍTULO IV: DIAGNÓSTICO

El objetivo de este capítulo es presentar el diagnóstico sobre la metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros actual de la DFOE de la CGR, para ello en este título se muestra en el primer apartado la delimitación del diagnóstico, de seguido, el desarrollo del diagnóstico , y por último se presenta el análisis de los datos recabados.

4.1 DELIMITACIÓN DEL DIAGNÓSTICO

4.1.1 Definición del problema

El presente estudio nace ante la obligatoriedad que presentan los principios y procedimientos básicos que se deben aplicar en las auditorías financieras, según lo expuesto en el Capítulo II sobre el enfoque de auditoría basado en riesgo de negocio o actividad, sobre conocer si las organizaciones han gestionado los riesgos y consecuentemente tienen implementados y en operación controles efectivos que mitiguen esos riesgos.

Ante la presencia de un entorno dependiente de las TI, que determina la forma en que es procesada la información y producidos los informes financieros, el estudio del riesgo asociado con el uso, la propiedad, operación, involucramiento, influencia y adopción de las TI en las instituciones y la forma en que podrían afectar el negocio, es fundamental.

Por tanto, ¿cuenta la DFOE de la CGR con una metodología para la evaluación de riesgos relacionados con TI que incorpore los elementos descritos en las mejores prácticas, para la evaluación del riesgo y qué

contribuya en el establecimiento del alcance de la auditoria, así como la naturaleza, y la oportunidad de los procedimientos a aplicar?

4.1.2 Objetivo

El estudio cualitativo sobre la metodología para la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros, tiene como objetivo central, determinar si la metodología aplicada por la DFOE, incorpora los elementos descritos en las mejores prácticas, para la evaluación del riesgo.

4.1.3 Objetivos específicos

El diagnóstico del objeto estudiado, tiene los siguientes objetivos específicos:

1. Identificar los elementos que incorpora la metodología aplicada por la DFOE para la evaluación de riesgos relacionados con TI.

2. Analizar cómo identifican, analizan y valoran los riesgos relacionados con TI, los funcionarios de la DFOE, en las auditorías financieras.

4.1.4 Recolección de información

De acuerdo con el apartado 1.4.5 Técnicas e instrumentos para la recolección de información, del Capítulo I, para el desarrollo de este diagnóstico se realizó la inspección del “Procedimiento de Auditoría y los criterios de calidad que se han elaborado para cada una de las tareas que conforman las actividades de planificación, examen y comunicación de resultados” V4 y V5, con el fin de identificar documentación atinente a la evaluación de riesgos relacionados con TI.

Además, se llevaron a cabo entrevistas abiertas, bajo el formato pregunta-respuesta, a funcionarios seleccionados por la Secretaría Técnica y se revisaron los papeles de trabajo de auditorías financieras realizadas durante el año 2017, con el fin de analizar cómo han abordado la evaluación de riesgos relacionados con TI, los equipos de auditoría de la DFOE.

4.2 DESARROLLO DEL DIAGNÓSTICO

A continuación, se presenta el desarrollo del diagnóstico que sintetiza el estado de la cuestión.

4.2.1 Metodología para la evaluación de riesgos

En este apartado, se desarrolla la documentación relacionada con la metodología y procedimientos aplicados por la DFOE para la evaluación de riesgos.

4.2.1.1 Principios y procedimiento

La CGR estableció[8] las NIA como principios y procedimientos básicos para la ejecución de auditorías a los estados financieros, desde el año 2000. (FOE, 2000). Además, tomó acuerdos para adoptar, adaptar e implementar las ISSAI, reconociendo los beneficios de utilizar estas normas en el desempeño de sus funciones, durante la XXII Asamblea General Ordinaria de Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS), realizada

[8] Establece la aplicación de las NIA mediante oficio N° FOE-ST-220 de fecha 21 de julio de 2000.

en noviembre de 2012, organización de la que es miembro. (OLACEFS, 2018)

Además, la CGR tiene implementado [9] un procedimiento de auditoría y criterios de calidad para cada una de las tareas que conforman las actividades de planificación, examen y comunicación de resultados, para el proceso y productos de las auditorías. Dicho procedimiento contiene, criterios de calidad, plantillas, modelos, instructivos, documentos históricos y normativa relacionada.

De seguido, se describirán los elementos del procedimiento de auditoría, que utiliza la CGR para los estudios de estados financieros, con énfasis en aquellos relacionados con la identificación de riesgos.

4.2.1.2 Manual Técnico de Auditoría Financiera

La CGR desarrolló el Manual Técnico de Auditoria Financiera y sus respectivos anexos, el cual fue actualizado en el 2013, basado en las Directrices de Auditoría de las ISSAI, en las NIA y en las mejores prácticas. (CGR, 2013, p. 16) Este manual esta disponible para ser usado por los equipos de auditoría financiera como referencia.

El Manual Técnico mencionado, en el Capítulo III Planeación, retoma los elementos mencionados por las ISSAI y las NIA sobre la identificación y valoración de riesgos.

En el Capítulo IV, indica que el auditor debe llevar a cabo una evaluación de controles para obtener un entendimiento de las

[9] Dispuso la implementación del procedimiento de auditoria, mediante la resolución de gerencia número R-DFOE-FE-01-2012.

actividades contables, de tal manera que le sea posible identificar y evaluar el riesgo de que ocurran errores significativos (CGR, 2013, p. 198), además, describe elementos que debe considerar la administración para una adecuada gestión y ejemplos de controles básicos que en caso de no ser efectivos representarían un riesgo.

Asimismo, aborda aspectos relacionados con TI desde la óptica de la operación de sistemas de información relacionados con el procesamiento de información contable y la emisión de estados financieros, controles generales de TI y su documentación, controles de configuración de sistemas y de correlación de cuentas, segregación de funciones, revisión de desempeño, controles físicos y controles sobre las estimación o revelaciones. (CGR, 2013, pp. 279-310)

Adicionalmente, el Manual Técnico presenta una guía[10] que tiene como propósito documentar el entendimiento, la evaluación del diseño y la implementación, de los niveles de control relevantes para la auditoría. (CGR, 2013, pp. 279-310)

4.2.1.3 Instructivo Evaluación de riesgos e identificar riesgos

En el procedimiento de auditoría se identificó el documento titulado ”Instructivo evaluación de riesgos e identificar riesgos” código I1-04-FI-01. El instructivo tiene como propósito detallar el procedimiento para evaluar e identificar riesgos.

[10] Ver anexo 1: Programa de Controles de Nivel de Entidad.

El documento menciona los riesgos a nivel de estados financieros, inherentes a nivel de aseveraciones, y de fraude; define el riesgo de negocio y eventos que podrían generar un riesgo de ese tipo; describe la relevancia de procedimientos de evaluación de riesgos, de forma general el propósito, la naturaleza, y alcance, así como lista algunos procedimientos que se podrían aplicar.

La evaluación, según el instructivo, se documenta en el "Documento de Planeación", el "Programa de Controles através de la Entidad" y en la "Matriz de planeación".

Por otro lado, la Secretaría Técnica como parte de los procesos de actualización al procedimiento de auditoría, se encuentra en la elaboración de una nueva versión del instructivo. En el borrador de esta versión, describe consideraciones particulares del sector público, de acuerdo con las ISSAI, además, desarrolla un modelo de seis pasos para la evaluación de riesgos (identificación de los riesgos inherentes, evaluación preliminar de riesgos inherentes, identificación de riesgos significativos, comprensión de control interno, evaluación de los controles internos, y evaluación final de riesgos), que solicita documentar en una "Hoja de riesgos" adicional.

4.2.1.4 Programa de trabajo sobre tecnologías de información

El procedimiento de auditoría presenta, en la sección de "Modelos", un programa de trabajo sobre tecnologías de información, que postula el siguiente objetivo, "Identificar y evaluar los riesgos asociados a las tecnologías de información, así como obtener evidencia apropiada respecto de los riesgos evaluados durante la auditoría, mediante el diseño e implementación de respuestas apropiadas".

El programa en mención, divide en cuatro apartados la evaluación, a saber; (1) acceso a programas y datos, (2) cambios a programas, (3) desarrollo de programas, y (4) computación de usuario final.

Tal como lo postula el objetivo del programa, cada sección posee enunciados que permiten al auditor identificar controles establecidos por la administración para gestionar aspectos relacionados con TI, así como enunciar implícita o explícitamente el riesgo que podría reducir si dicho control es apropiado, por otro lado, en algunos casos presenta el detalle de aspectos que debe solicitar el auditor para evaluar la efectividad del control que describe.

4.2.1.5 Herramienta para Valoración de riesgos en auditoría financiera

La herramienta para valoración de riesgos tiene como objetivo documentar el riesgo de incorrección material. En primer término, presenta ejemplos de factores de riesgo relacionados con cada uno de los componentes de control (ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, finalmente, monitoreo). De seguido, permite seleccionar los factores de riesgo identificados. Finalmente, la herramienta presenta un formulario que puede ser llenado para centralizar la información identificada de riesgos.

El formulario de riesgos tiene tres secciones, a saber; identificación del riesgo a nivel de aseveraciones y cuentas; la calificación del riesgo a nivel de estados financieros y aseveraciones; y finalmente, la estrategia de auditoría.

4.2.2 Evaluación de riesgos

Para fines de éste diagnóstico se realizaron seis entrevistas con funcionarios de la DFOE seleccionados por la Secretaría Técnica y se revisó la información relacionada con la evaluación de riesgos documentada en los estudios ejecutados para el período 2017, suministrada por los entrevistados.

4.2.2.1 Resumen de las entrevistas

La entrevista consistió en 10 preguntas sobre la forma en que los fiscalizadores, abordan la evaluación de riesgos derivados de las tecnologías de información en las auditorias de estados financieros. Para el detalle refiérase al Apéndice 2.

4.2.2.1.1 Metodología para la evaluación de riesgos

Los funcionarios entrevistados indicaron que no conocían si existía una metodología para la evaluación de riesgos, sin embargo, estuvieron de acuerdo en qué para definir las áreas de examen, se tratan de identificar de forma cualitativa riesgos que pudieran afectar la información financiera. Asimismo, acotaron que realizan diferentes procedimientos que les permite identificar riesgos generales y no se han enfocado en determinar riesgos relacionados con TI.

Los entrevistados indicaron que la metodología aplicada para la evaluación de riesgos, es seguir el “Programa de Trabajo de Planificación”, exteriorizaron que obtenían conocimiento sobre riesgos en las “Entrevistas iniciales con la administración”, la elaboración del “Cuestionario de Control Interno (CI)”, la ejecución del “Programa de auditoría sobre temas específicos con relación a fraude”; la “Evaluación del SEVRI” y en algunos casos, con la ejecución modificada, parcial o total del “Programa de trabajo sobre tecnologías de información”.

4.2.2.1.2 Evaluación de riesgos

Se les consultó a los entrevistados sí con los procedimientos realizados pudieron determinar: ¿cómo la institución ha gestionado los riesgos de TI?, sí ¿Identificaron factores de riesgo y los controles relacionados?, sí se ¿evaluó la efectividad de los controles?, y finalmente sí se ¿obtuvo comprensión del impacto de las TI para el estudio que estaba realizando? y ¿de qué forma?.

De las explicaciones en las entrevistas se desprende que con los procedimientos que se realizan, solo es posible conocer cómo son gestionados los riesgos en las instituciones auditadas, de forma general, ya que no se profundiza.

Los funcionarios entrevistados aseguran que los procedimiento les permiten identificar factores de riesgo y controles relacionados, sin embargo, no necesariamente los relacionados con TI.

En cuanto a la evaluación de efectividad de los controles, solo uno de los entrevistados, indicó que evaluaba la efectividad de algunos controles establecidos, en la etapa de planificación, el resto dijo que la revisión se limita a la verificación de la existencia de políticas y otros similares.

Finalmente, indicaron que mediante la aplicación de los procedimientos que se realizan, se logra obtener una comprensión general de los riesgos para la auditoría en ejecución, no así de su impacto para el estudio.

4.2.2.1.3 Documentación

Con respecto a la documentación de la evaluación de riesgos, los entrevistados indicaron que no se hace un documento de riesgos

específico, sino que se concluye en cada procedimiento realizado y se recopilan en la “Cedula Resumen de planificación” y en la cedula “Plan General de Auditoria Financiera”.

Además, al menos dos de los funcionarios entrevistados dijeron que realizaban un “documento de riesgos”, en el que se registraba cada uno de los riesgos identificados, no obstante, el mismo se descartaba de los papeles de trabajo una vez finalizada la etapa planificación.

Otros de los funcionarios, expresaron que identificaban factores de riesgos pero al no ser, a su juicio significativos, no los documentaban.

4.2.2.1.4 Respuesta a los riesgos

Se les consultó a los funcionarios, que sí a su juicio, con la información recabada y documentada podrían indicar el grado de confidencialidad, integridad y disponibilidad de la información que tiene la institución auditada.

Los funcionarios coincidieron en que con certeza no podrían indicar el grado de confidencialidad, integridad y disponibilidad de la información de la institución, debido a que los procedimientos realizados en la evaluación de riesgos no están definidos para determinar ese grado. Asimismo, indican que cualitativamente podrían identificarse aspectos que pueden dar una idea.

Los entrevistados indicaron, que la información obtenida no se utiliza directamente en la determinación del alcance, naturaleza y oportunidad de los procedimientos de la etapa de examen de la auditoría. Uno de los entrevistados señaló que los riesgos identificados se utilizan como análisis de la situación y que en los programas de

trabajo de la etapa de examen se indica en el procedimiento del riesgo relacionado.

4.2.2.1.5 Percepción sobre los elementos del procedimiento de auditoría para la evaluación de riesgos relacionados con TI

De los elementos descritos por los entrevistados sobre el procedimiento de auditoría, identificaron el modelo del "Programa de trabajo sobre TI" como un insumo para realizar la evaluación de riesgos, no obstante, consideran que el modelo "no es claro", así como que "utiliza terminología técnica" que no permite entender el procedimiento a ejecutar, su finalidad y la relevancia e integración para el trabajo de auditoría.

Además, consideran que se requiere más orientación sobre la evaluación de riesgos de TI, ya que, cuando se estableció el programa mencionado, no se brindó capacitación, por lo que el mismo es aplicado al mejor saber y entender de los equipos.

4.2.2.2 Revisión de documentación

Se revisaron los papeles de trabajo de 16 auditorías, con el fin de, identificar los elementos mencionados por los funcionarios sobre la forma en que se realiza la evaluación de riesgos. El resultado se describe en el Cuadro 1. Para mayor detalle de la información del procedimiento aplicado y la información que documenta refiérase al Apéndice 3.

Cuadro 1 Resultado de revisión de documentación

Documento	Resultado del análisis de documentos
Cuestionario de evaluación de control interno	En tres de los estudios se documentaron riesgos.
Cuestionario de evaluación de cuentas	
Programa de trabajo sobre tecnologías de información	En doce de los estudios no se utilizó. En los restantes, se desarrollaron pruebas específicas.
Cédula Resumen de Planificación	Dos de los estudios hacen referencia al PGA. Dos de los estudios no indican ningún riesgo. Seis presentan dos riesgos relacionados con la continuidad de la auditoría. Dos presentan un riesgo para cada área de examen (total de 4) Cuatro estudios presentan entre 6 y 40 riesgos identificados.
Discusión de la Estrategia	No se documenta información sobre riesgos.
Plan general de auditoría	Tres de los estudios hacen referencia general al riesgo de control, inherente y de auditoría. Uno de los estudios no indican ningún riesgo. Uno presenta dos riesgos relacionados con la continuidad de la auditoría. Tres presentan un riesgo para cada área de examen (total de 4) Ocho estudios presentan entre 6 y 36 riesgos identificados.

Fuente: elaboración propia.

4.3 ANÁLISIS DEL DIÁGNOSTICO

En términos generales, la CGR tiene establecidas normas y procedimientos que le permiten emprender cada una de las tareas que conforman las actividades de la auditoría. Asimismo, al examinar cómo identifican, analizan y valoran los riesgos, los funcionarios de la DFOE en las

auditorías financieras, se logró establecer que en la etapa de planificación se realizan procedimientos que permiten identificar riesgos y controles; valorar el control interno y controles por cuenta. Cabe destacar que lo mencionado deja de lado todo lo relacionado con TI.

Con respecto a lo indicado en el párrafo anterior, la sola identificación de esos elementos no es suficiente para indicar que existe una metodología para la evaluación de riesgos o que se realiza una auditoría basada en riesgo, según lo describen las normas (NIAS, ISSAI).

La documentación de la evaluación de riesgos debería ser la base para establecer el alcance de la auditoria, la naturaleza, y la oportunidad de los procedimientos a aplicar en la etapa de examen, de ahí su importancia. Sin embargo, de la revisión de los papeles de trabajo y de las entrevistas, se desprende que la evaluación de riesgos no es considerada para esos fines.. Los riesgos identificados que se consideran significativos son documentados en cada procedimiento realizado y se recopilan en la “Cedula Resumen de planificación” y en la cedula “Plan General de Auditoria Financiera”; no obstante, en doce de los estudios los riesgos resumidos en esos documentos son sobre la continuación del trabajo, del auditor, o inclusive riesgos por cada cuenta que se definió que se revisaría y en ninguno de los casos hay evidencia que se identificaran o consideraran riesgos relacionados con TI.

Por otro lado, de los elementos del procedimiento de auditoría, que utiliza la DFOE para la auditoria de estados financieros, los entrevistados señalaron que el “Programa de trabajo sobre tecnología de información” es el instrumento para la evaluación de riesgo en TI, no obstante, tal como se observa en el Cuadro Nº 1 solo en cuatro estudios fue aplicado de forma parcial.

El programa aborda cuatro áreas de TI, como se mencionó anteriormente, lo que podría limitar conocer todos los aspectos de alto riesgo

asociados a la integridad, confidencialidad o disponibilidad de la información sensible y critica y a los sistemas.

Los procedimientos de auditoría enunciados en el programa, no presentan los elementos básicos[11] (¿Cómo? ¿Qué? ¿Para qué? ¿Dónde y quién?), para lograr una comprensión universal del procedimiento a aplicar, no en todos los procedimientos se especifican las acciones sugeridas para la aplicación del procedimiento.

Además, se listan un grupo de riesgos reducido, que en algunos casos hay que descifrar del contexto del enunciado, o que es tan genérico que podría aplicar a cualquier cosa, imposibilitando a los diferentes equipos de auditoría, entender lo mismo de la lectura del programa.

Los aspectos comentados evidencian las afirmaciones hechas por los funcionarios en cuanto a que el modelo no es claro, así como que "utiliza terminología técnica que no permite entender el procedimiento a ejecutar, su finalidad y la relevancia e integración para el trabajo de auditoría.

Se considera importante indicar, que el programa en mención así como los otros elementos del procedimiento de auditoría descritos en el punto 3.2.1 de este Capítulo, son insuficientes para realizar y documentar una evaluación de riesgos que permita ser la base para establecer el alcance de la auditoria, la naturaleza, y la oportunidad de los procedimientos a aplicar en la etapa de examen.

La forma de identificación de riesgos imperante refleja un método de gestión de riesgos cualitativo cuyos resultados no son concluyentes, que los

---

[11] Elementos básicos establecidos en los criterios de calidad para redactar un procedimiento de auditoría.

funcionarios lo perciben como un fin que hay que cumplir, más preocupados de la información de riesgos que de su tratamiento. Este método, no permite a los auditores realizar una identificación de riesgos , que sirva de insumo para un análisis y valoración del riesgo.; así como lograr una comprensión del impacto de las TI, y consecuentemente, determinar el grado de confidencialidad, integridad y disponibilidad de la información.

Finalmente, a pesar de que la identificación de riesgos relacionados con las TI es fundamental, la DFOE no tiene una metodología establecida para la evaluación de riesgos, tal como lo sugieren las mejores prácticas.

Capítulo V

Metodología para evaluación de riesgos relacionados con TI

CAPÍTULO V: METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS RELACIONADOS CON TI

La finalidad de este capítulo es presentar una propuesta de una "Metodología para la Evaluación de Riesgos derivados de las TI" que proporcione los lineamientos mínimos que debe seguir la DFOE.

5.1 JUSTIFICACIÓN

Una vez realizada la investigación, se pudo constatar que la DFOE no cuenta con una metodología para la evaluación de riesgos relacionados con TI que esté de acuerdo a las mejores prácticas. Para subsanar la situación expuesta, se integrará en la metodología los requisitos establecidos en el Capítulo II.

5.2 FACTORES CRÍTICOS DE ÉXITO

Los factores críticos de éxito son los aspectos que permitirán que esta metodología al ser ejecutada logre los resultados deseados, a continuación su descripción.

5.2.1 Apoyo del nivel superior

En primer término, es necesario el liderazgo de la Gerencia de la Secretaría Técnica, para que está, tome las decisiones relacionadas con la inserción de la metodología en los procedimientos de auditoría, el seguimiento, la asignación de recursos, la aprobación de ajustes, en caso de ser necesario, al alcance de la metodología propuesta y a los procedimientos actuales que cambian con la aplicación de esta metodología.

5.2.2 Aprobación y divulgación de la metodología

Los procedimientos contenidos en la metodología de evaluación de riesgos propuestos, una vez tomada la decisión de la inserción como parte de los procedimientos de auditoría, deben ser aprobados por la Gerencia de División y divulgados al personal. El conocimiento de los procedimientos constituirá un elemento para que el personal comprenda las líneas de acción y se comprometa con ellas.

5.2.3 Recurso humano

Es necesario que a cada equipo de auditoría, con el fin de desarrollar la metodología, se le defina de manera clara y formal, sus responsabilidades, y funciones con respecto a la aplicación de la metodología. Para dicho fin, se requiere que se integre en el plan de capacitación la metodología aquí propuesta.

5.3 METODOLOGÍA PARA LA EVALUACIÓN DE RIESGOS

La Metodología para la Evaluación de Riesgos relacionados con TI (MERTI) tiene como objetivo fundamental ser el marco orientador para la evaluación de riesgos relacionados con TI en las auditorías financieras. La metodología busca apoyar el cumplimiento de los objetivos en la auditoría financiera mediante su aplicación. Los principales insumos para la elaboración de esta metodología fueron: el diagnóstico de la situación actual, las NIA, ISSAI

y los estándares de la serie de ISO[12] 31000, ISO/IEC 27005, COSO ERM y COBIT 5 Riesgos.

Esta metodología de evaluación deberá estar sujeta a seguimiento anual y ajustes para mantenerla actualizada a las necesidades de la DFOE. El Cuadro Nº 2 presenta la Metodología a alto nivel

Cuadro 2 Metodología para evaluación de riesgos relacionados con TI

CONCEPTO La metodología para la evaluación de riesgos relacionados con TI (MER-TI) se define como el procedimientos para identificar, analizar y valorar el riesgo.	INSUMOS Evaluación de Control Interno Evaluación de Control Interno a nivel de Cuentas Documentación previa de conocimiento del entorno
OBJETIVO Evaluar los riesgos relacionados con TI para establecer el alcance de la auditoria, así como la naturaleza, y la oportunidad de los procedimientos a aplicar.	ACTIVIDADES Establecimiento del contexto - Identificación de riesgos - Análisis de riesgos - Valoración de riesgos - Documentación
FUNDAMENTO Normas Internacionales de Auditoría (NIA o ISAs, por sus siglas en inglés) emitidas por la Federación Internacional de Contadores (IFAC, por sus siglas en inglés) Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI, por sus siglas en inglés).	PRODUCTO Evaluación de riesgos

Fuente: elaboración propia

[12] *International Organization for Standardization (ISO)*

5.3.1 Generalidades

5.3.1.1 Contenido y alcance

Esta metodología establece los lineamientos para la evaluación de riesgos relacionados con Tecnologías de Información en las auditorías financieras.

Se define los criterios con respecto a las actividades relacionadas con los elementos de la metodología, a saber; establecimiento del contexto, identificación de riesgos, análisis de riesgos, valoración de riesgos y documentación.

5.3.1.2 Definiciones

Activo: es algo de valor tangible o intangible que vale la pena proteger, incluyendo a personas, sistemas, infraestructura, finanzas y reputación. (ISACA, 2013)

Agente: es la persona que genera la amenaza que explota una vulnerabilidad. (ISACA, 2014)

Amenaza: cualquier cosa que es capaz de actuar contra un activo de manera que pueda ocasionar un perjuicio. (ISACA, 2014)

Análisis de riesgos: actividad de la metodología de evaluación de riesgos en la que se desarrolla la comprensión del riesgo, se evalúa la efectividad de los controles y se determina la probabilidad de ocurrencia, la magnitud del impacto y la visión general del riesgo (Cálculo del riesgo)

Cálculo del riesgo: cálculo matemático del impacto multiplicado por la probabilidad.

Consecuencias: hecho o acontecimiento derivado o que resulta inevitable y forzosamente de otro. (RAE, 2018)

Contramedida: cualquier proceso que reduce directamente una amenaza o vulnerabilidad. (ISACA, 2015)

Control compensatorio: un control interno que reduce el riesgo de una debilidad existente o potencial del control que tenga como resultado errores y omisiones. (ISACA, 2015)

Control correctivo: un control diseñado para corregir errores, omisiones y usos e intrusiones no autorizados una vez que se detectan. (ISACA, 2015)

Control preventivo: control interno que se utiliza para evitar eventos no deseados, errores y otros incidentes que una empresa haya determinado que podrían tener un efecto material negativo en un proceso o producto final. (ISACA, 2015)

Controles detectivo: existen para detectar e informar cuando se producen errores, omisiones y usos o entradas no autorizados. (ISACA, 2015)

Controles internos: políticas, procedimientos, prácticas y estructuras organizacionales que están diseñados para brindar una confianza razonable de que se alcanzarán los objetivos de negocio y que se evitarán, o bien, detectarán y corregirán los eventos no deseados. (ISACA, 2015)

Escenario de riesgos de TI: es la descripción de un posible evento que puede derivar en un impacto cuando y sí ocurre en la institución.

Establecimiento del contexto: actividad de la metodología de evaluación de riesgos que busca conocer el entorno y establecer criterios de riesgo. (ISACA, 2014)

Evento: algo que sucede en un lugar y/o tiempo específico. (ISACA, 2013)

Evento de amenaza: cualquier evento durante el cual un elemento/agente de amenaza actúa en contra de un activo de una manera que tiene el potencial de derivar directamente en un daño. (ISACA, 2014)

Evento de pérdida : cualquier evento durante el cual un evento de amenaza causa una pérdida. (ISACA, 2014)

Evento de vulnerabilidad : cualquier evento durante el cual se produce un aumento significativo en la vulnerabilidad. Tenga en cuenta que este aumento en la vulnerabilidad puede derivar de cambios en las condiciones de control o de cambios en la capacidad/fuerza de la amenaza. (ISACA, 2014)

Factor de riesgo: una condición que puede influir en la frecuencia y/o magnitud y, en última instancia, en el impacto que los eventos/escenarios relacionados con TI tienen en el negocio. (ISACA, 2014)

Identificación de riesgos: actividad de la metodología de evaluación de riesgos que permite, descubrir, reconocer y registrar riesgos, identificando las causas y su posible efecto.

Impacto: una medida de la gravedad potencial de la pérdida de los eventos/escenarios ocurridos. (ISACA, 2014)

Incidente: cualquier evento que no forma parte de la operación estándar de un servicio y que ocasiona, o puede ocasionar, una interrupción de, o una reducción en, la calidad de ese servicio. (ISACA, 2015)

Integridad: protección contra la destrucción o modificación inapropiada de la información, e incluye garantizar el no repudio y la autenticidad de la información. (ISACA, 2015)

Mapa de riesgos: herramienta gráfica para clasificar y mostrar el riesgo por rangos definidos de probabilidad e impacto. (ISACA, 2014)

Matriz de riesgos: repositorio de riesgos de TI potenciales y conocidos.

Metodología para la evaluación de riesgos: procedimientos para identificar, analizar y valorar el riesgo.

Mitigación del riesgo: la gestión de un riesgo mediante el uso de controles y contramedidas. (ISACA, 2015)

Objetivo de control: declaración del resultado deseado o propósito que se va a lograr mediante la implementación de procedimientos de control en un proceso en particular. (ISACA, 2015)

Probabilidad: cálculo de las posibilidades que existen de que una cosa se cumpla. (ISACA, 2014)

Procedimiento: documento que incluye una descripción detallada de los pasos necesarios para realizar operaciones específicas conforme a las normas aplicables. Los procedimientos se definen como parte de los procesos. (ISACA, 2015)

Proceso: en general, conjunto de actividades influenciadas por las políticas y los procedimientos de la empresa que toma entradas de varias fuentes (que incluyen otros procesos), manipula las entradas y produce las salidas. Los procesos tienen razones de negocio claras para existir, propietarios responsables, roles y responsabilidades claros en torno a la ejecución del proceso, y los medios para medir el desempeño. (ISACA, 2015)

Recurso: es cualquier cosa que ayuda a alcanzar una meta. (ISACA, 2014)

Riesgo: la combinación de la probabilidad de un evento y sus consecuencias (ISO/IEC 73).

Riesgo de Control: el riesgo de que haya un error material que no fuera evitado ni detectado oportunamente por el sistema de controles internos. (ISACA, 2015)

Riesgo de TI: el riesgo de la actividad asociado con el uso, la propiedad, la operación, la participación, la influencia y la adopción de TI dentro de una institución. (ISACA, 2013)

Tecnologías de información: dispositivos tecnológicos, integrados en medios de informática, telecomunicaciones y redes, que cuentan con protocolos comunes, que posibilitan la comunicación; utilizadas para la entrada, el almacenamiento, el proceso, el intercambio, la transmisión y la salida de datos.

Tiempo: dimensión, donde se podría describir, la duración del evento, el momento, detección, tiempo transcurrido entre el evento y la consecuencia. (ISACA, 2014)

Tipo de Evento: a los efectos de la gestión de riesgos de TI, uno de los tres posibles tipos de eventos: eventos de amenazas, eventos de pérdida y eventos de vulnerabilidades. (ISACA, 2013)

Valoración de riesgos: etapa de la metodología de evaluación de riesgos en la que se determinan los riesgos a tratar y la prioridad para implementar una respuesta adecuada. Implica comparar el nivel de riesgo estimado con los criterios de riesgos definidos, en el contexto.

Vulnerabilidad: una debilidad en el diseño, implementación, operación o control interno de un proceso que podría exponer al sistema a las adversidades de eventos de amenaza. (ISACA, 2014)

5.3.2 Actividades

5.3.2.1 Establecimiento del contexto

Después de establecer los términos de la auditoría, el proceso de auditoría financiera continúa con “comprender la entidad”, este principio es el fundamento para esta actividad, “Establecimiento del contexto”.

El establecimiento del contexto, es el punto de partida para la evaluación del riesgo, ya que, en esta actividad el auditor obtiene conocimiento del ambiente en el que opera la institución, es necesario establecer el contexto estratégico, organizacional, de administración de riesgos y desarrollar criterios de evaluación.

Se desarrolla conocimiento sobre los objetivos, las operaciones, el entorno regulatorio, los controles internos, los sistemas financieros, entre otros, que sean relevantes para la auditoría. Asimismo, se debe documentar sí la institución auditada cuenta con un procedimiento para

identificar los riesgos relevantes para los objetivos de los informes financieros y sí estima además la importancia de dichos riesgos evaluando la posibilidad de que ocurran.

El punto 5.3.4.1 presenta un modelo que permite documentar esta actividad. El modelo busca orientar la recolección de información, de manera que, se documente la investigación de los procesos relevantes para la auditoría, eventos de riesgos materializados y los criterios de evaluación.

5.3.2.2 Identificación de riesgos

Esta actividad permite descubrir, reconocer y registrar riesgos. Para la identificación de riesgos se requiere utilizar un procedimiento estructurado, porque los riesgos que no se identifica en esta actividad, serán excluidos del análisis de riesgos. Los riesgos deben identificarse para cada actividad de cada uno de los proceso relevante para la auditoria, establecidos en la actividad anterior.

Existen diferentes técnicas para identificar riesgos, entre ellas se encuentran, entrevistas, listas de verificación, análisis de causa - efecto y escenarios de riesgos. Cualquiera de las técnicas pueden ser utilizadas, en tanto, se documenten aspectos como: procesos y sus actividades, posibles eventos, activos, vulnerabilidades, amenazas, controles existentes, y personas que intervienen.

El punto 5.3.4.2, presenta un modelo para documentar esta actividad, utilizando una estructura de diagrama de procesos. Permite reconocer áreas y puestos claves por actividad del proceso y con ello identificar concentración de funciones; además, identificar dependencia de activos, y controles para los eventos relacionados.

El resultado de esta actividad es una lista de eventos que podrían afectar los procesos, se consideran causas y escenarios posibles. En el punto 5.3.4.3 se presenta un modelo para documentar los escenarios de riesgo de TI.

5.3.2.3 Análisis de riesgos

La actividad de análisis de riesgos pretende que el auditor desarrolle una visión general del riesgo, estimando la probabilidad de ocurrencia y la magnitud del impacto en caso de que se materialice el riesgo. Para ese fin, se analizan los tipos de riesgos, prestando atención al escenario de riesgo identificado, se consideran los factores que puedan afectarlos; y se evalúan los controles internos relacionados. De seguido, se explican cada aspecto a analizar.

Se puede llevar a cabo un análisis preliminar de los escenarios identificado, en el caso que se determine que alguno no es significativo, se debe analizar la posibilidad de excluirlo del análisis, documentando la razón.

Se evalúa la efectividad de los controles relacionados con los riesgos, analizando brechas que podrían afectar la determinación de la confianza en el control. Para este fin, en el punto 5.3.4.4 se presenta un modelo que permite documentar las brechas de los controles internos, y el nivel de confianza que utilizará el auditor. El insumo para realizar este análisis, es la autoevaluación del control interno.

En el caso de los activos que soportan las actividades relevantes relacionadas con la información, se deberá estimar la sensibilidad relacionada con la confidencialidad, integridad y disponibilidad; para determinar la magnitud del impacto de las consecuencia relacionadas. En el punto 5.3.4.5 se presenta un modelo para dicho fin.

Finalmente, se realiza el cálculo del riesgo, se estima el nivel de efectividad del control y la exposición al riesgo. Estas variables son documentadas en el Modelo “Cálculo del riesgo, nivel de efectividad del control y exposición al riesgo” que se presenta en el punto 5.3.4.6.

Como resultado de esta actividad, se obtiene una lista de controles relevantes para la auditoria y el análisis de brechas de controles, una lista de activos tecnológicos y el impacto que éstos tienen para la información financiera, y el cálculo de riesgo, nivel de efectividad de los controles y la determinación de la exposición al riesgo.

5.3.2.4 Valoración de riesgos

La finalidad de esta etapa es determinar los riesgos a tratar y la prioridad para determinar el alcance de la auditoria, la naturaleza, y la oportunidad de los procedimientos a aplicar. Implica comparar el nivel de riesgo estimado con los criterios de riesgos definidos, en la etapa de establecimiento del contexto. El resultado de esta etapa es una matriz priorizada de los elementos de riesgo.

Esta actividad es documentada mediante los modelo “Riesgos contra criterios de alto impacto”, “Matriz de riesgos” y un “Mapa de riesgos” que se presentan en el punto 5.3.4.7.

5.3.2.5 Documentación

Los resultados del proceso de evaluación del riesgo se deben documentar. De la ejecución de la metodología deben documentarse los siguientes aspectos.

- Objetivo y la descripción de las partes pertinentes de los procesos que se están auditando y sus funciones.
- Resumen del contexto y como se relaciona la situación.
- Criterios del riesgo aplicados y su justificación.
- Limitaciones, los supuestos y la justificación de las hipótesis.
- Metodología aplicada en la evaluación.
- Resultados de la identificación del riesgo.
- Datos, los supuestos y sus orígenes y validación.
- Resultados del análisis y valoración de los riesgos.
- Supuestos críticos y otros factores sobre los que se necesita seguimiento.
- Discusión de los resultados.

5.3.3 Revisión

La metodología y documentos relacionados con el fin de realizar una adecuada evaluación de riesgos relacionados con TI deberán ser revisados al menos una vez al año.

5.3.4 Anexos

Los modelos que se listan a continuación son parte integral de la metodología.

5.3.4.1 Descripción del proceso, eventos materializados y criterios de evaluación.

Este modelo se divide en tres partes esenciales que se describen a continuación.

1. Procesos relevantes: se documentan las características del proceso auditado, el área responsable, la importancia del proceso (Crítico, Sensible, Vital), canales que lo posibilitan (Leyes, Reglamentos, Regulaciones específicas) y áreas que interviene en el proceso, junto con su misión, visión, organigrama, personas claves y estrategias que desarrollan.
2. Eventos de riesgos materializados: es necesario conocer eventos materializados, por lo que el modelo solicita documentar el evento que haya ocurrido y afectado la operación normal, la cantidad de eventos materializados, la causa que los originó, el impacto (Financiero, regulatorio, reputación), las acciones realizadas y sí esas acciones mitigaron el riesgo.
3. Criterios de evaluación: se determinan restricciones existentes que limitan el proceso, por lo que se realiza un inventario de leyes, lineamientos, normativa regulatoria, entre otros. En el modelo se realiza una clasificación de la normativa (Leyes, Normas, Lineamientos, Políticas), se describen el tipo de sanción y el impacto por el incumplimiento.

Para ver el modelo refiérase al Apéndice 4.

5.3.4.2 Diagrama de actividades por proceso y descripción de eventos, activos y controles relacionados

Este modelo permite incluir información sobre las actividades de cada proceso, el área y puestos relacionados, una descripción general del evento, el activo y el control relacionado. Para ver el modelo refiérase al Apéndice 5.

5.3.4.3 Escenarios de riesgo de TI

El modelo de escenarios de riesgos que presenta el Apéndice 6, contiene los siguientes componentes: agente, tipo de amenaza, evento, activo/recurso y tiempo. Se utilizó la estructura de escenarios de riesgos que presenta COBIT 5 para Riesgos.

5.4.4.4 Análisis de brechas de controles

El análisis de brechas permite documentar las características de los controles, y evaluar si su diseño es suficiente para cumplir los objetivos de control (integridad y exactitud de la información, confiabilidad de la información, disponibilidad de la información, salvaguarda de los activos, eficacia de las operaciones y finalmente, cumplimiento de leyes y regulaciones), al respecto, se identifican brechas, lo que permite establece un nivel de confianza de acuerdo con una escala de 1 a 5 (Excelente, Muy Bueno, Bueno, Pobre e Insatisfactorio).

El modelo se presenta en el Apéndice 7.

5.3.4.5 Análisis de sensibilidad de la información

El modelo de “Análisis de sensibilidad de la información” documenta los activos que soportan las actividades de los procesos relacionados con la información financiera y los evalúa tomando en consideración la confidencialidad, integridad y disponibilidad, con el fin de determinar la magnitud del impacto en caso de materializarse el riesgo descrito en el escenario de riesgo. En el Apéndice 8 se presenta el modelo.

5.3.4.6 Cálculo del riesgo, nivel de efectividad del control y exposición al riesgo

El Apéndice 9, presenta el modelo “Cálculo del riesgo, nivel de efectividad del control y exposición al riesgo”. El modelo permite documentar el cálculo del riesgo, el nivel de efectividad del control y la determinación de la exposición al riesgo.

Para determinar la calificación del riesgo se multiplica el impacto por la probabilidad. El impacto y la probabilidad se evalúan en el contexto de los controles existentes. El impacto se extrae del análisis de sensibilidad, mientras que la probabilidad se deberá determinar tomando en consideración el resultado conjunto de las actividades de evaluación de riesgos anteriores. El modelo, presenta una escala propuesta de 1 a 5 (Catastrófico, Mayor, Moderado, Menor, e insignificante).

El nivel de efectividad de control, se determina restando al “Score Riesgo” el “Score Control”. El Score Control se calcula con el nivel de confianza determinado en el análisis de brechas de controles. Las fórmulas se presentan en el modelo.

5.3.4.7 Valoración de riesgos

En el Apéndices 10, 11 y 12 se presentan los modelos para documentar la actividad de “Valoración de los riesgos”.

El modelo “Riesgos contra criterios de alto impacto”, permite documentar la decisión de qué riesgos se priorizaran para determinar el alcance de la auditoria, la naturaleza, y la oportunidad de los procedimientos a aplicar en la etapa examen, de acuerdo con criterios de alto impacto. Este modelo, agrega a la matriz de riesgos

documentada una sección de “Criterios de alto impacto” y un espacio para su justificación de los mismos.

La “Matriz de Riesgos” es el resultado de las actividades de la evaluación de riesgos. La matriz que se obtiene proporciona una visión general de los riesgos relevantes, que permite desarrollar la estrategia para la etapa de examen, al seleccionar los riesgos que se cubrirán.

5.5 JUSTIFICACIÓN ECONÓMICA

Para la implementación formal de la Metodología no se requiere de gran inversión, ya que los funcionarios con los que cuenta la DFOE poseen conocimiento de los principios y procedimientos básicos, contenidos en las normas de auditoría, que facilitarán el entendimiento y puesta en operación de la metodología aquí planteada.

Por otro lado, el uso de esta metodología puede contribuir, una vez terminada la curva de aprendizaje, a disminuir el tiempo de ejecución de la auditoría, debido a que estructura la forma en que los equipos identifican, analizan y valoran riesgos, mediante un procedimiento que dirige la obtención de resultados a cada paso de la evaluación y concentra la atención del auditor en los riesgos significativos. Así como sirve para determinar el alcance, la naturaleza, y la oportunidad de los procedimientos a aplicar en la etapa examen de la auditoría.

La finalidad de este capítulo fue presentar los lineamientos mínimos que debe poseer una Metodología para la Evaluación de Riesgos de TI. En el siguiente capítulo, se presentarán las conclusiones y recomendaciones resultado de esta investigación.

Capítulo VI

Conclusiones y Recomendaciones

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

Después de realizada la investigación, se llega a las siguientes conclusiones y se plantean las recomendaciones pertinentes.

6.1 CONCLUSIONES

La evaluación de los riesgos relacionados con TI, en la auditoría financiera, ha adquirido relevancia por la adopción y la dependencia de las TI en las instituciones para procesar la información y producir los informes financieros. La Contraloría General de la República (CGR) no escapa a esa realidad, al ser el órgano rector del ordenamiento de control y fiscalización superior; y ejercer su potestad al realizar auditorías financieras sobre los entes y órganos que integran la Hacienda Pública.

La División de Fiscalización Operativa y Evaluativa (DFOE), como parte de los procesos de mejora continua y en cumplimiento de los principios y procedimientos que se deben aplicar en las auditorías financieras, contenidos en las Normas de Auditoría, requiere contar con una metodología de evaluación de riesgos relacionados con TI, integrada a su proceso de auditoría, que le permita determinar el alcance, la naturaleza y la oportunidad de los procedimientos a aplicar.

En el diagnóstico realizado se evidenció que la identificación de riesgos se realiza utilizando un método cualitativo cuyos resultados no son concluyentes, que los funcionarios lo perciben como un fin que hay que cumplir, más preocupados de la información de riesgos que de su tratamiento. Este método, no permite a los auditores realizar una identificación de riesgos , que sirva de insumo para un análisis y valoración del riesgo.

Finalmente, a pesar de que la evaluación de riesgos relacionados con las TI es fundamental, la DFOE no tiene una metodología establecida, tal como lo sugieren las mejores prácticas.

6.2 RECOMENDACIONES

Se recomienda a la DFOE implementar la Metodología de evaluación de riesgos de TI, propuesta en este trabajo, la cual contempla los criterios mínimos que le permitirán, lograr una mejor comprensión del impacto de las TI en la institución fiscalizada, conocer la forma en que se mitigan los riesgos originados por el uso de la tecnología, y consecuentemente, determinar el grado de confidencialidad, integridad y disponibilidad de la información.

Además, poner énfasis en los factores descritos en el apartado 4.2 (apoyo del nivel superior, aprobación y divulgación y recurso humano) ya que allí se describen los aspectos que permitirán que esta metodología al ser ejecutada logre los resultados deseados.

Aunado, con el fin de unificar criterios con respecto a escenarios de riesgos significativos relacionados con TI, para las auditorias financieras, se recomienda valorar la creación e implementación de escenarios de riesgos genéricos, que describan los posibles evento que puede derivar en un impacto en la información financiera.

Para finalizar, se espera que la metodología para evaluación de riesgos relacionados con TI, contribuya a que la DFOE logre determinar el alcance, la naturaleza y oportunidad de los procedimientos a aplicar en las auditorías financieras teniendo la certeza de que se consideraron todos los riesgos relacionados con TI relevantes para la auditoría. El contar con una metodología

integrada y formal, brindará un valor agregado que la Contraloría aportará, a los entes y órganos que integran la Hacienda Pública.

BIBLIOGRAFÍA

Cardona M, D. F. (2009). *Las Tecnologías de la Información y las Comunicaciones.* Bogotá, Colombia: Editorial Universidad del Rosario.

CGR. (noviembre de 2017). *Contraloría General de la República*. (CGR, Producer) Retrieved 21 de noviembre de 2017 from https://www.cgr.go.cr/

CGR. (3 de diciembre de 2017). Base de datos de consulta de estudios de la CGR. San José, Costa Rica.

CGR. (3 de febrero de 2012). MAGEFI 2011. *R-DC-13-2012 Manual General de Fiscalización Integral* , 80. San José, Costa Rica: Despacho Contralor, Contraloría General de la República.

CGR. (diciembre de 2013). Manual Técnico de Auditoría Financiera. San José, Costa Rica.

CGR. (25 de mayo de 2015). Memorando DFOE-ST-0030. *Actualización de la normativa del Procedimiento de Auditoría* .

CGR. (2014). NGASP. *Normas General de Auditoria para el Sector Público* .

CGR. (2007 de junio de 2007). Normas te□cnicas para la gestio□n y el control de las Tecnologi□as de Informacio□n (N-2-2007-CO-DFOE). 15. San José, Costa Rica: Publicada en La Gaceta Nro.119 del 21 de junio, 2007.

CGR. (octubre de 2016). Plan Estratégico Institucional 2013-2020 (Reformulado). San José, Costa Rica.

CGR. (17 de noviembre de 2006). R-CO-94-2006. *M-2-2006-CO-DFOE Manual de Normas Generales de Auditoría para el Sector Público* .

CGR. (11 de junio de 2010). R-DC-101-2010. *Detalle de atribuciones por área* .

CGR. (1 de julio de 2011). R-DC-97-2011 y sus modificaciones. *Reglamento Orgánico de la Contraloría General de la República* . San José, Costa Rica.

CGR. (1 de julio de 2011). Reglamento Orgánico de la Contraloría General de la República R-1-2011-DC-GC. San José, Costa Rica.

Cobo R., J. C. (2009). El concepto de tecnologi□as de la informacio□n. Benchmarking sobre las definiciones de las TIC en la sociedad del conocimiento. *ZER , 14* (27), 295-318.

Asamblea Legislativa. (4 de noviembre de 1994). Ley Nº 7428. *Ley Orgánica de la Contraloría General de la República* . San José, Costa Rica.

FOE. (21 de julio de 2000). FOE-ST-220. *Principios de Contabilidad Aplicables al Sector Público Costarricense y Adopción de las NIAs y NIC* .

Gurdián, A. (2007). *El Paradigma Cualitativo en la Investigación Socio-Educativa.* Agencia Española de Cooperación Internacional.

Hernández, R., Fernández, C., & Baptista, M. d. (2010). *Metodología de la Investigación* (5a ed.). México, D.F.: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V.

IFAC. (octubre de 2013). NIA 200 Objetivo globales del auditor independiente y realización de la auditoría de conforminidad con las Normas Internacionales de Auditoría.

INN. (2009). *NCh-ISO 31000 Gestión del riesgo - Principios y orientaciones.* (I. N. Normalización, Ed.) Santiago, Chile.

INN. (2013). *NCh-ISO 31010 Gestión del riesgo - Técnicas de evaluación del riesgo* (1era ed.). Santiago, Chile: Instituto Nacional de Normalización .

INTOSAI. (2008). Introducción General a las Directrices de auditoría financiera de la INTOSAI. *Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI)* .

INTOSAI. (diciembre de 2008). Principios Fundamentales de la Auditoría del Sector Público. *Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI)* .

INTOSAI. (diciembre de 2008). Principios Fundamentales de la Auditoría Financiera. *Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI)* .

ISACA. (2013). *COBIT 5 para riesgos.* EEUU.

ISACA. (2014). *Escenarios de riesgos, Utilizando Cobit 5 para Riesgos.* IL, EEUU.

ISACA. (2015). *Manual de preparación al examen CISA* (26º ed.). IL, EEUU: Asociación de Auditoría y Control de Sistemas de Información.

ISACA. (2015). *Manual de preparación al examen CISA 2015* (1ra ed.). IL, EEUU: Asociación de Auditoría y Control de Sistemas de Información.

OLACEFS. (2018). *Organización Latinoamericana y del Caribe de Entidades Fiscalizadores Superiores*. Retrieved 9 de abril de 2018 from http://www.olacefs.com/informacion-general-issai/

RAE. (2018). *Diccionario de la lengua española*. From http://dle.rae.es/?id=4NVvRTc

APÉNDICES

APÉNDICES

APÉNDICE 1: TÉCNICAS PARA LA EVALUACIÓN DEL RIESGO

Tabla A.1 - Aplicabilidad de las herramientas utilizadas para la evaluación del riesgo

Herramientas y técnicas	Proceso de evaluación del riesgo					Ver
	Identificación del riesgo	Análisis del riesgo			Valoración del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Tormenta de ideas	MA[1)]	NA[2)]	NA	NA	NA	B.1
Entrevistas estructuradas o semiestructuradas	MA	NA	NA	NA	NA	B.2
Delphi	MA	NA	NA	NA	NA	B.3
Listas de verificación	MA	NA	NA	NA	NA	B.4
Análisis preliminar de peligros	MA	NA	NA	NA	NA	B.5
Estudios de peligros y de operatividad (HAZOP)	MA	MA	A[3)]	A	A	B.6
Análisis de peligros y de puntos críticos de control (HACCP)	MA	MA	NA	NA	MA	B.7
Evaluación de riesgos ambientales	MA	MA	MA	MA	MA	B.8
Estructura "¿y si ?" (SWIFT)	MA	MA	MA	MA	MA	B.9
Análisis de escenario	MA	MA	A	A	A	B.10
Análisis de impacto en el negocio	A	MA	A	A	A	B.11
Análisis de la causa raíz	NA	MA	MA	MA	MA	B.12
Análisis de modos y efectos de fallas	MA	MA	MA	MA	MA	B.13
Análisis del árbol de fallas	A	NA	MA	A	A	B.14
Análisis del árbol de eventos	A	MA	A	A	NA	B.15
Análisis de causa-consecuencia	A	MA	MA	A	A	B.16
Análisis de causa y efecto	MA	MA	NA	NA	NA	B.17
Análisis de capas de protección (LOPA)	A	MA	A	A	NA	B.18
Árbol de decisiones	NA	MA	MA	A	A	B.19
Análisis de fiabilidad humana	MA	MA	MA	MA	A	B.20
Análisis bow tie	NA	A	MA	MA	A	B.21
Mantenimiento centrado en la fiabilidad	MA	MA	MA	MA	MA	B.22
Análisis del circuito de fuga	A	NA	NA	NA	NA	B.23

(continúa)

Fuente: tomado de NCh-ISO 31010 ((INN, 2013)

Apéndice 1: Técnicas para la evaluación del riesgo (Continuación)

Tabla A.1 - Aplicabilidad de las herramientas utilizadas para la evaluación del riesgo
(conclusión)

Herramientas y técnicas	Proceso de evaluación del riesgo					Ver
	Identificación del riesgo	Análisis del riesgo			Valoración del riesgo	
		Consecuencia	Probabilidad	Nivel de riesgo		
Análisis Markov	A	MA	NA	NA	NA	B.24
Simulación Monte-Carlo	NA	NA	NA	NA	MA	B.25
Estadísticas Bayesian y redes Bayes	NA	MA	NA	NA	MA	B.26
Curvas FN	A	MA	MA	A	MA	B.27
Índices de riesgo	A	MA	MA	A	MA	B.28
Matriz de consecuencia/ probabilidad	MA	MA	MA	MA	A	B.29
Análisis de costo/beneficio	A	MA	A	A	A	B.30
Análisis de decisión multi-criterios (MCDA)	A	MA	A	MA	A	B.31

1) Muy aplicable.

2) No aplicable.

3) Aplicable.

Fuente: tomado de NCh-ISO 31010 ((INN, 2013)

APÉNDICE 2: ENTREVISTA

El objetivo de la entrevista fue conocer como identifican, analizan y valoran los riesgos relacionados con TI, los funcionarios de la DFOE, en las auditorías financieras.

1. ¿Usted conoce si existe una metodología que aplique la DFOE para la evaluación de riesgos relacionados con TI?
2. ¿Cuál es la metodología que aplica para la evaluación de riesgos?
3. Mediante la aplicación de los procedimientos que realizó,
    i. Puede indicar claramente ¿cómo la institución ha gestionado los riesgos de TI?
    ii. ¿Identificó factores de riesgo y los controles relacionados?
    iii. ¿Evaluó la efectividad de los controles?
    iv. ¿Obtuvo comprensión del impacto de las TI para el estudio que estaba realizando? ¿De qué forma?
4. ¿Cómo documentó la información obtenida relacionada con la evaluación de riesgos?
5. Con la información recabada, ¿Puede indicar el grado de confidencialidad, integridad y disponibilidad de la información que tiene la institución auditada?
6. ¿Cómo utilizó la información obtenida en la determinación del alcance, naturaleza y oportunidad de los procedimientos de la etapa de examen de la auditoría?
7. ¿Considera que los procedimientos establecidos son adecuados para la evaluación del riesgo relacionado con las TI?

APÉNDICE 3: RESULTADO DE LA REVISIÓN DE DOCUMENTACIÓN

Documento	Procedimiento Ejecutado	Información que documenta	Resultado del análisis de documentos
Cuestionario de evaluación de control interno	Evaluación del Sistema de Control Interno a nivel de entidad y sobre las cuentas o grupos de cuentas contables y los riesgos asociados a los que se encuentra expuesto la institución. Con el fin de obtener un conocimiento actualizado de los controles que tiene diseñados e implementados la institución para minimizar la materialización de riesgos.	Conocer desde una óptica global el Sistema de Control Interno de la institución auditada. Se obtiene un índice general de evaluación de control interno, así como una calificación del riesgo general, madurez del sistema de control y la recomendación del enfoque para auditoría. Define tres posibles estados (Fuerte, Moderado, Débil) para cada uno de los componentes del sistema (ambiente de control, valoración de riesgos, actividades de control, información y comunicación, y seguimiento) Además, con el porcentaje obtenido en cada componente y subcomponente, se valora el riesgo según un rango preestablecido en "indeterminado", "bajo", "moderado", "alto".	En tres de los estudios se documentaron riesgos.
Cuestionario de evaluación de cuentas		Presenta preguntas relacionadas con controles que debería de tener la institución en cada cuenta. A cada control se le asigna un peso de acuerdo con el contexto de la institución auditada. La calificación de la cuenta se obtiene de la suma de las respuestas en las que se indicó que la institución cumple con el control. Se saca un promedio entre el resultado de la cuenta y el porcentaje obtenido en el "Cuestionario de evaluación de control interno". El porcentaje obtenido se valora según un rango preestablecido en "indeterminado", "bajo", "moderado", "alto".	
Programa de trabajo sobre tecnologías de información	Evaluación de temas específicos relacionados ambiente de TI. Considera los resultados de otros procedimientos de evaluación de riesgo.	Mediante la aplicación de algunas pruebas busca identificar y evaluar los riesgos asociados a las tecnologías de información, así como obtener evidencia apropiada respecto de los riesgos evaluados durante la auditoría, mediante el diseño e implementación de respuestas apropiadas.	En doce de los estudios no se utilizó. En los restantes, se desarrollaron pruebas específicas.

Fuente: elaboración propia.

Apéndice 3: resultado de la revisión de documentación (Continuación)

Documento	Procedimiento Ejecutado	Información que documenta	Resultado del análisis de documentos
Cédula Resumen de Planificación	Confección de la cedula Resumen de Planificación, con el fin de contar con un documento en el que se resuman los principales resultados obtenidos en el desarrollo de los procedimientos de la etapa de planificación.	Sección VI. Discusión sobre evaluación de riesgos y planeación. Resumen de los riesgos identificados: a) Riesgos identificados en el proceso de continuidad del trabajo con la entidad. (Riesgo - Cómo se tratarán) b) Riesgos identificados a nivel de estados financieros (Sección del Doc. Planeación - Descripción del riesgo) c) Riesgos identificados a nivel de aseveraciones para cuentas y revelaciones significativas (Sección del Doc. Planeación - ID riesgo - Naturaleza - Cuenta o revelación significativa - Aseveración pertinentes - Riesgo de fraude)	Dos de los estudios hacen referencia al PGA. Dos de los estudios no indican ningún riesgo. Seis presentan dos riesgos relacionados con la continuidad de la auditoría. Dos presentan un riesgo para cada área de examen (total de 4) Cuatro estudios presentan entre 6 y 40 riesgos identificados.
Discusión de la Estrategia	Discusión con el nivel gerencial de la estrategia de auditoría para las fases de examen y comunicación de resultados. Al respecto debe comentar lo siguiente: 4. Discusión sobre la evaluación de riesgos y planificación.	Sección III. Situaciones derivadas de la planificación.	No se documenta información sobre riesgos.
Plan general de auditoría	Elaboración del Plan General de Auditoría y los programas específicos de auditoría para guiar el desarrollo de la etapa examen. Indique la siguiente información: ➢ Procedimientos por realizar, consignando para cada uno: el propósito, la evidencia por recopilar y la fuente de donde se obtendrá la evidencia.	Sección II. Definición del enfoque de auditoría (Cuentas y revelaciones - Saldo - Enfoque de auditoría para el examen) Sección III. Otros asuntos de relevancia. 3.1 Resumen de riesgos identificados.	Tres de los estudios hacen referencia general al riesgo de control, inherente y de auditoría. Uno de los estudios no indican ningún riesgo. Uno presenta dos riesgos relacionados con la continuidad de la auditoría. Tres presentan un riesgo para cada área de examen (total de 4) Ocho estudios presentan entre 6 y 36 riesgos identificados.

Fuente: elaboración propia.

APÉNDICE 4: MODELO PARA LA DESCRIPCIÓN DEL PROCESO, EVENTOS MATERIALIZADOS Y CRITERIOS DE EVALUACIÓN

DESCRIPCIÓN DEL PROCESO, EVENTOS MATERIALIZADOS Y CRITERIOS DE EVALUACIÓN
Actividad: Establecimiento del contexto

Proceso: ⟶ *Se enfoca en conocer las características del proceso a evaluar.*

Características	Área responsable	Importancia	Canales	Áreas que intervienen	EVENTOS DE RIESGOS MATERIALIZADOS						CRITERIOS DE EVALUACIÓN		
					Descripción	Cantidad	Causa	Impacto	Acciones	Mitigado	Clasificación	Sanción	Impacto
Descripción sobre el diseño y la operación del proceso	*Quién es el dueño del proceso*	*Crítico Sensible Vital*	*Leyes Regulaciones Reglamentos*	*Cuáles áreas intervienen en el proceso. Entender visión, misión, organigrama para identificar personas claves y estrategicas que desarrollan*	*Descripción del evento de riesgo que haya ocurrido y afectado*	*Número de eventos en dos años*	*Descripción de la causa que lo originó*	*Financiero Regulatorio Reputación*	*Detalle de las acciones realizadas por la institución*	*Determinar si la acción mitigó el riesgo*	*Leyes y normas Lineamientos Políticas*	*Descripción del tipo de sanción*	*Cuál es el impacto por incumplimiento*

Fuente: elaboración propia.

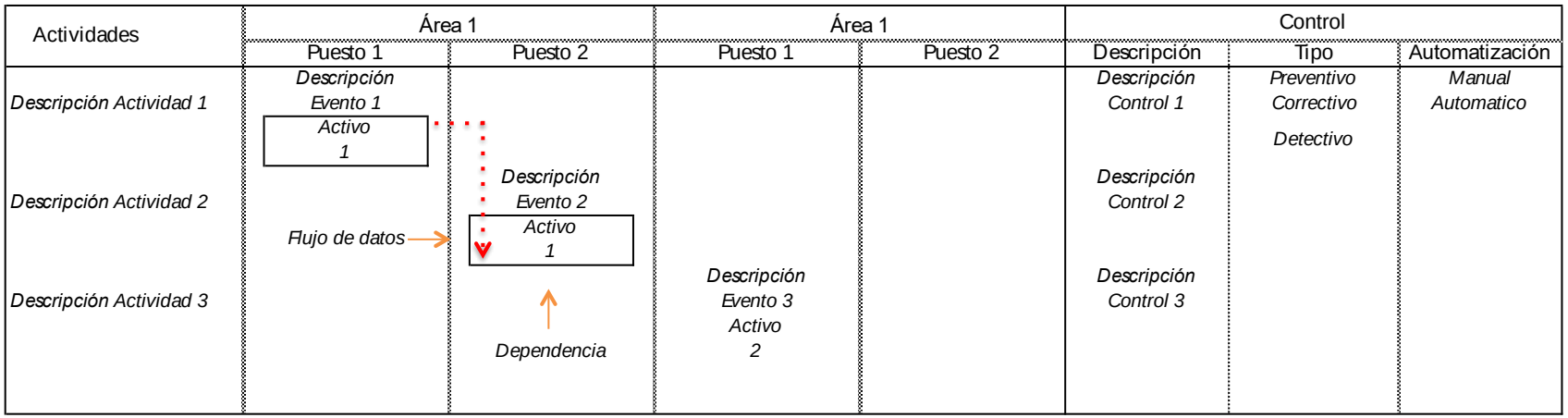
APÉNDICE 5: MODELO DIAGRAMA DE ACTIVIDADES POR PROCESO Y DESCRIPCIÓN DE RIESGOS, ACTIVOS Y CONTROLES RELACIONADOS

DIAGRAMA DE ACTIVIDADES DEL PROCESO E IDENTIFICACIÓN DE RIESGOS Y CONTROLES RELACIONADOS

Actividad: Identificar

Clave, concentración de funciones

Proceso:



Fuente: elaboración propia.

APÉNDICE 6: MODELO ESCENARIO DE RIESGOS

ESCENARIOS DE RIESGOS
Actividad: Identificar

			Componentes								
Proceso	Actividad	Escenario de riesgo	Tipo de amenaza	Agente	Evento	Activo/Recurso		Tiempo				Tipo de riesgo
						Causa	Efecto	Momento	Duración	Detección	Transcurrido	
		Describa el escenario de riesgo/oportunidad, incluyendo un razonamiento sobre el impacto negativo del escenario. La descripción aclara el tipo de amenaza/vulnerabilidad e incluye los agentes, eventos, activos y cuestiones de tiempo.	*La naturaleza del evento.* *Maliciosa* *Accidental* *Error* *Fallo* *Natural* *Requerimiento externo*	*Quién o qué desencadena la amenaza* *Interna* *Externo* *Humano* *No humano*	*Los eventos siempre tienen causas y suelen tener consecuencias.* *Divulgación* *Interrupción* *Modificación* *Robo* *Destrucción* *Diseño ineficaz* *Ejecución ineficaz* *Reglas y regulaciones* *Uso inapropiado*	*Proceso* *Personas y habilidades* *Estructura organizativa* *Infraestructura física* *Infraestructura de TI* *Información* *Aplicaciones*	*Proceso* *Personas y habilidades* *Estructura organizativa* *Infraestructura física* *Infraestructura de TI* *Información* *Aplicaciones*	*No crítico* *Crítico*	*Corta* *Moderada* *Extensa*	*Lenta* *Moderada* *Instantánea*	*Inmediato* *Demorado*	

Diagrama del proceso ← Fuente

Fuente: elaboración propia con información de COBIT 5 Riesgos (2013)

APÉNDICE 7: MODELO ANALISIS DE BRECHAS DE CONTROLES

ANÁLISIS DE BRECHAS DE CONTROLES
Actividad: Análisis

Proceso	Actividad	Riesgo			Control			Cumplimiento de los objetivo de Control						Brechas	Confianza
		Escenario	Tipo	Activo	Descripción	Tipo	Automatización	Integridad y exactitud de la información	Confiabilidad de la información	Disponibilidad de la información	Salvaguarda de los activos	Eficacia de las operaciones	Cumplimiento de leyes y regulaciones		
					Descripción del control	*Preventivo* *Correctivo* *Detectivo*	*Manual* *Automatico*							*Indicación de la brecha de Control Interno*	*5 - Excelente* *4 - Muy Bueno* *3 - Bueno* *2 - Pobre* *1 - Insatisfactorio*

Diagrama del proceso — Escenario de Riesgos — Diagrama del proceso — Fuente

Fuente: elaboración propia.

APÉNDICE 8: MODELO ANÁLISIS DE SENSIBILIDAD DE LA INFORMACIÓN

ANÁLISIS DE SENSIBILIDAD DE LA INFORMACIÓN
Actividad: Análisis

Proceso	Actividad	Escenario de Riesgo			Sensibilidad de la información			Impacto
		Activo	Riesgo	Causa/Efecto	Confidencialidad	Integridad	Disponibilidad	
					¿Qué daño causaría que lo conociera quién no debe?	*¿Qué perjuicio causaría que estuviera incompleta, dañado o corrupta?*	*¿Qué perjuicio causaría no tenerlo o no poderlo utilizar?*	*Promedio de la sensibilidad*

Diagrama del proceso

Escenario de Riesgos

Fuente

Sensibilidad	
5 - Altas pérdidas, daño crítico	*5 - Catastrófico*
4 - Pérdida o daño serio interrumpir	*4 - Mayor*
3 - Pérdida o daño serio verse afectados	*3 - Moderado*
2 - Pérdida o daño menor	*2 - Menor*
1 - Poca o nula pérdida o daño	*1 - Insignificante*

Fuente: elaboración propia.

APÉNDICE 9: CÁLCULO DEL RIESGO, NIVEL DE EFECTIVIDAD DEL CONTROL Y EXPOSICIÓN AL RIESGO

CÁLCULO DEL RIESGO, NIVEL DE EFECTIVIDAD DEL CONTROL Y EXPOSICIÓN AL RIESGO
Actividad: Análisis

Proceso	Actividad	Riesgo			Control			Cálculo del Riesgo				Nivel de Efectividad del Control			Exposición al Riesgo
		Escenario	Tipo	Activo	Descripción	Tipo	Automatización	Impacto	Probabilidad	Score Riesgo	Calificación del Riesgo	Confianza en el Control	Score Control	Nivel de Efectividad	
					Descripción del control	*Preventivo* *Correctivo* *Detectivo*	*Manual* *Automático*	*5 - Catastrófico* *4 - Mayor* *3 - Moderado* *2 - Menor* *1 - Insignificante*	*5 - Catastrófico* *4 - Mayor* *3 - Moderado* *2 - Menor* *1 - Insignificante*	*Impacto multiplicado por probabilidad*	*Bajo* *Moderado* *Alto* *Extremo*	*5 - Excelente* *4 - Muy Bueno* *3 - Bueno* *2 - Pobre* *1 - Insatisfactorio*	*Score Riesgo - (1/5*1)* *Score Riesgo - (1/5*2)* *Score Riesgo - (1/5*3)* *Score Riesgo - (1/5*4)* *Score Riesgo - (1/5*5)*	*Score Riesgo menos Score Control*	*Score Control dividido entre Score Riesgo*
		Diagrama del proceso		Escenario de Riesgos		Diagrama del proceso		Análisis de sensibilidad				Análisis de brecha	← Fuentes		

Fuente: elaboración propia.

APÉNDICE 10: RIESGOS CONTRA CRITERIOS DE ALTO IMPACTO

RIESGOS CONTRA CRITERIOS DE ALTO IMPACTO
Actividad: Valoración del riesgo

Proceso	Actividad	Riesgo	Control	Calificación del Riesgo	Nivel de Efectividad del Control	Exposición al Riesgo	Criterios de Alto Impacto				Justificación
							1	*2*	*3*	*4*	

Criterios
1. La materialización del riesgo ocasiona pérdidas financieras importantes.
2. Incumplimiento regulatorio con consecuencias graves.
3. Afecta la imagen ocasionando una exposición pública.
4. Inadecuado uso de recursos con repercusiones graves.

Fuente: elaboración propia.

APÉNDICE 11: MATRIZ DE RIESGOS

MATRIZ DE RIESGOS
Actividad: Valoración del riesgo

Referencia la papel de trabajo	Proceso	Actividad	Riesgo	Control	Calificación del Riesgo	Nivel de Efectividad del Control	Exposición al Riesgo	Criterio de Evaluación
Hacer referencia al formulario utilizado para documentar la fuente								*Descripción de la decisión tomada por el equipo de auditores.*

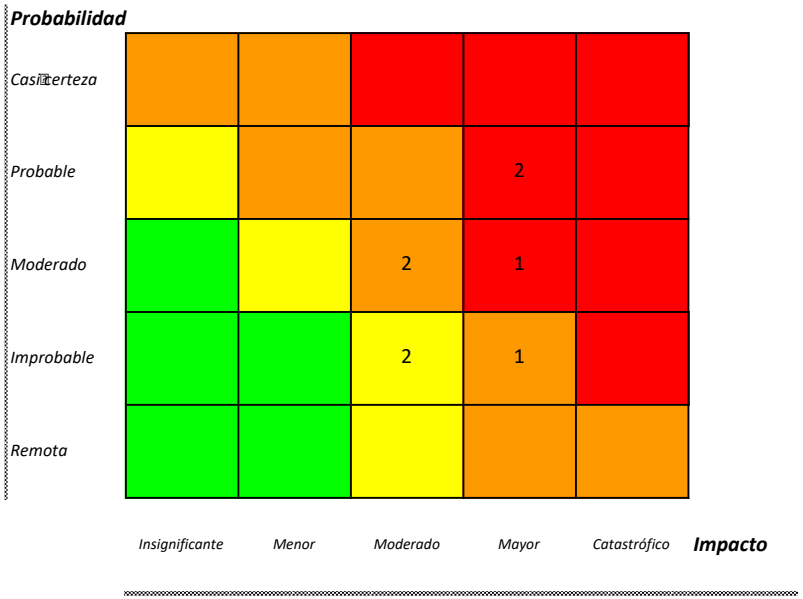
Fuente: elaboración propia.

APÉNDICE 12: MAPA DE RIESGOS

Gráfico por Riesgos

Total de Riesgos 8

Cantidad



Descripción Riesgo