UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

TÌTULO:

DISEÑO DE UN PLAN DE AUDITORIA INTERNA DE SISTEMAS, PARA UN MODELO DE AEROLÍNEA DOMÉSTICA ECUATORIANA, BASADO EN ANÁLISIS DE RIESGOS, Y TOMANDO COMO MARCO DE REFERENCIA COBIT 5

AUTORA:
Wither Delgado, Nelly Judith

Trabajo de Titulación previo a la Obtención del Título de INGENIERA EN CONTABILIDAD Y AUDITORÍA

TUTORA:
CPA. Yong Amaya, Linda Evelyn, Msc.

Guayaquil, Ecuador

2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por **Nelly Judith, Wither Delgado**, como requerimiento parcial para la obtención del Título de **Ingeniera en Contabilidad y Auditoría**.

TUTORA

_____

CPA. Yong Amaya, Linda Evelyn, Msc.

DIRECTOR DE LA CARRERA

_____

Ing. Ávila Toledo, Arturo Absalón, Msc.

Guayaquil, octubre del 2014

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

DECLARACIÓN DE RESPONSABILIDAD

Yo, **Nelly Judith Wither Delgado**

DECLARO QUE:

El Trabajo de Titulación **Diseño de un Plan de Auditoria Interna de Sistemas, para un modelo de Aerolínea doméstica ecuatoriana, basado en análisis de riesgos, y tomando como marco de referencia COBIT 5** previa a la obtención del Título **de Ingeniera en Contabilidad y Auditoría**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan al pie de las páginas correspondientes, cuyas fuentes se incorporan en la bibliografía. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del Trabajo de Titulación referido.

Guayaquil, octubre del 2014

LA AUTORA

_____
Nelly Judith Wither Delgado

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

AUTORIZACIÓN

Yo, **Nelly Judith Wither Delgado**

Autorizo a la Universidad Católica de Santiago de Guayaquil, la **publicación** en la biblioteca de la institución del Trabajo de Titulación: **Diseño de un Plan de Auditoria Interna de Sistemas, para un modelo de Aerolínea doméstica ecuatoriana, basado en análisis de riesgos, y tomando como marco de referencia COBIT**, cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

Guayaquil, octubre del 2014

LA AUTORA:

_____

Nelly Judith Wither Delgado

AGRADECIMIENTO

A mi familia, por el apoyo incondicional recibido en cada parte del camino, y la confianza que depositan en mí.

A mis maestros, tutora, y las personas de la Universidad Católica Santiago de Guayaquil, que me abrieron las puertas, me facilitaron el poder estudiar esta carrera, me enseñaron y motivaron para seguir aprendiendo y alcanzar esta meta.

A Dios, por todo… y lo que se me quede por fuera de agradecer.

Nelly Judith Wither Delgado

DEDICATORIA

He sido bendecida con una extensa familia, a la cual le dedico este trabajo con mucho cariño. Si bien la lista es larga para mencionarlos a todos, quisiera hacer una dedicatoria especial a mis padres y mi hermana, quienes me han acompañado de manera cercana en este camino. Más que un trabajo individual, ha sido un logro en equipo.

Nelly Judith Wither Delgado

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

FACULTAD DE CIENCIAS ECONÓMICAS Y ADMINISTRATIVAS
CARRERA DE INGENIERÍA EN CONTABILIDAD Y AUDITORÍA

CALIFICACIÓN

_____

CPA. Yong Amaya, Linda Evelyn, Msc.
TUTORA

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

RESUMEN

Dada la alta dependencia en tecnología de la Industria Aérea Comercial en general, los Departamentos de Auditoria Interna de las aerolíneas deben considerar el incorporar y mantener un análisis continuo de los Sistemas, Componentes y plataforma de TI, identificados como críticos.

Una de las principales acciones a tomar para lograrlo, es la de incluir en el Plan global de actividades, un Plan específico de Auditoria Interna de Sistemas / TI, que, de acuerdo a las Normas indicadas por el IIA (The Institute of Internal Auditors), esté basado en riesgos.

El objetivo principal de esta Tesis es el proponer un diseño de dicho Plan de Auditoria Interna de Sistemas / TI, aplicado a un modelo de una Aerolínea doméstica ecuatoriana, y tomando como referencia COBIT 5.

Dado lo extenso que puede llegar a ser una cobertura de toda la plataforma tecnológica de una aerolínea, se sugerirá un enfoque del Plan en aquellos elementos tecnológicos que estén directamente involucrados en la elaboración de los Estados Financieros, o tengan un impacto significativo en el resultado de los mismos.

El Marco de trabajo a ser usado, COBIT 5, facilitará el análisis del gobierno y la gestión de TI, y proveerá una metodología para analizar los riesgos de TI.

En el diseño del Plan de Auditoria de Sistemas / TI, se puede considerar las guías propuestas por el IIA, en donde las principales fases son: a) Entender el negocio, b) Definir el Universo de TI, c) Evaluar los Riesgos, y d) Formalizar el Plan.

La Industria aérea tiene un rol destacado en la economía global. Esto ayuda a que existan varias fuentes disponibles en donde obtener información relevante, tales como la IATA (International Air Transport

Association), análisis de firmas auditoras (PWC, KPMG, etc), informaciones de las DGACs (Direcciones de Aviación Civil) locales, medios informativos en los países, y reportes de aerolíneas que cotizan en Bolsas de valores.

En la identificación del Universo de TI, los principales sistemas de contabilidad y los componentes de TI que podrían afectar los estados financieros de manera relevante, serán identificados.

Una vez definido el Universo de TI, la siguiente fase será la de realizar un análisis de riesgos de TI, a través de la evaluación de escenarios de riesgo calificados de acuerdo a factores de posible impacto y frecuencia. El resultado de esta evaluación es un Mapa de Riesgos.

Y en la última fase de Formalización del Plan, se realizará un análisis de las actividades basado en prioridades, de acuerdo a criterios tales como recursos del Departamento, resultados de Auditorias previas, necesidades de los Usuarios Principales, etc. Dado que las tareas de Auditoria Interna pueden cambiar de acuerdo a las necesidades del negocio, es prudente tomar en cuenta las estimaciones de otras actividades.

El Comité de Auditoria, o el organismo de control en el que la Junta delegue las tareas, es el encargado de validar y dar la aprobación final al Plan de Auditoria Interna global, que incluye al Plan de Sistemas / IT.

Durante el desarrollo de esta Tesis se trabajará con un conjunto supuesto de condiciones y eventos, para realizar un ejercicio práctico. Es relevante aclarar que los supuestos presentados a lo largo del trabajo, son de responsabilidad de la autora de este trabajo, con la finalidad única y exclusiva de presentar una aplicación práctica del diseño de un Plan de Auditoria Interno de Sistemas / TI, dirigido a un modelo de negocios de una aerolínea doméstica ecuatoriana.

Palabras Clave: COBIT, TI, Sistemas, Plan, Auditoria Interna, Diseño

ABSTRACT

Given the high reliance on technology of the Commercial Airline Industry in general, the Internal Audit Departments of the airlines must consider to incorporate and maintain an ongoing analysis of the systems, IT components and infrastructure identified as critical.

In order to achieve it, one of the key actions to take, is to include into the overall Internal Audit Plan, a specific IT Audit Plan, which, according to the norms and guidelines of the IIA -The Institute of Internal Auditors-, needs to be based on risk analysis.

The main objective of this Thesis is to propose a design of the IT / System Internal Audit Plan, applied to a business model of an Ecuadorian Domestic Airline, and with reference to the IT framework COBIT 5.

Given how extensive could be a total coverage of the entire technological platform of an airline, it will be suggested to apply a focus of the exercise into those technological elements that are directly involved in the preparation of financial statements, or have a significant impact on the financial results.

The IT framework to be used, COBIT 5, will facilitate the analysis of the IT governance and management, and also will provide a methodology for analyzing IT risks.

In designing the IT / Systems Internal Audit Plan, we can consider the guidelines proposed by the IIA, where the main steps are: a) Understand the business, b) Define the IT Universe, c) Evaluate the Risks and d) Formalize the Plan.

The airline industry has a prominent role in the global economy. In order to understand it, there are several sources available where it is possible to obtain relevant information, such as the IATA (International Air

Transport Association), analysis of audit firms (PWC, KPMG, etc.), DGACs (Civil Aviation Authorities), local media, and public airline reports listed on stock exchanges.

In identifying the IT Universe, the main accounting systems and those IT components that could affect the financial results in a relevant manner, will be identified.

Once the IT Universe is defined, the next phase will be to perform an IT risk assessment, through the evaluation of risk scenarios ranked according to possible impact and frequency factors. The result of this evaluation is a Risk Map.

And at the last phase of formalization of the IT plan, an analysis based on priorities will be performed, according to criteria such as available department resources, previous audits results, stakeholders or key user's needs, etc. Since the internal audit activities could change due business requirements, it will be recommended to consider estimates of other activities.

The Audit Committee (or the corporate body assigned by the Board) is responsible for validate and give final approval to the Global Internal Audit Plan, including the IT Plan.

During the development of this thesis, this author will work with an assumed set of conditions and events, for a practical exercise. It is important to clarify that the cases presented throughout this Thesis, are responsibility of the author, with the sole purpose of presenting a practical application of the design of an IT Internal Audit Plan, aimed at a general business model of an Ecuadorian domestic airline.

Key Words: COBIT, IT, Systems, Plan, Internal Audit, Design

INTRODUCCIÓN

Entre las industrias con un alto uso de la tecnología, y que tiene un rol estratégico en la economía de los países, se puede mencionar el del Transporte aéreo Comercial de Pasajeros.

Eventos tales como una caída del Sistema de Reservas, fallas en los Sistemas Centrales, o problemas de configuración en el Website de venta de las aerolíneas, han sido noticia en los últimos años en la región Americana, y reflejan una alta exposición de la industria aérea comercial en general, a que una falla tecnológica en un componente o Sistema pueda afectar la operación completa de una aerolínea. Esto no solamente impacta a la aerolínea en sus finanzas, reputación, etc., sino que tiene repercusiones en los pasajeros, las empresas, industrias, etc., que usan los servicios de transporte aéreo y toman decisiones y/o realizan actividades confiando en una red de transporte aéreo estable y operativa.

Aquí la Auditoria Interna de Sistemas puede contribuir significativamente, aportando su enfoque en controles y análisis de riesgos, a los elementos de las operaciones tecnológicas considerados críticos.

Una de las tareas principales en las labores de los Departamentos de Auditoria Interna de las empresas, es la de desarrollar un Plan estructurado de Auditoria, que permita dar un aseguramiento a los accionistas / partes interesadas, y alta gerencia, en cuanto al nivel de los controles internos, los riesgos y el ambiente de gobierno que existen al interior de las organizaciones.

El diseño de un Plan anual de Auditoria de Sistemas, que pueda alimentar a un Plan macro de Auditoria, presenta desafíos en su elaboración, dado que tiene que tomar en cuenta tanto las herramientas y técnicas propias de la labor de Auditoria, como el conocimiento en tecnologías de cómputo y sistemas, y sus riesgos inherentes.

Este trabajo tiene como objetivo el brindar un Modelo de Diseño de un Plan anual de Auditoria de Sistemas / TI, que pueda ser aplicado en una aerolínea regional ecuatoriana, cuya operación esté orientada al transporte doméstico de pasajeros, y su matriz o sede principal se encuentre en territorio ecuatoriano.

Dada la amplitud que puede llegar a tener la Auditoria de Sistemas / TI, el trabajo se enfocará en aquellos sistemas y componentes tecnológicos que sean considerados críticos para la elaboración y generación de los Estados Financieros, o los que afecten los resultados de los mismos de manera relevante.

El análisis correspondiente tomará en cuenta el Marco de COBIT 5, de acuerdo a lo publicado por ISACA, aceptado ampliamente en las labores de Auditorias de Sistemas.

Para el diseño del Plan se usará la metodología sugerida en la Guía del IIA (GTAG 11), que establece como fases las siguientes: a) Entender el negocio, b) Definir el Universo de TI, c) Realizar evaluaciones de Riesgo, y d) Formalizar el Plan.

El entendimiento del negocio será cubierto en el Capítulo I así como en los siguientes Capítulos. El mismo estará basado en publicaciones relevantes de fuentes tales como la IATA, reportes de firmas de auditoría, fuentes locales, etc.

En el Capítulo II se expondrá el Marco Teórico a utilizar, con énfasis en COBIT 5 y COBIT 5 para riesgos.

La definición del Universo de TI se desarrollará en el Capítulo III, en donde serán realizados análisis de aerolíneas representativas en la región, tales como Avianca (aerolínea colombiana y con presencia en el mercado doméstico del Ecuador a través de Aerogal), Copa (aerolínea panameña), LaTam (Lan y Tam, chilena y brasileña respectivamente. Lan con presencia

en el mercado doméstico ecuatoriano a través de Lan Ecuador) y Volaris (Aerolínea Regional Mexicana), que permitirán brindar sugerencias acerca de los posibles sujetos o elementos de TI a considerar. Si bien cada aerolínea tiene su estrategia y modelo de negocios particular, se trabajará con la hipótesis de que existen similitudes dada la industria y la región, que permitirán realizar un ejercicio de identificación del Universo de TI, a nivel general.

Una vez identificado el Universo de TI, se procederá a evaluar los riesgos de TI asociados, en el Capítulo IV, apoyados en el marco de COBIT 5 para Riesgos.

Y por último, el Capítulo V presentará pasos sugeridos para realizar la formalización del Plan de Auditoria Interna de Sistemas / TI.

Durante el desarrollo de esta Tesis, se trabajará con un conjunto supuesto de condiciones y eventos, para realizar un ejercicio práctico en un modelo ficticio de aerolínea doméstica ecuatoriana. Las condiciones y eventos aquí presentados son de responsabilidad de la autora de este trabajo, con la finalidad única y exclusiva de presentar ejemplos prácticos de aplicación, para facilitar la comprensión del modelo propuesto de Diseño de un Plan de Auditoria Interna de Sistemas / TI, en el tipo de industria seleccionada.

CAPITULO I

1 Análisis del Problema a resolver

1.1 Planteamiento del Problema

Dada la creciente dependencia de la tecnología en las empresas, las labores de Auditoria se han visto ampliadas en los últimos años, con la inclusión de un enfoque especializado en el análisis del gobierno tecnológico, los componentes y los sistemas considerados críticos para el desempeño de las operaciones.

Esta rama de la Auditoria enfocada en los elementos que conforman la red tecnológica, se la conoce como Auditoria de Sistemas y/o de TI (Tecnologías de la Información). La misma, aparte de requerir los conocimientos y estándares de trabajo de la labor propia de Auditoria, necesita los conocimientos que le permitan analizar de manera apropiada el nivel de gobierno y los controles de TI.

Uno de los negocios altamente dependientes de la tecnología, es el del transporte aéreo comercial, tanto de Pasajeros como de Carga. Por lo que los Departamentos de Auditoria Interna de las aerolíneas deben considerar incluir un Programa sólido de Auditoria de Sistemas, para poder cumplir de manera eficiente su misión.

Durante este trabajo de tesis, se propondrá una Metodología para diseñar un Plan anual de Auditoria Interna de Sistemas / TI, que pueda ser aplicado a una Aerolínea regional Ecuatoriana. Este diseño tomará en cuenta a COBIT 5 publicado por la ISACA, como marco de trabajo para el análisis del nivel de control de TI y la medición de riesgos tecnológicos; y las Normas, Estándares y Prácticas emitidas por el IIA (“The Institute of Internal Auditors” o el Instituto de Auditores Internos)

Este Plan de Auditoria de Sistemas /TI estará enfocado en aquellos elementos que brindan los servicios tecnológicos al área Financiera, y que se consideren relevantes, tanto en la prestación de los servicios operativos financieros, como en la elaboración de los Estados Financieros; y en los elementos que, aunque no sean necesariamente del área Financiera, tienen un alto impacto en los Estados Financieros.

Cabe resaltar que los Servicios Financieros en una aerolínea generalmente son soportados como parte de una infraestructura tecnológica a nivel de empresa, por lo que podrán existir elementos o sujetos a ser auditados dentro de este modelo de Plan de Auditorias de Sistemas / TI, que sean relevantes para todas las áreas o departamentos de la aerolínea.

Se asumirá además, que la aerolínea mantiene su centro operativo y administrativo en Ecuador, tomando Guayaquil como base, en donde se concentren las operaciones principales de los Departamentos de IT y Financiero, y que desde los centros administrativos se controlan y/o distribuyen los servicios necesarios, al resto de las ciudades y aeropuertos al interior del país.

1.2 Formulación del Problema

1.2.1 Pregunta Principal

¿Cómo diseñar un Plan de Auditoria Interna de Sistemas / TI, que esté basado en Riesgos, para un modelo de una aerolínea doméstica nacional, y cuyo enfoque sea aquellos componentes tecnológicos que generen o afecten significativamente los Estados Financieros?

1.2.2 Preguntas Secundarias

¿Qué Marco de trabajo es recomendable para comprender el gobierno y la gestión de TI en las empresas, y analizar los riesgos tecnológicos?

¿Cómo se pueden identificar los elementos relevantes tecnológicos a auditar en un modelo de aerolínea doméstica ecuatoriana, y qué se audita?

¿Cómo se evalúa el riesgo tecnológico en un modelo de aerolínea doméstica ecuatoriana?

¿Cuáles son los pasos a seguir para formalizar un Plan de Auditoria Interna de Sistemas / TI, aplicable a una aerolínea doméstica ecuatoriana?

1.3 Objetivos

1.3.1 Objetivo Primario

El objetivo primario de este trabajo es el Diseñar un Modelo de Plan anual de Auditoria Interna de Sistemas / TI, con enfoque en los sistemas contables y financieros críticos, y los elementos de TI con alto impacto en los Estados Financieros, que pueda ser aplicable a una aerolínea comercial doméstica de Pasajeros Ecuatoriana, y que tome como marco de referencia a COBIT 5.

1.3.2. Objetivos Secundarios

Entre los objetivos Secundarios se pueden indicar:

A. Analizar el Marco de referencia de COBIT 5, a usar como apoyo para el Diseño del Plan de Auditoria Interna de Sistemas / TI, así como guías y mejores prácticas sugeridas por el IIA, pertinentes a la actividad.
B. Identificar los principales elementos a considerar en el Universo auditable, relativos a los componentes tecnológicos que tienen relevancia para la elaboración de los Estados financieros y/o impactan significativamente los resultados financieros en un modelo de negocio de una aerolínea ecuatoriana doméstica de pasajeros.

C. Analizar los riesgos relativos a TI del negocio, a tomar en cuenta para la elaboración del Plan de Auditoria de Sistemas / TI, con relación a los elementos identificados pertenecientes al Universo auditable.
D. Diseñar un modelo del Plan anual de Auditoria Interna de Sistemas / TI, basado en los elementos del análisis, y formalizarlo.

1.4 Justificación e importancia

El transporte aéreo de pasajeros es considerado en la mayoría de los países como un servicio de alta importancia, por su papel e influencia en la economía y en la sociedad, al facilitar los negocios, el flujo de pasajeros, el turismo, el transporte de Carga y Correo, etc. El desarrollo del transporte aéreo suele acompañar al desarrollo de la economía en los países. Generalmente es una industria compleja, que consume cantidades considerables de recursos (aviones, combustible, personal, tecnología, etc.), mueve cantidades significativas de dinero, y está altamente regulada (en términos de seguridad aérea, mantenimiento de aviones, etc.). Estos factores entre otros, hacen de las aerolíneas un modelo de empresa interesante a comprender y analizar desde el punto de vista de la Auditoria.

Y dado que las aerolíneas tienen una alta dependencia de la tecnología, la Auditoria Interna tiene que considerar el incluir un enfoque de Auditoria de Sistemas o de TI, en sus funciones, para poder cumplir con los objetivos de su rol principal, que es el de dar un nivel de aseguramiento sobre el gobierno, los niveles de riesgo y los controles internos en las empresas.

La rama de la Auditoría de Sistemas / TI presenta un nivel de complejidad, ya que su práctica exige, además del manejo de las técnicas de auditoria, y el cumplimiento de Normas y Prácticas de la profesión, un conocimiento de tecnologías suficiente como para dar una opinión objetiva acerca del nivel de control interno de los elementos tecnológicos seleccionados, y su desempeño.

Estas dos condiciones, por un lado una industria globalizada, dependiente en alto grado de la tecnología, y con un alto impacto para la economía y la sociedad en general; y por el otro, el enfoque de Auditoria Interna en Sistemas / TI, representan un desafío interesante.

Para el modelo de una aerolínea doméstica ecuatoriana, se pueden nombrar múltiples componentes tecnológicos, aplicables a los diversos departamentos y funciones, tales como la parte de Control del Vuelo y Servicio en Tierra (Chequeo de Pasajeros, Peso y Balance del Avión, Administración de tripulaciones), la parte de Ventas (Reserva y Venta de Boletos, Web Site/E-Commerce, manejo de relaciones con agencias), el Departamento de Ingeniería de Mantenimiento (Control del Inventario de Piezas y partes Aeronáuticas, Control del mantenimiento de aviones), etc.

Si bien todos estos componentes tienen un valor importante para el desempeño de las operaciones en la aerolínea, para efectos de esta tesis, el enfoque será en aquellos sistemas y componentes tecnológicos relativos a las principales funciones financieras y contables, y/o que puedan afectar de manera significativa los Estados Financieros.

1.5 Antecedentes de la Industria

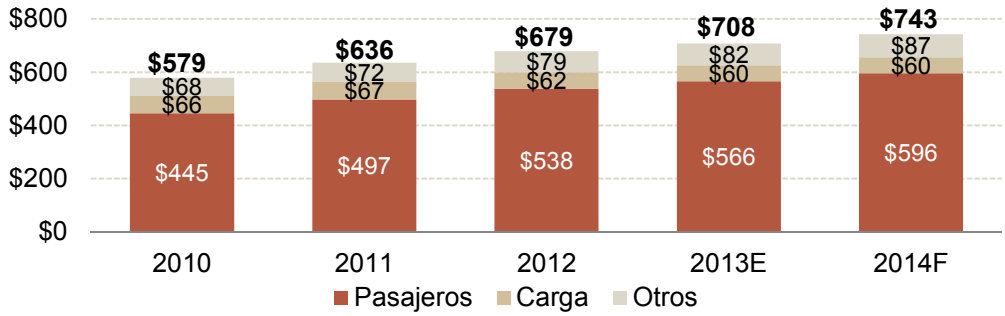
A continuación se presentan unos breves datos económicos a nivel global de la industria aérea comercial, seguido por un análisis de la aviación Comercial en el Ecuador, que apoyarán en el entendimiento del negocio de las aerolíneas.

1.5.1 Desempeño Económico del Transporte aéreo Comercial a nivel global

PWC (PriceWaterhouse Coopers), una de las principales firmas en Auditoria, en su reporte *"Tailwinds – 2014 Airline Industry Trends",* (2014:2)

presenta un análisis económico de la Industria Aérea a nivel global. De acuerdo al reporte, el ingreso global de las aerolíneas comerciales habría alcanzado los USD$ 708 Billones en el 2013, con expectativas de crecimiento del ~5% para el 2014 (Ver Gráfico No. 1).

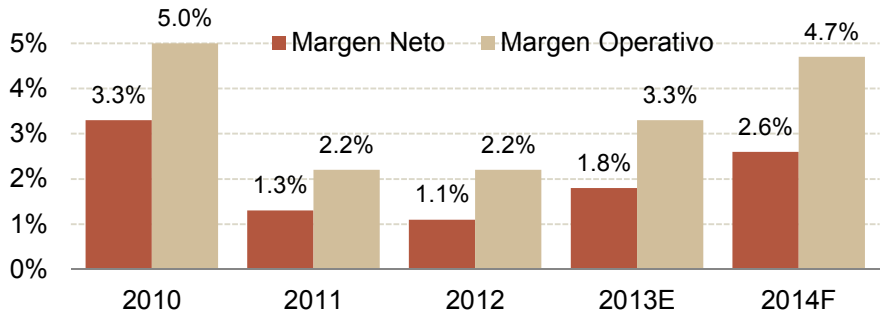
Gráfico No. 1 - Ingresos Globales 2010 a 2014 F - Aerolíneas Comerciales (*) *(En USD$ Billones)*



(*) TailWinds – 2014 Airline Industry Trends, PWC – Figura No. 1, " Global Commercial Airline Revenue", citando como fuentes a la IATA (International Air Transport Association) e ICAO (International Civil Aviation Organization)

Históricamente la aviación comercial tiene bajos márgenes de rendimiento (Ver Gráfico No. 2). Sus gastos operativos se ven afectados, en gran medida, por el costo del combustible, costos de mano de Obra, Servicio al Cliente, y Costos de operaciones aéreas y terrestres.

Gráfico No. 2 - % Márgenes Netos y Operativos Globales 2010 a 2014 F - Aerolíneas Comerciales (**)



(**) TailWinds – 2014 Airline Industry Trends, PWC – Figura No. 5, " Global Operating and Net Margins (%)", citando como fuentes a la IATA (International Air Transport Association) e ICAO (International Civil Aviation Organization)

Para aliviar el costo del combustible y del mantenimiento, las aerolíneas suelen invertir en nuevas aeronaves que sean más eficientes, optimicen el peso y el balance del avión, y consuman menos combustible. También se busca optimizar el gasto, usando mejores rutas de navegación y aproximaciones a las pistas.

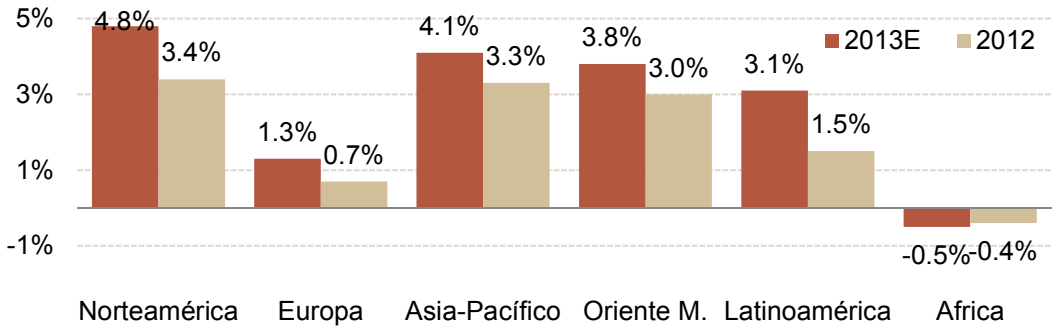
Los principales modelos de aeronaves actualmente más usados para rutas de mediano y largo alcance (en la región de América) pertenecen a las familias de aviones Airbus, Boeing y (en menor medida) Embraer, mientras que para rutas pequeñas son usados modelos tipos ATRs, CESNA, Fokker, etc.

El costo de la mano de obra es otro de los rubros significativos, y ha presentado en la última década dificultades en su manejo. Los temas de negociaciones con Sindicatos (especialmente de Pilotos y Tripulantes, personal de Mantenimiento y personal de Rampa – Servicios en Tierra) han sido noticia frecuente en la industria.

En el análisis previamente mencionado de PWC (2014: 5), se aprecia también que, de acuerdo a la región geográfica, existen diferencias en el EBIT promedio ("Earnings Before Interest and Taxes" o Ganancias antes de Intereses e Impuestos). Las mismas pueden ser explicadas tanto por el desempeño individual y/o colectivo de las aerolíneas en determinada región (mejores controles de gastos, consolidaciones, fusiones, etc), como las realidades económicas en las mismas (Recesiones, devaluaciones, crecimientos o disminuciones del PIB, variaciones locales en el precio del combustible, menor carga impositiva, etc). Por ejemplo, se puede suponer que el EBIT en las aerolíneas Europeas se ha visto afectado por los problemas económicos de la región en los últimos años.

Y para Latinoamérica se presenta un incremento del EBIT del doble entre el 2012 y el 2013 esperado. (Ver Gráfico No. 3)

Gráfico No. 3 - % Margen de EBIT por Región - 2012 y 2013 E - Aerolíneas Comerciales (*)



(*) TailWinds – 2014 Airline Industry Trends, PWC – Figura No. 6, " EBIT Margin by Region (%)", citando como fuente a la IATA (International Air Transport Association)

Las expectativas de crecimiento para los mercados domésticos de pasajeros a nivel mundial son favorables, de acuerdo a la IATA (Asociación Internacional de Líneas Aéreas), mostrando un 6.3% esperado de incremento, del 2013 al 2017. En lo expresado en el comunicado No. 67 de IATA emitido el 10 de diciembre del 2013, *"De los 10 países de más rápido crecimiento en el mercado doméstico de pasajeros, los cinco últimos están en Latinoamérica: Brasil, Perú, Colombia, México y Ecuador"* (http://www.iata.org/pressroom/pr/Documents/Spanish-PR-2013-12-10-01.pdf)

1.5.2 Transporte aéreo Comercial de Pasajeros en Ecuador

El artículo publicado en la Revista Ecuatoriana Vistazo, "Alarma a Bordo" (2014:14), brinda un análisis actualizado de la industria ecuatoriana de aerolíneas domésticas. En el análisis se muestra que, si bien el mercado Ecuatoriano del transporte aéreo de Pasajeros se ha expandido en la última década en más de 200% (tomando en cuenta el número de pasajeros transportados), desde 2010 hasta el presente, se observa una disminución en los Pasajeros nacionales.

Algunos factores señalados por el artículo son: el cambio en el comportamiento de vuelo de los usuarios en la ruta desde y hacia Quito, al trasladarse las operaciones del Aeropuerto Mariscal Sucre de Quito a Tababela; y la –posible- preferencia de los viajeros, al viajar en carreteras que se han ido mejorando, versus optar por un vuelo nacional. Es pertinente además mencionar como factor a la eliminación del subsidio a los combustibles (enero 2010) y su impacto en las tarifas domésticas, que pudo haber afectado la demanda del servicio.

Se indica además que los operadores locales se han reducido de siete a cuatro en los últimos 3 años. Entre las aerolíneas que cerraron operaciones se puede nombrar a Icaro, VIP, AirCuenca y Saereo.

Actualmente las aerolíneas constituidas como ecuatorianas y que sirven al mercado doméstico son:

- TAME: (Código Iata EQ) Aerolínea propiedad del estado, fundada en 1962 y considerada como la principal aerolínea de bandera del Ecuador, que abarca no solo rutas domésticas, sino también internacionales. En el país opera en Quito (Tababela), Latacunga, Cuenca, Tulcán, Loja, Guayaquil, Esmeraldas, Manta, Santa Rosa, Galápagos, Lago Agrio, Tena, Francisco de Orellana y Macas.
- LAN Ecuador: (Código Iata XL) Pertenece a la línea aérea de capital chileno, LAN, que ahora forma parte de la Holding LATAM (Unión de LAN y la brasileña TAM). Ingresó al país en el 2002, formando una aerolínea local, Aerolane, con la marca LAN Ecuador, y con base de operaciones en Guayaquil. En el 2009 le fueron asignadas rutas domésticas. De acuerdo a lo expresado por su Web Site (www.lan.com), tienen el 41% del mercado, y operan en los aeropuertos de Guayaquil, Quito, Cuenca y Galápagos.
- Aerogal: (Código Iata 2K) En Nov 2010 fue comprada por Avianca, la línea aérea Colombiana. En Junio del 2014 se realizó el cambio de marca comercial, uniendo así el servicio del mercado doméstico

ecuatoriano e internacional, en una sola marca, Avianca. Al presente la aerolínea sirve a siete destinos locales: Quito, Guayaquil, Cuenca, Manta, El Coca y Galápagos (San Cristóbal y Baltra).

- LAC (Líneas Aéreas Cuencanas): Empresa propiedad de inversionistas azuayos.

El ingreso de las tres primeras durante el 2013, de acuerdo al Ranking Empresarial de la revista ecuatoriana EKOS, fue el siguiente:

Tabla No. 1 - Ingresos de LAN Ecuador, TAME y Aerogal 2013 (*)

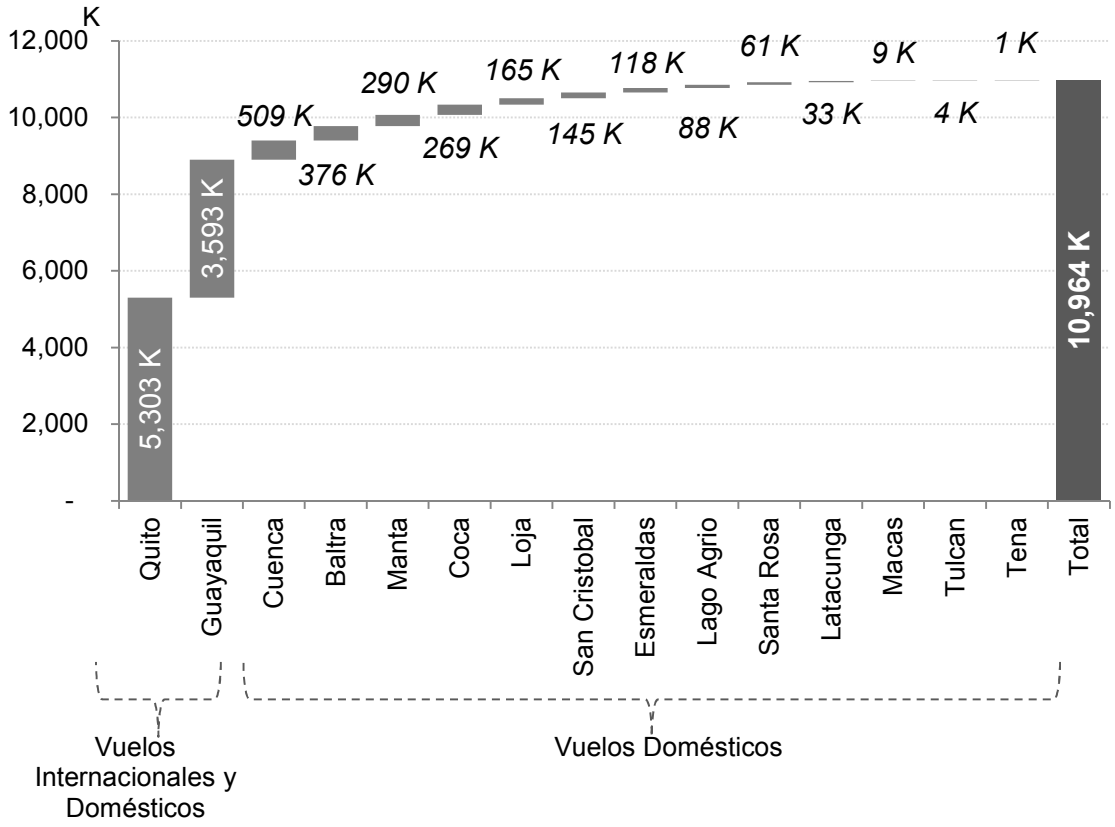
Aerolínea	Posición (Ingresos)	Ingresos (USD)
Aerolane Líneas Aereas Nacionales del Ecuador S.A. (LAN Ecuador)	24	357,596,422
TAME EP	96	154,804,181
Aerolíneas Galápagos S.A. AEROGAL	130	120,250,562

(*) Tabla compilada en base a datos tomados del portal www.ekosnegocios.com, relativos a desempeño financiero (ranking) de las empresas ecuatorianas en el 2013

De acuerdo al artículo del diario Ecuatoriano El Telégrafo "10.9 millones de personas se movilizaron en el 2013", publicado en mayo del 2014, que cita como fuente a la DGAC (Dirección General de Aviación Civil), durante el 2013 la red de transporte aéreo comercial del país (mercado internacional y doméstico) abarcó 15 aeropuertos.

Dos de ellos, Guayaquil y Quito, operan vuelos internacionales de pasajeros con rutas establecidas, además de rutas domésticas.

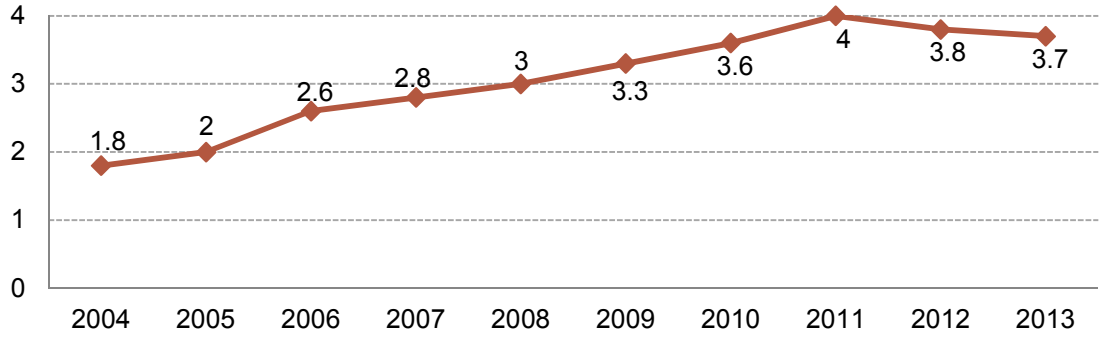
Gráfico No. 4 - Estadísticas de Pasajeros 2013 en Ecuador - Vuelos Internacionales y Domésticos (*) - (Expresado en Miles)



(*) Fuente: Artículo El Telégrafo – "10.9 millones de personas se movilizaron en avión en 2013" – Basado en estadísticas de la DGAC

En el análisis de la Revista Vistazo, del artículo "Alarma a Bordo" mencionado previamente (2014:14), se puede observar que la cantidad de pasajeros regulares, sólo en vuelos domésticos en el Ecuador, se encuentra en aproximadamente 3.7 Millones de Pasajeros. Esto es una disminución de la tendencia en alza que se venía manteniendo hasta el 2011. (Ver Gráfico No. 5).

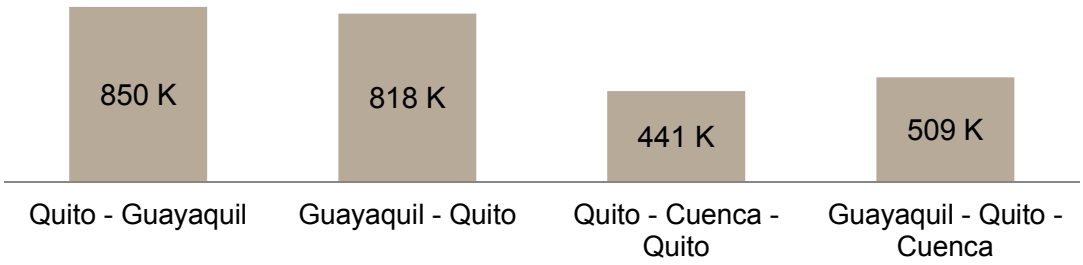
Gráfico No. 5 - Pasajeros Regulares en Rutas Nacionales (*) (En millones Pax)



(*) Revista Vistazo de Julio 10, 2014, Artículo "Alarma a Bordo" – Figura "Pasajeros regulares en rutas nacionales", citando como fuente a la DGAC

Entre las rutas más frecuentadas en el mercado doméstico se pueden mencionar las que unen a Quito, Guayaquil y Cuenca. De acuerdo a las estadísticas del 2013 mencionadas por El Telégrafo en el artículo previamente indicado, se tuvieron aproximadamente 2.6 millones de pasajeros en ellas.

Gráfico No. 6 - Estadísticas de Pasajeros 2013 en Ecuador, Rutas Domésticas más frecuentadas (*) (Expresado en Miles)



(*) Datos preparados en base al Artículo del diario El Telégrafo, "10.9 millones de personas se movilizaron en avión en 2013", que cita como fuente a la DGAC

La tendencia a nivel latinoamericano en expansión de nuevas rutas, y énfasis en aprovechar los mercados domésticos, podría sugerir que hay

posibilidades de que nuevas aerolíneas puedan surgir en el país, ya sea como competidoras de las grandes aerolíneas locales (TAME, LAN y Aerogal), o como aerolíneas concentradas en un nicho de mercado, sirviendo aeropuertos poco frecuentados, y/o dedicando servicios especializados a clientes de cierto perfil.

Por los hechos mencionados, se puede deducir que la industria aérea en el país es un mercado interesante. Es bastante dinámico y puede verse seriamente afectado por eventos externos, por lo que las aerolíneas deben tener estructuras y procedimientos que les permitan reaccionar rápidamente. En nuestro país tiene un rol significativo en el desarrollo económico por su función de brindar servicios de transporte de pasajeros y Carga.

CAPITULO II

2. MARCO TEÓRICO

En este capítulo se brindarán referencias de acuerdo a estándares y mejores prácticas, así como un marco de trabajo sugerido, que facilitarán el diseño del Modelo del Plan de Auditoria Internas de Sistemas / TI.

Entre las fuentes de referencias a usar están los organismos de la ISACA, y el IIA.

Una de las asociaciones que más ha contribuido a estandarizar, desarrollar y monitorear las labores relativas al gobierno de la Tecnología de la Información o TI, es la ISACA (www.isaca.org), fundada en 1969. En su Web site menciona que tiene más de 90K miembros y está presente en ~160 países. Este organismo define su objetivo como el ayudar a empresas y líderes de TI a construir confianza en y maximizar el valor de la información y de los sistemas de información.

Desde hace varios años ISACA ha publicado un conjunto de Estándares, Guías y Lineamientos para la labor de Auditoria de Sistemas.

Y con relación a la práctica de la Auditoria Interna en general, el organismo a tomar como referencia es el Instituto de Auditores Internos o IIA – The Institute of Internal Auditors- (www.iia.org), el cual fue establecido en 1941 y actualmente tiene más de 180K miembros, repartidos en 160 “Charters” o Sedes locales. La misión descrita en su Web Site es la de proveer un liderazgo dinámico para la profesión a nivel global de la Auditoria Interna.

2.1 Rol del Auditor de Sistemas / TI

En los últimos años existe una dependencia cada vez más creciente de las empresas, y las sociedades en general, de la tecnología. Las

empresas han invertido cantidades considerables de recursos económicos en Sistemas de Cómputo, Infraestructura, Bases de Datos, Redes, Aplicaciones, etc., para alcanzar sus objetivos corporativos, de una manera más eficiente, llegando cada vez más a más clientes, con mejores precios y mayor calidad, apoyados por la automatización y tecnificación de sus tareas y procesos internos.

Los modelos de economías de escalas que las empresas tienden a seguir, con frecuencia concentran los elementos críticos tecnológicos en unos pocos puntos (ej, Centros de Datos, o un Sistema unificado con múltiples funciones). Esta centralización, si bien facilita las operaciones, representa un potencial riesgo –incluso para la viabilidad de las empresas- en caso de que ese punto o puntos presenten fallas.

Se puede inferir que la dependencia creciente de las empresas con relación a la tecnología, ha llevado al Auditor de Sistemas / TI, a tener un rol más protagónico y de mayor responsabilidad, tanto para la Auditoria Externa como la Auditoria Interna.

Uno de los conceptos ofrecidos por el IIA, en su artículo, “So you want to Be an IT Auditor?/Usted desea ser un Auditor de TI?” (2012), menciona que los Auditores de IT/Sistemas, siguen todos los parámetros éticos y de independencia que los Auditores Financieros, pero que su enfoque es en el análisis del Gobierno de los Sistemas y Procesos de TI.

Entre las habilidades específicas que se mencionan sugeridos para este rol, están el tener un conocimiento sólido de controles de Cómputo, Infraestructura de Sistemas (Redes, Hardware, Sistemas Operativos, Bases de Datos, y Aplicaciones, entre otros), análisis de riesgos tecnológicos y capacidad de análisis de datos.

A continuación se presenta una breve descripción de los elementos y componentes de tecnología más comunes, y que deben ser comprendidos por los Auditores de Sistemas para el desarrollo de sus trabajos.

2.2 Elementos y Componentes Tecnológicos

El mundo de la tecnología es complejo y amplio, y constantemente se está expandiendo en nuevas ramas y desarrollando nuevos elementos. Sin embargo podemos identificar varias categorías o tipos comunes de componentes / elementos presentes en la mayoría de las empresas, cuya comprensión puede ayudar en el entendimiento de las tareas de la Auditoria de Sistemas y el desarrollo del Plan de Auditoria de sistemas, objeto de esta Tesis.

Estos elementos o componentes comunes son:

2.2.1 Infraestructura y Equipos

En esta categoría se puede nombrar a los elementos físicos que soportan la arquitectura tecnológica. Cuando se analiza la Infraestructura, un componente importante son los Centros de Datos (Data Centers), en donde se concentran los equipos principales que brindan los servicios tecnológicos a la organización: Servidores de alta capacidad en donde se corren las Aplicaciones principales y se guardan las Bases de Datos, centros de interconexión de redes, etc.

Entre los equipos usados actualmente se encuentran Servidores, PCs o computadoras, laptops o portátiles, impresoras, escáner, tabletas, etc.

2.2.2 Redes y Telecomunicaciones

Una definición de Redes se puede tomar del CPA José Antonio Rodríguez Samaniego (s.f.:19), *"Hoy en día es necesario comprender las redes como un conjunto de máquinas y dispositivos interconectados a través de un medio físico para compartir información y recursos".*

Los equipos están conectados entre sí mediante una arquitectura de redes que cuenta con protocolos de comunicación estándar, y permite la interacción de los mismos con los sistemas centrales. Se usa típicamente el

término LAN para una red local, mientras que la unión de LANs se la conoce como WAN.

Adicionalmente es común que las empresas tengan información, servicios y productos disponibles vía Internet. Esto requiere de un Portal o WebSite el cual presenta varias aplicaciones disponibles a los usuarios.

Otras tecnologías actuales de rápido crecimiento y que pueden ser relevantes en temas de análisis de Auditoria son la de la Computación en la Nube (en donde los datos de las aplicaciones se guardan y acceden vía Internet) y Computación móvil (o servicios vía celulares y Tabletas).

2.2.3 Sistemas Operativos

Tomando como referencia al CPA. José Antonio Rodríguez Samaniego (s.f.:25), "Un sistema Operativo (en ocasiones abreviado como "OS") es el programa que, después de haber sido cargado inicialmente mediante un programa de carga, administra todos los otros programas de un computador".

Es decir, es el programa principal que funciona en los equipos, y sobre el mismo, funcionan todos los demás programas o aplicaciones.

Entre los más reconocidos Sistemas Operativos se pueden nombrar: Microsoft (con diferentes familias tales como Windows XP, Windows 7 Windows Vista), Unix, Linux (software libre), OS400 (para los servidores de IBM AS/400, de rango medio), OS y Android para tabletas, etc.

2.2.4 Bases de Datos

Las aplicaciones o sistemas ya sean soluciones adquiridas o desarrollo interno, funcionan típicamente sobre repositorios o Bases de Datos, en donde se guarda la información. Entre las principales bases de datos utilizadas, se puede mencionar SAP y Oracle.

2.2.5 Aplicaciones o Sistemas

Se puede describir a las aplicaciones como un conjunto de programas que han sido desarrollados para cumplir propósitos específicos.

Estos programas pueden ser desarrollados por la empresa para objetivos particulares, o adquiridos a terceros.

Actualmente existen casas especializadas de desarrollo de software que proveen soluciones a las empresas, en un amplio rango de temas, aunque también las empresas pueden desarrollar sus propias aplicaciones.

Para el objetivo de esta Tesis, es relevante mencionar a un tipo de aplicaciones, conocido como ERP (por sus siglas, "Enterprise Resource Planning"). Este término se lo utiliza para soluciones de software que pueden abarcar varias operaciones dentro de la empresa tales como las Finanzas, Operaciones, Logística, Nómina, etc.

Como referencia para los ERPs con orientación contable - financiera, se pueden nombrar a SAP, Oracle y Microsoft Dynamics, entre otros.

2.3 Diseño de un Plan de Auditoria de TI – IIA

Esta tesis estará tomando como referencia para diseñar el Plan de Auditoria Interna de Sistemas / TI, la Guía publicada por el IIA, *"GTAG 11 - Developing the IT Audit Plan / Desarrollando el Plan de Auditoria de TI",* (2009). Basados en la misma, los pasos sugeridos para elaborar el Plan de Auditoria de Sistemas / TI, se pueden definir de la siguiente manera:

A. Entender el negocio:
   - Identificar los objetivos y las estrategias de la organización
   - Entender el perfil de riesgos significativos para la organización
   - Identificar cómo la organización estructura sus operaciones de negocio
   - Comprender el modelo de soporte de negocios de TI

B. Definir el Universo de TI:
   - Analizar los fundamentos del negocio
   - Identificar aplicaciones significativas que soportan las Operaciones del negocio
   - Identificar la infraestructura crítica para las aplicaciones significativas
   - Entender el rol de tecnologías de soporte
   - Identificar proyectos e iniciativas relevantes
   - Determinar sujetos / elementos realísticos a auditar

C. Realizar evaluaciones de Riesgo:
   - Desarrollar procesos para identificar Riesgos
   - Analizar / Evaluar riesgo y medirlos / evaluar los sujetos a auditar usando factores de Riesgos de TI
   - Analizar / Evaluar riesgo y priorizar los sujetos / elementos usando factores de riesgo del negocio

D. Formalizar el Plan de Auditoria:
   - Seleccionar los sujetos / elementos a auditar y repartirlos en actividades / tareas de auditoria
   - Determinar el ciclo de auditoría y la frecuencia
   - Añadir actividades apropiadas basadas en requerimientos de la Administración / accionistas / partes interesadas, u oportunidades para brindar consultoría
   - Validar el Plan con la Administración del Negocio

Para el Entendimiento del negocio, debido a que la Tesis estudia un modelo, no una aerolínea específica, se utilizará la información de la industria (Presentada en el Primer Capítulo y en análisis sucesivos).

El Definir el Universo de TI será el objetivo del Capítulo III, basado en benchmarkings[1] e información disponible de la industria.

En el Capítulo IV se realizará un modelo de Evaluación del Riesgo, sobre los sujetos / elementos de auditoria identificados en el Universo de TI.

Y por último, el Capítulo V, presentará una Formalización del Plan de Auditoria.

2.4. Diseño de un Plan de Auditoria de Sistemas - ISACA

ISACA también brinda un estándar, el *"IS Audit and Assurance Guideline 2201 Engagement Planning"* (efectivo en Septiembre 2014), el cual establece lineamientos para el Diseño de un Plan de Auditoria de Sistemas. Tomando como base el documento, y como guía complementaria a la práctica sugerida por la IIA, se pueden resaltar los siguientes conceptos y elementos claves que debe comprender un Plan de Auditoria de Sistemas, de acuerdo al criterio expresado por la ISACA:

- **Definición del "Plan de Auditoria de Sistemas"**: Se expresa como un Plan conteniendo la naturaleza, tiempo y extensión de los procesos de auditoria de tecnologías de la información a ser realizados, con el propósito de obtener suficiente evidencia de auditoria para formar una opinión
- **Tópicos relevantes a ser considerados en el diseño del Plan**: Entre los elementos a tomar en cuenta, se puede hacer el siguiente resumen, con los puntos más significativos, para los propósitos de esta Tesis.

[1] *"Benchmarking", es un anglicismo. De acuerdo a Wikipedia "... en las ciencias de la administración de empresas, puede definirse como un proceso sistemático y continuo para evaluar comparativamente los productos, servicios y procesos de trabajo en organizaciones". (Recuperado de http://es.wikipedia.org/wiki/Benchmarking)*

Tabla No. 2 - Resumen de Lineamientos para el Diseño de un Plan de Auditoria de Sistemas, de acuerdo a ISACA (*)

Tópicos Claves	Resumen Lineamientos relevantes
(2.1) Plan de Auditoria de Sistemas	(2.1.1.) Un Plan de Auditoria de Sistemas, basado en riesgos debe ser desarrollado y actualizado, al menos anualmente.
	Se recomienda que un Plan multianual (3 a 5 años) sea establecido e incorporado al Plan anual.
	Cada tarea de Auditoria debe estar referenciada, ya sea al Plan de Auditoria de Sistemas, o mencionar el mandato y objetivos específicos, y otros aspectos relevantes del trabajo a ser realizado.
(2.2) Objetivos	(2.2.1) Se deben definir los objetivos de las tareas de auditoria y documentarlas en el Plan. Los mismos deben ser establecidos para responder a los riesgos asociados durante la actividad bajo revisión.
(2.3) Alcance y conocimiento del Negocio	(2.3.1) Como parte del proceso de planeación, los auditores deben obtener un entendimiento de la empresa y sus procesos. Esto ayudará en determinar la importancia de los recursos a ser auditados, de acuerdo a cómo se relacionan a los objetivos de la empresa, y facilitará al enfoque de la auditoria en áreas que puedan ser sensibles a prácticas fraudulentas o irregulares / inexactas.
	(2.3.2) Se debe obtener un entendimiento del tipo de personal, eventos, transacciones y prácticas que pueden tener un efecto significativo en la empresa / función / proceso / dato que sea el sujeto de las tareas de auditoria
(2.4) Enfoque basado en Riesgos	(2.4.2) Un análisis de riesgos debe ser realizado para proveer un aseguramiento razonable de que todos los elementos materiales serán cubiertos durante las tareas de auditoria

	(2.4.4) Se deben establecer niveles de materialidad, para que el trabajo de auditoria sea suficiente para cumplir los objetivos propuestos, y los recursos de auditoria sean utilizados de manera eficiente
(2.5) Documentación del Proyecto del Plan de Tareas de Auditoria	(2.5.2) Se deben incluir en la Documentación del Plan: áreas a ser auditadas, tipo de trabajo planificado, objetivos de alto nivel y alcance del trabajo, entrevistas a ser conducidas, información relevante a ser obtenida, procedimientos para verificar o validar la información obtenida, etc.

(*) De la guía de ISACA "IS Audit and Assurance Guideline 2201 Engagement Planning", algunos puntos relevantes, con una traducción libre al español, para efectos de la presente Tesis. Los números en () hacen referencia a las secciones en la guía original.

2.5 COBIT como marco de Referencia para la Auditoria de Sistemas / TI

Si bien existen varios Marcos de trabajo o referencia de Gobierno y Control Interno de TI que pueden ser aplicados en el ámbito de Tecnologías de la Información, uno de los más usados a nivel de Auditoria de Sistemas es COBIT, actualmente en su versión 5. El mismo ha sido desarrollado y propulsado por la ISACA.

ISACA, en su documento "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa", (2012:13), brinda una descripción acerca de este Marco de Referencia:

> *COBIT 5 provee de un marco de trabajo integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas. Dicho de una manera sencilla, ayuda a las empresas a crear el valor óptimo desde TI manteniendo el equilibrio entre la generación de beneficios y la optimización de los niveles de riesgo y el uso de recursos. COBIT 5 permite a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando*

al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI, considerando los intereses relacionados con TI de las partes interesadas internas y externas. COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público.

A continuación se presenta un resumen de los elementos principales del Modelo de Trabajo COBIT 5, tomando como base el documento de ISACA ya mencionado, así como otros trabajos publicados por la organización.

2.5.1 Elementos del Modelo de Trabajo COBIT 5

2.5.1.1 Principios

Los principios claves del Modelo de COBIT 5 para el gobierno y la gestión de TI de las empresas son:

1. Satisfacer las necesidades de las Partes Interesadas: El marco incluye procesos y otros catalizadores para permitir la creación de valor de las empresas, mediante el uso de recursos tecnológicos.
2. Cubrir la Empresa de Extremo a Extremo: No hay un enfoque sólo en la función de TI, sino que trata la información corporativa y sus tecnologías relacionadas como activos en las empresas. Además se cubren las funciones y procesos necesarios para gobernarlos y gestionarlos.
3. Aplicar un Marco de Referencia Único Integrado: el modelo COBIT 5 está alineado con estándares y prácticas generalmente aceptadas
4. Hacer posible un enfoque Holístico: Se toma un enfoque que tenga en cuenta varios componentes o catalizadores / habilitadores interactivos.
5. Separar el Gobierno de la Gestión: Considera una separación entre el rol del Gobierno (ej, ejercido por la Junta, Comités, etc) y la Gestión

(ej, ejercida por el CEO [2] y su equipo). Ambos tienen roles, actividades, propósitos y estructuras diferentes.

Gráfico No. 7 - Principios de COBIT 5 (*)

(*) Tomado del documento publicado por la ISACA, "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" – Figura No. 2 - Principios de COBIT 5"

2.5.1.2 Habilitadores o Catalizadores

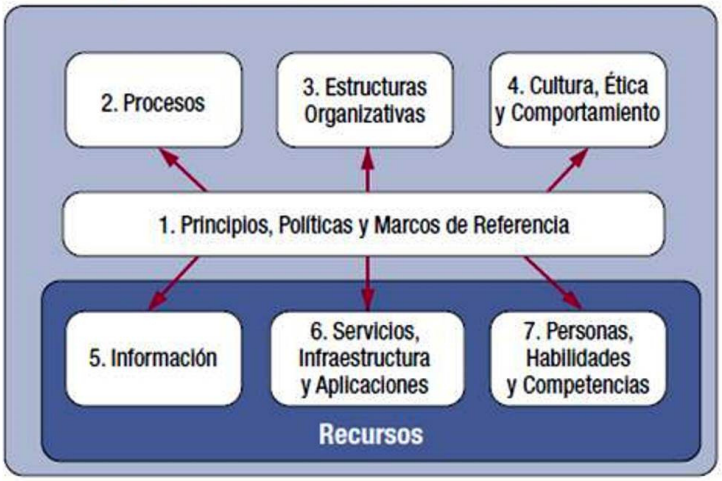
Los catalizadores (mencionados en el Principio No. 4), se definen como factores que influyen sobre el funcionamiento del gobierno de TI y la gestión de la empresa, y tienen como guía los objetivos y metas tanto de la organización como los específicos de TI. Ellos son:

- Principios, Políticas y Marcos de Referencia: Son el vehículo para traducir el comportamiento deseado para la gestión en las empresas.
- Procesos: Describen un conjunto organizado de prácticas y actividades encaminadas a lograr objetivos y resultados específicos de TI.

[2] *CEO, por sus siglas en Inglés, "Chief Executive Officer", representando el Presidente Ejecutivo o Gerente General de una empresa, y que responde directamente a los accionistas y/o Junta Directiva*

- Estructuras organizativas
- Cultura, Ética y Comportamiento
- Información: Son los datos que utilizan, procesan y producen las empresas para poder operar.
- Servicios, Infraestructura y Aplicaciones: Incluyen los elementos y componentes que brindan los servicios de TI en las empresas.
- Personas, Habilidades y Competencias

Gráfico No. 8 - Catalizadores de COBIT 5 (*)



(*) Tomado del documento publicado por la ISACA, "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" – Figura No. 12 – Catalizadores Corporativos"

2.5.1.3 Dimensiones de los Catalizadores

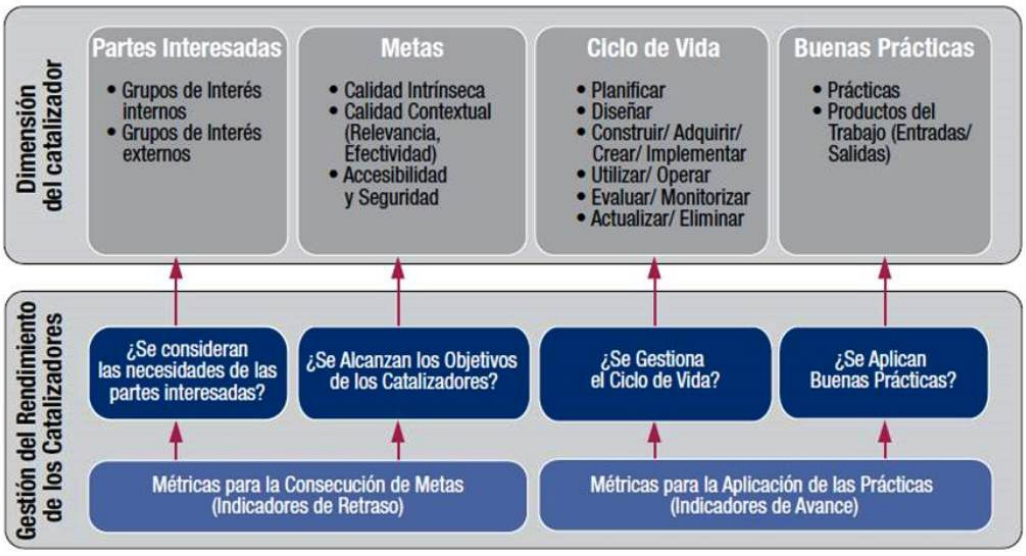
Para COBIT 5, los siete catalizadores tienen un conjunto de cuatro dimensiones comunes, lo que permite un análisis estandarizado de los catalizadores, el manejar interacciones complejas y facilita la comprensión de los resultados. Las dimensiones son:

- Grupos de Interés: Partes que juegan un rol activo y/o tienen interés en el catalizador. Las necesidades de los grupos de interés se

traducen en metas corporativas, que a su vez se traducen en objetivos de TI.

- Metas: Las mismas pueden ser definidas en términos de resultados esperados del catalizador y la aplicación u operación del mismo.
- Ciclo de Vida: Cada catalizador tiene un ciclo de vida, desde el comienzo, pasando por su vida útil, hasta su eliminación.
- Buenas Prácticas: Ayudan al logro de los objetivos del catalizador, al brindar ejemplos y sugerencias sobre implementación. Pueden ser también otros marcos de trabajo o referencia específicos al elemento o Habilitador que se está analizando.

Gráfico No. 9 - Dimensiones de los Catalizadores de COBIT 5 (*)



(*) Tomado del documento publicado por la ISACA, "Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" – Figura No. 13 – Catalizadores COBIT 5: Genéricos"

2.5.2 Enfoque de Aseguramiento de COBIT 5

Uno de los objetivos al momento de planificar las labores de Auditoria Interna, es el de poder brindar una opinión formal y estructurada, que permita a Usuarios claves / partes interesadas, el tener un entendimiento

acerca de aspectos considerados prioritarios, tales como eficacia de los controles internos, nivel de protección ante fraudes, cumplimiento de los objetivos, cumplimiento de parámetros, etc., relativos a elementos u objetos específicos.

Esta actividad se suele referir como la de brindar aseguramiento, ya que los Usuarios que reciben el resultado del análisis buscan adquirir un nivel de tranquilidad o confiabilidad acerca de estos elementos u objetos.

Dentro del Marco de COBIT 5, se tienen guías que cubren esta labor, y se puede mencionar tanto el Marco de los Componentes de Aseguramiento, como una metodología para llevar a cabo las labores.

A continuación se presenta un resumen de estos elementos, basado en la Guía "COBIT 5 for Assurance" (COBIT 5 para Aseguramiento), de la ISACA, que son de interés para los propósitos de esta Tesis.

2.5.2.1 Componentes de Aseguramiento

Es importante entender cuáles son los principales elementos, y participantes en las tareas de aseguramiento a incluirse dentro de un Plan de Auditoria de Sistemas. De acuerdo a COBIT 5, los mismos son:

- **Participantes:**
  - Los responsables directos: Son los individuos, grupos o entidades, que usualmente incluyen miembros de la Administración en una empresa, y que son los responsables finales o directos, por el sujeto en cuestión que está siendo analizado, el proceso y/o el alcance del mismo. Es decir, son los Auditados.
  - Los usuarios del análisis: Son quienes reciben los reportes de la Auditoria, y pueden incluir a una variedad de personas, tales como los accionistas / partes interesadas, la Junta Directiva, el

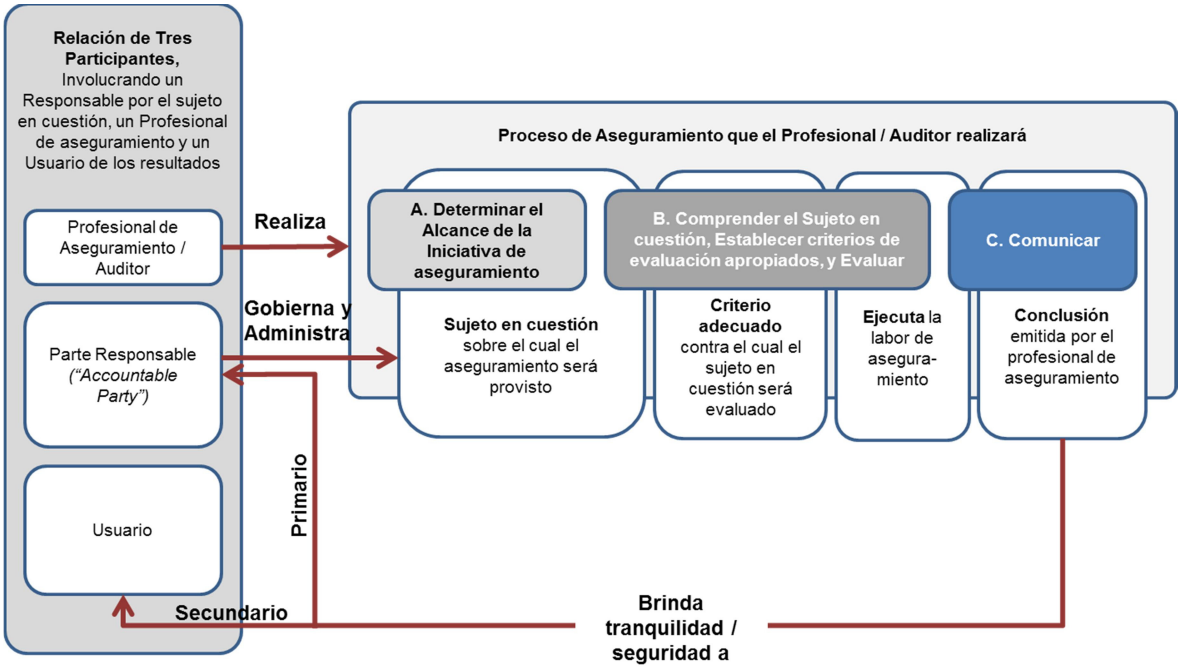
Comité de Auditoria, organismos de control, etc., así como también a la administración.

- El auditor o profesional de aseguramiento: Se refiere a la persona, o grupo de personas que tienen a su cargo la ejecución de la tarea de análisis, y la emisión formal de una opinión y/o reporte sobre el sujeto que se está revisando. Es decir, son los Auditores.

- **El Sujeto analizado o Sujeto en cuestión *("Subject Matter"):*** Este término hace referencia al objeto o sujeto que está siendo analizado por un auditor o profesional de aseguramiento. Puede incluir el diseño o la operación de control interno y prácticas administrativas sobre cualquier aspecto de la empresa, o niveles de cumplimiento establecidos por la organización u organismos regulatorios.
- **Los criterios adecuados de revisión *("Suitable Criteria")*,** son los estándares, mejores prácticas o benchmarkings, usados para medir y presentar el sujeto analizado, y contra el cual el profesional/auditor lo evalúa. No sólo se refiere a COBIT, sino a cualquier otro criterio o marco de referencia que se considere adecuado para efectos de la revisión.
- **Ejecución,** de la tarea de aseguramiento o auditoria, la cual suele tener una planificación (definición de objetivos, metas, tiempos, presupuestos, etc.) y estructura (Programa a seguir de actividades, etc.).
- **Conclusión,** en donde se recopila los resultados de las pruebas y análisis, se revisan los supuestos, se confirman los hallazgos relevantes con usuarios claves y/o personal de la administración, y se emite una opinión o reporte, el cual puede contener también recomendaciones de mejora con respecto a los Hallazgos y / o debilidades encontradas.

Una descripción gráfica de la interacción entre los componentes mencionados se puede apreciar en el siguiente Gráfico:

Gráfico No. 10 - Componentes presentes en las labores de Aseguramiento – COBIT 5 (*)



(*) Tomado del documento publicado por la ISACA, "COBIT 5 for Assurance" – Figura No.4 – "Assurance Components", y traducido libremente al español

2.5.2.2 Metodología de las actividades de aseguramiento

COBIT presenta dos Metodologías para realizar las tareas de aseguramiento, una que parte desde la función ("Assurance Function Perspective") y otra que utiliza una perspectiva de evaluación ("Assessment Perspective") en donde se revisan los procesos claves a analizar y se describe cómo proveer aseguramiento sobre los objetos de TI en análisis, representados por los catalizadores del Modelo COBIT 5.

Para los efectos de esta Tesis se presentará como sugerencia el utilizar el segundo modelo, de la Perspectiva de Evaluación ("Assessment Perspective"), dado que puede representar un modelo más fluido para las labores de Auditoria Interna, al ser aplicado sobre un conjunto de elementos u objetos de TI previamente seleccionados como de interés para la Auditoria, de acuerdo a ciertos criterios (nivel de riesgo, interés de usuarios principales, estadísticas de fraude, etc.).

2.5.2.3 Metodología de la Perspectiva de Evaluación, como modelo sugerido para las labores de aseguramiento

Si bien el alcance de esta Tesis no es el de detallar en profundidad un programa de trabajo para cada auditoria a incluirse dentro del Plan de Auditoria Interna de Sistemas / TI, agrega valor el comprender cómo las actividades pueden ser llevadas a cabo, y cuál es la relación entre la Metodología de la Perspectiva de Evaluación de COBIT 5 para aseguramiento ("Assessment Perspective"), y las técnicas comúnmente aceptadas de la Auditoria en general.

Basado en la Guía publicada por ISACA, "COBIT 5 for Assurance" (COBIT 5 para aseguramiento) (2013:55), se puede presentar un Modelo genérico de auditoria, aplicable a los objetos u elementos seleccionados de interés. Las fases de actividad de la mencionada Guía se describen a continuación:

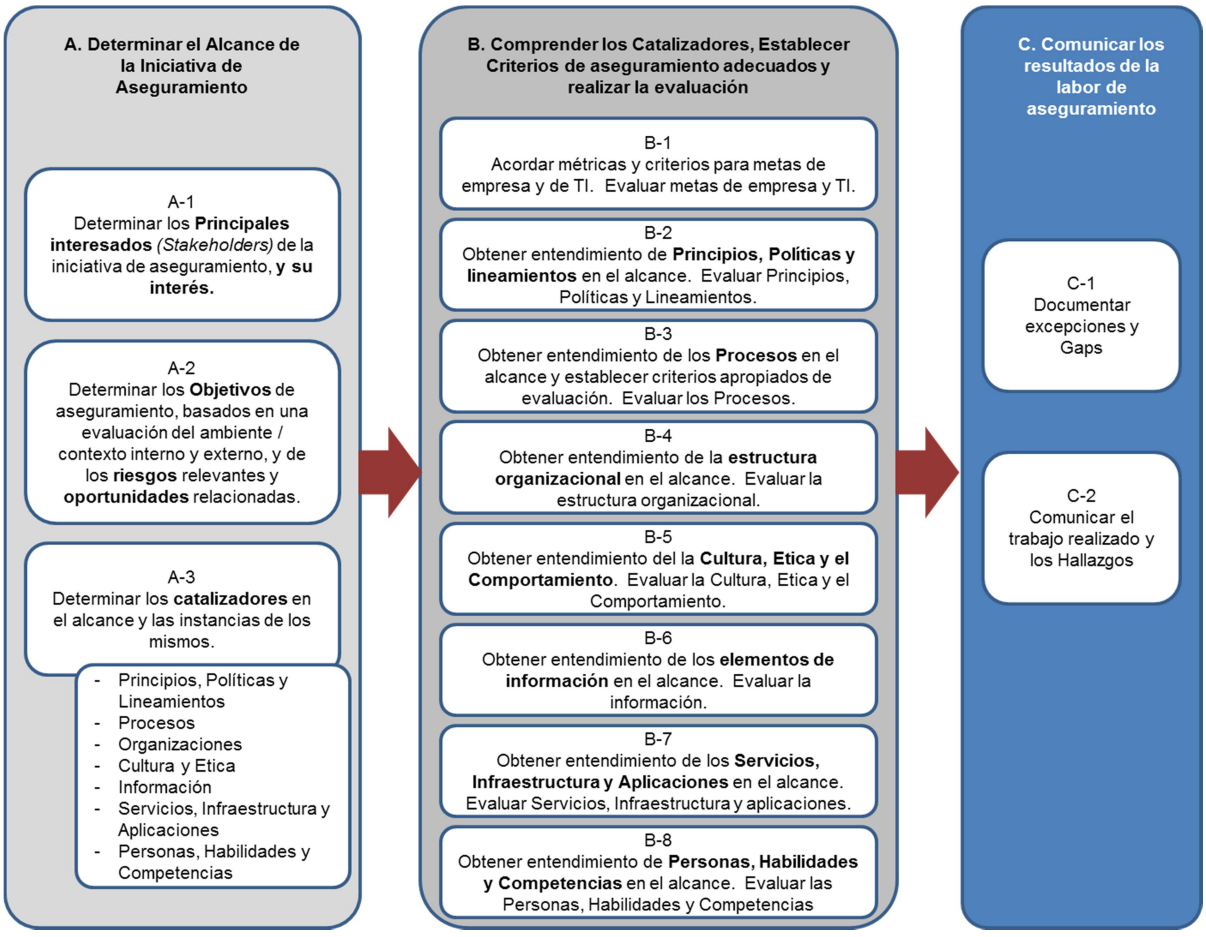
A. Planear y definir el alcance de la actividad de aseguramiento: Quiénes son los usuarios principales a recibir los resultados, cuáles son sus objetivos, cuáles son los riesgos identificados, cuál es la estructura organizacional, etc
B. Comprender / Entender el sujeto en cuestión o sujeto del análisis, establecer criterios apropiados de revisión / comparación, y realizar la evaluación: En esta fase se incluye:
    - Obtener un entendimiento suficiente (descrito en términos de los catalizadores), sobre el sujeto en cuestión que está siendo evaluado.
    - Llegar a un nivel de acuerdo sobre los criterios de evaluación que serán utilizados, que pueden ser basados en objetivos de la empresa, mejores prácticas, benchmarkings, u otro tipo de criterio considerado apropiado para evaluar al sujeto.

- Evaluar el diseño y los entregables de los catalizadores, relativos al sujeto en cuestión. Es importante el uso de técnicas apropiadas y generalmente aceptadas de auditoria, tales como:
    - Investigar y confirmar: Buscar excepciones o desviaciones y examinarlas, Investigar transacciones o eventos inusuales o no rutinarios, corroborar declaraciones de la administración con fuentes independientes, reconciliar transacciones, etc.
    - Inspeccionar: Revisar planes, políticas y procedimientos, revisar bitácoras de reporte de problemas o pistas de auditoria, rastrear transacciones a través de procesos y sistemas, recorrer físicamente instalaciones, etc.
    - Observar: Observar y describir los procesos, las personas y sus habilidades / competencias, observar las aplicaciones de software y su desempeño, etc.
    - Recalcular o Correr nuevamente: Correr nuevamente los controles, realizar nuevamente transacciones, recalcular con fuentes independientes, etc.
    - Revisar evidencia colectada automáticamente: Recoger datos de ejemplo, analizar datos con herramientas especiales, extraer excepciones o transacciones claves, etc.
    - Revisar / Determinar si algún incidente considerado de interés ha o no ocurrido, ya sea sobre el universo de eventos o sobre una muestra, etc.

C. Comunicar los resultados de la evaluación: Al finalizar la etapa de evaluación, se prepara la opinión del Auditor con respecto al sujeto evaluado. El informe o reporte debe documentar las excepciones encontradas y gaps, debe comunicar el trabajo realizado y los hallazgos de auditoria, y puede contener recomendaciones o sugerencias para cerrar o mitigar los hallazgos.

Esta Metodología se aprecia en el siguiente gráfico:

Gráfico No. 11 - Metodología genérica de las actividades de Aseguramiento - Perspectiva de Evaluación – COBIT 5 (*)



(*) Tomado del documento publicado por la ISACA, "COBIT 5 for Assurance" – Figura No.32 – "Generic COBIT 5-based Assurance Engagement Approach", y traducido libremente al español

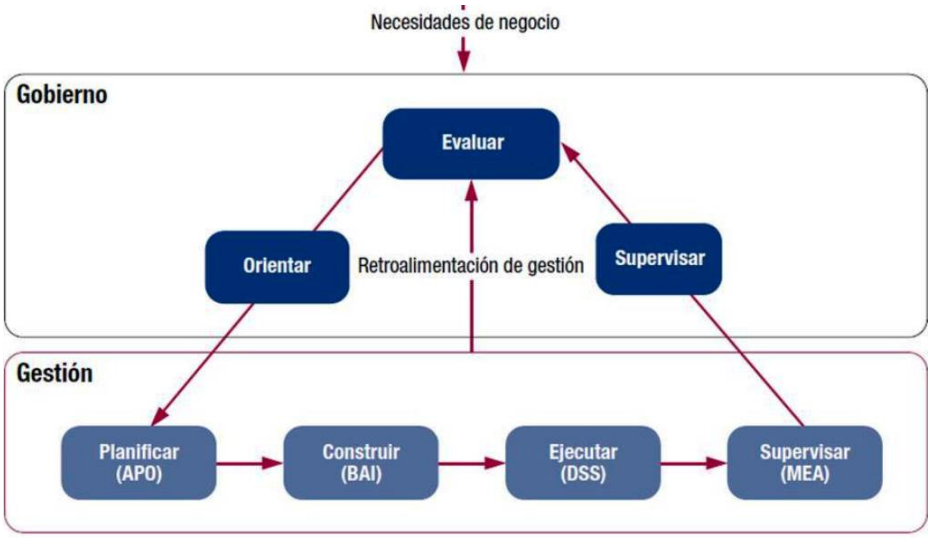
2.5.3 Modelo de Referencia de Procesos COBIT 5

COBIT 5 busca que las empresas implementen procesos de Gobierno y de Gestión de TI, que permita asegurar que las áreas más importantes estén cubiertas. Estos dos Dominios (Gobierno y Gestión) están diferenciados, de acuerdo al Principio No. 5, y tienen sus procesos definidos, con prácticas y actividades independientes, pero que se relacionan entre sí.

En las empresas generalmente los procesos de Gobierno están a cargo de la Junta o Consejo de Administración (quien los puede delegar a otros entes tales como el Comité de Auditoria), y los procesos de Gestión son responsabilidad de la Administración (representado por el Gerente General, el Presidente Ejecutivo o CEO, y su equipo de trabajo).

La ISACA en su Guía "COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" (2012), sugiere un modelo de referencia, sobre el cual las empresas pueden decidir aplicar procesos específicos de acuerdo a sus necesidades y tamaño del negocio.

Gráfico No. 12 - Las áreas clave de Gobierno y Gestión de COBIT (*)



(*) Tomado del documento publicado por la ISACA, "COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" – Figura No.15 – Las Áreas Clave de Gobierno y Gestión de COBIT 5

Este modelo de referencia está compuesto por 37 procesos, repartidos en los siguientes Dominios:

- **Gobierno:** Incluye prácticas de Evaluación, Orientación y Supervisión, identificadas por las siglas EDM *("Evaluate, Direct and Monitor")*

- **Gestión:** Contiene cuatro dominios, relacionados con planificar, construir, ejecutar y supervisar, identificados por las siglas PBRM ("*Plan, Build, Run and Monitor*"). Los mismos son:
  - Alinear, Planificar y Organizar *("Align, Plan and Organise", APO)*
  - Construir, Adquirir e Implementar *("Build, Acquire and Implement", BAI)*
  - Entregar, dar Servicio y Soporte *("Deliver, Service and Support", DSS)*
  - Supervisar, Evaluar y Valorar *("Monitor, Evaluate and Assess", MEA)*

Gráfico No. 13 - Procesos de Gobierno de TI Empresarial – COBIT 5 (*)

(*) Tomado del documento publicado por la ISACA, "COBIT 5 – Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa" – Figura No.16 – Modelo de Referencia de Procesos de COBIT 5

2.6 COBIT 5 para Evaluar el riesgo relativo a TI

COBIT 5 contempla un marco de referencia para analizar el riesgo de TI y apoyar en su administración. Basado en la Guía de la ISACA "COBIT 5 for Risk" (2013) por ISACA, podemos resaltar varios conceptos de interés para esta Tesis, especialmente en el desarrollo del Capítulo IV, relativo a Riesgos a considerar.

2.6.1 Definición de Riesgo de TI

En la referida Guía de ISACA (2013: 17) se menciona la definición de riesgo en general, de acuerdo a la Norma ISO, Guía 73, "Riesgo se define como la combinación de la probabilidad de un evento o suceso y su consecuencia".

Y se define al riesgo de TI (2013:17), como riesgos de negocios, específicamente los asociados con el uso, propiedad, operación, participación, influencia y adopción de TI (Tecnologías de información) al interior de una empresa. Además menciona que los riesgos de TI consisten en eventos relativos a TI que pueden –potencialmente- impactar el negocio, pueden ocurrir con frecuencia e impactos inciertos, y pueden crear dificultades o retos en alcanzar las metas y objetivos estratégicos.

La Guía de ISACA expresa también que los riesgos siempre existen, ya sean reconocidos o no por la organización, y deben ser considerados como duales, ya que pueden tener un lado tanto positivo como negativo. El riesgo no siempre debe ser evitado, ya que el hacer negocios es el tomar riesgos que sean consistentes con el apetito del riesgo de la empresa. El lado positivo de un riesgo puede representar una oportunidad de nuevos negocios, si es correctamente administrado.

2.6.2 Categorías de Riesgo de TI de acuerdo a COBIT 5

ISACA identifica tres tipos generales de Riesgos de TI en su Guía (2013:17). Los mismos son:

- Riesgos en la Habilitación de los Beneficios / Valor de TI: Asociados con oportunidades perdidas en el uso de Tecnología para mejorar eficiencia o efectividad de los procesos de negocios, o como un habilitador para nuevas iniciativas de negocios. Se los identifica también como Riesgos de tipo Estratégico.
- Riesgos en la entrega de Programas y Proyectos de TI: Asociados con la contribución de TI a nuevas o mejores soluciones de negocios, usualmente en la forma de proyectos y programas como partes de portafolios de inversión. Como ejemplos se puede indicar riesgos en calidad y relevancia de los proyectos, así como Sobre-ejecución de los mismos. Se los puede denominar Riesgos de Ejecución de Proyectos.
- Riesgos de la Operación y entrega de Servicios de TI: Se incluyen los riesgos asociados con todos los aspectos del rendimiento de los Sistemas y Servicios de TI, en las operaciones normales del negocio, los cuales pueden traer destrucción o reducción del valor de la empresa, en caso de materializarse. Como ejemplo de este tipo, podemos mencionar interrupciones del servicio de TI, Problemas en seguridad y Problemas en el cumplimiento de Normas / leyes. Se los identifica como Riesgos Operacionales.

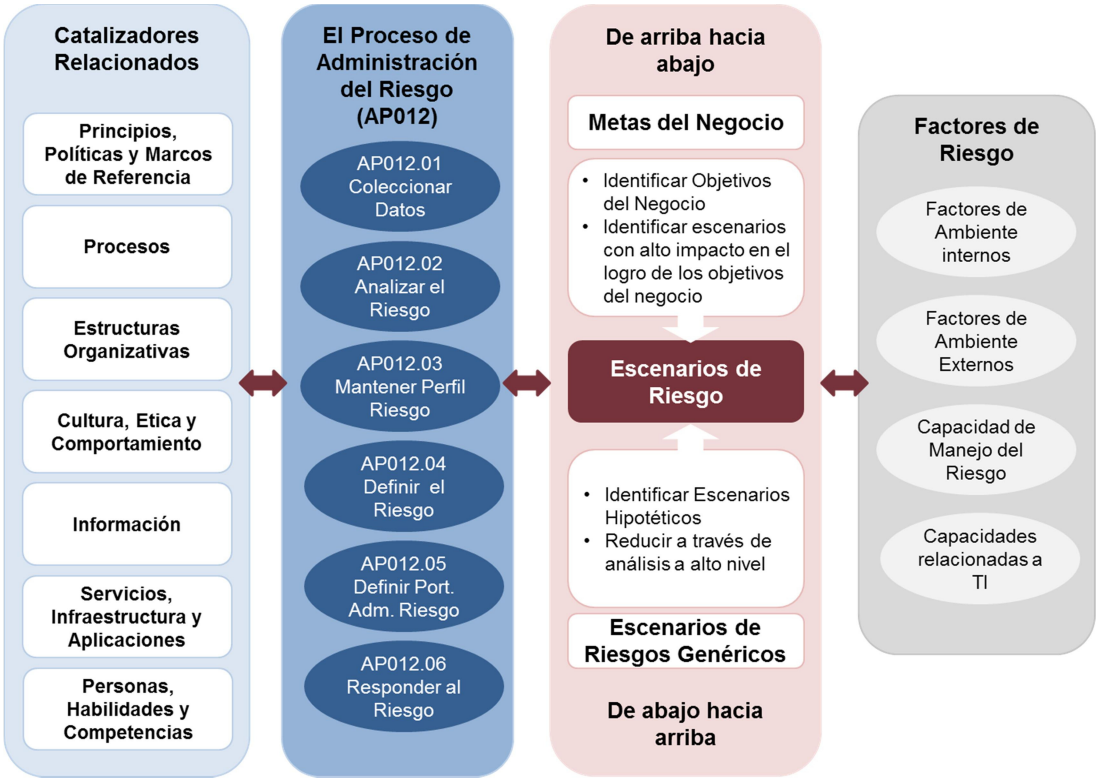
2.6.3 Escenarios de Riesgo de acuerdo a COBIT 5

ISACA establece el concepto de Escenario de Riesgos (2013:67), como una descripción de un posible evento o suceso que, en caso de ocurrir, tendrá un impacto incierto en el logro de los objetivos de la empresa.

COBIT 5 contempla un Proceso para el Manejo de riesgos, el APO12. Aunque para efectos de la Auditoria de Sistemas, el objetivo no es el de

implementar un Proceso formal del Manejo del Riesgo de TI, es de interés el conocer sus componentes, y estar en capacidad de aplicar algunas de sus metodologías, (por ej., recolectar datos y analizar riesgos), para determinar el Riesgo que pueda incidir o afectar al Universo a auditar.

Gráfico No. 14 - Escenario de Riesgos - COBIT 5 (*)



(*) Tomado de la Guía de ISACA "COBIT 5 for Risk" – Figura 34 – Risk Scenario Overview, y traducido libremente

Para construir los escenarios de Riesgos, COBIT 5 recomienda dos mecanismos (2013:59): el primero, partir de las Metas del Negocio en donde se inicia de los objetivos empresariales y se realiza un análisis de los escenarios de Riesgos de TI relevantes y probables; y el segundo, partir de Escenarios genéricos, para tomarlos como base y adaptarlos a las necesidades de la organización.

Estos dos mecanismos son complementarios e idealmente deben de converger en un conjunto de escenarios de Riesgos. Estos escenarios deben considerar los factores de Riesgos, los cuales pueden identificarse como:

- Factores de Ambiente Internos: Mayormente dentro del control de la empresa, aunque pueden no ser fáciles de cambiar
- Factores de Ambiente Externos: Mayormente por fuera del control de la empresa
- Capacidades de Manejo del riesgo: Relativos a la madurez de la empresa en realizar procesos de Manejo del Riesgo
- Capacidades relacionadas con TI: Relativos a la capacidad de los catalizadores identificados en COBIT 5

2.6.3.1 Estructura de los Escenarios de Riesgo de acuerdo a COBIT 5:

COBIT 5 contiene una estructura para que los Escenarios de Riesgos de TI sean eficientemente usados para los propósitos de análisis de Riesgo. Entre los elementos que la conforman están:

- Actores: Quienes generan la amenaza y se aprovechan de una vulnerabilidad. Los actores pueden ser internos (personal dentro de la empresa, ya sea propio o subcontratado), o externos (personas fuera de la empresa, competidores, reguladores, el mercado, etc.).
- Tipo de amenaza: Se refiere a la naturaleza del evento, si es malicioso, accidental, etc.
- Evento o Suceso: El tipo de suceso, que puede referirse a revelación de información confidencial, interrupción de un sistema o proyecto, robo o destrucción, etc.
- Activo o Recurso: Un activo es cualquier elemento de valor para la empresa que puede ser afectado por el evento y conducir a un impacto en el negocio. Un Recurso es cualquier elemento que ayuda al logro de las metas de TI.

- Tiempo: Se refiere a la dimensión donde puede describirse la duración del evento, el tiempo en que ocurre, la velocidad en la detección, el retardo de tiempo entre el evento y su consecuencia, etc.

Gráfico No. 15 - Estructura de los Escenarios de Riesgos - COBIT 5 (*)

(*) Tomado de la Guía de ISACA "COBIT 5 for Risk" – Figura 36 – Risk Scenario Structure, y traducido libremente

2.7 Rol del Auditor Interno con respecto al Riesgo

El IIA en su publicación "The three lines of defense in effective Risk Management and Control / Las tres líneas de defensa en un efectivo control y Administración del Riesgo", (2013), brinda una visión de cuáles deben ser las líneas de defensa en una empresa frente al riesgo, y específicamente el rol que el Auditor Interno puede / debe asumir. Estas líneas son:

- Primera línea de Defensa - La Gestión Operativa, la cual es el principal dueño del riesgo y lo administra. También es la responsable de implementar acciones correctivas para responder ante deficiencias de control y de procesos.

- Segunda Línea de Defensa – Las Funciones de Aseguramiento, establecidas por la alta administración para supervisar / monitorear el riesgo, es decir su objetivo primario es que la primera línea de defensa sea efectiva. Entre las responsabilidades se encuentran el soportar políticas de administración, definir roles, responsabilidades y establecer metas, proveer marcos de referencia para administrar el riesgo, identificar y alertar sobre amenazas, asistir a la administración en el desarrollo de procedimientos y controles para manejar riesgos, entre otros.
- Tercera Línea de Defensa – La Auditoria Interna, la cual, por su independencia de la Administración es la que puede proveer un verdadero aseguramiento independiente, al responder al Comité de Auditoria, y/o la Junta, o Consejo de Administración. La Auditoria Interna provee aseguramiento de la efectividad del gobierno, el manejo del riesgo y los controles internos, incluyendo también la manera en que la primera y segunda línea de defensa logran los objetivos de manejo del riesgo y el control interno.

Gráfico No. 16 - IIA - Las Tres Líneas de Defensa (*)

(*) Tomado del documento publicado por el Instituto de Auditores Internos de España, "Marco de Relaciones de Auditoria interna con otras Funciones de Aseguramiento – Guía Práctica" y haciendo referencia al documento de la IIA, "The Three lines of defense in effective Risk Management and Control"

Es importante el tener claras las distinciones, ya que la Auditoria Interna, frente al riesgo, no debe hacerse “dueña” o responsable del mismo (es de propiedad de la Primera Línea de defensa), ni definir el apetito del negocio, o administrar las herramientas para monitorearlo (función de la Segunda Línea de Defensa), pero si es un elemento clave, que debe ser tomado en cuenta para la planificación de actividades, y de cada tarea de auditoria, al dar opinión sobre la efectividad frente a la administración del riesgo en un Proceso, una actividad, tarea u objeto que se esté auditando. También dentro del rol de Auditoria Interna, se pueden dar recomendaciones para que la Primera y Segunda Línea de defensa mejoren su desempeño con relación al manejo y administración del riesgo.

CAPITULO III

3 IDENTIFICACION DEL UNIVERSO DE TI

De acuerdo al objetivo principal de esta Tesis, el enfoque de la Auditoria de Sistemas a diseñar es el análisis de los componentes y elementos tecnológicos, que sean críticos para los servicios financiero – contables, y los Estados Financieros del modelo de una Aerolínea doméstica en el Ecuador.

Tomando como referencia el Marco Teórico del Capítulo anterior, este Capítulo tiene como objetivo el identificar y sugerir varios elementos para conformar el Universo a Auditar, en términos de Componentes, Sistemas o Aplicaciones, y Procesos.

Una lista definitiva depende siempre de la arquitectura tecnológica de c/empresa y de la estrategia que haya seguido en la provisión de sus servicios tecnológicos, así como de un análisis de otros elementos tales como el nivel de riesgo presente, el interés de la alta gerencia, etc.

Por ejemplo puede haber un nivel de Outsorcing (contratación de servicios tecnológicos a terceros) que la aerolínea haya decidido mantener, y esto influirá en el diseño final de un Plan adecuado de Auditoria de Sistemas / TI.

Para facilidad de seguimiento, se incluirá una Nomenclatura de identificación, de acuerdo al tipo de componente / elemento.

3.1 Componentes y Elementos tecnológicos a considerar en el Plan de Auditoria de Sistemas

Entre los componentes y elementos del Universo probablemente presentes en un Modelo de Negocio de Aerolínea, y que pueden ser de interés para tomarlos en cuenta dentro de un Plan de Auditoria Interna de

Sistemas / TI, se pueden nombrar varios relativos a Infraestructura y Equipos, Redes, Bases de Datos, y Aplicaciones.

Cabe mencionar que en algunos casos, es difícil separar los componentes, o clasificarlos en una única categoría. Por esto es útil visualizarlos como pertenecientes a "Capas", en donde la capa más básica tiende a ser un componente físico o de Hardware, y la capa más alta puede ser un componente de aplicaciones o virtual.

3.1.1. Infraestructura y Equipos

Las labores de Auditoria interna generalmente se concentran en aquellos elementos que son materiales o críticos desde el punto de vista de la empresa. Por eso, y a menos que exista una necesidad específica del negocio, no se suelen considerar en el Plan de Auditorias, equipos de usuario final como de interés individual, pero si pueden ser analizados como parte de un tema mayor (ej. En Análisis de niveles de seguridad informática, si las computadoras en poder de los usuarios finales tienen seguridades específicas tanto físicas como de controles de usuario).

Si suele ser un tema de interés el considerar una auditoria con respecto a los Centros de datos en donde se concentran los principales servicios tecnológicos.

De acuerdo a esto, se pueden sugerir los siguientes elementos a considerar relativos a la Infraestructura tecnológica en una aerolínea:

Tabla No. 3 - Infraestructura - Posibles elementos a considerar dentro de un Plan de Auditoria de Sistemas / TI

ID	Tipo	Detalle
I1	Centro de Datos Principal, o "Data	Típicamente existe por lo menos un Data Center o Centro principal de datos, en donde se encuentran los servidores principales que soportan las

	Center”	aplicaciones críticas, el almacenamiento de las principales Bases de Datos, y los equipos centrales que conforman la red de conexión para que los usuarios de las aplicaciones se conecten. Este se convierte en el centro neurálgico de las Operaciones de TI.
I2	Centro de Datos Secundarios	Podrían existir Mini Data Centers, o Centros Secundarios de Datos, en donde se destinen algunos equipos que sirvan a Unidades de negocio. Ej, un Servidor de Datos que esté localizado físicamente en Quito y sirva para ciertas aplicaciones o repositorio de datos, a los usuarios de la zona Sierra.

Fuente: La Autora / Elaboración: La Autora

3.1.2 Redes

Dado que las aerolíneas tienen múltiples puntos de operación (en los Aeropuertos, Oficinas de Venta de Boletos y Oficinas de venta y administración de Carga), el correcto funcionamiento de las Redes de datos y telecomunicaciones es de vital importancia.

Así también lo es el tema de la seguridad de acceso a las redes de datos, tanto interna como externa.

Entre los posibles elementos de interés desde el punto de vista de Redes se pueden mencionar:

Tabla No. 4 - Redes - Posibles elementos a considerar dentro de un Plan de Auditoria de Sistemas / TI

ID	Tipo	Detalle
R1	Firewalls	Los firewalls (que pueden ser una combinación de hardware y software) protegen a una red de datos de accesos indebidos, por lo que su correcto

		funcionamiento es crítico para la seguridad de datos de la empresa.
R2	vLANs	Dentro de la estructura de redes pueden existir Redes Virtuales o vLANs, en donde se haya segmentado (vía hardware y/o software) y protegido el tráfico de datos para dar prioridad y/o proteger mejor a grupos de aplicaciones & usuarios considerados relevantes.
R3	Paneles o "Rack" de Conexiones	Los puntos de operación de una aerolínea en las diferentes ciudades (tanto en Aeropuertos como en Oficinas de Venta de boletos, y Carga), dependen de una conexión exitosa de las redes de datos y telecomunicaciones hacia su Casa Matriz / Centro Principal de Datos. Esta conexión de redes físicamente tiene un punto crítico en el Panel o "Rack" de conexiones presente en cada uno de ellos.

Fuente: La Autora / Elaboración: La Autora

3.1.3 Bases de Datos

La auditoría de las principales Bases de datos es una de las tareas frecuentemente presente en los Planes del departamento de Auditoria interna, especialmente con relación a las Bases de datos de los Sistemas o aplicaciones contable – financieros, ya que son el repositorio de las transacciones financieras que se consolidan en los Estados Financieros.

Las bases de datos pueden estar asociadas a aplicaciones o sistemas adquiridos, o pueden ser utilizadas en aplicaciones desarrolladas al interior de la empresa.

Algunos de los tipos de Bases de Datos más usados son Oracle, Microsoft SQL Server, etc.

Tabla No. 5 - Bases de Datos - Posibles elementos a considerar dentro de un Plan de Auditoria de Sistemas / TI

ID	Tipo	Detalle
B1	Data Bases o Base de Datos	Bases de datos consideradas críticas para los sistemas financiero – contable, y sistemas relacionados

Fuente: La Autora / Elaboración: La Autora

3.1.4 Aplicaciones o Sistemas

Las Aplicaciones o sistemas son probablemente los elementos fundamentales a considerar dentro del Plan de Auditoria Interna de Sistemas / TI, dado que los servicios de procesamiento de datos e información que requiere la empresa se realizan a través de los mismos.

Las aplicaciones o sistemas pueden haber sido adquiridas a terceros (y ser paquetes estandarizados de aplicaciones), o pueden haber sido desarrolladas por la aerolínea.

También es posible una mezcla, en donde, el “core” o centro sea un paquete de software adquirido, alrededor del cual la aerolínea haya desarrollado customizaciones o programación adicional, para cumplir ciertas funciones especializadas y no consideradas dentro del sistema original.

Es importante mencionar que la arquitectura tecnológica de implementación de los mismos, debe ser un factor a tomar en cuenta para el análisis. Por ej: quizás dé un mayor valor agregado el considerar como de interés para la auditoria un Sistema implementado localmente en la aerolínea - cuya aplicación y Base de datos esté físicamente instalada dentro de la red de la empresa, y la configuración es de responsabilidad exclusiva de la misma -, versus otro Sistema cuya Base de datos y conexión sea externa, es decir sea provisto por un tercero, y exista un contrato en

donde el proveedor se obliga a ciertos niveles de seguridad y calidad. En este caso el análisis podría realizarse sobre la interfase con la que interactúa la aerolínea con el proveedor, o sobre el nivel del servicio en general (calidad, seguridad, desempeño, servicio al cliente, etc.), que el proveedor y su Software estén proveyendo.

De acuerdo al énfasis de esta Tesis en análisis de Sistemas/TI que sean críticos para los Estados financieros, se sugiere dos clasificaciones generales para identificar las posibles Aplicaciones a incluir como de interés para la auditoria:

A. **Aplicaciones Financieras – Contables:** Las que han sido desarrolladas para realizar tareas o procesos financieros y/o contables, manejan las transacciones contables en detalle, e inciden directamente en la generación de los Estados Financieros, o los generan; y
B. **Otras Aplicaciones con incidencia en los Estados Financieros:** Las que, si bien su función primaria no es la financiera – contable, tienen sub-módulos dedicados a la contabilidad, o el Departamento Financiero de la aerolínea extrae información relevante / material para alimentar sus Estados Financieros.

A continuación se analizará más en detalle la identificación de los Sistemas, tomando como base la categorización sugerida:

3.1.4.1 Análisis de las Aplicaciones Financieras – Contables

El listado de Sistemas como candidatas a analizar depende de la arquitectura tecnológica y de aplicaciones que tenga cada aerolínea. Sin embargo, se pueden mencionar como probablemente presentes los siguientes tipos de sistemas Financiero - Contables:

- **ERP Financiero – Contable:**

  Un componente indispensable en el Plan de Auditoria de Sistemas, debe ser el analizar el Sistema Contable principal, que elabora los Estados Financieros de la aerolínea.

  Estos sistemas se los suele denominar ERPs, debido a que pueden abarcar varias funciones, ya sea del área Financiera o de otras funciones.

  Usualmente los paquetes de ERPs contienen no sólo el módulo del libro principal (o GL: General Ledger), sino también varios módulos que lo alimentan, tales como Cuentas por Pagar (AP: Accounts Payables), Cuentas por Cobrar (AR: Accounts Receivables), Activos Fijos (FA: Fixed Assests), etc.

  Entre algunos de los principales ERPs usados en la industria, se pueden mencionar SAP, Oracle E-Business Suite, Oracle JD Edwards y Microsoft Dynamics. Sin embargo algunas aerolíneas pequeñas pueden considerar utilizar algún software contable que esté ajustado a las Normas Contables y Tributación local, si es que la mayoría de sus operaciones están basadas en un país o región específico.

- **Sistema de Revenue Accounting o Control de Ingresos:**

  Dada las particularidades del transporte aéreo de pasajeros, hay que tener un registro de cada segmento de vuelo vendido y cuándo se vuela (momento en el cual se reconoce el ingreso contable de acuerdo a normas IFRS).

  Un boleto aéreo puede tener uno o más segmentos (ej: un pasaje GYE-UIO- GYE tiene dos segmentos o tramos de vuelo: GYE-UIO y UIO-GYE). O puede haber un componente de vuelo

internacional en el segmento, ya sea con la propia aerolínea, o con aerolíneas asociadas que tengan convenios de código compartido. (ej: MIA-GYE-GPS-GYE-MIA: Un boleto de Miami, con escala en Guayaquil, pero con destino final a Galápagos, ida y vuelta. Hay 2 segmentos internacionales, y 2 nacionales)

En el Ecuador, así como en la mayoría de los países de la región Latinoamericana, el Boleto Aéreo o pasaje es factura legal.

Mientras el boleto haya sido vendido, pero no esté volado, el registro contable de la Venta está en el Balance, y se lo registra como un pasivo (una obligación de la empresa a prestar un servicio en el futuro).

Estas particularidades entre otras, exigen un tipo de software especializado, conocido como Sistema de Revenue Accounting o Control de Ingresos, que esté preparado para leer la “mascarilla” de los boletos o formato internacionalmente reconocido para las aerolíneas.

Adicional a la venta de boletos existen otros servicios por los que las aerolíneas pueden cobrar, tales como exceso de equipajes, penalidades por cambio de fechas, servicios de acompañante, transporte de mascotas, etc., los cuales también pueden ser manejados por este tipo de software.

Entre otras funciones que pueden realizar estos sistemas están:

- Control de la tarifa del boleto por segmento o vuelo
- Control y registro de las comisiones de venta, en caso de ventas vía agentes o terceros
- Control y registro de los tipos de venta por boleto: cash, tarjeta de crédito, tarjeta de débito, redención de millas, otros

- Control y registro de los impuestos de venta si aplican
- Control y registro de la venta por punto de venta
- Control y registro de los impuestos y tasas aeroportuarias si aplican
- Control y registro del write-off: Cuando un boleto ha sido vendido y no ha sido utilizado, generalmente se reconoce el ingreso un año después
- Carga y registro de las Ventas de Canales indirectos tales como los provenientes de BSP-Iata, CASS-Iata, o GSAs

La industria suele usar sistemas especializados para este fin, tales como RAPID (de Mercator), AirMax (de Sabre), etc.

- **Sistema de Manejo de órdenes de compra – Bienes y Servicios No aeronáuticos:**

Este tipo de aplicación puede ser parte del ERP Financiero – Contable, o ser un sistema independiente, que, por alguna interfase, alimente al ERP.

El objetivo del mismo suele ser el manejo de los procesos de compra de bienes y servicios considerados no aeronáuticos, es decir, activos que no son componentes (piezas y partes) de los aviones. Esta separación entre Activos aeronáuticos y No Aeronáuticos es propia de la industria, ya que por su complejidad y criticidad los bienes Aeronáuticos suelen ser manejados por Sistemas especializados.

Los Sistemas de Manejo de órdenes de compra pueden comprender funciones tales como creación de la orden de compra, autorización de la orden de compra, y registro de la entrega o aceptación del bien o servicio, entre otros.

- **Otros Sistemas Financiero – Contables:**

Aparte de los tipos de Sistemas mencionados, otras aplicaciones pueden ser parte del Universo tecnológico dedicado a tareas del área financiera, ya sea que sean soluciones adquiridas (compradas a terceros) o producto de un desarrollo interno.

El hecho de incluirlas o no en un listado de sistemas de interés para la auditoria interna, dependerá del nivel de impacto sobre los Estados Financieros, el interés de las partes interesadas / la alta administración, y algunos otros factores que el auditor de sistemas tome en consideración al momento de diseñar su Plan de actividades.

Algunos de estos podrían ser:

- Sistema de Conciliaciones Bancarias: Dedicado a conciliar los movimientos de las Cuentas Bancarias de la aerolínea (Depósitos versus Pagos).
- Sistema de Control de Provisiones Contables: Dedicado a controlar las provisiones técnicas de una aerolínea, especialmente las relativas a gastos de las Operaciones de vuelo (Navegación Aérea, Comunicaciones Tierra – Aire, Hoteles de Tripulación, etc.) y Operaciones Terrestres (Aterrizajes, Estacionamiento, Uso de Mangas o Puentes de Abordaje, Servicio de Rampa, etc.); y mantener una conciliación entre la provisión contable y el gasto real cuando se genera.
- Sistema de análisis de Datos Financieros: Enfocado a la gestión de la información financiera y generación de reportes para toma de decisiones gerenciales (rentabilidad de rutas, rentabilidad de productos, etc.)
- Sistema de Control de Presupuesto: Dedicado a la creación, y administración del Presupuesto anual de la aerolínea.

- Sistema de Control de Viáticos: Para administrar los gastos de viaje de personal operativo y/o de personal administrativo.

Un resumen de los Sistemas Financiero – Contables mencionados se presenta a continuación. Para efectos de la Tesis se estará considerando los elementos identificados como de probable interés principal.

Tabla No. 6 - Sistemas Financiero - Contables - Posibles elementos a considerar dentro de un Plan de Auditoria de Sistemas / TI

ID	Tipo	Detalle
S1	ERP Contable-Financiero	Software que lleva los registros contables de la aerolínea y produce los Estados Financieros
S2	Sistema de Revenue Accounting	Sistema dedicado al Control del registro de los ingresos de la aerolínea, por segmento, punto de venta, tipo de venta, producto, etc.
S3	Sistema de Compras - No Aeronáuticas	Sistema que controla el proceso de Órdenes de compra

Fuente: La Autora / Elaboración: La Autora

3.1.4.2 Análisis de otras Aplicaciones con incidencia en los Estados Financieros

Tomando como benchmarking los Estados Financieros e información relevante de algunas aerolíneas públicas con presencia en la región latinoamericana, y/o con operaciones en Ecuador, (tales como Avianca, Copa, Lan, y Volaris), podemos sacar deducciones de cuáles tipos de Sistemas o Aplicaciones No Financieras - Contables, aparte de los ya mencionados en el segmento anterior, podrían impactar de manera relevante el Estado Financiero.

Los sistemas presentes en esta categoría tienen otras funciones primarias, tales como control de mantenimiento, control de activos aeronáuticos, etc., pero, o presentan algún módulo / sección con el reflejo de sus actividades específicas en transacciones contables, o generan reportes los cuales son tomados como base por el Departamento Financiero – Contable para alimentar transacciones en los ERPs contables.

Las aerolíneas a ser mencionadas en esta Tesis, por ser públicas (cotizar en bolsas locales y/o internacionales, tales como NYSE – New York Stock Exchange), tienen como obligación el presentar su Información Financiera, incluyendo Estados financieros e información relevante, la cual puede ser libremente consultada por el público en general, ya sea en sus WebSites Corporativos, o sino en los portales de las Bolsas de valores en donde cotizan y organismos de control.

Cabe resaltar que cada aerolínea, de acuerdo a su estrategia y modelo de negocios tendrá un esquema propio de ingresos, costos, activos, etc.; sin embargo, existen tendencias que se pueden usar para comprender a la industria.

3.1.4.2.1 Análisis tomando como base los Ingresos Operativos

En las aerolíneas de Transporte Comercial de pasajeros, se percibe que el principal ingreso Operativo es el de Venta de boletos a Pasajeros, representando más del 80% de los mismos. (Ver Gráfico No. 1, Ingresos Globales 2010 a 2014 F – Aerolíneas Comerciales).

En nuestra región latinoamericana, por ejemplo, para Avianca y Copa, ese porcentaje se incrementa a 84% y 97%. (Ver Gráfico No. 17)

Otros Ingresos Operativos pueden ser:

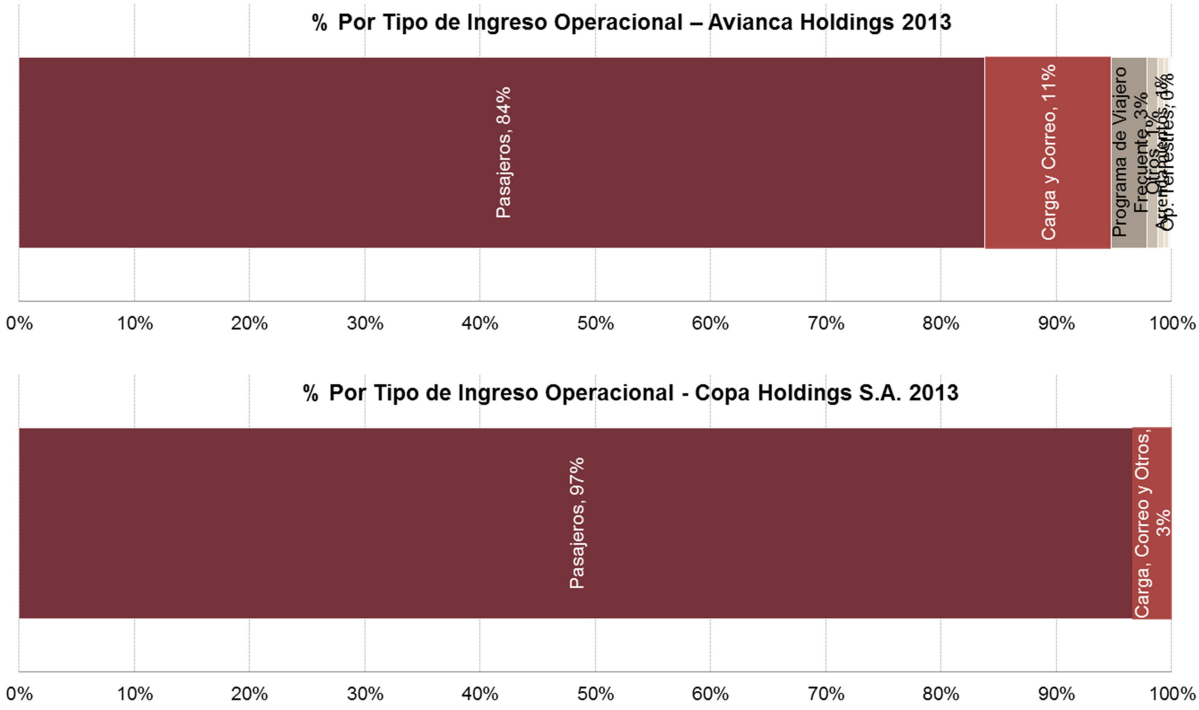
- Venta de Servicios de Carga y/o Correo: Transporte de productos perecederos y no perecederos, ya sea en los “bellys” o panzas de los

aviones, o en aviones dedicados como cargueros, y/o Transporte de documentos / paquetes pertenecientes a correos del país

- Venta de Servicios Complementarios: Tales como atención a otras aerolíneas (Servicios de Mantenimiento, atención en rampa, etc),
- Venta de Millas: Ventas relacionadas con el producto de Lealtad o Millas

Para el ejercicio de esta Tesis, se estará enfocando el análisis en las aplicaciones relacionadas al negocio de Pasajeros.

Gráfico No. 17 - % Tipo de Ingreso Operacional 2013 - AV y CM (*)



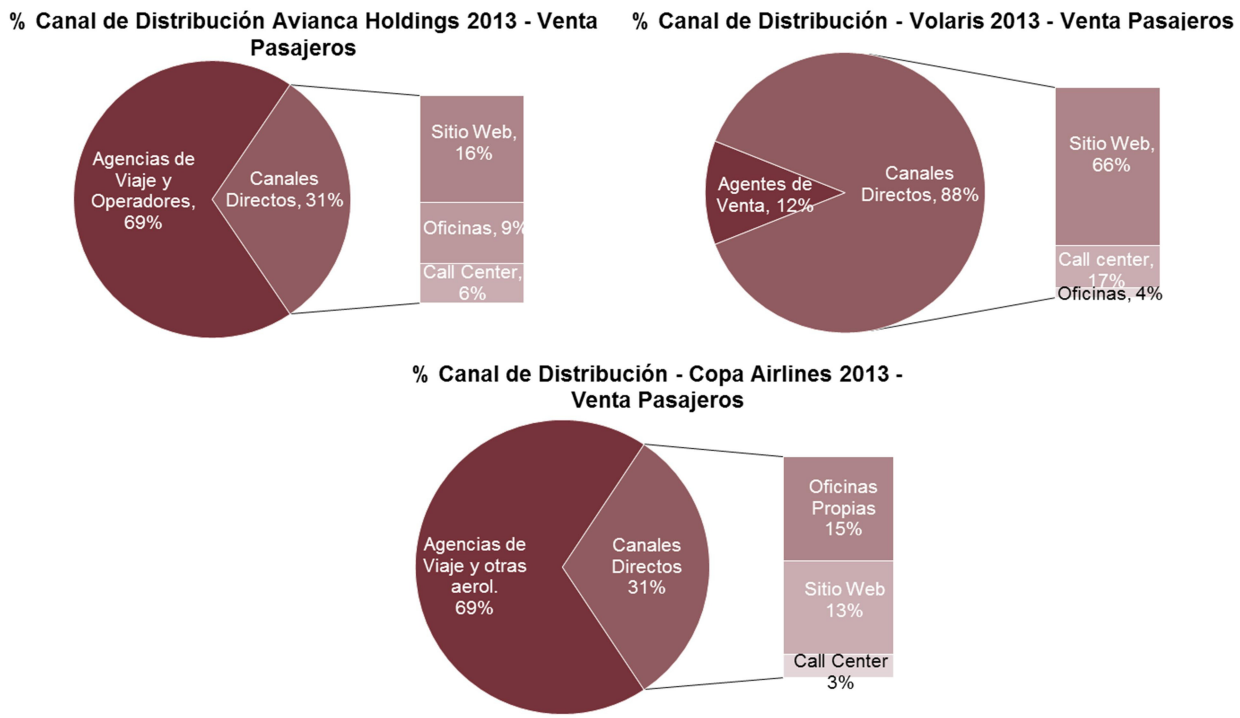
(*) Datos preparados en base a los Formularios F-20 enviados por las aerolíneas que cotizan en Bolsa de New York, a la SEC (Security Exchange Commision) (www.Sec.gov), correspondiente al año 2013

En cuanto a los Canales de distribución, para la Venta de Tiquetes a Pasajeros, se puede mencionar los siguientes tipos de Canales:

- Venta Indirecta: Vía Agencias de Viaje, Operadores Turísticos, etc
- Venta Directa:
    - En Oficinas propias, ya sean CTOs (City Ticketing Office por sus siglas - Oficina de Venta de tiquetes), o ATOs (Airport Ticketing Office – Oficinas de Venta en Aeropuertos)
    - Vía Call Center
    - Vía WebSite
    - Por Agentes exclusivos de Venta o GSAs: Agentes de venta que tienen un contrato de representación/Venta exclusiva de una aerolínea

Comparando aerolíneas tales como Avianca, Copa o Volaris, se tiene que la estrategia de c/negocio incide en el porcentaje del Canal de Distribución.

Gráfico No. 18 - % de Venta de Boletos por Canal de Distribución (*)



(*) Datos preparados en base los Formularios F-20 enviados por las aerolíneas que cotizan en Bolsa de New York, a la SEC (Security Exchange Commision) (www.Sec.gov)

De acuerdo al análisis presentado de Ingresos Operativos, podemos identificar los siguientes Sistemas o aplicaciones que probablemente estarán presentes en el modelo de negocio de una Aerolínea doméstica en el Ecuador:

- **Sistemas de Venta on-line (WebSite):**

  Entre los Canales de venta directa se puede encontrar el Sistema de venta vía Internet, o plataforma E-Commerce. Típicamente el "hosting" o almacenamiento de la aplicación y su apertura a internet, son proporcionados por algún proveedor especializado.

  Dado que existe una tendencia a que este canal de venta se siga incrementando, resulta de interés incluirlo en los Planes de Auditoria de Sistemas. Aparte de poner el producto más cerca y a disposición de los Pasajeros 24/7 [3], es más ventajoso para la aerolínea ya que no hay un gasto de comisión asociado al mismo.

  Adicionalmente el WebSite podría proporcionar otras funciones, tales como chequeo en línea, consulta de estado de vuelos, etc.

  En el Gráfico No. 18 se presentan porcentajes de venta vía WebSite que van desde el ~13% de Copa Airlines, hasta el ~66% para Volaris, una aerolínea regional Mexicana.

- **Sistemas de Venta en Oficinas Propias:**

  Este tipo de Sistemas puede interactuar con algún sistema de reserva, y presentar una interfase adaptada a los intereses de la aerolínea.

[3] *24/7 es usado para indicar que un servicio o atención está disponible las 24 horas al día, los 7 días de la semana*

O las aerolíneas pueden decidir utilizar algún sistema desarrollado internamente, para controlar la Venta en sus puntos de venta propios, típicamente en CTOs y ATOs.

La función de estos sistemas es el de registrar la venta, controlar los tipos de pago, generar los comprobantes necesarios, y manejar un cierre diario (o periódico) de las ventas del punto de operación / cajero, con conciliación de los depósitos.

- **Sistemas de Reservación (GDS – Global Distribution System):**

Los sistemas utilizados para mostrar el inventario de sillas disponibles de las aerolínea (la oferta), son conocidos como GDS o Sistemas de Distribución Global. Estos pueden ser parte de un conjunto de sistemas denominado de atención a los Pasajeros.

Los GDSs suelen ser usados por las agencias de ventas, aerolíneas y otros vendedores, y facilitan su interacción con el proceso de facturación y cobro de BSP-IATA[4].

Se pueden nombrar como los líderes de este tipo de aplicaciones a Sabre, Amadeus, Galileo y WorldSpan.

Sin embargo una aerolínea pequeña puede escoger otro sistema para su interacción con agentes de venta. La desventaja de esto es que al no usar los GDSs internacionales es difícil o imposible acceder al Sistema de Facturación y Cobro de BSP – IATA, y los vuelos no serían visibles a nivel internacional (no estarían en los sistemas) para su venta por cualquier agencia afiliada a IATA.

[4] *BSP, por sus siglas, "Billing and Settlement Plan", es un sistema administrado por la IATA, diseñado para facilitar y simplificar la venta, reporte, facturación y cobranza, entre los agentes de venta acreditados, y las aerolíneas asociadas. De acuerdo a IATA, al 2013 el sistema se extiende a 179 países y comprende aprox. 400 aerolíneas (www.iata.org/services/finance/bsp/)*

Desde el punto de vista de Auditoria de Sistemas puede ser interesante la interfase o conexión de los Sistemas propios de la aerolínea con los GDSs. O si el sistema usado está implementado localmente y/o es de desarrollo propio, puede ser considerado como de interés para realizar una auditoría más a fondo.

3.1.4.2.2 Análisis tomando como base los Gastos Operativos

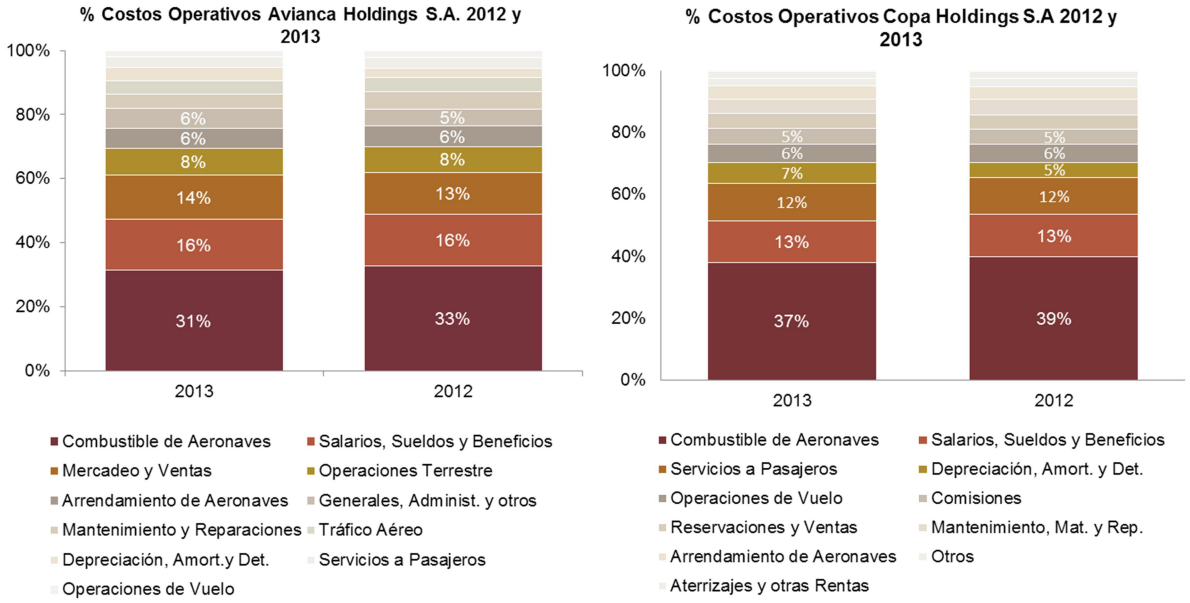
Si bien la estructura contable específica de una aerolínea en tema de los Estados Financieros, y en especial los Gastos del Estado de Resultados puede variar, dependiendo de las leyes en donde se tenga que presentar los Estados Financieros, las normas contables consideradas en la elaboración de los mismos (ej, USGAAP, IFRS, o Normas Contables locales) y otros factores, se pueden identificar tendencias comunes.

Por ejemplo, el combustible, que es el principal gasto operativo de una aerolínea, suele tener una clasificación bastante similar y es muy visible en los Estados Financieros de aerolíneas públicas.

Otros gastos podrían variar en la agrupación de cuentas que la aerolínea use, y es preciso un análisis a fondo de los Estados Financieros, sus notas de soporte y otras fuentes de la aerolínea, para realizar comparaciones exactas.

Basado en los Estados de Resultados 2012 y 2013, de Avianca (Ver Anexo No. 1: Estado Financiero de Resultados Avianca Holdings S.A.) y Copa (Ver Anexo No. 2: Estado Financiero de Resultados Copa Holdings S.A.), los principales Gastos Operativos presentes se pueden identificar como: Combustible de Aeronaves, Salarios, Sueldos y Beneficios, Mercadeo y Ventas, Servicios a Pasajeros, y Op. Aéreas y terrestres, entre otros.

Gráfico No. 19 - % de Gastos Operativos (*)



(*) Datos preparados en base a los Formularios F-20 enviados por las aerolíneas que cotizan en Bolsa de New York, a la SEC (Security Exchange Commision) (www.Sec.gov), correspondiente al año 2013

La estrategia que escoja la aerolínea influenciará varios de los gastos. Por ejemplo, si la flota en un porcentaje significativo es arrendada, el gasto de Arrendamiento de aeronaves será alto. O si hay un alto porcentaje de la venta de boletos que se realiza vía canales indirectos (agencias de viaje, operadores turísticos, etc.), el gasto de Comisiones será un rubro importante en el Estado de Resultados.

De acuerdo al análisis presentado de Gastos Operativos, podemos identificar los siguientes Sistemas o aplicaciones que tienen una alta probabilidad de estar presentes en el modelo de negocio de una Aerolínea doméstica en el Ecuador:

- **Sistemas asociados al Control de Combustible:**

  El control del Combustible en las aerolíneas es una tarea que abarca varios frentes: por ejemplo uno de los principales se refiere al control en la propia aeronave, supervisado por los pilotos. Otros

controles pueden ser el realizar las maniobras más óptimas para la aproximación de la aeronave, el optimizar las rutas de vuelo, etc.

Pero también puede existir algún Sistema, conjunto de controles financieros, o manejo de provisiones, encargado específicamente de velar por la correcta representación de este gasto en el Estado de Resultados, controlar la correcta facturación del mismo de acuerdo a los precios negociados con los proveedores, reportar índices por fuera de los niveles esperados del consumo, etc.

Dependiendo del tipo de herramientas tecnológicas a nivel de Sistemas presentes para controlar este gasto, y de la apreciación del nivel de riesgo de TI, puede ser de interés de la Auditoria Interna el incluirlo en sus Planes.

- **Sistema de Nómina:**

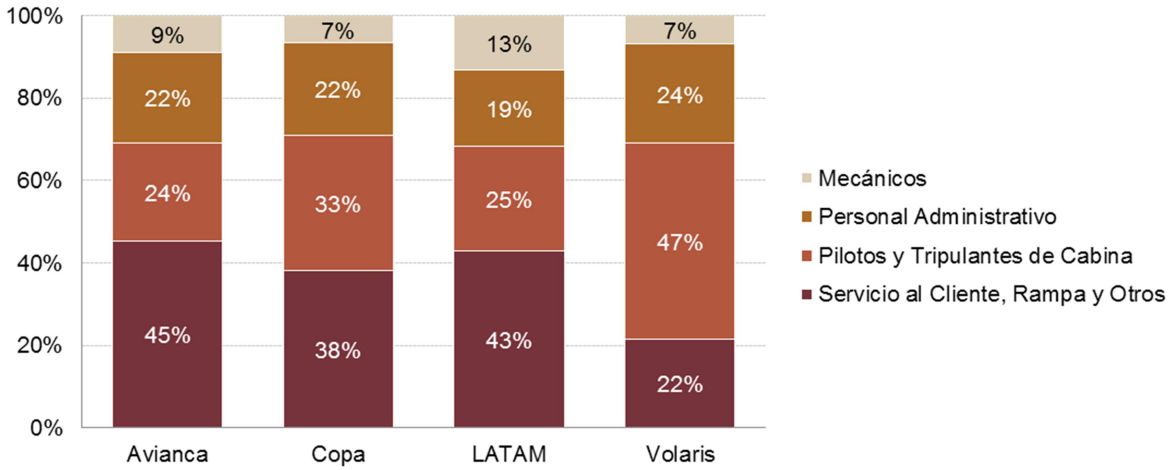
Otro rubro significativo de los costos de la Aerolínea se encuentra en el costo del Recurso Humano, que abarca tanto lo concerniente a la tripulación como al resto del personal operativo y administrativo.

Este sistema puede ser específico para el cálculo de la planilla y los impuestos correspondientes así como las cargas sociales, o puede formar parte de un ERP de Gestión del Talento Humano, que contenga otras funciones relativas a la administración de este recurso.

Es posible que se encuentren otros Sistemas asociados, para administrar rubros relativos a la tripulación, tales como Perdiems o Viáticos, en donde, dependiendo de las leyes de los países, los mismos podrían ser considerado parte de los salarios.

Una comparación del peso de distribución del Personal en varias aerolíneas se puede apreciar en el siguiente Gráfico:

Gráfico No. 20 - % de Tipo de Empleados - 2013 (*)



(*) Datos preparados en base a los Formularios F-20 enviados por las aerolíneas que cotizan en Bolsa de New York, a la SEC (Security Exchange Commision) (www.Sec.gov), correspondiente al año 2013

- **Sistemas asociados al Control de gastos de Operaciones Terrestres y Aéreas:**

  En las Operaciones Terrestres (Bienes y Servicios relativos a las operaciones en tierra) y las Operaciones Aéreas (Bienes y Servicios prestados durante el vuelo o relativos al vuelo), la naturaleza del gasto puede surgir ya sea por cada Pasajero (Tasas Aeroportuarias por Pasajero volado, Comidas a bordo, etc.), por cada avión (tarifas de aterrizaje y estacionamiento, por tipo de avión, etc.), o por cada vuelo (uso del Puente de abordaje, servicios de navegación aérea, etc.).

  En estos casos los proveedores típicos son los Aeropuertos, entidades en control del espacio aéreo y que prestan servicios de apoyo a la navegación, proveedores de Servicio a Bordo (Catering, Entretenimiento, Limpieza de las aeronaves), DGAC, etc.

Y las facturas presentadas pueden ser complejas de analizarlas. Algunas aerolíneas podrían contar en su modelo de negocios con algún tipo de herramienta de Sistemas, que le permitan revisar y controlar los gastos, tanto para efectos contables (asegurar la calidad del registro contable a través de provisiones), como para efectos financieros (asegurar que la facturación es correcta y/o estar en capacidad de presentar reclamos en caso de que existan transacciones incorrectamente facturadas).

Si existe algún tipo de Sistemas dedicado a estos fines, podría ser de interés el incluirlos en el listado de Aplicaciones a auditar.

3.1.4.2.3 Análisis tomando como base los Activos y Pasivos

Al analizar los Activos y Pasivos generalmente presentes, se pueden presentar los siguientes tipos de Sistemas o Aplicaciones:

- **Sistemas MRO ("Maintenance, Repair and Overhaul"):**

  A nivel de la Industria Aérea, los principales Activos suelen ser los relativos a la operación aeronáutica: los aviones y las piezas y partes aeronáuticas gastables (de un solo uso) y rotables (de un uso prolongado en donde la pieza se puede reparar / rehusar, por ej., los motores). Los mismos podrían llegar a representar un porcentaje significativo del total de Activos en el Balance. Además los gastables se reflejan en los Costos de Mantenimiento al momento de su uso, el cual tiene un porcentaje visible en el Estado de Resultados.

  Los sistemas dedicados al control de la logística relativa al mantenimiento y reparación de los aviones se los conoce como MRO ("Maintenance, Repair and Overhaul). Los mismos pueden llegar a ser un ERP, con múltiples funciones tales como:

  - Control de los mantenimientos de aviones
  - Control de la configuración técnicas de los aviones

- Control y trazabilidad de las piezas y partes, tanto las instaladas en los aviones como las que constan en los inventarios físicos, que es una función altamente regulada en la industria
- Compra de materiales aeronáuticos
- Manejo de órdenes de reparación, etc.

Estos Sistemas suelen contar con un sub módulo que genera movimientos contables y alimenta al ERP contable - financiero.

Algunos fabricantes conocidos en la industria son: SAP, Oracle, RAMCO, AMOS, etc.

- **Sistemas de Control de Millas – Programa de Lealtad:**

Actualmente se suele esperar que una aerolínea tenga algún programa para incentivar la lealtad de sus pasajeros. Estos tipos de programas se conocen como de Lealtad o de Millas, en donde la aerolínea otorga una equivalencia en Puntos o Millas por los vuelos, ya sea en base a la distancia volada, al costo del boleto o algún otro parámetro relevante.

A medida que se acumulan los puntos o Millas, el cliente frecuente puede, al llegar a los niveles establecidos por la aerolínea, cambiarlos o redimirlos, ya sea por boletos gratis, o sino por servicios adicionales tales como maletas extras, no pago de penalidad por cambio de fecha, etc. En algunos casos, las aerolíneas ofrecen también un catálogo de productos o servicios varios (ej. Artículos eléctricos, noches de hotel, entre otros) redimibles por las Millas / Puntos.

La aplicación podría incluir el acceso vía Internet y/o tener un Website para facilitar que los Clientes frecuentes administren sus Cuentas de Millas / Puntos.

Los sistemas dedicados a estos Programas se conocen como Sistemas de Lealtad, y pueden ser o soluciones adquiridas a terceros, desarrollos internos o una mezcla de ambos tipos.

Entre las funciones que suelen brindar están:

- Venta de Millas: Cuando el cliente compra a un valor previamente establecido, una cantidad de Millas adicionales, y las acredita a su cuenta.
- Creación y Administración de Cuentas de Millas: Administración de las cuentas que cada Pasajero frecuente tiene con la aerolínea, con reportes periódicos de los acumulados, acreditación por segmentos de vuelo volados, etc
- Redención de Millas por boletos, o productos y servicios: Compra de boletos o productos / servicios, recibiendo como forma de pago, las Millas que el Pasajero frecuente tenga en su cuenta.

Resumiendo los sistemas mencionados, correspondientes a Aplicaciones no financieras – contables, podemos señalar los siguientes como de probable interés para el Departamento de Auditoria Interna de una aerolínea regional:

Tabla No. 7 - Sistemas No Financiero - Contables - Posibles elementos a considerar dentro de un Plan de Auditoria de Sistemas / TI

ID	Tipo	Detalle
S4	Sistema de Venta On-line / WebSite	Aplicativo que administra la Venta directa vía Internet, a través del Portal Corporativo de la aerolínea
S5	Sistemas de Venta en Oficinas	Sistemas “front-end” que permiten / facilitan la operación de venta en los Puntos propios (CTOs y ATOs), y la conciliación entre la venta y el

	Propias	depósito
S6	GDS – Sistemas de Reserva	Sistemas que brindan la información del inventario de sillas para su reserva y venta
S7	Sistemas de Control del Combustible	Sistemas o Herramientas que apoyan en el control del registro contable y la administración del gasto del Combustible
S8	Sistemas de Nómina	Sistemas o ERPs de Gestión Humana, que realizan el cálculo de la Nómina: Salarios, Impuestos asociados y Cargas Sociales, entre otras funciones
S9	Sistemas de Control del Gasto de Operaciones Aéreas y Terrestres	Sistemas de apoyo en la administración, registro de las provisiones y conciliación de la misma, relativo a los Gastos de Operaciones Aéreas y Terrestres
S10	MROs	Sistemas de administración y control de los activos aeronáuticos (gastables y rotables)
S11	Sistema de Programas de Lealtad	Sistemas dedicados a la administración y posterior registro contable de los puntos o Millas ofrecidos por la aerolínea

Fuente: La Autora / Elaboración: La Autora

3.2 Procesos de Gobierno y Gestión de TI a considerar en el Plan de Auditoria de Sistemas

Basados en el Marco de Trabajo de COBIT 5 descrito brevemente en el Capítulo II, y que cuenta con 37 procesos relativos a Gobierno y Gestión de Sistemas / IT, se pueden seleccionar varios en los cuales enfocar las actividades de las Auditorias de Sistemas / TI.

Si bien todos los Procesos son relevantes, y contribuyen a reforzar y desarrollar dentro de un marco de control los bienes y servicios de TI, ciertos temas tales como Seguridad, Administración de los Cambios, etc., suelen estar en los primeros lugares de preocupaciones de los accionistas / partes interesadas / Alta Administración.

A continuación se sugieren una lista de Procesos o Temas a considerar como de interés para las actividades de Auditoria Interna. Esta lista está basada en sugerencias dadas por los artículos de ISACA, publicados en su Revista Journal: “Critical Information Systems Processes” (Volumen 2, 2014), y “The Minimun IT controls to Assess in a Financial Audit” (Volumen 2, 2010).

- **Administración de los Cambios:**

  Los Sistemas o Aplicaciones raramente son estáticos. Continuamente existen mejoras al código o programación, instalación de “parches” para corregir errores, nuevas funciones añadidas, funciones modificadas por necesidades de los Clientes, nuevas versiones de los softwares desarrolladas, etc.

  Y cada vez que se produce un cambio o modificación del software o las estructuras de datos, el mismo debe ser implementado de una manera controlada, para asegurar que no exista algún compromiso en la seguridad de los datos, y minimizar riesgos de afectaciones a otros sistemas / estructuras.

  Dentro del Marco de COBIT 5, el Proceso de Gestión que puede apoyar en la auditoria es el BAI06 – Gestionar los Cambios. En la guía provista por ISACA, “COBIT 5 – Procesos Catalizadores” (2012), podemos encontrar una descripción del proceso, metas, indicadores, prácticas sugeridas, etc. Esto podrá ayudar en la revisión de auditoria, sobre los elementos del Universo tecnológico escogido.

Gráfico No. 21 - BAI06 - Gestión de Cambios COBIT 5 - Descripción, Metas e Indicadores (*)

BAI06 Gestionar los Cambios	Área: Gestión Dominio: Construir, Adquirir e Implementar
Descripción del Proceso Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.	
Declaración del Propósito del Proceso Posibilitar una entrega de los cambios rápida y fiable para el negocio, a la vez que se mitiga cualquier riesgo que impacte negativamente en la estabilidad e integridad del entorno en que se aplica el cambio.	

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Los cambios autorizados son realizados de acuerdo a sus cronogramas respectivos y con errores mínimos.	• Cantidad de trabajo rehecho debido a cambios fallidos • Reducción en el tiempo y esfuerzo necesarios para aplicar los cambios • Número y antigüedad de peticiones de cambio en cartera
2. Las evaluaciones de impacto revelan el efecto de los cambios sobre todos los componentes afectados.	• Porcentaje de cambios sin éxito debidos a evaluaciones de impacto inadecuadas
3. Todos los cambios de emergencia son revisados y autorizados una vez hecho el cambio.	• Porcentaje sobre el total de cambios que corresponde a cambios de emergencia • Número de cambios de emergencia no autorizados una vez hecho el cambio
4. Las principales partes interesadas están informadas sobre todos los aspectos del cambio.	• Ratios de satisfacción de las partes interesadas con las comunicaciones de los cambios

(*) Tomados de la Guía de ISACA, COBIT 5 - Procesos Catalizadores- BAI06 – Gestionar los cambios

- **Seguridad de la Información:**

Los datos o Información de una empresa representan un Activo importante, al cual hay que protegerlo, tanto de ataques externos como de ataques internos, que puedan llegar a comprometer la seguridad y confiabilidad de las operaciones o la capacidad de la empresa para brindar sus productos y servicios a los clientes.

Este es uno de los Procesos en los cuales se debe mantener un análisis continuo de los riesgos, para poder estar preparados en caso de una eventualidad relativa a seguridad de la información.

Dentro de COBIT 5 se encuentra el Proceso APO13 – Gestionar la Seguridad, la cual puede proporcionar una referencia para el análisis de la Auditoria. En la guía provista por ISACA,

"COBIT 5 – Procesos Catalizadores" (2012), podemos encontrar la siguiente descripción del Proceso así como sugerencias de Metas e Indicadores a considerar:

Gráfico No. 22 - APO13 - Gestionar la Seguridad COBIT 5 - Descripción, Metas e Indicadores (*)

APO13 Gestionar la Seguridad	Área: Gestión Dominio: Alinear, Planificar y Organizar
Descripción del Proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.	
Propósito Mantener el impacto y ocurrencia de los incidentes de la seguridad de la información dentro de los niveles de apetito de riesgo de la empresa.	

Objetivos y Métricas del Proceso	
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos •Número de incidentes relacionados con la seguridad
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa • Número de soluciones de seguridad que se desvían del plan • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad • Número de incidentes de seguridad causados por la no observancia del plan de seguridad • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad

(*) Tomados de la Guía de ISACA, COBIT 5 - Procesos Catalizadores- APO13 – Gestionar la Seguridad

- **Administración de los ambientes físicos relacionados a TI:**

En la arquitectura tecnológica de las aerolíneas probablemente existan físicamente puntos críticos para la prestación de los Servicios de TI, en donde se concentre una cantidad de equipos / Hardware, tales como en los Centros de Datos, en los Racks de comunicaciones, etc.

Si esos puntos críticos tienen alguna interrupción en la provisión de sus servicios, probablemente gran parte o toda la empresa se verá afectada. Por lo tanto es importante el mantener una correcta administración del ambiente físico de TI considerado prioritario.

- **Capacidad de continuidad de los servicios de TI:**

  Dado que la labor de las aerolíneas es constante, en algunos casos llegando a ser 24/7, los servicios tecnológicos considerados como críticos para las operaciones y con énfasis en aquellos que afecten los Estados Financieros, deben poder asegurar un nivel de disponibilidad, es decir, un porcentaje suficiente en el que los mismos estén disponibles, con niveles de servicio mínimos para poder continuar con las labores.

  Dentro de este aspecto se puede analizar además la calidad de los Procesos de Respaldo y recuperación, de aquellas Bases de Datos y Sistemas considerados de interés para efectos de esta Tesis.

- **Administración de los Servicios de Terceros:**

  Dependiendo de la estrategia de la aerolínea, varios servicios tecnológicos, ya sea a nivel de Sistemas, o incluso a nivel de gran parte de la infraestructura tecnológica, pueden estar en modalidad de Outsorcing o Subcontratados.

  En estos casos es importante el poder asegurar que los servicios tecnológicos subcontratados están siendo correctamente administrados: si los proveedores estén entregando los servicios y productos con la calidad esperada y en los tiempos acordados, si la administración de los contratos es la adecuada, si a su vez los proveedores pueden dar un nivel de aseguramiento sobre sus procesos, si existen controles de seguridad, si los procesos de respaldo son los adecuados, etc.

- **Estrategia de TI y Controles asociados a TI**

  Dada la importancia de la tecnología para una aerolínea, un elemento a considerar en la auditoria de Sistemas, es de si existe un

adecuado Gobierno de TI, si hay una infraestructura de control, hay metas, indicadores, objetivos, si hay roles y perfiles claramente definidos, si existen Políticas y Procedimientos, etc.

Resumiendo los Procesos y Tópicos de TI mencionados, podemos señalar los siguientes como de probable interés para el Departamento de Auditoria Interna de una aerolínea regional:

Tabla No. 8 - Procesos y Tópicos de TI - Posibles elementos a considerar dentro de un Plan de Auditoria de Sistemas / TI

ID	Tipo	Detalle
P1	Administración de los Cambios	Administración de los cambios realizados a las aplicaciones, estructuras de datos, etc.
P2	Seguridad de la Información	Seguridad de los datos, frente a amenazas / riesgos tanto internos como externos
P3	Administración de los Ambientes Físicos relacionados a TI	Administración de aquellos puntos físicos de infraestructura y equipos, considerados críticos para brindar los servicios de TI
P4	Capacidad de Continuidad de los Servicios de TI	Capacidad de poder asegurar un nivel de disponibilidad de los servicios, y la continuidad de las operaciones ante eventos o incidentes
P5	Administración de los Servicios de Terceros	Para el caso de sistemas / elementos / infraestructura otorgados por terceros y considerados críticos
P6	Estrategia de TI y Controles asociados a TI	Revisión de que exista un Gobierno de TI alineado con los objetivos de la empresa, con Políticas, procedimientos, etc.

Fuente: La Autora / Elaboración: La Autora

CAPITULO IV

4 EVALUACIÓN DEL RIESGO DE TI

El análisis del Riesgo es una actividad que acompaña las tareas de la Auditoria Interna. EL IIA, en sus Normas y Estándares – Normas de Desempeño (2013), resalta la importancia de basar el Plan de actividades en los riesgos:

2010 – Planificación

El director ejecutivo de auditoría debe establecer un plan basado en los riesgos, a fin de determinar las prioridades de la actividad de auditoría interna. Dichos planes deberán ser consistentes con las metas de la organización

Interpretación:

El director ejecutivo de auditoría es responsable de desarrollar un plan basado en riesgos. Para ello, debe tener en cuenta el enfoque de gestión de riesgos de la organización, incluyendo los niveles de aceptación de riesgos establecidos por la dirección para las diferentes actividades o partes de la organización. Si no existe tal enfoque, el director ejecutivo de auditoría utilizará su propio juicio sobre los riesgos después de considerar las aportaciones de la alta dirección y el Consejo. El director ejecutivo de auditoria debe revisar y ajustar el plan, cuando sea necesario, como respuesta a los cambios en el negocio de, los riesgos, las operaciones, los programas, los sistemas y los controles.

2010.A1 *- El plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos documentada, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección y del Consejo.*

2010.A2 *– El director ejecutivo de auditoría debe identificar y considerar las expectativas de la alta dirección, el Consejo y otras partes interesadas de cara a emitir opiniones de auditoría interna y otras conclusiones.*

2010.C1 *El director ejecutivo de auditoría debería considerar la aceptación de trabajos de consultoría que le sean propuestos, basándose en el potencial del trabajo para mejorar la gestión de riesgos, añadir valor y mejorar las operaciones de la*

organización. Los trabajos aceptados deben ser incluidos en el plan

Los recursos del Departamento suelen ser restringidos, tanto en tiempo como en Auditores, especialmente de Sistemas / TI, así que un buen análisis de riesgo ayuda a poder enfocar estos recursos en aquellas áreas / procesos / entes, etc., donde pueden dar un mejor valor agregado.

El análisis del Riesgo no es estático, sino es dinámico, ya que continuamente aparecen nuevos Riesgos, mientras que otros pueden verse reducidos o eliminados. También las organizaciones cambian y evolucionan, así que es necesario el mantener un ciclo de análisis periódico que brinde una perspectiva adecuada sobre el mismo.

De acuerdo a las Guías expresadas por el IIA, y mencionadas en el Capítulo II, de Marco Teórico, el rol de la Auditoria Interna está definido como perteneciente a la Tercera Línea de Defensa frente al Riesgo, en donde puede dar un nivel de aseguramiento independiente.

Al momento de diseñar un Plan de Auditoria Interna de Sistemas / TI, es de utilidad revisar si la empresa, en este caso, el Modelo de Aerolínea regional en Ecuador, tiene algún sistema implementado de ERM ("Enterprise System Management"), ya sea a nivel corporativo o sino específico para TI. Si existe este sistema, la Auditoria Interna debe considerarlo para su análisis, tomando las evaluaciones de riesgo que considere relevantes, y complementándolas de acuerdo a los objetivos definidos por el Departamento, y los intereses expresados por el Comité de Auditoria, la Junta de accionistas, etc., como objetivos prioritarios de la organización.

En caso de que no exista un ERM de donde la Auditoria Interna pueda tomar información de los riegos relevantes de TI, hay que considerar en las actividades de Planificación del Plan de Auditoria, el dedicar el tiempo requerido para realizar el respectivo análisis.

Un resultado de este análisis es el de crear un Mapa de Riesgos, en donde se pueda detectar, revisando el posible impacto y la frecuencia de los eventos, en donde deben de enfocarse los esfuerzos de la Auditoria Interna.

Este capítulo presenta un ejercicio resumido de una evaluación de Riesgos sugeridos relativos a TI, tomando como marco de referencia la Metodología de Riesgos de COBIT 5 mencionada en el Capítulo II de esta Tesis, e información relevante de la industria aérea y del entorno.

Como primer paso se identificarán posibles escenarios de Riesgo de TI aplicados a la industria, y luego se dará una valuación en términos de impacto y probabilidad para construir un Mapa de Riesgos de TI sugerido.

4.1 Escenarios de Riesgo de TI aplicables a la Industria aérea

Uno de los pasos en la identificación de posibles escenarios de riesgo, es el de revisar la incidencia de eventos significativos presentes en la industria, y apreciaciones de riesgos generales de TI que otros competidores (otras aerolíneas) pudieran manejar.

Es conveniente mantener un conjunto de escenarios de Riesgos de TI que sea manejable, y agregue valor: no solamente hay que pensar en escenarios de Riesgos catastróficos (que suelen ocurrir con muy poca frecuencia), sino también en otros Riesgos menos severos (que tienen una más alta frecuencia), sin caer en el extremo de intentar listar todos los escenarios posibles de TI.

De acuerdo a esto, a continuación se presenta un resumen de:

- Eventos significativos relativos a TI de aerolíneas, difundidos por medios informativos, que afectaron a la Operación y/o pasajeros, representando una pérdida de ingresos o costos inesperados, y que respondieron a materializaciones de Riesgos de TI en aerolíneas de la Región

- Riesgos anunciados por aerolíneas públicas, relativos a TI, en sus declaraciones anuales 2013 ante la SEC (*"Security Exchange Commision")* y el público en general.

4.1.1 Eventos significativos (Materialización del Riesgo) en la industria aérea de la Región, relativos a TI (2011 a 2014)

En una búsqueda por Internet, se pueden encontrar algunos eventos concernientes a TI, en donde las aerolíneas fueron objeto de fraudes, o vieron afectadas de manera significativa sus operaciones, ingresos o reputación, con impacto hacia los Pasajeros.

Si bien el objetivo de esta Tesis no es el de presentar un detalle exhaustivo de los mismos, ni listar todos los eventos históricos en el universo de las aerolíneas, los mencionados a continuación ocurridos entre el 2011 y el 2014, pueden servir como referentes o casos de estudio en el análisis de riesgo para un Plan de Auditoria Interna de Sistemas / TI de un Modelo de Aerolínea Ecuatoriana:

Tabla No. 9 - Eventos en la Industria Aérea de la Región (*)

#	Aerolínea - Fecha	Detalle	Análisis de acuerdo a la Estructura de Riesgo COBIT 5	
1	Volaris - 1 a 3 dic 2011	Fraude en la Venta de Boletos en su Web Site o Portal Corporativo: Más de 3,600 pasajeros compraron boletos a través de internet en el Web Site de Volaris, con tarifa 0, sólo pagando tasas e impuestos asociados. La aerolínea alegó que había sido víctima de un fraude y se negó a reconocer los boletos por los valores pagados. Posteriormente la Procuraduría general del consumidor en México le impuso una multa por no haber reconocido esos boletos.	Actores	Se puede presumir internos
			Amenaza	Maliciosa
			Evento	Modificación / Destrucción del Ingreso
			Recursos	Aplicaciones - Venta on-line o WebSite
			Tiempo	3 días

2	Avianca - dic 2011	Fraude en Cuentas de su programa de Lealtad: 5 personas vinculadas a proveedores de servicios fueron apresadas, acusadas de acumulación fraudulenta de Millas y su posterior redención en boletos y productos, valiéndose de manipulación informática. De acuerdo a artículos en prensa colombiana, alrededor de 80 Cuentas de Clientes de Millas fueron afectadas. La aerolínea restituyó las Millas defraudadas a sus clientes	Actores	Internos (vinculados a contratistas)
			Amenaza	Maliciosa
			Evento	Robo
			Recursos	Aplicaciones - Sistema de Lealtad / Millas
			Tiempo	N/A
3	United Airlines - mar 2012	Problemas en la implementación de Sistema de Reservaciones: En marzo del 2012, United cambió su Sistema de Reservaciones. 4 meses después, su indicador de arribos a tiempo (indicador crítico de la industria aérea) era de apenas 64.1%. Esto fue atribuido a problemas en la migración del nuevo sistema y que impactaban en la operación.	Actores	Internos
			Amenaza	Error / Falla
			Evento	Diseño / Ejecución ineficiente
			Recursos	Aplicaciones - Sistema de Reservas
			Tiempo	aprox. 4 meses
4	United Airlines - sep 2012	Problemas con su Web Site o Portal corporativo en Venta de boletos: En septiembre del 2012, el WebSite permitió comprar vuelos con tarifas de $ 0, $ 5 y $10, por un espacio de tiempo, por error. United decidió honrar los boletos comprados por los pasajeros con esas tarifas.	Actores	Internos
			Amenaza	Se presume Accidental
			Evento	Modificación / Destrucción del Ingreso
			Recursos	Aplicaciones - Venta on-line o WebSite
			Tiempo	Horas, no especificadas

5	American Airlines - 16 abr 2013	<u>Problemas en su plataforma Tecnológica – Sistema de Reservas:</u> American Airlines presentó problemas tecnológicos, descritos como una inhabilidad de obtener acceso a su sistema de Reservaciones SABRE, el cual, además de realizar las reservas, maneja otras funciones tales como check-in (chequeo de pasajeros), impresión de Pases de abordar, etc. Estos problemas ocasionaron la cancelación de más de 400 vuelos, y el retraso de otros adicionales.	Actores	Internos y Externos (proveedores de servicio)
			Amenaza	Falla
			Evento	Interrupción de operaciones
			Recursos	Infraestructura de TI / Aplicaciones - Sist. Reservas
			Tiempo	Horas, no especificadas
6	Aerolíneas Argentinas - jul 2013	<u>Problemas con la plataforma tecnológica:</u> En julio del 2013, Aerolíneas Argentinas presentó cancelaciones en ~60 vuelos y demoras, en su centro de operaciones en el Aeroparque Jorge Newbey, debido a fallas en los sistemas informáticos de comunicaciones.	Actores	Internos y Externos (proveedores de servicio)
			Amenaza	Falla
			Evento	Interrupción de operaciones
			Recursos	Infraestructura de TI / Aplicaciones - Sist. Reservas
			Tiempo	Horas, no especificadas
7	Copa Airlines - 19 y 20 de oct 2013	<u>Problemas en su plataforma tecnológica:</u> Durante el 19 y 20 de octubre, Copa Airlines canceló más de 75 vuelos de su red de operaciones, llegando a afectar a un estimado de 10K pasajeros, debido a fallas en su plataforma tecnológica que ocasionaron una interrupción en la red de operaciones. El aeropuerto internacional de Panamá, Centro de la Red de vuelos de Copa, llegó a colapsar en su capacidad,	Actores	Internos
			Amenaza	Falla
			Evento	Interrupción de operaciones
			Recursos	Infraestructura de TI / Aplicaciones

		debido a la cantidad de pasajeros represados por las cancelaciones y retrasos.	Tiempo	2 días
8	Delta Airlines - dic 2013	<u>Problemas con su WebSite en Venta de Boletos:</u> En diciembre del 2013, el WebSite de Delta permitió comprar vuelos con tarifas de hasta $25 en rutas que normalmente costaban ~$400, por dos horas. Delta decidió honrar los boletos comprados.	Actores	Internos
			Amenaza	Se presume Accidental
			Evento	Modificación / Destrucción del Ingreso
			Recursos	Aplicaciones - Venta on-line o WebSite
			Tiempo	2 horas
9	United Airlines - 18 feb 2014	<u>Problemas con sus sistemas de pasajeros</u>: El 18 de febrero del 2014, durante 3 horas se presentaron problemas intermitentes con sus sistemas de servicio al pasajero (reservas, check-in, etc), causando retrasos en los vuelos.	Actores	Se presume internos
			Amenaza	Se presume Accidental
			Evento	Interrupción de operaciones
			Recursos	Aplicaciones - Sistemas de Servicio al Pasajero
			Tiempo	3 horas

(*) Fuente: Los eventos han sido tomados de Medios informativos consultados en Internet, así como declaraciones de aerolíneas en sus WebSites Esos medios están referenciados en la Sección de Bibliografía de esta Tesis. La estructura del Riesgo sugerida está basada en apreciaciones de la Autora, en base a las informaciones disponibles, y no constituyen una declaración formal de los acontecimientos.

4.1.2 Riesgos declarados por aerolíneas públicas, relativas a TI

Revisando los formularios F-20 presentados ante la SEC, de algunas aerolíneas que cotizan en la bolsa de NYSE, tales como Avianca, Copa, Lan o Volaris, para la declaración de los Estados Financieros e información relevante del 2013, podemos encontrar algunos factores de riesgos en donde TI tiene un rol significativo, que estas aerolíneas han identificado, y publican libremente.

Los documentos o formularios F-20 residen en la SEC (www.sec.gov), donde pueden ser consultados libremente vía internet. Por aerolínea, se puede resaltar las siguientes menciones de Riesgo (se adjunta el texto original en inglés, y una traducción sugerida. Los nombres de algunos Sistemas han sido subrayados para facilitar su identificación):

4.1.2.1 Factores de Riesgos Avianca 2013 – relacionados con TI

- Se está en proceso de incorporar nuevos sistemas de TI (Mantenimiento, Operaciones de Vuelo, ERP), en donde la fase transitoria puede tener un impacto negativo en los Servicios y estándares de operación:

> *We are in the process of incorporating new information technology systems to improve our maintenance and flight operations and integrate our legacy Avianca and Taca systems… In transitioning to new systems, we may lose data or experience interruptions in service, wich could harm our business. Additionally, we are implementing a new Enterprise Resource Planning (ERP) system to handle business, human resources and financial process… / Estamos en el proceso de incorporar nuevos sistemas de TI para mejorar nuestras operaciones de Mantenimiento y Operaciones de vuelo, e integrar nuestros sistemas antiguos de Avianca y Taca…. En la transición a los nuevos sistemas, podríamos perder datos o experimentar interrupciones en el servicio, lo cual puede afectar negativamente nuestro negocio. Adicionalmente, estamos implementando un nuevo sistema de ERP para manejar el negocio, recursos humanos y los procesos financieros…*

- Existe dependencia de sistemas automáticos para operar, y cualquier falla de los mismos puede impactar negativamente el negocio.

> *We are dependent on automated systems and technology to operate our business, enhance customer service and reduce operating cost. The performance and reliability of our automated systems and data center is critical to our ability to operate our business and compete effectively. These systems include our computerized airline reservation system, flight operations systems, telecommunications systems, website, maintenance systems, check-in kiosks, in-flight entertainment systems and our primary and redundant data centers. / Somos dependientes en sistemas automáticos y tecnologías para operar nuestro negocio, mejorar el servicio al cliente y reducir el costo de operación. El rendimiento y confiabilidad de nuestros sistemas automáticos y Centro de Datos es crítico para nuestra habilidad de operar nuestro negocio y competir efectivamente. Estos sistemas incluyen nuestro sistema computarizado de reservas de la aerolínea, sistemas de Operaciones de Vuelo, Sistemas de Telecomunicaciones, WebSite, Sistemas de Mantenimiento, Kioskos de auto-chequeo, sistemas de Entretenimiento a Bordo, y nuestros Centros de Datos primario y de respaldo.*
>
> *Our Website and reservation system must be able to accommodate a high volume of traffic and deliver important flight information. / Nuestro WebSite y Sistema de Reservaciones deben ser capaces de acomodar un alto volumen de tráfico y entregar información importante de vuelos.*
>
> *We rely on the third party providers of our current automated systems and data center infraestructura for technical support. / Dependemos de los proveedores (terceros) de nuestros sistemas automáticos actuales, y los de soporte técnico para la infraestructura de nuestro Centro de Datos.*
>
> *Our automated systems cannot be completely protected against events that are beyond our control, including natural disasters, computer viruses, other security breaches or telecommunications failures / Nuestros Sistemas no pueden ser completamente protegidos frente a eventos que están por fuera de nuestro control, incluyendo desastres naturales, virus de computadoras, violaciones de la seguridad o fallas en las telecomunicaciones.*

4.1.2.2 Factores de Riesgos Copa 2013 – relacionados con TI

- Existe dependencia de sistemas automáticos para operar, y cualquier falla de los mismos puede impactar negativamente el negocio.

> *We rely upon information technology systems to operate our business and increase our efficiency. We are highly reliant on certain systems for flight and operations, maintenance, reservations, check-in, revenue management, accounting and cargo distribution…. / Dependemos de sistemas de TI para operar nuestro negocio e incrementar nuestra eficiencia. Somos altamente dependientes en ciertos sistemas para vuelos y operaciones, mantenimiento, reservaciones, chequeo, Revenue Management, Contabilidad y distribución de Carga…*
>
> *Information systems could also suffer disruptions due to events beyond our control, including natural disasters, power failures, terrorist attacks, equipment or software failures, computer viruses or cyber security attacks. / Los sistemas de información podrían sufrir interrupciones debido a eventos por fuera de nuestro control, incluyendo desastres naturales, virus de computadores o ataques cibernéticos.*
>
> *Substantial or repeated website, reservations systems or telecommunication system failures or disruptions, including failures or disruptions related to our integration of technology systems could reduce the attractiveness of our Company versus our competitors… / Fallas o interrupciones significativas o repetitivas de nuestro website, sistemas de reserva o sistemas de Telecomunicaciones, incluyendo fallas relativas a la integración de nuestros sistemas de tecnología pueden reducir el atractivo de nuestra Compañía versus nuestros competidores….*

4.1.2.3 Factores de Riesgos LATAM 2013 (LAN y TAM) – Relacionados con TI:

- Problemas con sistemas de Control de Tráfico Aéreo u otras fallas técnicas pueden interrumpir las operaciones y tener un efecto material adverso en el negocio. Existe dependencia de los Sistemas de Mantenimiento y de Reservas, entre otros factores.

Our operations, including our ability to deliver customer service are dependent on the effective operation of our equipment, including our aircraft, maintenance systems and Reservation systems / Nuestras operaciones, incluida nuestra habilidad para entregar servicio al cliente son dependientes de la operación efectiva de nuestro equipo, incluyendo nuestras aeronaves, sistemas de Mantenimiento y Sistemas de Reserva

- La aerolínea puede no ser capaz de alcanzar completamente los beneficios esperados de la combinación de LAN y TAM. Existe complejidad en la combinación de negocios (Procedimientos, sistemas, etc).

Potencial difficulties include the increased complexity associated with managing both companies, the need to integrate procedures and systems…." / Las dificultades potenciales incluyen el aumento en la complejidad asociada con administrar ambas compañías, la necesidad de integrar Procedimientos y Sistemas….

4.1.2.4 Factores de Riesgos Volaris 2013 – relacionados con TI

- Existe una alta dependencia en tecnología y sistemas automáticos para operar. Fallas de TI pueden afectar negativamente el negocio.

We are highly dependent on technology and automated systems to operate our business and achieve low operating costs. These technologies and systems include our computerized airline Reservation system, flight operations systems, financial planning, management and accounting system, telecommunications systems, website, maintenance systems and check-in kiosks. / Somos altamente dependientes en tecnología y sistemas automatizados para operar nuestro negocio y alcanzar bajos costos de operación. Estas tecnologías y sistemas incluyen nuestro Sistema computarizado de Reservas, Sistemas de Operaciones de Vuelo, Planificación Financiera, Sistemas de administración y Contabilidad, Sistema de Telecomunicaciones, WebSite o Portal, Sistemas de Mantenimiento y kioscos de check-in.

For our operations to work efficiently, our website and reservations systems must be able to accommodate a high volume of traffic, maintain secure information and deliver flight information. Substantially all of our tickets are issued to

passengers as electronic tickets. / Para que nuestras operaciones trabajen eficientemente, nuestro Website o Portal y los Sistemas de Reservación deben ser capaces de acomodar un alto volumen de tráfico, manteniendo la información segura y entregando información del vuelo. Substancialmente, todos nuestros boletos son emitidos a los pasajeros como boletos electrónicos.

We depend on our Reservation system, which is hosted and maintained by third-party service providers… If our reservation system fails or experiences interruptions and we are unable to book seats for any period of time, we could lose significant amounts of revenues… if our flight operations system were to fail, our operations would be materially and adversely affected / Dependemos de nuestro Sistema de Reservaciones, el cual es provisto y mantenido por terceros… si nuestro Sistema de Reservaciones falla o experienta interrupciones y no somos capaces de reservar sillas de vuelo por algún periodo de tiempo, podemos perder montos significativos de ingresos…. Si nuestro Sistema de Operaciones de vuelo fuera a fallar, nuestras operaciones serían material y adversamente afectadas.

We also rely on third-party service providers of our other automated systems for technical support, system maintenance and software upgrades / Tambien dependemos de proveedores de Servicios de nuestros otros sistemas automáticos, para soporte técnico, mantenimientos de Sistema y actualizaciones de software.

We retain personal information received from customers and have put in place security measures to protect against unauthorized access… Personal information held both offline and online is highly sensitive and, if third parties were to access such information…our reputation could be adversely affected and customers could bring legal claim against us… In addition, we may be liable to credit card companies should any credit card information be accessed and misused as a result of lack of sufficient security systems implemented by us / Mantenemos informacion personal recibida de nuestros clientes y hemos implementado medidas de seguridad para protección ante accesos no autorizados … La Información personal mantenida tanto offline como online es altamente sensitiva y, si terceros fueran a acceder a esa información … nuestra reputación puede ser adversamente afectada y los clientes podrían iniciar reclamos legales en contra nuestra…. En adición, podríamos ser legalmente responsables ante compañías de tarjetas de crédito en caso de que cualquier información de tarjeta de

crédito sea obtenida y mal utilizada como resultado de falta de suficientes sistemas de seguridad implementados por nosotros.

… Our automated systems cannot be completely protected against events that are beyond our control, including natural disasters, computer viruses or telecommunications failures... / Nuestros sistemas automáticos no pueden ser completamente protegidos ante eventos que están por fuera de nuestro control, incluyendo desastres naturales, virus de computadores o fallas de telecomunicaciones...

4.1.3 Elección de escenarios de Riesgos de TI aplicables a la Industria Aérea

Basados en los escenarios de Riesgos Genéricos de TI sugeridos por el Modelo COBIT 5 (Ver Anexo No. 3 para la lista completa), y tomando en cuenta factores tales como:

- Características de la industria,
- Eventos relevantes sucedidos durante los últimos 3 años a aerolíneas comerciales de la región,
- Factores de riesgo mencionados por aerolíneas de la región, y
- La localización del modelo de aerolínea escogido: Basada en Ecuador, con su Centro de Datos / Operaciones en la ciudad de Guayaquil

Se propone para efectos de esta Tesis, considerar 40 de los 78 escenarios genéricos de riesgo que brinda COBIT 5.

Algunas de las eliminaciones hechas son evidentes dados los factores mencionados. Por ejemplo, en la ciudad de Guayaquil no se tienen registros de afectación de tsunamis (Referencia No 1902 en los escenarios genéricos de COBIT 5), ni huracanes o ciclones (Referencia No. 1903)

Otros escenarios de riesgo pueden no ser tan aplicables o relevantes en la industria aérea, tal como el escenario de espionaje industrial

(Referencia No. 1604), dado que las aerolíneas no tienen como su objetivo primario el desarrollar nuevos productos, en contraposición a otras, como por ejemplo, empresas fabricantes de aviones.

Y por último escenarios tales como Riesgos Geopolíticos, pudieran no ser relevantes durante un período de tiempo específico, pero podrían tener la capacidad de convertirse en relevantes, de acuerdos a cambios en las condiciones políticas / económicas / regulatorias, tanto del país sede (Ecuador de acuerdo al caso de estudio planteado), como de los países en donde la aerolínea piense expandir la operación de vuelos.

Como se mencionó al inicio del Capítulo, los riesgos cambian y las empresas también lo hacen, por lo que es importante el mantener un análisis periódico de estos escenarios.

La lista sugerida de 40 escenarios de Riesgos de TI a considerar es:

Tabla No. 10- Escenarios de Riesgo de TI a considerar para el Modelo de Aerolínea Doméstica Ecuatoriana (*)

			Tipos de Riesgo			
No.	**Ref. COBIT 5**	**Categoría de Escenario de Riesgo**	**Estratégico**	**Proyectos**	**Operativos**	**Escenarios Negativos**
1	0601	Información (violación de Datos: daños, fuga de información y accesos)	S		P	Componentes de Hardware son dañados, conduciendo a una (parcial) destrucción de datos por personal interno
2	0602		S	S	P	La Base de datos está corrompida, conduciendo a datos inaccesibles
3	0604		S	S	P	Datos sensitivos están perdidos / revelados debido a ataques lógicos
4	0605		S	S	P	Medios de respaldo están perdidos o los backups no son revisados para comprobar efectividad

5	0606		P	S	P	Información sensitiva es accidentalmente revelada debido a fallas en guías de cómo manejar información
6	0607		P	S	P	Datos (contables, relativos a seguridad, datos de ventas, etc), son modificados intencionalmente
7	0609		P	S	P	Información Sensitiva es liberada debido a ineficiente retención / archivo / eliminación de información
8	0801	Infraestructura (Hardware, Sistemas Operativos y Tecnologías de Control) (Selección / Implementación, Operaciones y Supresiones definitivas o Retiros)	P	S	P	Nueva (innovativa) infraestructura es instalada y como resultado los sistemas se vuelven inestables, conduciendo a incidentes operacionales
9	0802		P	S	P	Los sistemas no pueden manejar los volúmenes transaccionales cuando el volumen de usuarios se incrementa
10	0803		P	S	P	Los sistemas no pueden manejar la carga de sistemas cuando nuevas aplicaciones o iniciativas son desarrolladas e instaladas
11	0805		P	S	P	La tecnología en uso es obsoleta y no puede satisfacer los requerimientos de nuevos negocios (networking, seguridad, Bases de Datos, almacenamiento, etc)
12	0901	Software	P		S	Hay una inabilidad para usar el software para realizar los beneficios o salidas esperados (por ej. Fracaso para realizar modelos de negocios requerido o cambios organizacionales)
13	0903		P		S	El software equivocado (en costos, rendimiento, funcionalidades, compatibilidad, etc) es seleccionado para implementación
14	0904		P		S	Hay glitches (fallas intermitentes) operacionales cuando nuevo software es puesto a producción / operación
15	0905		P		S	Los usuarios no pueden usar y explotar el nuevo software de aplicación
16	0906		P		S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas

17	0907		P		S	Modificación no intencional de software conduciendo a resultados inesperados
18	0908		P		S	Ocurren errores de configuración no intencional y en administración de cambios
19	0909		P		S	Ocurre un mal funcionamiento de softwares comunes, de sistemas de aplicaciones críticas
20	0910		P		S	Ocurren problemas de software intermitentes con Sistemas importantes
21	0911		P		S	El software de aplicación es obsoleto (por ej, tecnología antigua, con pobre documentación, costoso de mantener, con dificultad para extenderse, no integrado en la arquitectura actual)
22	1002	Propiedad del negocio sobre TI	P	S	S	Hay una dependencia excesiva y uso de computación de usuario final y soluciones ad hoc para necesidades importantes de información, conduciendo a deficiencias en seguridad, datos inexactos o incremento de costos / uso ineficiente de recursos
23	1004				P	Inadecuados requerimientos conducen a acuerdos en niveles de servicio inefectivos (SLA: " Service Level Agreements")
24	1103	Selección / Desempeño, Cumplimiento contractual, terminación del servicio y transferencia de proveedores		S	P	El soporte y los servicios entregados por vendedores son inadecuados y no están de acuerdo con los SLAs
25	1104			S	P	El rendimiento de un outsorcing es inadecuado en un esquema de gran escala y a largo plazo
26	1201	Cumplimiento Regulatorio	P	S	S	Hay incumplimiento con regulaciones (ej. Privacidad, contabilidad, manufactura)
27	1401	Robo de Infraestructura o destrucción	S	S	P	Hay un robo de un dispositivo con información sensitiva
28	1403		S	S	P	Ocurre destrucción del centro de datos (sabotaje, etc)

29	1404		S	S	P	Hay una destrucción accidental de dispositivos individuales
30	1501	Malware o Software maligno	S		P	Hay una intrusión de software maligno (malware) en servidores operacionales críticos
31	1502		S		P	Regularmente, hay infección de laptops con malware
32	1503		S		P	Un empleado molesto / insatisfecho implementa una "bomba de tiempo" de malware, que conduce a pérdida de datos
33	1504		S		P	Datos de la compañía son robados a través de acceso no autorizado alcanzado por un ataque tipo "phishing"
34	1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de ingresar a los sistemas
35	1602		S		P	Hay una interrupción del servicio debido a ataque de "negación de servicios"
36	1603		S		P	El website es desconfigurado / alterado
37	1605		S		P	Hay un ataque de virus
38	1606		S		P	Hay un ataque de "hackers"
39	1901	Actos de la Naturaleza	S	S	P	Hay un terremoto
40	1905		S	S	P	Hay inundaciones

(*) Fuente: COBIT 5 for Risk – ISACA – Escenarios genéricos seleccionados de TI, impactos negativos. La lista completa se encuentra en el Anexo No. 3

(Ref COBIT 5 = Número de Identificación de COBIT 5 / P= Implicación primaria / S = Implicación Secundaria)

4.2 Elaboración del Mapa de Riesgos de TI aplicable al modelo de negocio de Aerolínea Doméstica Ecuatoriana

Una vez seleccionados y depurados los Escenarios de Riesgos de TI, se debe proceder a aplicarlos a los elementos del Universo de TI previamente identificados como de interés para la Auditoria Interna (Capítulo III del presente trabajo) para formar un Mapa de Riesgos.

Este Mapa tiene como objetivo analizar cuáles elementos (Hadware, Sistemas, Procesos, etc) presentan un riesgo más alto dentro del negocio, considerando calificaciones relativas al probable impacto en caso de que el riesgo se materialice y la frecuencia.

La Matriz formada al tomar en cuenta estas dos dimensiones de impacto y frecuencia es la que forma el Mapa de Riesgos.

No existe un estándar único para el tamaño de la matriz, pero se suelen usar matrices de 3x3, 4x4 y 5x5. Para efectos de esta Tesis se propondrá una matriz de 4x4.

En cuanto a la elección de los criterios de Impacto y Frecuencia, si existe algún sistema de ERM a nivel de la organización, se puede escoger usar criterios similares (ej: para las mediciones de posibles impactos financieros, una escala de porcentajes en afectación a ingresos, costos, etc, puede estar ya definida y asociada a niveles de impacto).

Si no existe un benchmarking al interior de la organización para calificar Impacto y Frecuencia, es aconsejable elaborar una propuesta y revisarla con usuarios clave (la alta administración, el Comité de auditoría, etc), para poder afinarlos y estar seguros de que reflejan apropiadamente las percepciones más aceptadas de impacto y frecuencia.

4.2.1 Definición de Niveles de Impacto

Se propone un análisis de impacto cubriendo tres tipos generales:

- Impactos financieros: Impactos negativos sobre los ingresos, costos o flujo de caja,
- Impactos operativos: Interrupciones o paralización de la operación normal, ya sea de vuelos, servicios al clientes, sistemas de TI, e
- impactos reputacionales: Impactos negativos en la reputación de la aerolínea, en los mercados donde opera.

En caso de considerarlo conveniente, se pueden incluir otros tipos tales como Impactos Legales, Impactos Regulatorios, etc.

A continuación se presenta un ejercicio de definición de cuatro niveles de impacto, para usar en el análisis de los escenarios de riesgos, con mediciones sugeridas exclusivamente para efectos de esta Tesis:

Tabla No. 11 - Niveles de Impacto a considerar - Mapa de Riesgos de TI

Impacto	1 = Bajo	2 = Medio	3 = Alto	4 = Crítico
Financiero	- Disminución de menos del 3% en los ingresos - Incremento de menos del 3% en los costos - Impacto negativo en flujo de caja de menos del 3%	- Disminución entre el 3% y el 5% en los ingresos - Incremento entre el 3% y el 5% en los costos - Impacto negativo en flujo de caja, entre el 3% y el 5%	- Disminución entre 5% y 7% de los ingresos - Incremento entre 5% y 7% de los costos - Impacto negativo en flujo de caja entre el 5% y el 7%	- Disminución de +7% en los ingresos - Incremento de +7% en los costos - Impacto en flujo de caja en +7%
Operativo	- Inabilidad de operar (vuelo, atención al cliente, etc), menor a 4 horas, en un único punto de operación	- Inabilidad de operar (vuelo, atención al cliente, etc), entre 0 y 12 horas, afectando a todos los puntos - Inabilidad de operar (vuelo, at. al cliente, etc) afectando por un día, una ciudad	- Inabilidad de operar (vuelo, atención al cliente, etc), entre 12 y 24 horas, que afecte toda la red de Operación - Retrasos de vuelos de más del 80% de la planificación normal	- Inabilidad de operar (vuelo, atención al cliente, etc) por +1 día

Reputacional	- Nivel bajo de comentarios negativos en medios sociales	- Difusión negativa de noticias, con presencia en medios regionales - Nivel medio de comentarios negativos en medios sociales	- Difusión negativa de noticias, con presencia en medios nacionales - Nivel alto de comentarios negativos en medios sociales	- Difusión negativa de noticias, con presencia en medios nac. e internacionales - Nivel alto de comentarios negativos en medios sociales.

Fuente: La Autora / Elaboración: La Autora

4.2.2 Definición de Niveles de Frecuencia

Se propone un análisis de Frecuencia cubriendo cuatro tipos de medición:

- Frecuencia de las Operaciones: Medición de la frecuencia con que se realizan las operaciones relacionadas a un elemento del Universo de TI,
- Volumetría de las transacciones mensuales: Cantidad de registros, movimientos o transacciones mensuales realizadas,
- Centralización / Descentralización: Medición del grado de Centralización en cuanto al control del elemento, proceso, etc. analizado, y
- Cantidad de ocurrencias negativas previas (industria o al interior de la empresa): Cantidad de eventos negativos ocurridos durante un año, ya sea relativos a la industria (competidores, líderes del mercado, etc.), o a eventos pasados en la aerolínea.

En caso de considerarlo conveniente, se pueden incluir otros tipos.

A continuación se presenta un ejercicio de definición de cuatro niveles de Frecuencia, para usar en el análisis de los escenarios de riesgos, con mediciones sugeridas exclusivamente para efectos de esta Tesis:

Tabla No. 12 - Niveles de Frecuencia a considerar - Mapa de Riesgos de TI

Frecuencia	1 = Improbable	2 = Remoto	3 = Ocasional	4 = Frecuente
Frecuencia de las operaciones	- Una vez al año o menos	- Una vez en el trimestre o menos	- Una vez al mes	- 1 vez al día o más
Volumetría de las transacciones mensuales	- Menos de 1K transacciones mensuales	- Entre 1K y 5K transacciones mensuales	- Entre 5K y 10K transacciones mensuales	- +10K transacciones mensuales
Centralización / Descentralización	- Centralizado	- Centralizado	- La mayor parte centralizado / dependiente de una unidad	- Descentralizado
Cantidad de ocurrencias negativas previas (industria o al interior de la empresa)	- No hay eventos negativos en el año	- Entre 1 y 2 ocurrencias negativas en el año	- Entre 3 y 5 ocurrencias negativas en el año	+ de 5 ocurrencias negativas en el año

Fuente: La Autora / Elaboración: La Autora

4.2.3 Evaluación de escenarios seleccionados de Riesgos de TI de acuerdo a Impacto y Frecuencia

Una vez definidos los criterios de medición de Impacto y Frecuencia, se puede proceder a aplicar los escenarios de riesgo seleccionadas frente a los elementos identificados del Universo de TI.

No todos los escenarios son necesariamente aplicables a cada elemento, por lo que se requiere el mejor criterio del Auditor Interno de Sistemas, para seleccionar los más relacionados. Es aconsejable mantener

un límite razonable, por ejemplo hasta un máximo de 15 escenarios, para no hacer el ejercicio complejo o caer en una dilución del resultado, al ponderar las calificaciones.

También no todas las evaluaciones son 100% exactas, sino que se requerirá de la mejor estimación posible.

Los resultados promedio del Impacto y la Frecuencia, servirán para situar cada elemento a ser auditado en el Mapa de Riesgos.

A continuación se presenta un ejercicio aplicado a elementos destacados del Universo de TI en cada una de las categorías. Los criterios presentados son únicamente para efectos de esta Tesis, y pueden variar al ser aplicados a la realidad de cada aerolínea o de acuerdo a la experiencia / información recopilada por el Auditor Interno de Sistemas / TI.

4.2.3.1 Evaluación de Riesgos TI - Centro de Datos

Se asume que el Centro de Datos es propio (administrado por la aerolínea), y está situado en la ciudad de Guayaquil. El país está situado en una zona de probabilidad de sismos.

La evaluación indica que, si bien el impacto es alto en caso de materializarse algún escenario de riesgo, (puede poner en peligro la viabilidad de la aerolínea), la frecuencia es baja.

Tabla No. 13 - Evaluación del Nivel de Riesgo TI - Centro de Datos (*)

Elemento	Ref. COBIT 5	Categoría de Escenario de Riesgo	Tip. de Riesgo			Escenarios Negativos	Impacto	Frecuencia
			Estratégico	Proyectos	Operativos			
Centro de Datos	0601	Información	S		P	Componentes de Hardware son dañados, conduciendo a una (parcial) destrucción de datos por personal interno	4	1

0605		S	S	P	Medios de respaldo están perdidos o los backups no son revisados para comprobar efectividad	4	4
0801	Infraestructura	P	S	P	Nueva (innovativa) infraestructura es instalada y como resultado los sistemas se vuelven inestables, conduciendo a incidentes operacionales	4	2
0805		P	S	P	La tecnología en uso es obsoleta y no puede satisfacer los requerimientos de nuevos negocios	3	2
1004	Propiedad del Negocio sobre TI			P	Inadecuados requerimientos conducen a acuerdos en niveles de servicio inefectivos (SLA: " Service Level Agreements")	3	2
1103	Proveedores		S	P	El soporte y los servicios entregados por vendedores son inadecuados y no están de acuerdo con los SLAs	3	2
1401		S	S	P	Hay un robo de un dispositivo con información sensitiva	3	1
1403	Robo de Infraestructura o destrucción	S	S	P	Ocurre destrucción del centro de datos (sabotaje, etc)	4	1
1404		S	S	P	Hay una destrucción accidental de dispositivos individuales	3	1
1901	Actos de la Naturaleza	S	S	P	Hay un terremoto	4	2
1905		S	S	P	Hay inundaciones	4	1
Promedio						**3.55**	**1.73**

(*) Fuente: Escenarios genéricos de Riesgo TI propuesto por COBIT 5, ajustados de acuerdo a los supuestos del ejercicio de la Tesis / Elaboración: La Autora

4.2.3.2 Evaluación de Riesgos TI - Firewalls:

Se asume que la aerolínea ha adquirido soluciones de firewalls reconocidas en el mercado, por lo que se podría esperar niveles adecuados

en confiabilidad y funcionalidad del producto. Las soluciones están instaladas y son controladas / monitoreadas de manera centralizada.

La solución implementada consiste en una mezcla de hardware y software.

La evaluación indica que, si bien el impacto es alto en caso de materializarse algún escenario de riesgo, (puede poner en peligro la seguridad de los datos), la frecuencia es baja.

Tabla No. 14 - Evaluación del Nivel de Riesgo TI – Firewalls (*)

			Tipos de Riesgo					
Elemento	**Ref. COBIT 5**	**Categoría de Escenario de Riesgo**	**Estratégico**	**Proyectos**	**Operativos**	**Escenarios Negativos**	**Impacto**	**Frecuencia**
Firewalls	0604	Información	S	S	P	Datos sensitivos están perdidos / revelados debido a ataques lógicos	4	1
	0801	Infraestructura	P	S	P	Nueva (innovativa) infraestructura es instalada y como resultado los sistemas se vuelven inestables, conduciendo a incidentes operacionales	3	1
	0805		P	S	P	La tecnología en uso es obsoleta y no puede satisfacer los requerimientos de nuevos negocios	3	1
	0906	Software	P		S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas	3	1
	0907		P		S	Modificación no intencional de software conduciendo a resultados inesperados	3	1
	0908		P		S	Ocurren errores de configuración no intencional y en administración de cambios	3	1
	0911		P		S	El software de aplicación es obsoleto	3	1

1501	Malware o Software maligno	S	P	Hay una intrusión de software maligno (malware) en servidores operacionales críticos	4	1
1502		S	P	Regularmente, hay infección de laptops con malware	2	3
1504		S	P	Datos de la compañía son robados a través de acceso no autorizado alcanzado por un ataque tipo "phishing"	2	2
1601	Ataques lógicos	S	P	Usuarios no autorizados tratan de ingresar a los sistemas	3	2
1605		S	P	Hay un ataque de virus	3	2
1606		S	P	Hay un ataque de "hackers"	4	1
Promedio					**3.00**	**1.45**

(*) Fuente: Escenarios genéricos de Riesgo TI propuesto por COBIT 5, ajustados de acuerdo a los supuestos del ejercicio de la Tesis / Elaboración: La Autora

4.2.3.2 Evaluación de Riesgos TI - Bases de Datos Críticas

Se asume que la aerolínea ha adquirido soluciones de Bases de Datos reconocidas en el mercado, por lo que se podría esperar niveles adecuados en confiabilidad y funcionalidad del producto. Las mismas están instaladas en el Centro de Datos principal.

Además se cuenta con un Departamento dentro de TI y personal especializado para la Administración de las Bases de Datos.

La evaluación indica que, si bien el impacto es alto en caso de materializarse algún escenario de riesgo, (puede poner en peligro la seguridad de los datos), la frecuencia es baja.

Tabla No. 15 - Evaluación del Nivel de Riesgo TI - Bases de Datos (*)

Elemento	Ref. COBIT 5	Categoría de Escenario de Riesgo	Tipos de Riesgo			Escenarios Negativos	Impacto	Frecuencia
			Estratégico	Proyectos	Operativos			
Base de Datos	0602		S	S	P	La Base de datos está corrompida, conduciendo a datos inaccesibles	4	2
	0604		S	S	P	Datos sensitivos están perdidos / revelados debido a ataques lógicos	4	2
	0605		S	S	P	Medios de respaldo están perdidos o los backups no son revisados para comprobar efectividad	4	4
	0606		P	S	P	Información sensitiva es accidentalmente revelada debido a fallas en guías de cómo manejar información	4	2
	0607		P	S	P	Datos (contables, relativos a seguridad, datos de ventas, etc), son modificados intencionalmente	4	4
	0609		P	S	P	Información Sensitiva es liberada debido a ineficiente retención / archivo / eliminación de información	4	2
	0906	Software	P		S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas	4	2
	0907		P		S	Modificación no intencional de software conduciendo a resultados inesperados	4	2
	0908		P		S	Ocurren errores de configuración no intencional y en administración de cambios	4	2
	1501	Malware o Software maligno	S		P	Hay una intrusión de software maligno (malware) en servidores operacionales críticos	4	1

1503		S	P	Un empleado molesto / insatisfecho implementa una "bomba de tiempo" de malware, que conduce a pérdida de datos	4	1
1504		S	P	Datos de la compañía son robados a través de acceso no autorizado alcanzado por un ataque tipo "phishing"	3	1
1601	Ataques lógicos	S	P	Usuarios no autorizados tratan de ingresar a los sistemas	3	1
Promedio					**3.82**	**2.00**

(*) Fuente: Escenarios genéricos de Riesgo TI propuesto por COBIT 5, ajustados de acuerdo a los supuestos del ejercicio de la Tesis / Elaboración: La Autora

4.2.3.4 Evaluación de Riesgos TI - Sistema ERP Contable - Financiero

Se asume que el Sistema ERP de la aerolínea es una solución reconocida en el mercado, y por lo tanto es probable que haya una mejor calidad, estabilidad y confiabilidad del producto.

La evaluación contempla que el ERP está instalado localmente, y la responsabilidad de funciones tales como seguridad, respaldos, configuración, etc., están a cargo de la aerolínea.

La administración de roles y perfiles, así como la parametrización del sistema es de responsabilidad del Departamento Financiero de la aerolínea, el cual está situado en Guayaquil principalmente, aunque existen usuarios específicos en Quito y Cuenca.

Dado el alto nivel de transacciones, y lo crítico del sistema para la elaboración de los Estados Financieros, la calificación se la considera como alta.

Tabla No. 16 - Evaluación del Nivel de Riesgo TI - ERP Financiero – Contable (*)

Elemento	Ref. COBIT 5	Categoría de Escenario de Riesgo	Tipos de Riesgo			Escenarios Negativos	Impacto	Frecuencia
			Estratégico	Proyectos	Operativos			
ERP Finan-ciero - Contable	0602	Información	S	S	P	La Base de datos está corrompida, conduciendo a datos inaccesibles	4	4
	0604		S	S	P	Datos sensitivos están perdidos / revelados debido a ataques lógicos	2	1
	0605		S	S	P	Medios de respaldo están perdidos o los backups no son revisados para comprobar efectividad	4	4
	0606		P	S	P	Información sensitiva es accidentalmente revelada debido a fallas en guías de cómo manejar información	2	4
	0607		P	S	P	Datos (contables, relativos a seguridad, datos de ventas, etc), son modificados intencionalmente	4	4
	0609		P	S	P	Información Sensitiva es liberada debido a ineficiente retención / archivo / eliminación de información	2	2
	0901	Software	P		S	Hay una inabilidad para usar el software para realizar los beneficios o salidas esperados	2	2
	0906		P		S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas	4	1
	0907		P		S	Modificación no intencional de software conduciendo a resultados inesperados	4	1
	0908		P		S	Ocurren errores de configuración no intencional y en administración de cambios	4	1

	1002	Propiedad del negocio sobre TI	P	S	S	Hay una dependencia excesiva y uso de computación de usuario final y soluciones ad hoc para necesidades importantes de información, conduciendo a deficiencias en seguridad, datos inexactos o incremento de costos / uso ineficiente de recursos	4	4
Promedio							**3.27**	**2.55**

(*) Fuente: Escenarios genéricos de Riesgo TI propuesto por COBIT 5, ajustados de acuerdo a los supuestos del ejercicio de la Tesis / Elaboración: La Autora

4.2.3.5 Evaluación de Riesgos TI – Sistema de Ventas on-Line / WebSite

Tomando en cuenta los eventos significativos de fraude y/o mal funcionamiento en otras aerolíneas (casos de Volaris, United, Delta, etc.), así como apreciaciones de un alto riesgo en las declaraciones anuales de aerolíneas públicas en la región, el resultado aplicando el análisis de riesgos es alto.

Tabla No. 17 - Evaluación del Nivel de Riesgo TI – WebSite (*)

			Tipos de Riesgo					
Elemento	**Ref. COBIT 5**	**Categoría de Escenario de Riesgo**	**Estratégico**	**Proyectos**	**Operativos**	**Escenarios Negativos**	**Impacto**	**Frecuencia**
Web Site	0607	Información	P	S	P	Datos (contables, relativos a seguridad, datos de ventas, etc), son modificados intencionalmente	2	4
	0802	Infraestructura	P	S	P	Los sistemas no pueden manejar los volúmenes transaccionales cuando el volumen de usuarios se incrementa	4	4
	0905	Software	P		S	Los usuarios no pueden usar y explotar el nuevo software de aplicación	4	4

0906		P		S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas	4	1
0907		P		S	Modificación no intencional de software conduciendo a resultados inesperados	4	1
0908		P		S	Ocurren errores de configuración no intencional y en administración de cambios	3	4
0910		P		S	Ocurren problemas de software intermitentes con Sistemas importantes	2	4
1103	Proveedores		S	P	El soporte y los servicios entregados por vendedores son inadecuados y no están de acuerdo con los SLAs	4	3
1503	Malware	S		P	Un empleado molesto / insatisfecho implementa una "bomba de tiempo" de malware, que conduce a pérdida de datos	2	2
1602	Ataques lógicos	S		P	Hay una interrupción del servicio debido a ataque de "negación de servicios"	2	2
1603		S		P	El website es desconfigurado / alterado	3	4
1605		S		P	Hay un ataque de virus	3	4
1606		S		P	Hay un ataque de "hackers"	3	4
Promedio						**3.08**	**3.15**

(*) Fuente: Escenarios genéricos de Riesgo TI propuesto por COBIT 5, ajustados de acuerdo a los supuestos del ejercicio de la Tesis / Elaboración: La Autora

4.2.3.6 Evaluación de Riesgos TI - Sistema de Reservas

Se asume que el Sistema de Reservas usado en la aerolínea Modelo ecuatoriana, es uno provisto por alguno de los proveedores más reconocidos el mercado (Sabre, Amadeus, etc), y por lo tanto es probable que haya una

mejor estabilidad y calidad en el producto. Además, dado que es usado por varias aerolíneas, aspectos tales como seguridad, respaldos, etc, se puede esperar que estén con un alto nivel de confiabilidad.

La Base de datos así como la aplicación residen en el proveedor, y la aerolínea se conecta vía internet y/o enlaces privados, para usar los servicios.

Sin embargo, el hecho de que sea uno de los Sistemas críticos para que la aerolínea realice funciones de Reserva, check-in, etc, que hay eventos de fallas en competidores (United, American Airlines), y que varias aerolíneas lo mencionen en sus declaraciones de riesgo, incide para que el resultado promedio de la evaluación sea medio – alto.

Tabla No. 18 - Evaluación del Nivel de Riesgo TI - Sistema de Reservas

			Tipos de Riesgo					
Elemento	**Ref. COBIT 5**	**Categoría de Escenario de Riesgo**	**Estratégico**	**Proyectos**	**Operativos**	**Escenarios Negativos**	**Impacto**	**Frecuencia**
Sistema de Reservas	0602	Información	S	S	P	La Base de datos está corrompida, conduciendo a datos inaccesibles	4	1
	0604		S	S	P	Datos sensitivos están perdidos / revelados debido a ataques lógicos	4	1
	0605		S	S	P	Medios de respaldo están perdidos o los backups no son revisados para comprobar efectividad	1	1
	0606		P	S	P	Información sensitiva es accidentalmente revelada debido a fallas en guías de cómo manejar información	3	1
	0607		P	S	P	Datos (contables, relativos a seguridad, datos de ventas, etc), son modificados intencionalmente	2	4

0609		P	S	P	Información Sensitiva es liberada debido a ineficiente retención / archivo / eliminación de información	2	4
0901	Software	P		S	Hay una inabilidad para usar el software para realizar los beneficios o salidas esperados	2	4
0906		P		S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas	2	1
0907		P		S	Modificación no intencional de software conduciendo a resultados inesperados	2	1
0908		P		S	Ocurren errores de configuración no intencional y en administración de cambios	3	1
0910		P		S	Ocurren problemas de software intermitentes con Sistemas importantes	4	4
0911		P		S	El software de aplicación es obsoleto	4	1
1004	Propiedad del negocio sobre TI			P	Inadecuados requerimientos conducen a acuerdos en niveles de servicio inefectivos (SLA: " Service Level Agreements")	3	1
1103	Proveedores		S	P	El soporte y los servicios entregados por vendedores son inadecuados y no están de acuerdo con los SLAs	4	4
1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de ingresar a los sistemas	3	4
Promedio						**2.87**	**2.20**

(*) Fuente: Escenarios genéricos de Riesgo TI propuesto por COBIT 5, ajustados de acuerdo a los supuestos del ejercicio de la Tesis / Elaboración: La Autora

4.2.4 Mapa de Riesgos de TI – Resultado de la Evaluación

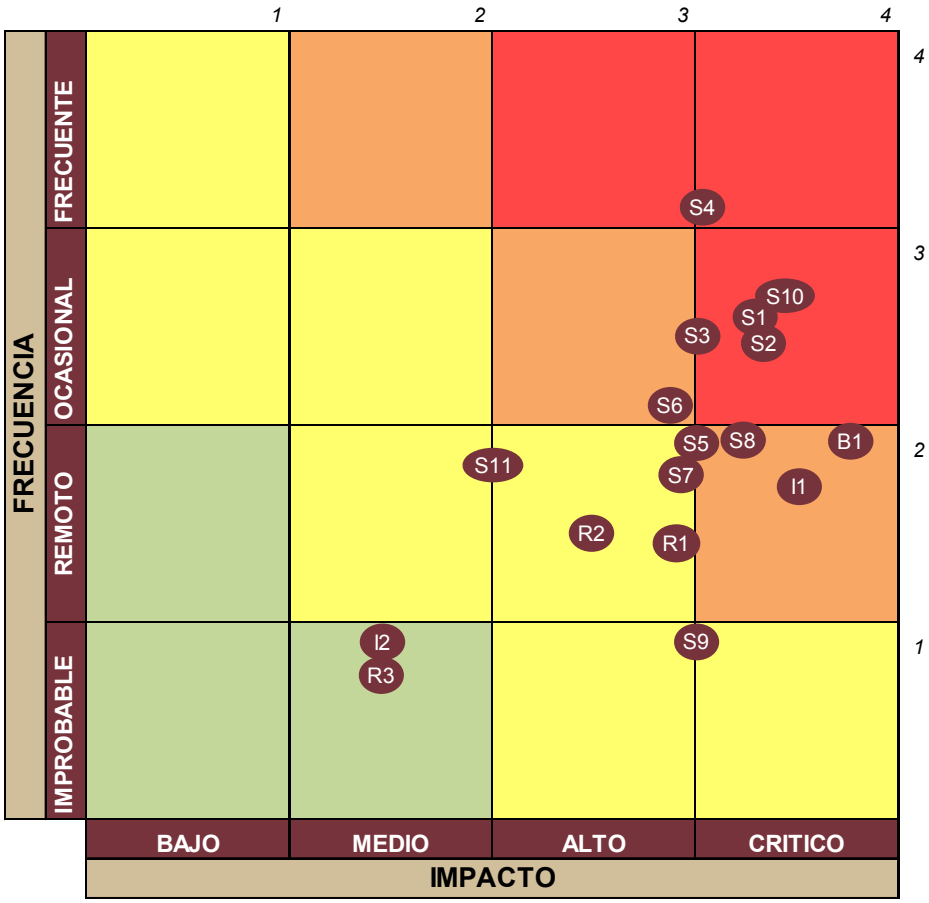
Una vez completado el análisis para cada uno de los elementos del Universo identificado de TI, se puede graficarlos en el Mapa de Riesgo.

Para efectos de este trabajo, se estará simulando el resultado de los elementos adicionales no cubiertos en los análisis individuales de Riesgo presentados en la sección anterior.

Es conveniente, al tener la calificación final, el revisar los resultados con Usuarios claves, para verificar que no existan condiciones que hagan modificar las apreciaciones del riesgo, y/o confirmar de que se tiene una visión similar.

El resultado aplicado al Mapa de Riesgos de TI, se lo puede apreciar en el siguiente Gráfico:

Gráfico No. 23 - Mapa de Riesgos de TI - Modelo de Aerolínea Doméstica Ecuatoriana



Las calificaciones individuales (basadas en los análisis individuales de elementos específicos y en estimaciones generales) son:

Tabla No. 19 - Calificaciones de Impacto y Frecuencia del Universo de TI

Ref	Elemento	Impacto	Frecuencia	
I1	**Data Center**	3.55	1.73	*(*)*
I2	**Centro Datos Secundarios**	1.5	1	
R1	**Firewalls**	3.00	1.45	*(*)*
R2	**vLANs**	2.5	1.45	
R3	**Racks de Conexiones**	1.5	0.8	
B1	**Bases de Datos**	3.82	2.00	*(*)*
S1	**ERP**	3.27	2.55	*(*)*
S2	**Sist. Rev. Accounting**	3.27	2.55	
S3	**Sist. Compras N.A.**	3	2.55	
S4	**WebSite**	3.08	3.15	*(*)*
S5	**Sist. Venta of. Propias**	3	2	
S6	**Sistema Reservas**	2.87	2.20	*(*)*
S7	**Sist. Control de Combustible**	3	1.8	
S8	**Sist. Nómina**	3.3	2	
S9	**Sist. Control Gastos Op.**	3	1	
S10	**MROs**	3.3	2.6	
S11	**Sist. De Lealtad**	2	1.8	

(*) Análisis individual de Riesgo desarrollado en detalle

Fuente: La Autora / Elaboración: La Autora

Aquellos elementos que caen en las casillas señaladas en rojo, en el Mapa, representan las de mayor riesgo, y por lo tanto pueden ser de un

mayor interés para la Auditoria y/o pueden requerir de un Plan de actividades más extenso.

Los elementos que se encuentran en la zona naranja representan el siguiente grupo de interés para la Auditoria interna, en donde el riesgo es medio – alto. Se puede realizar planes de auditoría con alcances focalizados, para cubrir aquellos aspectos que se perciben de valor agregado el auditarlos.

En la siguiente zona amarilla, el riesgo es medio – bajo. La Auditoria Interna puede decidir auditar una muestra, en caso de percibir interés en la organización y/o usuarios claves, con enfoques puntuales en procesos, tópicos, etc, que sean los más representativos y/o críticos.

Por contraste, aquellos elementos que están en la zona verde (ej. Centro de Datos Secundarios o Rack de Conexiones) se aprecian con un nivel de riesgo bajo, y por lo tanto la Auditoria Interna debe definir si es de interés el cubrirlas en su Plan de Actividades o no.

CAPITULO V

5 FORMALIZACIÓN DEL PLAN DE AUDITORIA INTERNA DE SISTEMAS / TI

De acuerdo a la Guía Práctica del IIA, *"GTAG 11 - Developing the IT Audit Plan / Desarrollando el Plan de Auditoria de TI",* mencionada en el Capítulo II – Marco Teórico de esta Tesis, los pasos sugeridos para elaborar el Plan de Auditoria de Sistemas / TI, son:

A. Entender el Negocio
B. Definir el Universo de TI
C. Realizar evaluaciones de Riesgo
D. Formalizar el Plan de Auditoria

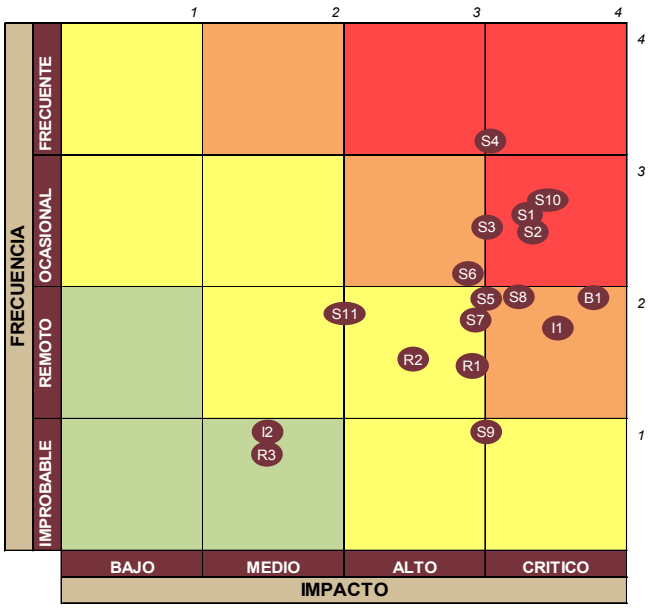
La cobertura de las tres primeras fases, ya ha sido realizada en Capítulos previos.

Para el Entendimiento del Negocio, se ha presentado información de la industria aérea en general, de la región, y del Ecuador en el Capítulo I. Adicional en otros capítulos se ha presentado información específica de algunos competidores relevantes para Latinoamérica y/o Ecuador, tales como Avianca, Copa, Lan y Volaris.

Para la Definición del Universo de TI, se realizó un ejercicio en el Capítulo III de esta Tesis, identificando varios posibles sujetos o elementos a auditar.

La Evaluación del Riesgo de TI fue el objetivo del Capítulo IV, llegando al siguiente modelo propuesto de sujetos y riesgo asociado:

Gráfico No. 24 - Matriz de Riesgos de TI y Sujetos del Universo de TI



Ref	Elemento	Impacto	Frecuencia	
I1	**Data Center**	3.55	1.73	*(*)*
I2	**Centro Datos Secundarios**	1.5	1	
R1	**Firewalls**	3.00	1.45	*(*)*
R2	**vLANs**	2.5	1.45	
R3	**Racks de Conexiones**	1.5	0.8	
B1	**Bases de Datos**	3.82	2.00	*(*)*
S1	**ERP**	3.27	2.55	*(*)*
S2	**Sist. Rev. Accounting**	3.27	2.55	
S3	**Sist. Compras N.A.**	3	2.55	
S4	**WebSite**	3.08	3.15	*(*)*
S5	**Sist. Venta of. Propias**	3	2	
S6	**Sistema Reservas**	2.87	2.20	*(*)*
S7	**Sist. Control de Combustible**	3	1.8	
S8	**Sist. Nómina**	3.3	2	
S9	**Sist. Control Gastos Op.**	3	1	
S10	**MROs**	3.3	2.6	
S11	**Sist. De Lealtad**	2	1.8	

(*) Análisis individual de Riesgo desarrollado en detalle

A continuación se desarrollará la Formalización del Plan de Auditoria de Sistemas / TI en este Capítulo, teniendo como referencia sugerencias dadas en la Guía GTAG-11 de la IIA, mencionada previamente.

5.1 Formalización del Plan de Auditorias de Sistemas / TI

Una vez analizado el Universo de TI y los Riesgos asociados a los sujetos o elementos de interés de la auditoria, en la elaboración del Plan se pueden considerar las siguientes actividades:

- Retroalimentación / requerimientos de Usuarios claves / Accionistas / Partes interesadas
- Alineación con Auditoria Externa y otras áreas de control, en caso de estar presentes en el negocio
- Alineación con el área de TI y otras áreas del negocio
- Alineación con requerimientos externos (regulatorios, de seguros, etc.)

- Alineación con otras actividades de Auditoria en el Departamento (Auditorias Financieras, Operativas, etc.)
- Priorización de los sujetos / elementos a auditar
- Análisis de los recursos de Auditores de Sistemas / TI versus las posibles tareas y actividades del departamento.
- Elaboración de un Plan preliminar de Auditoria de Sistemas / TI
- Presentación al Comité de Auditoria / Junta de accionistas, y alta Gerencia
- Publicación / Difusión del Plan aprobado.

En las siguientes secciones se presenta un desarrollo de las actividades mencionadas.

5.1.1 Retroalimentación / requerimientos de Usuarios claves / Partes interesadas

Dado que uno de los objetivos del Departamento es el de proveer aseguramiento sobre los controles, el nivel de gobierno y los riesgos a sus usuarios principales (El Comité de Auditoria / Junta / Partes interesadas, y la Alta administración), una actividad en la Fase de formalización del Plan es el de obtener retroalimentación acerca de cuáles son las preocupaciones y las percepciones de riesgo que pudieran tener las Partes interesadas / personas claves de la organización.

Las Fases anteriores, de identificar el Universo de TI y de analizar los riesgos relacionados, muy probablemente cubrirán gran parte de las inquietudes que puedan tener los usuarios principales. Sin embargo siempre puede haber temas que no hayan sido previamente identificados y /o futuros proyectos que estén por desarrollarse dentro de la organización, y que pueden enriquecer el Plan y/o hacer énfasis en tópicos específicos. Son los usuarios principales los que tienen una visión del estado actual de la organización, y hacia dónde se dirige / evoluciona, por lo que la retroalimentación de ellos es importante.

Además es posible que se presenten requerimientos a la Auditoria Interna en su rol de proporcionar un soporte de consultoría, por ejemplo acompañando a algún proyecto específico de cambio de sistemas, desarrollo de nuevos productos, etc.

Para efectos de este ejercicio, se supondrán los siguientes requerimientos y retroalimentación dados a la Auditoria Interna, como producto de las reuniones llevadas a cabo con el Comité de Auditoria / Accionistas / Partes Interesadas / Personal Clave de la organización (C-Level, VPs, etc.):

- La aerolínea iniciará un proyecto de Cambio de ERP de Gestión de Talento Humano, para lo cual se pide un apoyo de acompañamiento de la Auditoria en su rol de Consultor. Algunas de las fases del proyecto son selección del proveedor, rediseño de procesos, migración del Sistema actual al nuevo ERP y revisión de nivel de control (operativo, financiero, de TI) una vez el ERP esté instalado. Se espera migrar al nuevo Sistema el 01 de Noviembre.
- La aerolínea, como parte de su plan de renovación y cambio de flota, estará saliendo del modelo de avión más antiguo de manera escalonada (en un período de 2 años), reemplazándolo por otros aviones de un nuevo modelo. Este plan contempla una venta de las piezas y partes que se tengan del modelo antiguo, tanto en la Bodega central ubicada en GYE, como las mantenidas para el Mantenimiento de línea en cada aeropuerto, por lo que la confiabilidad en los inventarios de piezas y partes aeronáuticas manejadas por el MRO es importante. Además se desea tener un nivel de aseguramiento sobre la efectividad y los controles del sistema MRO actual en general, debido a la inversión en nuevas piezas y partes de los nuevos aviones, y a la implementación de los nuevos programas de mantenimiento para las Aeronaves que serán integradas a la flota.

- No se percibe un nivel de riesgo importante en los Sistemas para el Control de los Gastos Operativos, y los Sistemas de Control de combustible. Se maneja en pocas personas de la contabilidad de manera centralizada, y los proveedores Aeroportuarios y de Combustible son pocos. Además está un proyecto en marcha para unificar los proveedores de Catering (Comidas de Servicio a Bordo), y Transporte de Pasajeros y Empleados (Para la movilización de la Tripulación, Personal de Operaciones Terrestres, Entrega de equipaje rezagado de pasajeros, etc) a nivel nacional, en vez de tener proveedores diferentes en c/aeropuerto. Esto hará que el control de los gastos sea más fácil y se tendrán facturas unificadas.

Los efectos de estos requerimientos y retroalimentación al Diseño del Plan anual de Auditoria Interna de Sistemas / TI serán:

- Incorporar una nueva tarea de acompañamiento al Proyecto de nuevo ERP de Gestión del Talento Humano, con actividades reducidas, en un rol de Consultoría
- Dar un mayor nivel de prioridad a la Auditoria del Sistema de MRO, que ya era parte del Universo a Auditar, con énfasis en el Control de los inventarios de Piezas y Partes aeronáuticas.
- Eliminar o reducir las Auditorias relativas al Sistema de Control de Gastos Operativos y de Combustible.

5.1.2 Alineación con Auditoria Externa y otras áreas de control, en caso de estar presentes en el negocio

En caso de existir otras áreas de control dentro de la organización, se puede considerar el compartir los proyectos de actividades del área, para evitar caer en revisiones exhaustivas del mismo tema / sujeto, a la vez, y detectar qué posibles áreas / sujetos / elementos, no están siendo auditados o revisados por ninguna área de control.

En caso de existir la presencia de Auditoria externa, puede que las tareas se complementen. Por ejemplo en el caso de Bases de Datos, un ente de control puede analizar las Bases de Datos de dos o tres Sistemas Financieros, y la Auditoria interna puede enfocarse en analizar las otras Bases de Datos no cubiertas por la Auditoria Externa.

Otro punto a destacar es que se puede analizar los reportes emitidos por la Auditoria Externa y otros organismos de control, para revisar si existen algunos sujetos / elementos / Hallazgos, que no hayan sido considerados en análisis previos, y sea de valor agregado el incluirlos en el Plan de actividades.

En esta Tesis se supondrá que la información disponible de Auditoria Externa y otros organismos de control de la aerolínea, no modifica el ejercicio del diseño del Plan.

5.1.3 Alineación con el área de TI y otras áreas del negocio

En una auditoria se requiere la participación tanto del auditor como del auditado. Es por esto que es aconsejable tomar en cuenta en el Diseño del Plan de Actividades de Auditoria, posibles restricciones de tiempo en las áreas a auditar y/o Usuarios del negocio con quienes se piensa trabajar.

Algunos Usuarios Principales del negocio, a considerar para hacer esta alineación de las actividades son:

- El CIO, o responsable del Departamento de TI dentro de la organización: Es quien lidera, administra, coordina y toma gran parte de las decisiones referentes a tecnología en la empresa. Debido al carácter de Auditoria de Sistemas / TI, esta es una de las alineaciones más importante a considerar.
- El CFO, o responsable del Departamento Contable – Financiero dentro de la organización. Es quien tiene a su cargo la parte contable y financiera de la empresa, quien elabora los Estados Financieros,

vela por los activos, proporciona información financiera para toma de decisiones, y maneja el flujo de caja, entre otras funciones. Dado que el énfasis de las Auditorias a considerar en el Plan es el del impacto en Estados Financieros, probablemente se requerirá tiempo de las áreas financieras durante el desarrollo de las auditorias.

- Vicepresidentes, Directores, gerentes de otras áreas: Dependiendo de la estructura organizacional de la empresa, se encontrarán diferentes departamentos: por ej., Talento Humano, Mantenimiento, Comercial, Operaciones de Vuelo, Operaciones Terrestres, Atención al Cliente, etc. Es una buena práctica el considerar las actividades de aquellos departamentos con los que se va a trabajar en las auditorias.

Para propósitos del ejercicio de esta Tesis, se supondrá las siguientes condiciones mencionadas por los Usuarios, las cuales influenciarán el calendario de las actividades de las auditorias planificadas:

- Tanto el Departamento de TI como el Financiero no tendrán mucha disponibilidad de tiempo, debido al atendimiento a la Auditoria Externa, y al Cierre Contable, durante el Primer Trimestre del Año.
- Se espera la venta de piezas y partes aeronáuticas del modelo viejo a ser realizado a inicios del 2do. Semestre. Nuevas piezas y partes de los nuevos modelos de avión se espera empezar a recibir a partir del Cuarto Trimestre.
- El nuevo Proyecto del ERP de Talento Humano inicia en Enero.
- Hay un lineamiento de la empresa, de no tocar los sistemas e infraestructura de TI durante la Temporada alta Navideña, iniciando el 1 de diciembre y terminando el 31 de enero del siguiente año. Durante esas fechas no hay cambios de sistemas, ni desarrollo de proyectos de TI, a menos que sea urgentemente requerido por algún problema de estabilidad en los servicios de TI. Personal en ciertos cargos de TI podrían estar en vacaciones.

5.1.4 Alineación con requerimientos externos (regulatorios, de seguros, etc.)

La industria aérea es una actividad altamente regulada. Y como tal, podrían existir exigencias con relación a ser capaz de probar un adecuado monitoreo y evaluación internos, de ciertos elementos / procesos, etc.

Un ejemplo es el caso de las aseguradoras; para ciertos productos tales como Pólizas de fidelidad de empleados (que aseguran a la empresa en caso de existir un incidente de fraude ocasionado por personal interno), podrían exigir a la aerolínea el mantener periódicamente una auditoria sobre elementos / procesos / sistemas considerados de alto impacto para los Estados Financieros.

Es conveniente al momento del Diseñar el Plan, recabar información sobre las posibles exigencias, y revisar si existe alguna actividad a considerar.

Para los efectos del ejercicio de esta Tesis, se asume que no existen actividades adicionales a considerar, producto de regulaciones y/o condiciones de Seguros.

5.1.5 Alineación con otras actividades de Auditoria en el Departamento (Auditorias Financieras, Operativas, etc.)

Las Auditorias de Sistemas / TI no necesariamente deben de verse o planificarse como auditorias aisladas, sino que, idealmente, debiera de trabajarse con un enfoque de Auditorias integrales: En donde el sujeto / elemento a ser auditado, sea analizado por un equipo integral de Auditores Financieros, Operativos, y de TI.

Esta visión integral de actividades permite dar una opinión objetiva más completa: que no sólo abarque un punto de vista financiero o de TI, sino que de un vistazo completo.

Además la tecnología existe como soporte a las operaciones de la empresa. En algunas ocasiones hallazgos de debilidades en TI tienen su raíz en el negocio, y las remediaciones no necesariamente inician en TI.

Es conveniente, por lo tanto, el integrar / alinear el Diseño de las actividades de Auditoria de Sistemas / TI con el resto del área de Auditoria Interna, y trabajar en encontrar sinergias y complementos con los auditores de otras ramas. Por ejemplo, al analizar el ERP se puede complementar con una auditoria de los Procesos de consolidación de los Estados Financieros, o al auditar el Sistema de Programa de Lealtad agrega valor si la revisión contempla el análisis financiero: la metodología de cálculo de las principales variables y su reflejo en los Estados Financieros.

En el ejercicio desarrollado en esta Tesis, se asumirá que las actividades están alineadas al interior del Departamento de Auditoria Interna, y que para ciertas auditorias de Sistemas, se estará trabajando con programas de Auditorias Financieras y/o Operativas sobre el mismo elemento o sujeto.

5.1.6 Priorización de los sujetos / elementos a auditar

Dado que los recursos del Departamento de Auditoria Interna son limitados (en disponibilidad de Auditores de Sistemas / TI, en tiempo y presupuesto), es conveniente realizar una priorización de las auditorias identificadas hasta el momento, considerando factores tales como:

- La nueva información disponible, proporcionada por las Partes interesadas y Usuarios Principales, en cuanto a requerimientos adicionales, modificación de la percepción de riesgo, etc.
- Resultados de Auditorias anteriores. Por ejemplo, si en años anteriores un sujeto ya fue auditado, y los resultados fueron considerados altamente negativos, existe un mayor interés por volver a realizar la auditoria, para poder medir si hubo avances en el nivel del control interno y/o las recomendaciones fueron implementadas.

- La estabilidad del sujeto o elemento a auditar. Si algún sujeto (Proceso, Unidad, Sistema, etc.) está siendo agresivamente modificado, probablemente no es un buen momento para auditar, ya que los catalizadores estarán variando significativamente (Procesos, Organización, etc.), y se correría el riesgo de que, cuando se termine la auditoria, los Hallazgos ya no sean relevantes, porque no corresponden a la realidad del sujeto o elemento, o había inestabilidad en los datos debido a los cambios y podría dar lugar a Hallazgos que no son válidos.
- Planificaciones de Años anteriores: Si un sujeto quedó por fuera de la planificación en años previos, puede haber un compromiso de la Auditoria Interna por auditarlo en el siguiente ejercicio.

Se debe de tener además una perspectiva, de manera general, de cuántas horas podrían consumir las labores, y cuáles tópicos o procesos de TI se van a considerar.

El cálculo de las horas a dedicar en las auditorias individuales suele ser realizado tomando el mejor estimado de tiempo, basado en factores tales como: experiencias anteriores de auditoria, la complejidad de los procesos o tópicos a discutir, la extensión geográfica donde residen los sujetos o elementos, la habilidad de los Auditores, la expectativa de atención de los auditados, disponibilidad de tiempo de Usuarios claves, el alcance deseado, la profundidad de la revisión, etc.

Para efectos del ejercicio de esta Tesis, se presenta a continuación el listado de las posibles auditorias, con los Procesos o Tópicos mencionados en el Capítulo II, y con un estimado de horas.

Gráfico No. 25 - Lista de Sujetos o Elementos a Auditar (Prioridades, Tópicos y Horas estimadas)

Nivel de Riesgo	Ref	Elemento	Impacto	Frecuencia	I x F	Procesos - Tópicos de TI a considerar: Administración de Los Cambios	Seguridad de la Información	Administración Amb. Físicos	Continuidad de los Servicios	Administración de Serv. Terceros	Estrategia TI y Controles Asoc.	Otros	Horas Estimadas
	S4	**WebSite**	*3.08*	*3.15*	9.70	☑	☑		☑	☑	☑		200
	S10	**MROs**	*3.3*	*2.6*	8.58	☑	☑		☑		☑	☑	250
	S2	**Sist. Rev. Accounting**	*3.27*	*2.55*	8.34	☑	☑		☑		☑		200
	S1	**ERP**	*3.27*	*2.55*	8.33	☑	☑		☑		☑		200
	S3	**Sist. Compras N.A.**	*3*	*2.55*	7.65	☑	☑		☑		☑		150
	B1	**Bases de Datos**	*3.82*	*2.00*	7.64	☑	☑		☑		☑		150
	S6	**Sistema Reservas**	*2.87*	*2.20*	6.31		☑		☑	☑	☑		100
	I1	**Data Center**	*3.55*	*1.73*	6.12	☑	☑	☑	☑	☑	☑	☑	100
	S5	**Sist. Venta of. Propias**	*3*	*2*	6.00	☑	☑		☑		☑		150
	R1	**Firewalls**	*3.00*	*1.45*	4.36	☑	☑	☑	☑		☑		100
	R2	**vLANs**	*2.5*	*1.45*	3.63	☑	☑	☑	☑	☑	☑		100
	S11	**Sist. De Lealtad**	*2*	*1.8*	3.60	☑	☑		☑		☑	☑	200
	I2	**Centro Datos Secundarios**	*1.5*	*1*	1.50	☑	☑	☑	☑		☑		50
	R3	**Racks de Conexiones**	*1.5*	*0.8*	1.20	☑		☑	☑		☑		100
													2050

Fuente: La Autora / Elaboración: La Autora

Los cambios que refleja esta lista son:

- Más tiempo para la Auditoria de MRO, con el fin de cubrir un análisis relativo al inventario de Piezas y Partes Aeronáuticas pedida por los Usuarios Principales.
- Eliminación de las Auditorias de Costos Operativos y Combustible, debido a la apreciación de bajo riesgo por parte de las Partes interesadas.
- Eliminación de la Auditoría de Nómina, debido a que el Sistema va a cambiar a un nuevo ERP, y además Auditoria Interna estará acompañando el proyecto en un rol de consultoría.

5.1.7 Análisis de los recursos de Auditores de Sistemas / TI versus las posibles tareas y actividades del departamento

En base a la lista de sujetos o elementos de interés para la Auditoria de Sistemas, y tomando en cuenta la prioridad y estimación de horas requerida para cada actividad, es necesario revisarla versus los recursos disponibles, y las otras actividades del Departamento.

Algunos factores claves en la revisión son:

- El número de Auditores Internos de Sistemas / TI: Dado el perfil en conocimientos técnicos de TI, aplicaciones, manejo de Bases de Datos, etc., los Auditores internos de Sistemas suelen ser la minoría en el Departamento, y no son fáciles de reemplazar. Únicamente un conocimiento de TI no es suficiente, sino que se requiere además una formación en técnicas y conocimientos de Auditoria.
- El Nivel de conocimientos técnicos de los Auditores internos de Sistemas / TI versus las posibles actividades y tareas. Frente a la amplitud de temas de TI, puede presentarse el caso de que los Auditores Internos de Sistemas no tengan los conocimientos específicos como para dar una opinión sobre el sujeto o elemento a auditar. En estos casos se puede considerar adquirir el conocimiento (lo cual conlleva tiempo), o realizar un outsorcing con algún proveedor / Firma de Auditores que si lo tengan.
- Un estimado de otras actividades no planificadas que pueden ser pedidas al Departamento de Auditoria Interna (involucramiento en temas de investigación de fraudes, acompañamiento en actividades puntuales de la operación, etc.).
- Un estimado de otras actividades internas del Departamento de Auditoria, tales como entrenamientos, asistencias a Congresos, vacaciones, etc.

En esta Tesis, se considerará que se cuentan con dos auditores internos de Sistemas / TI, con las calificaciones y conocimientos adecuados para los alcances globales planteados en el ejercicio de Diseño del Plan.

Sin embargo, las horas disponibles anuales, considerando los temas arriba mencionados (imprevistos, entrenamiento, vacaciones, etc.), sólo permiten una disponibilidad de 1,600 horas en total. No se considera la incorporación de ningún Auditor Interno de Sistemas / TI adicional para el año que se está planificando.

Dados los recursos mencionados en cuanto a horas de Auditoria de Sistemas / TI, y revisando la lista de sujetos con sus prioridades, se pueden tomar varias decisiones:

- Reducir el alcance de las auditorias para optimizar el Número de Horas y abarcar todos los sujetos. Esta opción tiene el peligro de que se puede sacrificar la calidad de las auditorias, y un alcance reducido podría obviar debilidades importantes,
- Considerar mover algunas Auditorias a otros años, enfocándose en aquellas que tienen un nivel de Riesgo más alto y/o son de interés para las Partes interesadas / Usuarios principales. Esta opción debe de mantener una planificación con un horizonte de varios años. Existe un peligro de que, en cada año, algunos sujetos o elementos siempre queden por fuera de la planificación, por aparecer consistentemente en el análisis como de Riesgo bajo.
- Considerar “partir” las Auditorias en diversos períodos: en el año 1 realizar un grupo de revisiones, y en el año 2, realizar otro grupo sobre el mismo sujeto. Esta opción conlleva un riesgo de que la visión final de la auditoria no sea consistente, ya que 2 (o más años) puede ser un plazo largo para suponer que el sujeto auditado permanecerá sin cambios significativos. Y si se desea mantener la misma muestra de datos del año 1, en el siguiente año puede no ser relevante para demostrar Hallazgos válidos.

- Considerar opciones de subcontratar la actividad a terceros, si el presupuesto lo permite y existe el interés del negocio, o pedir apoyo a otras áreas de control al interior de la empresa, ya sea en préstamo de recursos, o en inclusión de la actividad en el calendario de las otras áreas.

En el ejercicio planteado, se tomará la decisión eliminar algunos sujetos o elementos que tengan menor prioridad o nivel de riesgo, para cubrirlos en años posteriores.

La nueva lista, ajustada de acuerdo a la capacidad del Departamento de Auditoria Interna, sería:

Gráfico No. 26 - Lista ajustada de Sujetos o elementos a Auditar (Prioridades, Tópicos y Horas estimadas)

Nivel de Riesgo	Ref	Elemento	Impacto	Frecuencia	I x F	Procesos - Tópicos de TI a considerar: Administración de Los Cambios	Seguridad de la Información	Administración Amb. Físicos	Continuidad de los Servicios	Administración de Serv. Terceros	Estrategia TI y Controles Asoc.	Otros	Horas Estimadas
	S4	**WebSite**	*3.08*	*3.15*	9.70	☑	☑		☑	☑	☑		200
	S10	**MROs**	*3.3*	*2.6*	8.58	☑	☑		☑		☑	☑	250
	S2	**Sist. Rev. Accounting**	*3.27*	*2.55*	8.34	☑	☑		☑		☑		200
	S1	**ERP**	*3.27*	*2.55*	8.33	☑	☑		☑		☑		200
	S3	**Sist. Compras N.A.**	*3*	*2.55*	7.65	☑	☑		☑		☑		150
	B1	**Bases de Datos**	*3.82*	*2.00*	7.64	☑	☑		☑		☑		150
	S6	**Sistema Reservas**	*2.87*	*2.20*	6.31		☑		☑	☑	☑		100
	I1	**Data Center**	*3.55*	*1.73*	6.12	☑	☑	☑	☑	☑	☑	☑	100
	S5	**Sist. Venta of. Propias**	*3*	*2*	6.00	☑	☑		☑		☑		150
	R1	**Firewalls**	*3*	*1.455*	4.36	☑	☑	☑	☑		☑		100
													1600

Fuente: La Autora / Elaboración: La Autora

5.1.8 Elaboración de un Plan preliminar de Auditoria de Sistemas / TI

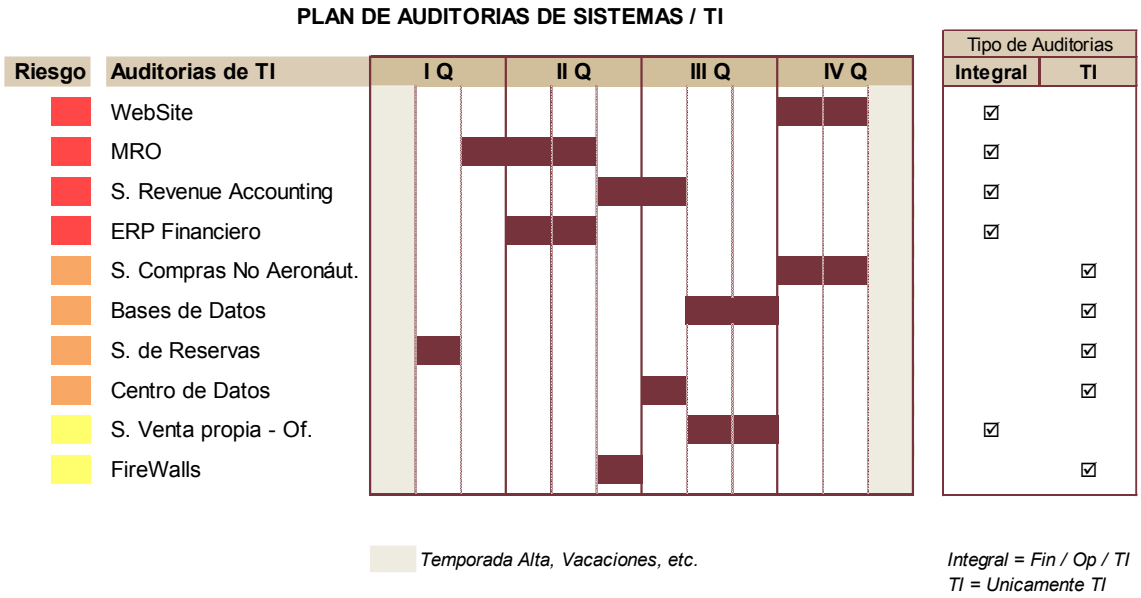
A partir de la lista depurada de sujetos o elementos a auditar, se debe elaborar un Calendario de las Auditorias individuales, tomando en cuenta (en la medida de lo posible), cualquier restricción mencionada por los Usuarios a

auditar, en cuanto a tiempos y recursos disponibles para atender a la Auditoria Interna.

Si bien la negociación de tiempos es difícil con las diferentes áreas, una auditoria puede alargarse innecesariamente, si es que los auditados no cuentan con la disponibilidad para atender la auditoria, por lo que es una práctica recomendable el encontrar el mejor tiempo disponible, tanto para el auditor como para el auditado.

Un ejemplo del Calendario, basado en el ejercicio de esta Tesis se presenta a continuación:

Gráfico No. 27 - Calendario Preliminar de Auditorias de Sistemas / TI



El mismo toma en cuenta:

- La no disponibilidad de recursos de Usuarios de TI / Temporada alta Navideña (diciembre y enero)
- La baja disponibilidad de las áreas de TI y CFO durante el I Q debido a la atención a la Auditoria Externa y Cierre Contable anual
- El inicio de actividades de Auditoria de MRO durante el I Semestre, en adelanto a los eventos del II Semestre

- El tipo de Auditoria: Integral, si es que hay análisis de Auditoria Financiera y Operativa, aparte del enfoque de TI, o TI puro, es decir, alcance de la actividad únicamente con Auditoria de Sistemas / TI

5.1.9 Presentación al Comité de Auditoria / Junta de accionistas, y alta Gerencia

El IIA en sus Normas para el ejercicio profesional de la Auditoria Interna, (Norma 1110 – Independencia dentro de la Organización, 2013), resalta que el Departamento de Auditoria Interna depende funcionalmente del Consejo / Comité de Auditoria. Y algunas de las labores del Consejo o Comité son la de aprobar el Plan de Auditoria basado en Riesgos, aprobar el Presupuesto y el Plan de recursos.

Por consiguiente, es necesario como siguiente paso en la Formalización del Plan de Auditoria, el presentarlo para aprobación al Consejo o Comité de Auditoria.

En la presentación se puede incluir un resumen de:

- Las bases del análisis: Entorno de la industria y competidores, el Universo de TI a auditar, y la Matriz del Riesgo,
- Los objetivos globales de la auditoria de Sistemas / TI: Enfoque en temas tales como administración del cambio, continuidad de la operación, etc., y basado en el Marco de referencia COBIT 5,
- Los recursos con los que se cuenta: Los auditores internos de Sistemas / TI y sus calificaciones / certificaciones / conocimientos, etc., y si fuera pertinente un presupuesto (viajes, capacitaciones, etc),
- Los pasos previos realizados para recabar retroalimentación y/o confirmación con Usuarios principales / Usuarios del negocio,
- La lista depurada de sujetos o elementos a auditar, con sus niveles de riesgo y temas macro a analizar, incluyendo una revelación de cuáles sujetos o elementos se eliminaron del Plan, los criterios en que se

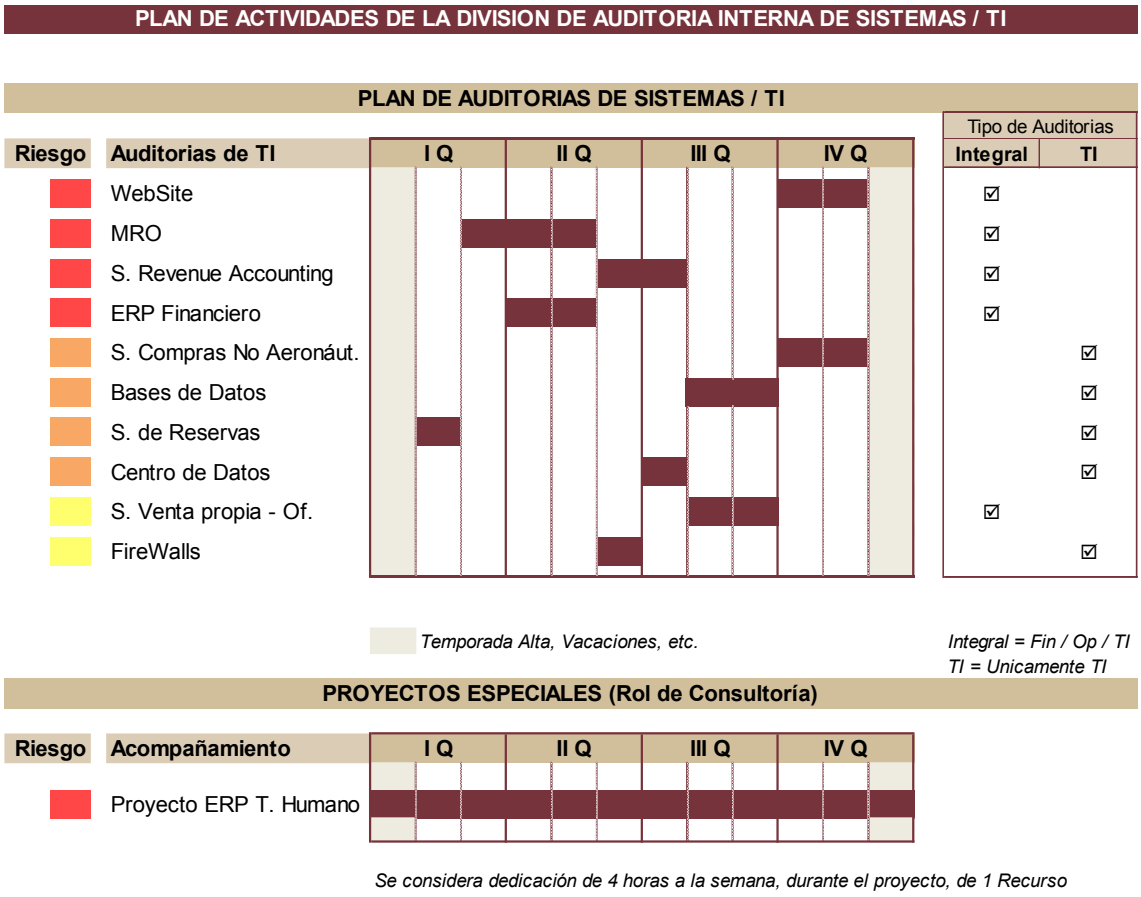
basó esa eliminación y las medidas posibles a tomar (incremento de más recursos de Auditores, traslado de las actividades a años posteriores, etc.)

- El Calendario de las Auditorias Planificadas
- Otras actividades relevantes si las hubiere: Por ej. acompañamiento a proyectos, seguimiento de Auditorias anteriores, etc.

Para efectos de este ejercicio, se asume que no hubo cambios a la Planificación de actividades, y el Plan de Auditorias de Sistemas / TI fue aprobado.

Un ejemplo del Calendario presentado, así como de información de otras actividades se presenta a continuación:

Gráfico No. 28 - Calendario de Actividades de Auditoria Interna de Sistemas / TI



5.1.10 Publicación / Difusión del Plan aprobado:

Una vez aprobado el Plan de Auditorias, se puede difundir al interior del equipo de Auditoria Interna, y también se puede compartir con Usuarios claves del negocio, por ejemplo a nivel de CFO, CIO y CEO.

El área debe empezar a preparar planes de actividades más detallados y elaborar una programación para cada auditoria, a medida que se van desarrollando las actividades.

CONCLUSIONES

Dada la alta dependencia de la tecnología en la industria aérea comercial, el diseño de un Plan anual de Auditoria Interna de Sistemas / TI, basado en riesgos, debe ser un componente permanente de un Plan de Auditoria Interna global, para el modelo de una Aerolínea Doméstica Ecuatoriana.

El rol de Auditor de Sistemas / TI, necesita manejar tanto las habilidades y herramientas de la auditoría interna, como los conocimientos técnicos apropiados para dar una opinión.

Ante lo complejo que puede ser el entender la arquitectura tecnológica, es conveniente tener un Marco de trabajo apropiado para usar como referencia en el diseño del Plan. Esta Tesis ha trabajado con COBIT 5, difundido por la ISACA, el cual, aparte de facilitar el entendimiento del Gobierno y la Gestión de TI, brinda una metodología para el análisis de escenarios de Riesgos de TI.

En la evaluación de los Riesgos de TI, es importante tener el criterio adecuado para escoger los escenarios más apropiados a cada sujeto o elemento identificado de TI, y realizar una evaluación de posible impacto y frecuencia.

El mapa de Riesgos obtenido, frecuentemente debe priorizarse, para adaptar la lista de las posibles auditorias, a los recursos del Departamento, y las necesidades de la organización / partes interesadas.

RECOMENDACIONES

Una aerolínea tiene múltiples sistemas y componentes tecnológicos. Para establecer el Universo auditable de TI, es conveniente basarse en un criterio (impacto en operaciones, en resultados financieros, etc.) que ayude a identificar qué es crítico o importante.

En la fase de evaluación del riesgo, se debe preferir manejar un número limitado de escenarios. El tratar de utilizar todos los escenarios posibles, probablemente no sea realista, y puede ocasionar que la Auditoria pierda enfoque de aquellos riesgos que tienen una mayor probabilidad de materializarse.

En la fase de formalización del Plan, se debe considerar las necesidades o inquietudes de Usuarios claves (El comité de Auditoria / Junta / Alta administración) y estar alineados con las percepciones de riesgo y expectativas del rol de Auditoria Interna de sistemas / TI, que ellos puedan tener.

Otros actores tales como reguladores externos, compañías de seguros, Bancos, etc., pudieran también requerir el mantener evaluaciones internas específicas, por lo que el Departamento de Auditoria Interna debe estar consciente de esas regulaciones, e incluirlas, si amerita, en su calendario de actividades.

Por último, dado que las actividades del Departamento son dinámicas, y pueden cambiar o tener que adaptarse de acuerdo a las necesidades del negocio (ej. atención a proyectos urgentes, investigación de fraudes, etc.), se recomienda considerar un calendario de actividades que tome en consideración un estimado de tiempo para auditorias no planificadas, y otros eventos que suela manejar el área.

BIBLIOGRAFÍA

Avianca Holdings S.A. (2014) *FORM 20-F Annual Report… for the fiscal year ended December 31, 2013*
Recuperado de http://www.sec.gov/Archives/edgar/data/1575969/000119312514171823/d717144d20f.htm

"Benchmarking". Wikipedia.
Recuperado de http://es.wikipedia.org/wiki/Benchmarking

CnnExpansión (2012) Profeco multa a Volaris con 2.5 mdp. *CnnExpansión, 14 de agosto del 2012*
Recuperado de http://www.cnnexpansion.com/negocios/2012/08/14/volaris-pagara-multa-de-25-mdp

Diario El Telégrafo (2013) 10.9 Millones de personas se movilizaron en el 2013. *Diario El Telégrafo, 16 de Mayo del 2013.*
Recuperado de http://www.telegrafo.com.ec/economia/item/10-9-millones-de-personas-se-movilizaron-en-avion-en-2013.html

Diario La Prensa (2013) Continúan las demoras en los vuelos de Aerolíneas, tras las 60 cancelaciones por problemas tecnológicos. *Diario La Prensa - Argentina, 11 de Julio del 2013*
Recuperado de http://www.laprensa.com.ar/409880-Continuan-las-demoras-en-los-vuelos-de-Aerolineas-tras-las-60-000119312514167633/d715762d20f.htm

Donathan, Cliff (2013) So you want to be an IT Auditor, *IIA Ia Magazine*
Recuperado de https://na.theiia.org/

Finanzas Personales (2011) Avianca se pronuncia sobre fraude a cuentas de Millas. *Finanzas Personales - Colombia.*
Recuperado de http://www.finanzaspersonales.com.co/ultimas-noticias/articulo/avianca-pronuncia-sobre-fraude-cuentas-millas/43765

Hernandez, Alex Enrique (2013) Copa Airlines confirma la cancelación de 75 vuelos, *La Prensa*
Recuperado de http://www.prensa.com/uhora/locales/copa-airlines-pasajeros-varados-tocumen-panama/216943

IATA (s.f.) Billing and Settlement Plan (BSP)
Recuperado de http://www.iata.org/services/finance/bsp/Pages/index.aspx

IATA (2014) *Comunicado No. 67 - Aerolíneas elevan en 31% su pronóstico de demanda de pasajeros para 2017 - 930 millones de pasajeros más que en 2012 -*
Recuperado de http://www.iata.org/pressroom/pr/Documents/Spanish-PR-2013-12-10-01.pdf

IIA - The Institute for Internal Auditors (2008) *Global technology audit guide - Developing the IT Audit Plan.*
Recuperado de https://na.theiia.org/standards-guidance/ recommended-guidance/practice-guides/Pages/Practice-Guides.aspx

IIA - The Institute for Internal Auditors (2013) *Normas internacionales para el ejercicio profesional de la Auditoria Interna*
Recuperado de https://na.theiia.org/standards-guidance/mandatory-guidance/Pages/Standards.aspx

IIA - The Institute for Internal Auditors (2013)*The three lines of defense in effective risk management and control*
Recuperado de https://na.theiia.org/standards-guidance/ recommended-guidance/Pages/Position-Papers.aspx

ISACA (2012) *COBIT 5 - Un marco de negocio para el gobierno y la gestión de las TI de la empresa*. USA: Autor.
Recuperado de http://www.isaca.org/

ISACA (2012) *COBIT 5 - Procesos catalizadores*. USA: Autor.
Recuperado de http://www.isaca.org/

ISACA (2013) *COBIT 5 for Assurance.*
Recuperado de http://www.isaca.org/

ISACA (2013) *COBIT 5 for risk*. USA: Autor.
Recuperado de http://www.isaca.org/

ISACA (2014) Evaluate, direct and monitor.
Recuperado de http://www.isaca.org/

ISACA (2014) *IS Audit and Assurance guideline 2201 engagement planning*
Recuperado de http://www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Documents/2201-Engagement-Planning_gui_Eng_0614.pdf

La Fábrica de Pensamiento - Instituto de Auditores Internos de España (2014) *Cobertura del riesgo tecnológico: hacia una Auditoría Interna de TI integrada*
Recuperado de http://www.iaiecuador.org/

La Fábrica de Pensamiento - Instituto de Auditores Internos de España (2014) *Marco de relaciones de Auditoría Interna con otras funciones de Aseguramiento - Guía práctica*
Recuperado de http://www.iaiecuador.org/

LATAM Airlines Group S.A. (2014) *FORM 20-F Annual Report… for the fiscal year ended December 31,2013*
Recuperado de http://www.sec.gov/Archives/edgar/data/1047716/000119312514172411/d710308d20f.htm

Martín, Hugo (2014) United Airlines computer glitch causes flight delays, *Los Angeles Times, February 18, 2014*
Recuperado de http://articles.latimes.com/2014/feb/18/business/la-fi-united-computer-fritz-20140219

Moreno Mendoza, Cecilia (2014) Alarma a bordo. *Revista Vistazo, Volumen 1125 -Julio 10 / 2014*, (14-17).

Mouawad, Jad (2013) American Airlines resumes flights after a computer problem, *The New York Times, April 16, 2013*
Recuperado de http://www.nytimes.com/2013/04/17/business/american-airlines-cancels-flights-after-outage.html?_r=1&

Oxford Economics (2011) Economic benefits from Air Transport in Ecuador
Recuperado de http://www.benefitsofaviation.aero/Documents/Benefits-of-Aviation-Ecuador-2011.pdf

Pearce, Brian (2013) Airlines worldwide: The value they create and the challenges they face.
Recuperado de http://www.iata.org/economics

PWC - PriceWaterhouse Coopers (2014) *Tailwinds 2014 airline industry trends*
Recuperado de http://www.pwc.com/us/en/industrial-products/publications/tailwinds-the-connected-airline.jhtml

Quevedo H., Norvey (2011) Los "aviones' de las millas. *Diario El Espectador - Colombia, 06 dic 2011*
Recuperado de http://www.elespectador.com/noticias/judicial/los-aviones-de-millas-articulo-315364

Revista Ekos, Ranking de Empresas (2013) (www.ekosnegocios.com)

Recuperado de http://www.ekosnegocios.com/empresas/RankingEcuador.aspx

Rodríguez Samaniego, CPA José Antonio (s.f.) *Texto guía - Auditoria de sistemas*. Guayaquil:UCSG

Singleton, Tommie W. (2010) The minimum IT Controls to assess in a Financial Audit (Part I and Part II). *ISACA Journal 1*

The Guardian (2013) Delta Air Lines sells ultra-low fares after computer glitch. *The Guardian, 26 December 2013*
Recuperado de http://www.theguardian.com/business/2013/dec/26/delta-airlines-ultra-low-fares-computer-glitch

The Huffington Post (2013) United Airlines honors tickets bought during computer glitch*. The Huffington Post, August 09, 2013*
Recuperado de http://www.huffingtonpost.com/2013/09/13/united-airlines-cheap-tickets_n_3922275.html

Volaris Aviation Holding Company. (2014) *FORM 20-F Annual Report… for the fiscal year ended December 31, 2013*
Recuperado de http://www.sec.gov/Archives/edgar/data/1520504/000119312514168329/d713334d20f.htm/

Yildirim, Tugba (2014) Critical information systems processes. *ISACA Journal 2*
Recuperado de http://www.isaca.org/Journal/Past-Issues/2014/Volume-2/Pages/Critical-Information-Systems-Processes.aspx

ANEXOS

Anexo No. 1: Estado Financiero de Resultados Avianca Holdings S.A. (*)

Estado Financiero de Resultados Avianca Holdings S.A.(*)

(En Miles de USD)

	2013		2012	
Ingresos Operacionales				
Pasajeros	3,862,397	*84%*	3,550,559	*83%*
Carga y Otros	747,207	*16%*	719,097	*17%*
Total Ingresos Operacionales	**4,609,604**	***100%***	**4,269,656**	***100%***
Gastos Operacionales				
Operaciones de Vuelo	82,872	*2%*	84,774	*2%*
Conbustible de Aeronaves	1,325,763	*31%*	1,305,396	*33%*
Operaciones Terrestre	343,812	*8%*	321,552	*8%*
Arrendamiento de Aeronaves	273,643	*6%*	255,566	*6%*
Servicios a Pasajeros	143,512	*3%*	132,823	*3%*
Mantenimiento y Reparaciones	188,659	*4%*	222,705	*6%*
Tráfico Aéreo	180,140	*4%*	169,650	*4%*
Mercadeo y Ventas	584,468	*14%*	522,645	*13%*
Generales, Administrativos y otros	257,273	*6%*	206,666	*5%*
Salarios, Sueldos y Beneficios	674,951	*16%*	644,901	*16%*
Depreciación, amortización y Deteric	169,580	*4%*	122,080	*3%*
Total Gastos Operacionales	**4,224,673**	***100%***	**3,988,758**	***100%***
Utilidad de Operación	**384,931**		**280,898**	
Gastos por intereses	(113,330)		(122,112)	
Ingresos por intereses	11,565		25,006	
Instrumentos Derivados	(11,402)		(24,042)	
Diferencial Cambiario	23,517		(56,788)	
Utilidad antes de IR	**295,281**		**102,962**	
Gasto de IR - Corriente	(40,269)		(49,884)	
Gasto de IR - Diferido	(6,164)		(14,821)	
Total Gasto por IR	(46,433)		(64,705)	
Utilidad Neta del año	**248,848**		**38,257**	
% Utilidad / Ingresos	*6%*		*1%*	

(*) Fuente: Estados Financieros publicados por Avianca Holdings S.A. (www.aviancaholdings.com) - Sección 20F/Informes Anuales. Los % son presentados únicamente para efecto de análisis de esta Tesis.

Anexo No. 2: Estado Financiero de Resultados Copa Holdings S.A. (*)

Estado Financiero de Resultados Copa Airlines (*)

(En Miles de USD)

		2013		2012	
Operating Revenue	*Ingresos Operacionales*				
Passenger Revenue	*Pasajeros*	2,519,650	*97%*	2,163,136	*96%*
Cargo, Mail & Other	*Carga, Correo y Otros*	88,682	*3%*	86,252	*4%*
Total Operating Revenue	***Total Ingresos Operacionales***	**2,608,332**	***100%***	**2,249,388**	***100%***
Operating Expenses	*Costos Operacionales*				
Aircraft Fuel	*Combustible de Aeronaves*	783,092	*37%*	725,763	*39%*
Salaries and Benefits	*Salarios y Beneficios*	276,156	*13%*	247,405	*13%*
Passenger Servicing	*Servicio a Pasajeros*	250,604	*12%*	217,137	*12%*
Commisions	*Comisiones*	103,685	*5%*	89,378	*5%*
Reservations and Sales	*Reservaciones y Ventas*	99,822	*5%*	84,992	*5%*
Maintenance, Materials and repairs	*Mantenimiento, Materiales y Rep.*	92,993	*4%*	92,166	*5%*
Depreciation, amortization and impairment	*Depreciaciones, Amor. y Deterioro*	137,412	*7%*	89,217	*5%*
Flight Operations	*Operaciones de Vuelo*	121,903	*6%*	104,993	*6%*
Aircraft Rentals	*Arrendamiento de Aeronaves*	90,233	*4%*	72,468	*4%*
Landing Fees and other Rentals	*Aterrizaje y otros arrendamientos*	50,288	*2%*	46,233	*3%*
Other	*Otros*	84,590	*4%*	77,101	*4%*
Total Operating Expenses	***Total Costos Operacionales***	**2,090,778**	***100%***	**1,846,853**	***100%***
Operating Income	***Utilidad de Operación***	**517,554**		**402,535**	
Non-Operating Income (expense):	*Ingresos No Operativos*				
Interest expense	*Gastos por Intereses*	(30,180)		(32,795)	
Interest capitalized	*Intereses Capitalizados*				
Interest income	*Ingresos por Intereses*	12,636		11,689	
Other, net	*Otros, Neto*	(11,440)		(15,086)	
Total Non-Operating Income (expense), net	***Total Ingresos No Operativos***	**(28,984)**		**(36,192)**	
Income before income taxes	***Utilidad antes de Impuestos***	**488,570**		**366,343**	
Provision for income taxes	*Provisión por impuestos de renta*	61,099		39,867	
Net income	***Utilidad Neta***	**427,471**		**326,476**	
	% Utilidad Neta / Ingresos	*17%*		*15%*	

(*) Fuente: Estados Financieros publicados por Copa Holdings S.A. (www.copaair.com) - Sección de Inversores - Annual Reports - 2013 Annual Report (Form 20F). Los % son presentados únicamente para efecto de análisis de esta Tesis. El texto original está redactado en ingles, pero para facilidades de comparación de este trabajo, se incluye una traducción sugerida del Inglés al español.

Anexo No. 3: Escenarios Genéricos de Riesgo sugeridos por el Modelo COBIT 5

(*Basados en libre traducción de los Escenarios Genéricos de TI, presentados en la Guía "COBIT 5 for Risk" publicada por la ISACA)*

		Tipos de Riesgo			
Ref.	**Categoría de Escenario de Riesgo**	**Estratégico**	**Proyectos**	**Operativos**	**Escenarios Negativos**
0601	Información (violación de Datos: daños, fuga de información y accesos)	S		P	Componentes de Hardware son dañados, conduciendo a una (parcial) destrucción de datos por personal interno
0602		S	S	P	La Base de datos está corrompida, conduciendo a datos inaccesibles
0603		S	S	P	Medio portable conteniendo datos sensitivos (CD, USBs o Pen Drives, Discos portables, etc) está perdido / revelado
0604		S	S	P	Datos sensitivos están perdidos / revelados debido a ataques lógicos
0605		S	S	P	Medios de respaldo están perdidos o los backups no son revisados para comprobar efectividad
0606		P	S	P	Información sensitiva es accidentalmente revelada debido a fallas en guías de cómo manejar información

0607		P	S	P	Datos (contables, relativos a seguridad, datos de ventas, etc), son modificados intencionalmente
0608		P	S	P	Información sensitiva es revelada vía email o medios sociales
0609		P	S	P	Información Sensitiva es descubierta debido a ineficiente retención / archivo / eliminación de información
0610		P	S	P	Propiedades Intelectuales están perdidas y/o información competitiva es filtrada debido a personal clave dejando la organización
0611		P	S	P	La empresa tiene una sobreabundancia de datos y no puede deducir la información de negocios relevantes de los datos (ej. "Big Data" problem)
0701	Arquitectura (Visión y Diseño)	P	P	P	La arquitectura empresarial es compleja e inflexible, obstruyendo una posible evolución y expansión, y conduciendo a oportunidades perdidas de negocio
0702		P	S	P	La arquitectura empresarial no es la adecuada para los propósitos y no soportan las prioridades del negocio
0703		P	S	S	Hay una falla en adoptar y explotar nueva infraestructura de manera oportuna
0704		P	S	S	Hay una falla en adoptar y explotar nuevo software (funcionalidad, optimización,

					etc) de manera oportuna
0801	Infraestructura (Hardware, Sistemas Operativos y Tecnologías de Control) (Selección / Implementación, Operaciones y Supresiones definitivas o Retiros)	P	S	P	Nueva (innovativa) infraestructura es instalada y como resultado los sistemas se vuelven inestables, conduciendo a incidentes operacionales
0802		P	S	P	Los sistemas no pueden manejar los volúmenes transaccionales cuando el volumen de usuarios se incrementa
0803		P	S	P	Los sistemas no pueden manejar la carga de sistemas cuando nuevas aplicaciones o iniciativas son desarrolladas e instaladas
0804		P	S	P	Hay fallas de servicios públicos intermitentemente (telecomunicaciones, electricidad, etc)
0805		P	S	P	La tecnología en uso es obsoleta y no puede satisfacer los requerimientos de nuevos negocios (networking, seguridad, Bases de Datos, almacenamiento, etc)
0806				P	El hardware falla debido a sobrecalentamiento
0901	Software	P		S	Hay una inabilidad para usar el software para realizar los beneficios o salidas esperados (por ej. Fracaso para realizar modelos de negocios requerido o cambios organizacionales)

0902		P	S	Software inmaduro (adoptadores tempranos, fallas de software o "bugs", etc) es implementado
0903		P	S	El software equivocado (en costos, rendimiento, funcionalidades, compatibilidad, etc) es seleccionado para implementación
0904		P	S	Hay glitches (fallas intermitentes) operacionales cuando nuevo software es puesto a producción / operación
0905		P	S	Los usuarios no pueden usar y explotar el nuevo software de aplicación
0906		P	S	Modificación intencional de software conduciendo a datos errados o acciones fraudulentas
0907		P	S	Modificación no intencional de software conduciendo a resultados inesperados
0908		P	S	Ocurren errores de configuración no intencional y en administración de cambios
0909		P	S	Ocurre un mal funcionamiento de softwares comunes, de sistemas de aplicaciones críticas
0910		P	S	Ocurren problemas de software intermitentes con Sistemas importantes

0911		P		S	El software de aplicación es obsoleto (por ej, tecnología antigua, con pobre documentación, costoso de mantener, con dificultad para extenderse, no integrado en la arquitectura actual)
0912		P		S	Hay una inabilidad para reversar a la versión anterior, en caso de que se presenten issues operacionales con la nueva versión
1001	Propiedad del negocio sobre TI	P	P	S	El negocio no asume responsabilidad sobre aquellas áreas de TI que debería (ej: requerimientos funcionales, prioridades de desarrollo, evaluación de oportunidades vía nuevas tecnologías)
1002		P	S	S	Hay una dependencia excesiva y uso de computación de usuario final y soluciones ad hoc para necesidades importantes de información, conduciendo a deficiencias en seguridad, datos inexactos o incremento de costos / uso ineficiente de recursos
1003		P	S	S	Costos e inefectividad es relacionada a compras de TI por fuera de los procesos de procurement
1004				P	Inadecuados requerimientos conducen a acuerdos en niveles de servicio inefectivos (SLA: " Service Level Agreements")
1101	Selección / Desempeño, Cumplimiento contractual, terminación del		S	P	Hay una falta de análisis previos ("due diligence") relativos a la viabilidad financiera, capacidad de entrega y sostenibilidad de los

	servicio y transferencia de proveedores				servicios del proveedor
1102			S	P	Términos no razonables de negocio son aceptados de proveedores de TI
1103			S	P	El soporte y los servicios entregados por vendedores son inadecuados y no están de acuerdo con los SLAs
1104			S	P	El rendimiento de un outsorcing es inadecuado en un esquema de gran escala y a largo plazo
1105			S	P	Hay un incumplimiento con acuerdos de uso de licencia de software (uso y/o distribución de software sin licencias, etc)
1106			S	P	Hay una inabilidad en el realizar transferencia a proveedores alternativos, debido a una sobre dependencia en el proveedor actual
1107			S	P	Servicios de computación en la nube ("Cloud Services") son comprados por el negocio sin involucrar a TI, resultando en inabilidad para integrar el servicio con los servicios del negocio
1201	Cumplimiento Regulatorio	P	S	S	Hay incumplimiento con regulaciones (ej. Privacidad, contabilidad, manufactura)
1202		P	S	S	No hay conocimiento / no existe conciencia de cambios regulatorios potenciales que tengan un impacto en el

					ambiente operacional de TI
1203		P	S	S	Los reguladores previenen / impiden flujo de datos a través de fronteras debido a controles insuficientes
1301	GeoPolítica			P	No hay acceso debido a incidentes disruptivos
1302				P	Interferencia del gobierno y políticas nacionales limitan la capacidad del servicio
1303				P	Acción destinada en contra de la empresa resulta en destrucción de la infraestructura
1401	Robo de Infraestructura o destrucción	S	S	P	Hay un robo de un dispositivo con información sensitiva
1402		S	S	P	Hay un robo de un número substancial de servidores de desarrollo
1403		S	S	P	Ocurre destrucción del centro de datos (sabotaje, etc)
1404		S	S	P	Hay una destrucción accidental de dispositivos individuales
1501	Malware o Software maligno	S		P	Hay una intrusión de software maligno (malware) en servidores operacionales críticos
1502		S		P	Regularmente, hay infección de laptops con malware

1503		S		P	Un empleado molesto / insatisfecho implementa una "bomba de tiempo" de malware, que conduce a pérdida de datos
1504		S		P	Datos de la compañía son robados a través de acceso no autorizado alcanzado por un ataque tipo "phishing"
1601	Ataques lógicos	S		P	Usuarios no autorizados tratan de ingresar a los sistemas
1602		S		P	Hay una interrupción del servicio debido a ataque de "negación de servicios"
1603		S		P	El website es desconfigurado / alterado
1604		S		P	Se presenta espionaje industrial
1605		S		P	Hay un ataque de virus
1606		S		P	Hay un ataque de "hackers"
1701	Acción industrial	S	S	P	Facilidades y edificios no son accesibles debido a una huelga o paro
1702		S	S	P	Personal clave no está disponible debido a una acción industrial (ej: huelga de transportes)
1703		S	S	P	Un tercero no es capaz de proveer servicios debido a una huelga o paro

1704		S	S	P	No hay acceso a capital causado por una huelga oparo de la industria bancaria
1801	Ambiente	S	S	P	El equipo usado no es amigable con el ambiente (ej. Consumo de energía, etc)
1901	Actos de la Naturaleza	S	S	P	Hay un terremoto
1902		S	S	P	Hay un Tsunami
1903		S	S	P	Hay una tormenta tropical - ciclones
1904		S	S	P	Hay un incendio forestal
1905		S	S	P	Hay inundaciones
1906		S	S	P	El nivel del agua está subiendo
2001	Innovación	P	S	S	Nuevas e importantes tendencias tecnológicas no son identificadas
2002		P		S	Hay un fracaso en adoptar y explotar nuevo software (funcionalidad, optimización, etc) de manera oportuna
2003		P		S	Nuevas e importantes tendencias de software no son identificadas

(P= Principal implicación o impacto, S=Implicación o Impacto Secundario)