PONTIFICIA UNIVERSIDAD CATÓLICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

PROCESO DE AUDITORÍA DE LA INFORMACIÓN Y COMUNICACIÓN DENTRO DEL CONTROL INTERNO SEGÚN EL MARCO COSO II - ERM

Tesis para optar por el Título de Ingeniero Informático, que presenta el bachiller:

Victor Johao Villarroel Yabar

ASESOR: Manuel Tupia Anticona

Lima, Junio del 2013

DEDICATORIA

A mis padres Victor y Nilda, porque creyeron en mí , me sacaron adelante dándome ejemplos dignos de superación y entrega, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi carrera. Todo este trabajo va por ustedes, por lo que valen, porque admiro su fortaleza y su incansable e ilimitado apoyo y amor incondicional a lo largo de mi vida.

A mis hermanas Jamile y Johanna que sin saberlo fueron la fuente de mi fortaleza y templanza.

AGRADECIMIENTOS

A Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mi madre, por hacer de mí una mejor persona a través de sus consejos, enseñanzas y amor.

A mi padre, por brindarme los recursos necesarios y estar a mi lado apoyándome y aconsejándome.

Al Dr. Manuel Tupia, por aceptarme para realizar este trabajo bajo su dirección, por su predisposición permanente e incondicional en aclarar mis dudas y por sus substanciales sugerencias durante la redacción de la Tesis, por su apoyo y asesoría.

A mi amiga Lesly Lagos por su paciencia, comprensión y apoyo en los últimos años de mi carrera universitaria, por confiar en mí.

En general quisiera agradecer a todas y cada una de las personas que han vivido conmigo la culminación de mi carrera universitaria, que no necesito nombrar por que tanto ellas como yo sabemos que desde lo más profundo de mi corazón les agradezco el haberme brindado todo el apoyo, colaboración, ánimo pero sobre todo cariño y amistad.

Índice

Resumen **6**

1. Generalidades **7**

1.1. Identificación del problema 7

1.2. Marco Conceptual 8

1.2.1. Proceso: **8**

1.2.3. Controles: 12

1.2.4. Control Interno: 12

1.2.5. COSO: 16

1.2.6. NAGU: 18

1.2.7. ISO 27001 19

1.2.8. ISO 27002 20

1.3. Estado del Arte 20

1.4. Métodos y procedimientos 21

1.4.1. PDCA: 21

1.4.2. COBIT 22

1.5. Planificación 23

1.6. Descripción y sustentación de la Solución 23

2. Desarrollo del alcance y los objetivos del proceso de auditoría **28**

2.1. Proceso de definición de alcance de auditoría 28

2.2. Proceso de definición del objetivo general de auditoría 30

2.3. Definición de las herramientas a utilizar en la auditoría 30

2.4. Definición de los criterios a seguir en la auditoría 31

3. Descripción de los mecanismos de relevamiento de información para los procesos de auditoría **33**

3.1. Proceso de relevamiento de evidencias para la auditoria 33

3.2. Proceso de documentación de hallazgos de la auditoria 35

3.3. Proceso de comunicación de las conclusiones de la auditoria 35

4. Prueba del proceso de auditoría propuesto **38**

4.1. Descripción del caso prueba 38

4.2. Objetivo de la prueba 38

4.3. Conducción de la prueba 39

4.3.1. Relevamiento de evidencias 39

4.3.2. Documentación de hallazgos 44

4.3.3. Conclusiones y Recomendaciones 46

5. Conclusiones y Recomendaciones 47

5.1. Conclusiones 47

5.2. Recomendaciones y Trabajos futuros 48

Bibliografía 49

Índice de Figuras

Figura 1.1 Componentes del Control Interno según COSO 16
Figura 1.2 Componentes de COSO I 17
Figura 1.3 Componentes de COSO II 18
Figura 1.4 Ciclo PDCA 21
Figura 1.5 COBIT 23
Figura 1.6 WBS del proyecto 24
Figura 1.7 Gant del proyecto 27
Figura 2.1 Estructura del control interno dentro de COSO II 29
Figura 4.1 Gobierno Corporativo del "Banco XYZ" 39

Índice de Tablas

Tabla 3.1 Ejemplo de relevamiento de evidencias* 36
Tabla 3.2 Ejemplo de relevamiento de hallazgos 37
Tabla 4.1 Relevamiento de evidencias del caso de prueba 43
Tabla 4.2 Documentación de hallazgos del caso de pruebas 46

Resumen

En la actualidad, las empresas financieras son exigidas por la superintendencia de banca, seguros y AFP (SBS) a asegurar la efectividad de sus operaciones, confiabilidad de los datos financieros y cumplir con las leyes y regulaciones aplicadas al rubro. Para esto la SBS sugiere implementar el control interno propuesto por el marco COSO II, dicho control interno tiene como pilares la información y la comunicación, las cuales son muy importantes ya que sin ellas no se podría analizar los riesgos y establecer las estrategias que los mitiguen, cumplir con la leyes y normativas, minimizar pérdidas operacionales, exponer claramente la filosofía y enfoque de la gestión de riesgos corporativos de la empresa, reforzar o modificar la cultura de una empresa, etc.

En el presente proyecto de fin de carrera se ha realizado una investigación de las normas y estándares internacionales, rescatándose los aspectos más saltantes de cada norma y estándar, relacionados a la información y comunicación.

Se elaboró un proceso de auditoría para dos aspectos específicos del control interno: información y comunicación según COSO II, dentro del cual se incluye una guía para el relevamiento de evidencias para las variables información y comunicación del control interno, así como también la documentación de hallazgos y conclusiones.

Así mismo para la elaboración del presente proyecto se empleó la metodología PDCA propuesta por Walter A. Shewhart y para el desarrollo del proceso de auditorio se usó como referencia el modelo COBIT 5.

1. Generalidades

En este capítulo se desarrollan los conceptos necesarios para entender el problema que se desea resolver mediante la realización de este proyecto, luego se mostrará la planificación del mismo, así como las soluciones existentes en la actualidad al problema en mención.

1.1. Identificación del problema

Muchas empresas a nivel mundial fueron protagonistas de escándalos financieros debido a la dudosa reputación y mala dirección de sus altos directivos a finales de los años 90 del siglo XX y principios del siglo XXI, situación que se agudizó debido a la falta de una gestión de información y comunicación seria y eficaz [Tupia 2009] .Tómese como ejemplo el escándalo protagonizado por la empresa estadounidense *ENRON,* la cual a comienzos del 2001 reportó ganancias de un millón de dólares; sin embargo en diciembre del mismo año se declaró en quiebra por contar con deudas superiores a los treinta millones de dólares. Dicha situación perjudicó directamente a los empleados que no solo se quedaron sin empleo, sino que además vieron cómo se desplomaban las acciones (de noventa a cuarenta y dos dólares) que ellos compraron estimulados

por el directorio de la empresa, el cual ya sabía (desde 1997) que las ganancias de la empresa no estaban del todo bien. Es decir, ocultaron información a sus accionistas para que estos compren o conserven acciones [British Broadcasting Corporation 2011]. Otro caso es de la empresa italiana *PARMALAT* que llevó a cabo una serie de manejos fraudulentos de información contable en el 2003 .Estos dos —como muchos otros— escándalos financieros mundiales pudieron ser evitados con el desarrollo de un eficaz mecanismo de control interno diseñado y aplicado formalmente en la empresa [J. Lam 2003] .

El control interno es un sistema estructural y organizacional conformado por un conjunto de procedimientos que puede ayudar a una empresa a conseguir sus metas de desempeño y rentabilidad, y prevenir la pérdida de recursos. Puede ayudar a asegurar información financiera confiable, y a asegurar que la empresa cumpla con las leyes y regulaciones, evitando pérdidas de reputación y otras consecuencias. En suma puede ayudar a una entidad a cumplir sus metas, evitando peligros no reconocidos y sorpresas a lo largo del camino. Si es que no se cumple con este control se pueden tener riesgos tales como devaluación e hiperinflación financiera, pérdidas de empleados clave, existencia de productos erróneos entre otros [CIEC 2009].

Existen estándares internacionales, normas de auditoría gubernamental y marcos teóricos que hablan acerca de la seguridad de la información, de las comunicaciones y más en general de las tecnologías de información, sin embargo dichas explicaciones son muy genéricas y muy poco precisas en cuanto a definir un proceso de auditoría de la información y comunicación dentro del control interno.

Sobre la base de este escenario, el presente proyecto de fin de carrera propone la elaboración de un proceso para la auditoría de los aspectos de información y comunicación dentro del control interno, según COSO II y otras normas y estándares relacionados.

1.2. Marco Conceptual

1.2.1. Proceso:

Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados y tiene como característica [ISO24774 2010]:

- **Título:** Es una descripción del proceso corto que presenta un encabezado descriptivo para el proceso.
- **Objetivo:** Es el propósito para realizar el proceso, el cual se indica en forma general.
- **Resultados:** Es el producto observable de concretar los fines del proceso.
- **Actividades:** Describen un conjunto de acciones que pueden ser comprometidos en la ejecución del proceso.
- **Los elementos de información:** Son productos de procesos que son de particular interés para la gestión del ciclo de vida del proceso.

1.2.2. Auditoria:

Es un proceso sistemático por el cual un especialista independiente obtiene y evalúa evidencia respecto a un proceso, sistema, producto o estructura organizacional con el fin de emitir una opinión profesional sobre ello y reportar sobre el grado en que dicha información se ajusta a un estándar establecido.

Los objetivos de la auditoria [Tupia 2009] son:

- Analizar y definir el desempeño de un determinado aspecto (proceso, producto o estructura organizacional).
- Apoyar a la organización a corroborar que dicho aspecto este alineada con los objetivos del negocio.
- Evaluar los riesgos y los controles que se aplican sobre ese aspecto y opinar sobre su idoneidad, costo, capacidad de respuesta, etc.
- Proponer mejoras sobre los aspectos que se están analizando.
- Reportar a quien corresponda (la Alta Gerencia, Junta Directiva o de Accionistas) sobre una situación en particular detectada.

Las principales actividades de la Auditoria [ISO19011 2002] son las siguientes:

- **Inicio de la auditoría:** Se debe definir al líder del equipo auditor, los objetivos, alcance y criterios de la auditoria, la viabilidad de la auditoria y seleccionar al equipo de auditoría para establecer el primer contacto con el ente a auditar.
- **Revisión de documentos:** Antes de ejecutar el proceso de auditoría se debe de revisar los documentos del auditado para revisar la conformidad del sistema, dichos documentos pueden incluir registros, informes de auditorías anteriores. En

situaciones en donde la revisión de la documentación no ayuda para obtener una visión de la organización, una visita preliminar puede ser la mejor opción.

- **Preparación de las actividades de la auditoría in situ:** Se debe elaborar un plan de auditoría en el momento de la auditoria especificando los objetivos, criterios, alcance, fecha y lugar donde se llevará a cabo la auditoria, los roles y responsabilidades de las personas implicadas en la auditoria. Además se debe asignar el trabajo al grupo de auditoría y preparar los documentos de trabajo.
- **Conducción de las actividades de auditoría in situ:** Realizar la reunión de apertura con el auditado para confirmar el plan de auditoría, brindar un pequeño resumen de cómo se desarrollará el proceso de auditoría, confirmar los canales de la comunicación y brindar una oportunidad al auditado de hacer preguntas.
- **Preparar, aprobar y difundir el informe de auditoría:** Se debe preparar un reporte de auditoría, el cual debe incluir o hacer referencia a los objetivos, referencias, alcance, el cliente auditado, el auditor líder, el grupo de auditoría, las fechas y los lugares en donde se realizó la auditoria y recomendaciones y conclusiones finales. Al término del reporte este se debe aprobar y distribuir a la alta dirección de la organización auditada.
- **Finalización de la auditoria:** El proceso de auditoría termina cuando todas las actividades descritas en el plan de auditoría se han aprobado y distribuido. Todo documento referido a la auditoria deberá ser destruido y cualquier información de la misma debe ser confidencial.
- **La realización de la auditoría de seguimiento:** Las conclusiones de la auditoría pueden indicar la necesidad de acciones correctivas, preventivas o de mejora, tales acciones son generalmente decididas y realizadas por el auditado dentro de un plazo acordado.

Un auditor [CIEC 2009] debe seguir el código de ética básico que comprende:

- **Conducta ética:** Lo fundamental en el profesionalismo, las actitudes de confianza, integridad, confidencialidad y discreción son importantes para la auditoria.
- **Presentación razonable:** La capacidad de reportar con veracidad y exactitud. Las divergencias de opiniones entre el equipo de auditoría y el auditado deben ser reportadas.
- **El debido cuidado profesional:** La aplicación de diligencia y juicio en la auditoría. Los auditores deben actuar con cuidado de acuerdo con la importancia de las

tareas, además en ellos se deposita confianza de los clientes y otras partes interesadas, por lo tanto tener competencia es un factor muy importante.

- **Independencia:** Es fundamental para garantizar la objetividad del proceso de auditoría. Los auditores deben ser independientes del proceso que auditan y mantener una mente objetiva durante el proceso de auditoría para asegurar que los resultados de la auditoria y las conclusiones estén basadas únicamente en las evidencias de la auditoría.
- **Basado en evidencia:** El proceso de auditoría sistemática es el principal para llegar a conclusiones fiables basado en evidencias igualmente fiables.

Además la Asociación de Auditoría y Control de Sistemas de Información (Information Systems Audit and Control Association, conocida como ISACA) establece un Código de Ética Profesional para guiar la conducta profesional y personal de los miembros de su asociación y/o los portadores de sus certificaciones. La cual consiste en [ISACA 2012]:

- Apoyar la implementación de y alentar al cumplimiento de los estándares, procedimientos y controles apropiados para los sistemas de información.
- Realizar sus funciones con objetividad, debida diligencia y celo profesional, de acuerdo con las normas y mejores prácticas profesionales.
- Servir a los intereses de las partes relevantes de manera diligente, leal y honesta, manteniendo altos estándares de conducta y carácter, y no ser parte de ninguna actividad deshonrosa para la profesión.
- Mantener la privacidad y confidencialidad de la información obtenida en el transcurso de sus funciones a menos que la autoridad legal requiera su divulgación. Dicha información no deberá ser usada para beneficio personal ni divulgada a las partes que no correspondan.
- Mantener la competencia en sus respectivos campos y acordar realizar sólo aquellas actividades que de modo razonable puedan esperar cumplir con competencia profesional.
- Informar a las partes apropiadas los resultados del trabajo realizado; revelando todos los hechos significativos de los que tengan conocimiento.
- Apoyar la educación profesional de los interesados para mejorar su comprensión en seguridad y control de sistemas de información.

1.2.3. Controles:

Son las políticas, procedimientos, prácticas y estructuras organizacionales que sirven para reducir riesgos y además proporcionan cierto grado de seguridad de que se alcanzarán los objetivos del negocio detectando e indicando errores de planeación, organización o dirección. Los controles deben ser definidos por la Alta Gerencia, formar parte de la cultura organizacional del control, lo que implica un proceso de capacitación, y determinar sus objetivos de forma clara y precisa [Tupia 2009].

Los tipos de controles son [Tupia 2009]:

- **Disuasivos:** Su presencia quita la voluntad de realizar una acción en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de seguridad, señalética.
- **Preventivos:** Previenen errores antes de que se manifiesten por medio de monitoreo constante. Por ejemplo: política de contratación y segregación de funciones
- **Detectivos:** Detectan que ha ocurrido un error, una omisión o un acto malicioso y lo reportan. Por ejemplo: auditoria de accesos, mensajes de error, doble verificación de cálculos.
- **Correctivos:** Solucionan los problemas detectados por los controles detectivos, minimizando el impacto de una amenaza, corrigiendo los errores y modificar el sistema para minimizar los problemas futuros. Por ejemplo: planes de contingencia y restauración, copias de seguridad.
- Propios de cada área administrativa y operativa de las organizaciones, como financieros, contables, de Sistema de Información, entre otros.

1.2.4. Control Interno:

Es el proceso realizado por el personal de una entidad, diseñado para garantizar el cumplimiento de los siguientes objetivos [Tupia 2009]:

- Efectividad de las operaciones.
- Confiabilidad de los datos financieros.
- Cumplimiento de las leyes y regulaciones aplicables.

El control interno también busca que los riesgos no deseados sean evitados, detectados y corregidos.

Como beneficios de la implementación del control interno se tiene [CIEC 2009]:

- Sirven como herramientas que la gerencia utiliza para garantizar el cumplimiento de metas y logros.
- Es un canal que integra al personal con los objetivos.
- Ayuda al personal a medir su desempeño y mejorarlo.
- Mitiga las posibilidades de fraude.
- Facilita a la gerencia reportar como han invertido los recursos y logrado los objetivos propuestos.

Los niveles de madurez de la estructura del control interno son [CIEC 2009]:

- **Nivel 1 -No confiable:** Ambiente en donde el control no existe y no están diseñados los controles.
- **Nivel 2 -Informal:** Los controles existen y están diseñados pero no están debidamente documentados, dependiendo básicamente de las personas.
- **Nivel 3 -Estandarizado:** Los controles existen y están diseñados, los empleados los conocen pero un desvío de las actividades de control probablemente no será detectado.
- **Nivel 4 -Monitoreado:** Controles estandarizados en la preparación y diseño de reportes a la gerencia, se pueden utilizar herramientas para soportar las actividades de control.
- **Nivel 5 -Optimizado:** Una estructura integrada de control interno, con un monitoreo en tiempo real y mejoramiento continuo, utilizando herramientas para soportar dichas actividades de control y así efectuar cambios rápidos si es necesario.

El control interno, según The Committee of Sponsoring Organizations (COSO) [COSO 2011], consta de cinco componentes relacionados entre sí:

- **Ambiente de control:** Abarca la actitud de la organización, que influye en la conciencia de los empleados sobre los riesgos y forma la base de los demás componentes del control interno. Incluye la filosofía de gestión de riesgos de una identidad, su riesgo aceptado, el monitoreo ejercido por el consejo de la administración, valores éticos y competencia de su personal y forma de cómo la gerencia designa la autoridad y la responsabilidad y organiza y desarrolla a sus empleados.

- **Medición de riesgos:** Comprende la identificación, análisis y clasificación de los riesgos relevantes para el cumplimiento de los objetivos, constituyendo una base de cómo se les debe de administrar. Los riesgos según su origen pueden ser :
  - **Externos:** Son riesgos normativos, de mercado, económicos, de la naturaleza y sociopolíticos.
  - **Externos-Internos:** Son ambientales, comerciales, de crecimiento y de ética.
  - **Internos:** Son operacionales.

Además los riesgos deben de clasificarse según su impacto y la probabilidad con la que esta pueda ocurrir.

- **Actividades de control:** Son las políticas y procedimientos que ayudan a cumplir lo estipulado en la administración de riesgos, están presentes en todos los niveles y funciones de la organización, son tan diversas como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones.
- **Información y comunicación:** La información relevante se identifica, capta y distribuye de una forma y dentro de un marco de tiempo que permita a los empleados llevar a cabo sus responsabilidades, en este sentido los sistemas de información funcionan como apoyo a la gerencia integrando la necesidad de tener un flujo constante de información y comunicación entre todos los empleados de una entidad. Dichos sistemas utilizan datos generados internamente y otras entradas de fuentes externas y sus salidas informativas facilitan la gestión de riesgos y la toma de decisiones informadas con la finalidad de alcanzar los objetivos predeterminados.

La información debe de tener las siguientes características:

- **Privacidad:** La información confidencial no debe ser revelada.
- **Integridad:** La información debe estar completa, valida y exacta.
- **Confidencialidad:** La información solo debe ser revelada a quien corresponda.
- **Disponibilidad:** La información debe estar disponible siempre cuando se le solicite.

Además se debe definir estándares de clasificación de la información para identificar el nivel del riesgo. Dicha clasificación sería la siguiente:

- **Secreta:** Información altamente sensible, alto nivel de control.

- **Confidencial:** Información menos sensible, nivel medio de control.
- **Privada:** Información privada de clientes y empleados, nivel medio de control.
- **Publica:** No se ajusta a ninguna de las anteriores, mínimos controles.

- **Monitoreo:** La gestión de riesgos se supervisa a lo largo del tiempo revisando la presencia y el funcionamiento de sus componentes mediantes actividades permanentes de supervisión, evaluaciones independientes o una combinación de ambas técnicas. De esta manera la gestión de riesgos podrá reaccionar dinámicamente, cambiando según las condiciones lo requieran.

En la Figura 1.1 se puede observar la interacción entre los cinco componentes antes descritos.

Sin embargo no importa que tan bien esté hecho el control interno, no garantiza la eliminación absoluta de errores.

Dicha seguridad parcial es dada por la existencia de factores limitantes como son [CIEC 2009]:

- **Criterio:** Depende de las malas decisiones (juicio) que pueden tomar los empleados.
- **Fracasos:** Las personas que están a cargo de los controles puede que no lo ejecuten correctamente.
- **Disfunciones del Sistema:** Por la existencia de actitudes de las personas como dejadez, fatiga o despistes.
- **Transgregacion Gerencial:** Un gerente utiliza la información de la organización para beneficio suyo.
- **Confabulación:** Dos personas o más pueden coordinar para romper controles.
- **Costo vs. Beneficio:** Los recursos son limitados y los gerentes optan por un control cuyo costo es mayor que su beneficio.

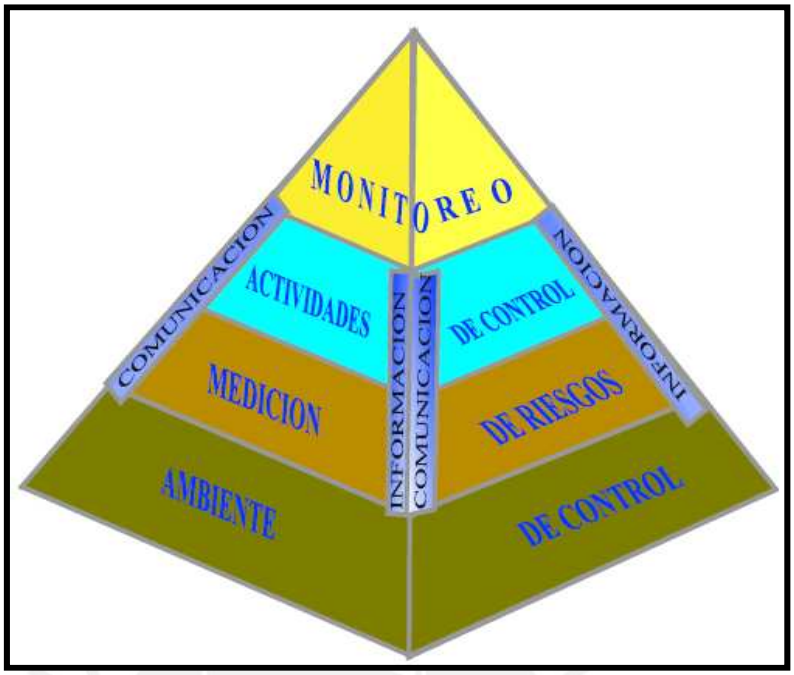

Figura 1.1 Componentes del Control Interno según COSO [CIEC 2009]

1.2.5. COSO:

El Committee of Sponsoring Organizations of the Treadway Commission (COSO) es la unión de cinco organizaciones, las cuales son: American Accounting Association, American Institute of CPAs, Financial Executives International, The Association for Accountants and Financial Professionals in Business y The Institute of Internal Auditors y tiene como objetivo proveer marcos generales y orientación sobre la gestión de riesgos empresarial, control interno, evitar el fraude y mejorar el desempeño organizacional.

COSO se creó en 1985 debido a cuestionables prácticas políticas corporativas de financiamiento de campañas y de las prácticas corruptas extranjeras en la década de 1970, los EE.UU. Securities and Exchange Commission (SEC) y el Congreso de EE.UU. aprobó una campaña de reformas a la Ley de Finanzas y en 1977 a la Ley de Prácticas Corruptas en el Extranjero (FCPA), que tipificaba como delito el soborno transnacional y obligaba a las empresas a implementar programas de control interno.

COSO elaboró recomendaciones para empresas públicas y sus auditores independientes, para la Securities and Exchange Commission y otros reguladores, y para las instituciones educativas. Actualmente es un líder reconocido en el mercado

global en el desarrollo en las áreas de gestión de riesgos y control que permiten el buen manejo de la organización y mitigan el fraude [COSO 2011].

Desde su creación COSO publicó dos modelos, los cuales son:

- **COSO I "Control Interno-Marco Conceptual Integrado":** Comprende el plan de organización, los métodos y las medidas tomadas por la dirección de una empresa para apoyar y medir la eficiencia y exactitud en las operaciones y el cumplimiento de los objetivos de la entidad [COSO 1992].
  En la Figura 1.2 se puede apreciar los componentes de COSO I.

Figura 1.2 Componentes de COSO I [ELN2000]

- **COSO II ERM "Administración de Riesgos en las Empresas":** A diferencia del primer modelo, el cual se refiere a una mejor práctica en auditoría interna, este modelo añade los riesgos que se crean a causa de las presiones externas. El Esquema de Administración de Riesgos en las Empresas (ERM por sus siglas en inglés) ha surgido como una valiosa herramienta para establecer objetivos organizacionales, identificar y catalogar riesgos y oportunidades, determinar las mejores respuestas y supervisar la eficacia del proceso y de sus componentes en el transcurso del tiempo. Además agrega tres componentes más a los seis componentes del control interno definido en el primer modelo, los cuales son [COSO ERM 2004] :
  - ✓ Fijación de objetivos
  - ✓ Identificación de riesgos

- ✓ Respuesta al riesgo

En la Figura 1.3 se puede apreciar los componentes de COSO II.

Figura 1.3 Componentes de COSO II [UPN2010]

En el futuro COSO pretende centrarse en los siguientes puntos [COSO 2011]:

- Actualización de Control Interno - Marco Integrado de 1992. Con esta iniciativa se espera que el actual marco y las herramientas relacionadas con la evaluación más relevante en el entorno empresarial, que son cada vez más complejas, sirvan a las organizaciones de todo el mundo a diseñar, implementar y evaluar un mejor control interno.
- Aportar documentos adicionales que sirvan como ayuda a las partes interesadas en la promoción de ERM a lo largo de la "curva de madurez" de un proceso de ERM efectivo.
- Proporcionar investigación y orientación sobre el entorno de control que tratan con problemas de conducta y temas de investigación como la "racionalización" y el exceso de confianza, en parte en respuesta a las ideas contenidas en el estudio de fraude en investigaciones más recientes.
- Proporcionar orientación sobre el control interno en el sector público.

1.2.6. NAGU:

Son las Normas de Auditoria Gubernamental desarrolladas por la Contraloría General de la República del Perú. En la cual se pueden encontrar ciertas normas relacionadas con la auditoria y el control interno, como son [CGRP 2011]:

- El auditor debe planear adecuadamente su trabajo a fin de garantizar la realización de una auditoria de calidad, así como también debe conocer todo lo relacionado a la organización, el tipo de auditoría a realizar y cuáles son las leyes y normativas que tomará como base.
- Para cada auditoria específica se debe realizar programas que incluyan los objetivos, procedimientos que se deben aplicar, naturaleza, alcance y oportunidad de su ejecución, así como el personal idóneo para su desarrollo.
- Cada organización sujeta a auditoria debe implantar, organizar y mantener actualizado el archivo permanente.
- Se debe evaluar la estructura del control interno de la organización a examinar, con la finalidad de definir cuál es la efectividad de la estructura del control interno implementado y determinar el riesgo de la auditoria.
- Se debe corroborar el cumplimiento de todas las leyes y normas vigentes dentro de la organización.
- El trabajo de auditoría debe ser supervisado durante todo su ciclo de vida.
- El auditor debe recolectar evidencia suficiente, competente y relevante mediante la aplicación de pruebas de control y procedimientos sustantivos que le permita fundamentar una conclusión respecto al organismo, programa, actividad o función que sea objeto de auditoría.

1.2.7.ISO 27001

Es un Estándar Internacional de Sistemas de Gestión de Seguridad de la Información que permite a una organización evaluar su riesgo e implementar controles apropiados para preservar la confidencialidad, la integridad y la disponibilidad del valor de la información. El objetivo es proteger la información de una organización para que no caiga en manos incorrectas o se pierda para siempre [ISO 27000].

Los beneficios de usar este estándar son:

- Algunas licitaciones internacionales empiezan a solicitar una gestión ISO 27001.
- Reducción de los costos vinculados a incidentes.
- Posibilidad de disminución de las primas de seguro.
- Mejora del conocimiento de los sistemas de información, sus problemas y los medios de protección.
- Mejora de la disponibilidad de los materiales y datos.

- Protección de la información.
- Diferenciación sobre la competencia y mercado.

1.2.8. ISO 27002

Es el cambio de nombre de la norma ISO 17799, y es un código de prácticas para la seguridad de la información. Se describen en ella una larga lista de controles y mecanismos de control, que pueden ser aplicados, según la orientación de la norma ISO 27001 [ISO 27000].

Las secciones del contenido de la norma ISO 27002 son las siguientes:

- Estructura
- Evaluación de riesgos y tratamiento
- Política de seguridad
- Organización de Seguridad de la Información
- Gestión de activos
- Recursos humanos de seguridad
- Seguridad Física
- Comunicaciones y gestión de operaciones
- Control de Acceso
- Sistemas de Información de adquisición, desarrollo, mantenimiento
- Seguridad de la información de gestión de incidentes
- Continuidad del Negocio
- Conformidad

1.3. Estado del Arte

En la actualidad la auditoria de control interno tiene una gran importancia ya que garantiza el cumplimiento de los objetivos de la organización y evita la posibilidad de fraudes y el mal manejo de información. Según este contexto la Contraloría de muchos países desarrollan normas para regular dicha auditoria. Por ejemplo la contraloría de Panamá agrupa dichas normas específicas relativas a cada uno de los componentes de la estructura del control interno como se muestra en el Anexo A [CGRP 1998]:

En nuestro país las normas de auditoría gubernamental que se refieren al control interno se muestran en el Anexo B [CGRP 2011]:

Según lo revisado en la contraloría de Panamá y de Perú se puede observar que existen muchas normas para desarrollar una auditoria eficaz, sin embargo dichas normas se refieren al proceso de Auditoria en general y no hacen énfasis en la auditoria de la información y comunicación del control interno como pretende realizar el presente proyecto de fin de carrera.

1.4. Métodos y procedimientos

1.4.1. PDCA:

Para este proyecto de fin de carrera se utilizó esta metodología con la finalidad de plantear una estrategia de mejora continua de la calidad de dicho proyecto.

Los cuatros pasos de esta metodología son [IES 2007]:

- **Plan (Planificar):** Se planificó con anticipación los entregables y las tareas a realizar para cumplir con todos los objetivos de dichos entregables.
- **Do (Hacer):** Se elaboró todos los capítulos del proyecto teniendo como producto final el proceso de auditoría de la información y comunicación
- **Check (Verificar):** Este paso se desarrolló cuando el producto final fue culminado y se procedió a corroborar que cumpla con el objetivo general y los objetivos específicos definidos en el paso de planificación.
- **Act (Actuar):** En este proyecto de fin de carrera no está incluido en el alcance el mejoramiento continuo del producto.

En la Figura 1.4 se puede observar de forma dinámica la interacción entre los 4 pasos descritos formando un ciclo continuo de mejora.

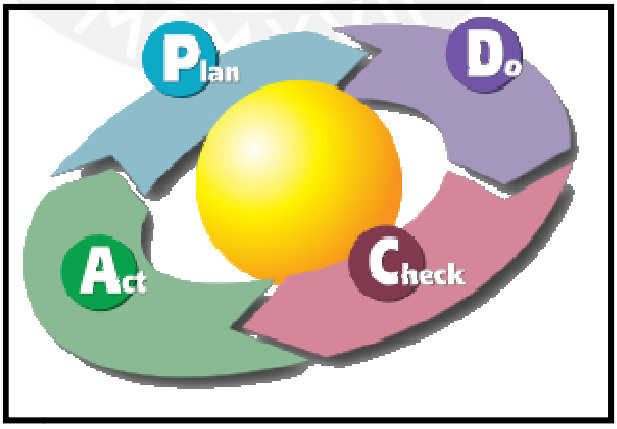

Figura 1.4 Ciclo PDCA [CIEC 2009]

1.4.2. COBIT

Es el Control Objectives for Information and related Technology o COBIT por sus siglas y para el presente proyecto de fin de carrera se utilizó todos los objetivos de control definidos dentro de los dominios de COBIT que tenga relación con la información y comunicación.

Está compuesto por cinco dominios, los cuales son [ISACA 2012]:

- **Evaluar, dirigir y monitorear:** Consiste en analizar y articular los requisitos para el gobierno de TI de la empresa, y establecer y mantener estructuras eficaces de apoyo, principios, con claridad de responsabilidades y autoridad para lograr las misiones, metas y objetivos de la empresa
- **Alinear, planificar y organizar:** Consiste en definir una estrategia para identificar cómo las tecnologías de información pueden ayudar al cumplimiento de la organización, dicha estrategia debe de ser planeada, comunicada y administrada.

Por último se debe de establecer una organización y una infraestructura apropiada

- **Construir, adquirir e implementar:** Para desarrollar la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso de negocio.
- **Entregar, proveer y dar soporte:** Se refiere a la entrega de los servicios requeridos, que abarca desde la capacitación para su uso, pasando por seguridad y aspectos de continuidad. Este dominio incluye los procesos de soporte necesarios y el procesamiento de datos por sistema de aplicación.
- **Monitorear, evaluar y analizar**: Todos los procesos requieren ser supervisados periódicamente para corroborar su calidad y suficiencia en cuanto a los requerimientos de control.

En la Figura 1.5 se puede apreciar la participación de la información dentro del modelo de COBIT.

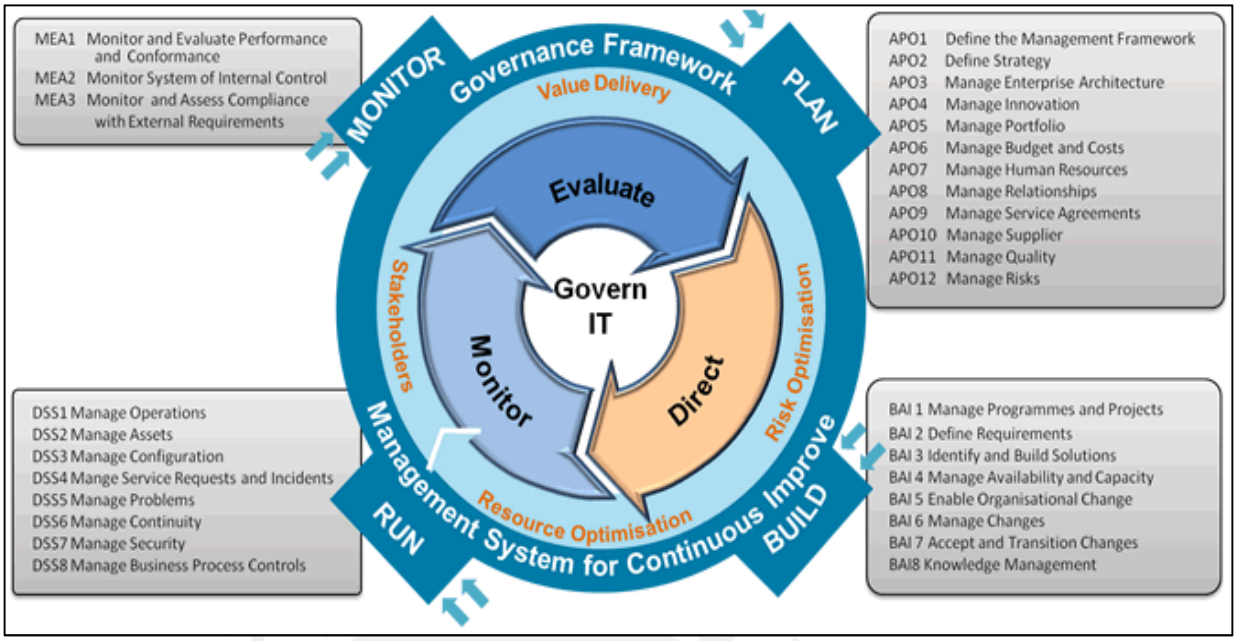

Figura 1.5 COBIT [ISACA 2012]

1.5. Planificación

En la Figura 1.6 se muestra la planificación del proyecto de tesis según los entregables y el índice especificados en la página Web del curso.

En la Figura 1.7 se puede observar el Gant del proyecto de tesis que tiene como duración poco más de 3 meses, indicando los días de duración y los entregables con sus respectivos contenidos.

1.6. Descripción y sustentación de la Solución

Los factores tales como globalización, tecnología, regulación, reestructuración, mercados cambiantes y competencia, generan en las empresas altos niveles de incertidumbre y exposición a riesgos. Ésta consiste en la incapacidad de determinar en forma precisa, la probabilidad de que ocurran algunos eventos potencialmente dañinos y sus resultados asociados, es decir, las empresas no tienen la capacidad de conocer cuándo, dónde y de qué forma se presentarán los riesgos que amenazarán el cumplimiento de los objetivos de la empresa.

Para minimizar el impacto de estos riegos es importante implementar un correcto control interno, pues al no hacerlo, las empresas son propensas a fraudes financieros,

perder empleados claves, no cumplir con los objetivos establecidos, entre otros riesgos.

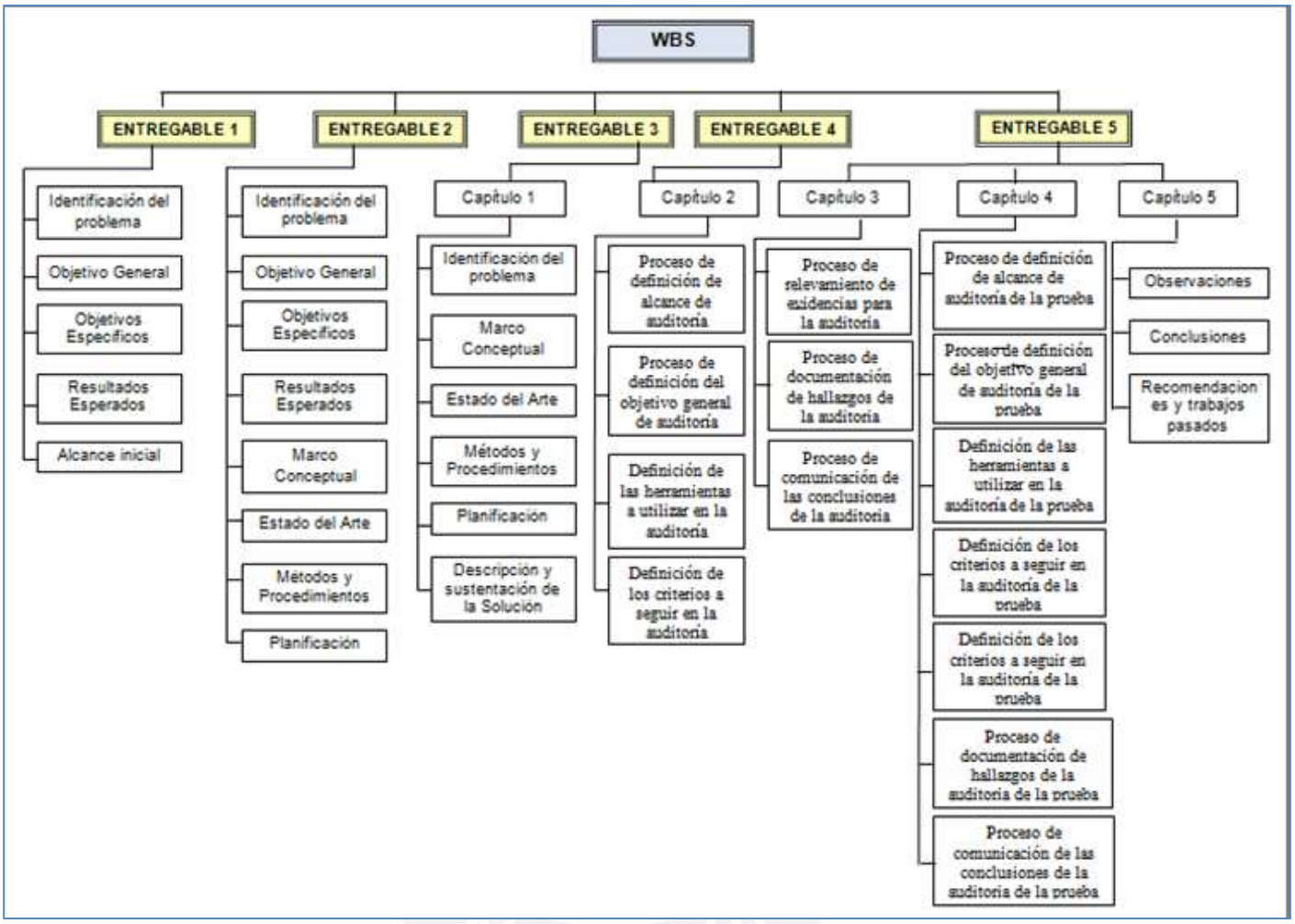

Figura 1.6 WBS del proyecto

Además las empresas no podrían:

- Analizar los riesgos y establecer las estrategias que los mitiguen
- Cumplir con las leyes y normativas
- Minimizar pérdidas operacionales
- Aprovechar los riesgos para buscar oportunidades de cambio o modificar los procesos existentes
- Establecer los objetivos y metas operacionales
- Brindar información financiera y operacional confiable, creíble y relevante.

- Dirigir la empresa y conseguir sus objetivos

En lo referente al control interno de las comunicaciones, si su continuidad es puesta en duda, no se podrán cumplir con:

- Exponer claramente la filosofía y enfoque de la gestión de riesgos corporativos de la empresa
- Reforzar o modificar la cultura de una empresa
- Transportar de forma eficiente la información entre todas las líneas jerárquicas de la empresa
- Comentar o informar sobre un comportamiento ilegal, no ético o inadecuado

Con la implementación de un marco de control interno basado en COSO-II y haciendo uso de la norma ISO 27002 para los aspectos de seguridad tanto de información como de comunicaciones (pilares de la pirámide del control interno tal como lo define COSO II), estos riesgos pueden ser gestionados convenientemente.

Esto da como resultado una empresa con los procesos bien definidos, segregación del trabajo, comunicación eficaz y clara a lo largo de todas las líneas jerárquicas de la empresa e información integrada, confidencial y disponible

Además podrán:

- Crear políticas de la empresa
- Crear manuales de procedimientos y guías
- Asignar responsabilidades
- Brinda un mejor ambiente de trabajo
- Genera confianza
- Protege los derechos de los inversionistas
- Promueve la competitividad y la eficiencia
- Confiar en la información por lo tanto podrán tomar decisiones basados en ellos
- Comunicación siempre fluida en todas las partes de la jerarquía de la empresa

Con estas características la empresa podrá tener:

- Visión correcta sin derivarse de ella
- Participación correcta en el mercado
- Consistencia con la misión de la organización
- Consistencias en los estados financieros

Entregable 1	**11 días**	**mar 17/07/12**	**mar 31/07/12**
Identificación de problema	3 días	mar 17/07/12	jue 19/07/12
Objetivos generales	2 días	vie 20/07/12	lun 23/07/12
Objetivos específicos	2 días	mar 24/07/12	mié 25/07/12
Resultados Esperados	2 días	jue 26/07/12	vie 27/07/12
Alcance inicial	2 días	lun 30/07/12	mar 31/07/12
Entregable 2	**14 días**	**mié 01/08/12**	**lun 20/08/12**
Identificación de problema	1 día	mié 01/08/12	mié 01/08/12
Objetivos generales	1 día	jue 02/08/12	jue 02/08/12
Objetivos específicos	1 día	vie 03/08/12	vie 03/08/12
Resultados Esperados	1 día	lun 06/08/12	lun 06/08/12
Marco conceptual	3 días	mar 07/08/12	jue 09/08/12
Estado del Arte	3 días	vie 10/08/12	mar 14/08/12
Métodos y Procedimientos	2 días	mié 15/08/12	jue 16/08/12
Planificación	2 días	vie 17/08/12	lun 20/08/12
Capitulo 1 : Generalidades	**7 días**	**mar 21/08/12**	**lun 27/08/12**
Identificación de problema	1 día	mar 21/08/12	mar 21/08/12
Planificación	1 día	mié 22/08/12	mié 22/08/12
Marco conceptual	1 día	jue 23/08/12	jue 23/08/12
Estado del Arte	1 día	vie 24/08/12	vie 24/08/12
Descripción y Sustentación de la Solución	1 día	lun 27/08/12	lun 27/08/12
Capitulo 2 : Desarrollo del alcance y los objetivos del proceso de auditoría	**20 días**	**mar 28/08/12**	**lun 24/09/12**
Proceso de definición de alcance de auditoría	5 días	mar 28/08/12	lun 03/09/12
Proceso de definición del objetivo general de auditoría	5 días	mar 04/09/12	lun 10/09/12
Definición de las herramientas a utilizar en la auditoría	5 días	mar 04/09/12	lun 10/09/12
Definición de los criterios a seguir en la auditoría (50%)	5 días	mar 11/09/12	lun 17/09/12
Definición de los criterios a seguir en la auditoría (50%)	5 días	mar 18/09/12	lun 24/09/12
Capitulo 3: Descripción de los mecanismos de relevamiento de información para los procesos de auditoría	**35 días**	**mar 25/09/12**	**lun 19/11/12**
Proceso de relevamiento de evidencias para la auditoria	15 días	mar 25/09/12	lun 15/10/12
Proceso de documentación de hallazgos de la auditoria	15 días	mar 16/10/12	lun 05/11/12
Proceso de comunicación de las conclusiones de la auditoria	5 días	mar 06/10/12	lun 19/11/12
Capitulo 4: Prueba de los procesos de auditoría propuestos	**13 días**	**mar 20/11/12**	**juv 06/12/12**
Proceso de definición de alcance de auditoría de la prueba	5 días	mar 20/11/12	lun 26/11/12
Proceso de definición del objetivo general de auditoría de la prueba	5 días	mar 20/11/12	lun 26/11/12
Definición de las herramientas a utilizar en la auditoría de la prueba	5 días	mar 20/11/12	lun 26/11/12
Definición de los criterios a seguir en la auditoría de la prueba	5 días	mar 27/11/12	lun 03/12/12
Proceso de relevamiento de evidencias para la auditoria de la prueba	5 días	mar 27/11/12	lun 03/12/12
Proceso de documentación de hallazgos de la auditoria de la prueba	3 días	mar 04/12/12	juv 06/12/12
Proceso de comunicación de las conclusiones de la auditoria de la prueba	3 días	mar 04/12/12	juv 06/12/12
Capitulo 5: Observaciones, Conclusiones y Recomendaciones	**10 días**	**vie 07/12/12**	**jue 20/12/12**

Observaciones	5 días	vie 07/12/12	jue 13/12/12
Conclusiones	5 días	vie 07/12/12	jue 13/12/12
Recomendaciones y Trabajos futuros	5 días	vie 14/12/12	jue 20/12/12

Figura 1.7 Gant del proyecto

2. Desarrollo del alcance y los objetivos del proceso de auditoría

En el presenta capítulo, se detallan los procesos de cada uno de los aspectos que son cubiertos por la auditoría: desde la determinación del alcance y los criterios, hasta los mecanismos de relevamiento de evidencias y documentación de hallazgos. Visto el proceso de auditoría como un todo, se puede afirmar que estaría compuesto por cinco etapas cuyos subprocesos se describen en los próximos apartados.

2.1. Proceso de definición de alcance de auditoría

Toda evaluación que tenga el tipo de de auditoría, tiene un alcance. Éste está referido al conjunto de aspectos, procesos o procedimientos considerados necesarios de cubrir en dicha evaluación para lograr los objetivos de la auditoria.

Para definir el alance, es necesario conocer la empresa a auditar (los procesos, procedimientos y normativas involucradas) con el propósito de averiguar en detalle sus características, y así tener los elementos de juicio suficientes y necesarios que permitan un adecuado planeamiento (calendarización) del trabajo a realizar y dirigirlo hacia los aspectos que resulten de mayor interés de acuerdo con los objetivos que se definirán en etapas posteriores (empleo de las técnicas de auditoría adecuadas).

La participación de la entidad cliente es fundamental para estos estudios, los cuales se pueden efectuar a través de entrevistas con los principales actores de los aspectos involucrados en la —futura— auditoría, procurando profundizar datos en cuanto a estructura, cantidad de dependencia, desenvolvimiento de la actividad que desarrolla, flujo de la información (proceso) o de los servicios que presta, peculiaridades de las áreas específicas en donde se desea desarrollar la auditoria entre otros.

Las mismas investigaciones conducirán a la determinación de los criterios de auditoría tal como lo menciona [ISO 19011 2002]. Los resultados de esta exploración en la empresa permitirán, además, hacer la selección de la metodología y el resto de técnicas a utilizar.

En cuanto al objeto de auditoría que está siendo cubierta, es menester conocer los conceptos de control interno en el interior de la empresa (valorar la importancia del control interno) así como el uso de marcos tales como COSO II para organizar esta función. Esto facilitará la etapa de planeamiento de la evaluación garantizando su calidad.

Para definir el alcance de la auditoria se debe conocer la estructura del Control Interno y el papel COSO II, específicamente los aspectos de información y control tal como se puede apreciar en la Figura 2.1.

Figura 2.1 Estructura del control interno dentro de COSO II

A continuación se presenta una lista de criterios a tomar en cuenta en la definición del alcance de una auditoría de la información y comunicación del control interno informático (ver Anexo C).

2.2. Proceso de definición del objetivo general de auditoría

Conociendo el alcance de la auditoría —definida en la etapa anterior— se procede a definir los objetivos de la misma. El objetivo general regula de manera holística lo que se pretende evaluar. Es complementado por los objetivos específicos denominados por la ISO 19011 como criterios de auditoría. La forma de definir el objetivo general en este tipo de auditoría es sencilla: ubicar los principales aspectos involucrados en información y comunicaciones que podrían ser objeto de revisión dentro del control interno u otras auditorías relacionadas.

La siguiente lista muestra ejemplos de objetivos generales de una auditoría de control interno para las dimensiones información y comunicaciones:

- Evaluar los controles internos con la finalidad de determinar su performance y su alineamiento hacia políticas y cumplimiento regulatorio al que está sujeto la empresa auditada
- Evaluar el cumplimiento de las metas de control interno
- Determinar el grado de confiabilidad de los estados financieros
- Evaluar la gestión empresarial, el cumplimiento de las medidas de austeridad o comprobar la performance de determinado aspecto de la Administración General de la empresa que guarde correspondencia con control interno
- Efectuar un seguimiento con las recomendaciones dadas en anteriores evaluaciones (auditorías previas)

Dichos objetivos deben estar basados en criterios o marcos de referencias como: leyes, reglamentos, cartas, procedimientos, normas de control interno, norma de sana administración, principios de contabilidad generalmente aceptada, opinión de un experto o finalmente juicio del auditor.

2.3. Definición de las herramientas a utilizar en la auditoría

Para auditorías informáticas, de seguridad y TI usualmente se emplean las siguientes herramientas:

- **COBIT:** Herramienta guía para evaluar controles referentes a información y comunicaciones.
- **ISO 19011:** Buenas prácticas para la realización de auditoría en general.
- **ISO 27001:** Buenas prácticas para elaborar un plan auditoria de la información.
- **ISO 27002:** Buenas prácticas para realizar controles durante la ejecución de la auditoria de la información.
- **NIST 800-34:** Consideraciones técnicas de planificación de contingencia en telecomunicaciones, en servidores y en los sistemas cliente/servidor

2.4. Definición de los criterios a seguir en la auditoría

Partiendo de los objetivos y alcance previstos y considerando toda la información obtenida, se procederá a escoger los criterios (ver Anexo C) de la lista (no exhaustiva).

Adicionalmente, los criterios que podrían ser planteados según la norma ISO 27002 [ISO 27000] para los aspectos de seguridad tanto de información como de comunicaciones, serían los siguientes:

Con respecto a la información:

- Manejar la seguridad de la información dentro de la organización y establecer un marco gerencial referencial para iniciar y controlar su implementación interna
- Manejar la seguridad de accesos de terceras personas, es decir, la presencia de terceros tanto para proveer servicios externos como los clientes, expone a la información a riesgos que deben ser mitigados o controlados
- Delegar responsabilidades a los usuarios, tales como manejar correctamente sus contraseñas, sus equipos informáticos y mantener sus pantallas y escritorios limpios
- Controlar el acceso a red, mediante el establecimiento de políticas de uso de los servicios de red
- Controlar el acceso a los sistemas operativos, con identificación y autenticación de usuarios, gestión de contraseñas para sistemas operativos, etc
- Controlar la computación móvil y teletrabajo, restringir el uso de la computación móvil y teletrabajo para evitar que la información se filtre por cualquier canal de comunicación

Con respecto a las comunicaciones:

- Establecer procedimientos y responsabilidades sobre la documentación de los procesos operativos, procesos de gestión de cambio y separación de entorno de desarrollo, pruebas y operaciones
- Gestionar la entrega del servicio por parte de terceros, desarrollando un procedimiento para monitorear, revisar y manejar los cambios dichos servicios
- Controlar código malicioso y código móvil
- Gestionar un proceso de copias de seguridad y respaldo
- Gestionar la seguridad dentro de las topologías de las redes
- Gestionar medios de soporte, monitoreando el procesamiento de información en dichos medios y asegurando la documentación de los sistemas que brindan soporte al sistema principal de la empresa
- Controlar el intercambio de información, definiendo acuerdos inter-empresas para dicho intercambio y asegurando la seguridad de los medios de soporte que se encargan del intercambio de información

3. Descripción de los mecanismos de relevamiento de información para los procesos de auditoría

En el siguiente capítulo se describe los procesos de relevamiento de evidencias, hallazgos y finalmente documentación de las conclusiones y recomendaciones del proceso de auditoría de la información y comunicación del control interno según COSO II.

3.1. Proceso de relevamiento de evidencias para la auditoria

Se tomó en cuenta los siguientes conceptos para el relevamiento de evidencias

- **Criterio:** Aspecto a tomar en cuenta en la definición de evidencias para la auditoría de la información y comunicación del control interno
- **Auditado:** Ente al cual le pedimos la información a auditar y al quien se entregan los resultados de la auditoria.

- **Documentos a pedir:** Testimonio material que se analizó y recolectó para el relevamiento de evidencias, los cuales pueden ser los siguientes:
  - ✓ Normativas del Control Interno de la empresa
  - ✓ Normativa legal que tenga que cumplir la empresa relacionada al Control Interno
  - ✓ Planes y procedimientos de seguridad de la información
  - ✓ Modelo de arquitectura de información empresarial
  - ✓ Diccionario de datos empresarial y reglas de sintaxis de datos
  - ✓ Procedimientos para la integridad de datos
  - ✓ Listado y características de dispositivos (firewall, routers y switchs)
  - ✓ Tecnología de difusión que la red utiliza
  - ✓ Capacidad de transmisión de la red
  - ✓ Medios de comunicación que se utiliza (cable coaxial, telefónico y fibra óptica)
  - ✓ Alcance de la red
  - ✓ Organización y distribución de servidores

- **Objetivo de revisión del documento:** Es el fin por el cual se revisan los documentos al auditado
- **Ejecutar trabajo de campo:** Son técnicas de recolección de evidencias como las siguientes:
  - ✓ Revisar la estructura organizativa del área de TI
  - ✓ Revisar las políticas, procedimientos y estándares de Sistemas de Información
  - ✓ Revisar los estándares de documentación de los sistemas de información
  - ✓ Entrevistar al personal apropiado
  - ✓ Observar los procesos y el desempeño de los empleados
  - ✓ Revisión de documentación

En la Tabla 3.1 se presenta un ejemplo de cómo interactúan los conceptos anteriormente explicados para el relevamiento de evidencias para el proceso auditoria.

El resultado de utilizar la matriz descrita anteriormente es una evidencia, la cual es toda información utilizada para determinar si la empresa o los datos que están siendo auditados cumplen con los criterios u objetivos establecidos de una auditoria [Tupia 2009]

Para asegurar la confiabilidad de la evidencia esta debe cumplir con los siguientes criterios:

- Independencia del proveedor de la evidencia: La evidencia debe ser obtenida de fuentes externas y no de fuentes internas de la empresa
- Calificación de la persona que suministra la información o evidencia: Se debe considerar la calificación de las personas que brindan las evidencias y del auditor ya que si este no tiene un buen entendimiento del área técnica que está en revisión , la información recopilada puede ser no confiable
- Objetividad de la evidencia: La evidencia se debe entender sin ningún tipo de explicación o interpretación.

3.2. Proceso de documentación de hallazgos de la auditoria

Después de ejecutar el plan de auditoría y de recolectar la evidencia, se debe evaluar la información recopilada para desarrollar una opinión de auditoría.
En la Tabla 3.1 se puede apreciar un ejemplo de levantamiento de evidencias.

Se debe determinar las fortalezas y las debilidades de las evidencias encontradas, y luego determinar su eficacia para alcanzar los criterios establecidos como parte del plan de auditoría; como resultado se produce un hallazgo.

Para documentar un hallazgo se desarrolla atributos que se relacionan con él, como la evidencia, el criterio, el hallazgo, el resultado y las recomendaciones. En la Tabla 3.2 se puede observar la relación que tienen dichos atributos con el hallazgo.

3.3. Proceso de comunicación de las conclusiones de la auditoria

Siendo las conclusiones, el último aspecto de la documentación dentro de los informes de auditoría, éstas deben:

- Basarse en evidencias suficientes, relevantes y competentes.
- Incluir también comentarios positivos y/o constructivos en relación con el estado actual de los procesos y controles instalados.
- Cubrir no solamente las no conformidades a partir de los hallazgos, sino también las oportunidades de mejora que puedan surgir por la misma causa de la no conformidad.

Aspecto	Criterio	Auditado	Documentos a pedir	Objetivo de revisión del documento	Ejecutar trabajo de campo
Información	Políticas de seguridad de la información	Gerencia	Documento de la política de seguridad de la información	Verificar una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información Verificar un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales Verificar un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo Verificar una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información	Recolectar la siguiente información: • Resultados de revisiones independientes • Estado de acciones preventivas y correctivas • Resultados de revisiones gerenciales previas • Desempeño del proceso y conformidad con la política de seguridad de la información • Cambios que podrían afectar el enfoque de la organización en el manejo de la seguridad de la información, incluyendo los cambios en el ambiente organizacional; las circunstancias comerciales; la disponibilidad de recursos; condiciones contractuales, reguladoras y legales; o el ambiente técnico;
Comunicación	Administrar los problemas	Gerencia	Identificación y clasificación de problemas Rastreo y resolución de problemas Cierre de problemas Integración de las administraciones de cambios, configuración y problemas	Dar suficiente autoridad al gerente de problemas. Hacer análisis de causa raíz de los problemas reportados. Tomar propiedad de los problemas y del progreso de la resolución de problemas. Registrar y rastrear problemas de operación hasta su resolución. Investigar las causas raíz de todos los problemas significativos. Definir soluciones para los problemas operativos identificados. Garantizar la satisfacción de los usuarios finales con ofrecimientos de servicios y niveles de servicio. Reducir el re-trabajo y los defectos de la solución y de la prestación de servicios. Proteger el logro de los objetivos de TI	Revisar: Duración promedio entre el registro de un problema y la identificación de la causa raíz. % de problemas para los cuales se realizó un análisis de causa raíz. La frecuencia de reportes o actualizaciones de un problema en curso, con base en la severidad del problema. % de problemas registrados y rastreados % de problemas recurrentes (en un periodo de tiempo) por severidad.

Tabla 3.1 Ejemplo de relevamiento de evidencias*

**La lista completa se puede apreciar en el Anexo C*

N°	Evidencia	Criterio	Hallazgo	Resultado	Recomendaciones
1	Los contratos del personal del departamento de sistemas no cuentan con clausulas contractuales de Confidencialidad y Propiedad Intelectual	Políticas de seguridad de la información	Se podría generar conflictos legales en caso de vinculación de los funcionarios y litigios respecto a la propiedad del software	No satisfactorio	Se recomienda a corto o largo plazo incluir en los contratos clausulas de Confidencialidad y Propiedad Intelectual Formalizar e implementar una Política de Seguridad que tome como base la ISO 27002 o mediante una Evaluación de Riesgos

Tabla 3.2 Ejemplo de relevamiento de hallazgos

Además antes de comunicarlas, se debe considerar discutir los hallazgos con la empresa auditada, el objetivo de esta discusión es llegar a un acuerdo sobre los hallazgos y desarrollar un curso de acción para corregirlos.

Durante la sustentación final de hallazgos, conclusiones y recomendaciones ante el ente que solicitó la auditoría (incluyendo al auditado), el auditor puede:

- Asegurarse que los hechos presentados en el reporte estén correctos y sean entendidos por todas las partes involucradas.
- Asegurarse que las recomendaciones sean realistas y eficientes desde diferentes ámbitos: financieros, organizacionales, culturales, regulatorios, entre otros.
- Establecer fechas de implementación para las recomendaciones acordadas.

4. Prueba del proceso de auditoría propuesto

El objetivo de este capítulo es comprobar la idoneidad del proceso de auditoría de la información y comunicación del control interno según COSO II descrito y elaborado en los capítulos anteriores

4.1. Descripción del caso prueba

El caso prueba está basado en el "banco XYZ" el cual es un banco privado comercial especializado en microfinanzas. Inició sus operaciones el 4 de mayo de 1998, actualmente es la entidad de microfinanzas líder en el Perú, contando con 117 agencias y con más de 600 mil clientes a nivel nacional. Tiene un impacto crucial tanto a nivel social, económico, como en el desarrollo y evolución del sector financiero en el país. En la Figura 4.1 se puede apreciar el Gobiernos Corporativo que implementa dicho banco.

4.2. Objetivo de la prueba

El objetivo de la prueba fue contrastar los criterios de Políticas de Seguridad de la información y Gestión de continuidad del negocio (véase el Anexo C) con los documentos respectivos del caso prueba. Teniendo como resultado las evidencias, hallazgos y posteriormente la emisión de conclusiones y recomendaciones del proceso de auditoría.

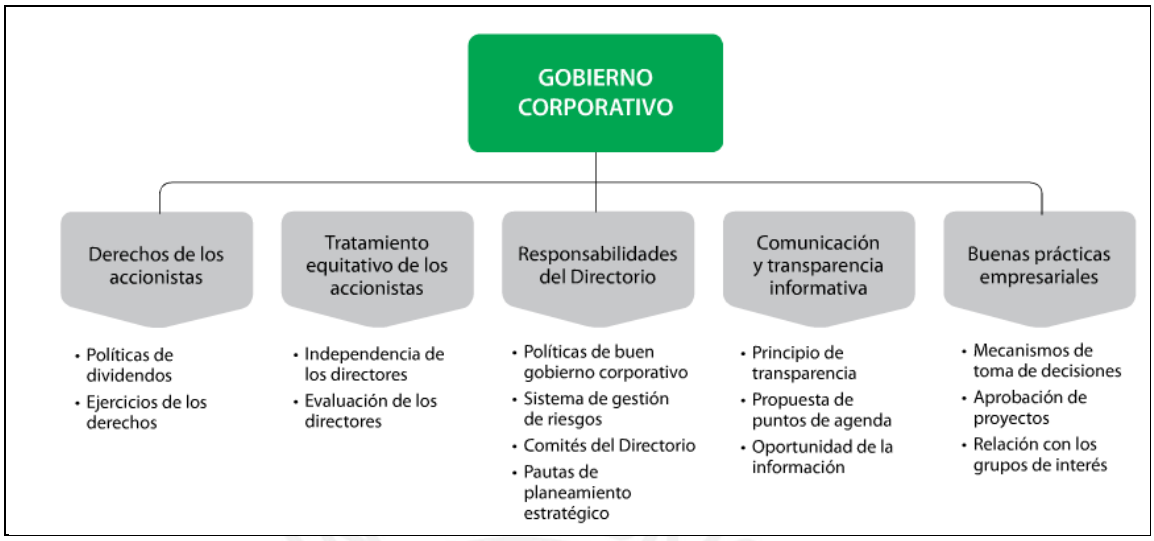

Figura 4.1 Gobierno Corporativo del "Banco XYZ"

4.3. Conducción de la prueba

Para la prueba se procedió a recolectar los documentos del "Banco XYZ" relevantes para contrastar los criterios antes mencionados, los cuales son:

- Política Corporativa de Seguridad de la Información
- Plan de Recuperación ante desastres de los servicios de TI

Posteriormente, utilizando los documentos recolectados, se aplicaron los procesos de relevamiento de evidencias, documentación de hallazgos y conclusiones y recomendaciones descritos en el presente proyecto de fin de carrera.

4.3.1. Relevamiento de evidencias

En esta sección se utilizó la Tabla 4.1 para el relevamiento de evidencias revisando los documentos recolectados del "Banco XYZ" y haciendo hincapié en los objetivos de los criterios escogidos con anterioridad.

Criterio	Auditado	Documentos a pedir	Objetivo de revisión del documento	Evidencias
Políticas de seguridad de la información	Gerencia	Documento de la política de seguridad de la información	Verificar una definición de seguridad de la información, sus objetivos y alcance generales y la importancia de la seguridad como un mecanismo facilitador para intercambiar información Verificar un enunciado de la intención de la gerencia, fundamentando sus objetivos y los principios de la seguridad de la información en línea con la estrategia y los objetivos comerciales Verificar un marco referencial para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación del riesgo y la gestión de riesgo Verificar una explicación breve de las políticas, principios, estándares y requerimientos de conformidad de la seguridad de particular importancia para la organización, incluyendo: 1. conformidad con los requerimientos legislativos, reguladores y restrictivos, 2. educación, capacitación y conocimiento de seguridad, 3. gestión de la continuidad del negocio, 4. consecuencias de las violaciones de la política de seguridad de la información Verificar una definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información incluyendo el reporte de incidentes de seguridad de la información Verificar referencias a la documentación que fundamenta la política; por ejemplo, políticas y procedimientos de seguridad más detallados para sistemas de información específicos o reglas de seguridad que los usuarios debieran observar.	• El documento no cuenta con las definiciones de seguridad de la información, objetivos, ni alcance correctamente identificadas y separadas • El documento si cuenta con la intención de la gerencia y la fundamentación de sus objetivos y principio de seguridad • El documento menciona un marco referencial, sin embargo no es claro ni está bien identificado • El documento no define los principios, estándares y requerimientos de conformidad de la seguridad • El documento si cuenta con las definiciones de las responsabilidades generales y especificas para la gestión de la seguridad • El documento pretende hacer referencia a documentos mas específicos sobre las políticas de seguridad de otros sistemas como las Comunicaciones y Operaciones o Control de Accesos

Criterio	Auditado	Documentos a pedir	Objetivo de revisión del documento	Evidencias
Gestión de continuidad del negocio	Gerencia	Plan de Recuperación ante desastres de los servicios de TI	Verificar que la gestión de continuidad del negocio incluya: a) entender los riesgos que enfrenta la organización en términos de la probabilidad y el impacto en el tiempo, incluyendo la identificación y priorización de los procesos comerciales críticos b) identificar todos los activos involucrados en los procesos comerciales críticos c) entender el impacto que probablemente tendrán las interrupciones causadas por incidentes en la seguridad de la información en el negocio (es importante encontrar las soluciones que manejen los incidentes que causan el menor impacto, así como los incidentes serios que pueden amenazar la viabilidad de la organización), y establecer los objetivos comerciales de los medios de procesamiento de la información; d) considerar la compra de un seguro adecuado que pueda formar parte de un proceso general de la continuidad del negocio, y que también sea parte de la gestión del riesgo operacional; e) identificar y considerar la implementación de controles preventivos y atenuantes adicionales; f) identificar los recursos financieros, organizacionales, técnicos y ambientales suficientes para tratar los requerimientos de seguridad de la información identificados; g) garantizar la seguridad del personal y la protección de los medios de procesamiento de la información y la propiedad organizacional h) formular y documentar los planes de continuidad del negocio tratando los requerimientos de seguridad de la información en línea con la estrategia acordada para la continuidad del negocio i) asegurar que la gestión de la continuidad del negocio se incorpore a los procesos y estructura de la organización; se debe asignar la responsabilidad del proceso de la gestión de la continuidad del negocio en el nivel apropiado dentro de la organización Probar que el proceso de planeación de la continuidad del negocio	• El documento es muy explicito en cuanto a la definición de los escenarios a presentarse, responsables, identificación de los recursos, seguridad del personal y actividades a ejecutarse en caso de un siniestro. Además también menciona prioridades de recuperación y que cuentan con un seguro para el caso de incendios, terremotos, etc. • El documento cuenta con un buen plan de prueba del proceso de planeación de la continuidad del negocio ya que define y aplica todo lo estipulado en el plan de continuidad, identifica la perdida de la información aceptable, educación apropiada del personal, toma de tiempos (cuanto tiempo se demora en recuperase de un desastre),etc. • El documento menciona un cronograma de ejecución de pruebas que se elabora por año. • El documento describe apropiadamente las operaciones antes, durante y después de desastre. Además de un plan de manteniendo del plan de contingencia.

			considere lo siguiente: a) identificar y acordar todas las responsabilidades y los procedimientos de continuidad del negocio b) identificar la pérdida aceptable de la información y los servicios c) implementación de los procedimientos para permitir la recuperación y restauración de las operaciones comerciales y la disponibilidad de la información en las escalas de tiempo requeridas; se debiera prestar particular atención a la evaluación de las dependencias comerciales internas y externas y el establecimiento de los contratos debidos d) los procedimientos operacionales a seguir dependiendo de la culminación de la recuperación y restauración; e) documentación de los procesos y procedimientos acordados; f) educación apropiada del personal en los procedimientos y procesos acordados, incluyendo la gestión de crisis g) prueba y actualización de los planes. Examinar que la planeación de continuidad del negocio trate los requerimientos de seguridad de la información y considere lo siguiente: a) las condiciones para activar los planes que describen el proceso a seguirse (por ejemplo, cómo evaluar la situación, quién va a participar) antes de activar cada plan b) los procedimientos de emergencia que describen las acciones a realizarse después del incidente que pone en riesgo las operaciones comerciales c) procedimientos de contingencia que describen las acciones tomadas para trasladar las actividades comerciales esenciales de los servicios de soporte a locales temporales alternativos, y regresar los procesos comerciales a la operación en las escalas de tiempo requeridas d) procedimientos operacionales temporales a seguirse hasta la culminación de la recuperación y restauración; e) procedimientos de reanudación que describen las acciones a tomarse para regresar a las operaciones comerciales normales f) un programa de mantenimiento que especifica cómo y cuándo se va a probar el plan, y el proceso para mantener el plan	

			g) las actividades de conciencia, educación y capacitación diseñadas para crear el entendimiento de los procesos de continuidad del negocio y asegurar que los procesos continúen siendo efectivos; h) las responsabilidades de las personas, describiendo quién es el responsable de ejecutar cuál componente del plan. Se debieran nombrar alternativas conforme sea necesario. i) los activos y recursos críticos necesitan ser capaces de realizar los procedimientos de emergencia, de respaldo y reanudación.	

Tabla 4.1 Relevamiento de evidencias del caso de prueba

4.3.2. Documentación de hallazgos

En la Tabla 4.2 se puede apreciar la forma de cómo documentar los hallazgos utilizando las evidencias recolectadas anteriormente.

N°	Evidencia	Criterio	Hallazgo	Resultado	Recomendaciones
1	El documento no cuenta con las definiciones de seguridad de la información, objetivos, ni alcance correctamente identificadas y separadas	Políticas de seguridad de la información	Se podría generar confusión y desinformación entre el personal	No satisfactorio	Se recomienda a corto o mediano plazo incluir las definiciones concretas, claras y bien diferenciadas de seguridad d la información, objetivos y alcance al documento
2	El documento si cuenta con la intención de la gerencia y la fundamentación de sus objetivos y principio de seguridad		La gerencia expresa su intención y preocupación sobre definir políticas de seguridad adecuadas para la empresa	Satisfactorio	
3	El documento menciona un marco referencial, sin embargo no es claro ni está bien identificado		Al no contar con un marco referencial bien identificado se puede perder los objetivos reales de las políticas de seguridad de la información	No satisfactorio	Se recomienda a corto o mediano plazo definir concreta, clara y bien diferenciada el marco de referencia del documento de política de seguridad
4	El documento no define los principios, estándares y requerimientos de conformidad de la seguridad		Se podría generar conflictos legales en caso se incumpla con leyes de las cuales se basa las política de seguridad	No satisfactorio	Se recomienda a corto o media plazo definir o hacer referencia a los principios, estándares y requerimientos de conformidad de la seguridad
5	El documento si cuenta con las definiciones de las responsabilidades generales y especificas para la gestión de la seguridad		El documento define correctamente las responsabilidades y responsables para cada aspecto de la seguridad de la información	Satisfactorio	
6	El documento pretende hacer referencia a documentos más específicos sobre las políticas de seguridad de otros sistemas como las Comunicaciones y Operaciones o Control de Accesos		El documento no se encuentra bien estructurado ni ordenado, en ese sentido puede confundir a la ubicación de los documentos que hace referencia	No satisfactorio	Se recomienda a corto o media plazo ordenar y organizar de una mejor forma el documento de tal forma que la comprension sea la mas clara y entndible posible

N°	Evidencia	Criterio	Hallazgo	Resultado	Recomendaciones
1	El documento es muy explicito en cuanto a la definición de los escenarios a presentarse, responsables, identificación de los recursos, seguridad del personal y actividades a ejecutarse en caso de un siniestro. Además también menciona prioridades de recuperación y que cuentan con un seguro para el caso de incendios, terremotos, etc.	Gestión de continuidad del negocio	El documento describe perfectamente los conceptos necesarios para desarrollar un buen plan de continuidad de negocio	Satisfactorio	
2	El documento cuenta con un buen plan de prueba del proceso de planeación de la continuidad del negocio ya que define y aplica todo lo estipulado en el plan de continuidad, identifica la pérdida de la información aceptable, educación apropiada del personal, toma de tiempos (cuanto tiempo se demora en recuperase de un desastre),etc.		Se cuenta con un plan de prueba del proceso de planeación bien desarrollado y claro de modo que cualquier empleado en cualquier nivel jerárquico puede seguir y entender dicho plan.	Satisfactorio	
3	El documento menciona un cronograma de ejecución de pruebas que se elabora por año.		El documento cuenta con un cronograma validado por todas las áreas relacionadas al plan de contingencia.	Satisfactorio	
4	El documento describe apropiadamente las operaciones antes, durante y después de desastre. Además de un plan de		Se describe muy acertadamente los procedimientos a tomar en cuenta antes , durante y después de un desastre; además de definir los responsables en cada una de esas	Satisfactorio	

	manteniendo del plan de contingencia.		etapas.		

Tabla 4.2 Documentación de hallazgos del caso de pruebas

4.3.3. Conclusiones y Recomendaciones

Se concluyó que el documento de Política Corporativa de Seguridad de la Información no es satisfactorio debido a que no cumple con la mayoría de los objetivos definidos por el criterio de Política de la de Seguridad de la Información.

Se concluyó que el documento de Plan de Recuperación ante desastres de los servicios de TI si es satisfactorio ya que cumple con los objetivos especificados en el criterio de Gestión de continuidad del negocio.

Se recomendó a corto o mediano plazo reestructurar el documento de Política Corporativa de Seguridad de la Información a fin de contar con una buena base en la gestión de seguridad de la información.

5. Conclusiones y Recomendaciones

Para concluir con este proyecto de fin de carrera, este capítulo se dedicará a mostrar las conclusiones y recomendaciones obtenidas al finalizar este proyecto. Para después explicar las recomendaciones y los trabajos futuros a presentarse tomando como base este proyecto.

5.1. Conclusiones

- Se consiguió efectuar los objetivos planteados en este proyecto de fin de carrera, cumpliendo con el cronograma y los entregables establecidos en la etapa de planificación de este proyecto. Lo cual significó aplicar un sentido de responsabilidad, disciplina, investigación y constancia.
- Los resultados de este proyecto de fin de carrera se cumplieron al 100% ya que se definieron los elementos del control interno partiendo de los estipulado en COSO I y II, los aspectos a evaluar para las variables de información y comunicación del control interno, riesgos y controles de los aspectos anteriormente determinados, para efectos de definir los criterios de auditoría. Además de determinar un proceso de relevamiento de evidencias, hallazgos y documentación de conclusiones.
- El presente proyecto de fin de carrera puede ser aplicable a COSO III , Basile II – III

- Para desarrollar el presente proyecto de tesis se aplicó los conocimientos de los cursos de Seguridad de la Información, Sistemas de Información, Sistemas de Control y Auditoria de Sistemas de Información, Administración de las Funciones Informáticas, Seguridad Computacional, Temas Avanzados en Tecnología de la Información, entre otros. Además se cumplió con el objetivo de desarrollar un proyecto de fin de carrera en un año académico.

5.2. Recomendaciones y Trabajos futuros

- Se recomienda ampliar o actualizar los conceptos de control interno con los nuevos marcos como COSO III y Basile II – III.
- Se recomienda ampliar el proceso de auditoría no solo ya a la información y comunicación si no a los demás aspectos del control interno según COSO II en primera instancia para después desarrollarlo para COSO III.
- Se recomienda aplicar el proceso de auditoría no solo al control interno de las empresas financieras del mercado, si no también aplicarla a la seguridad de las denominadas empresas circulares por la Superintendencia de Banca y Seguros.

Bibliografía

[British Broadcasting Corporation 2011] British Broadcasting Corporation (BBC)
2002 "ENRON: radiografía de un escándalo".bbc.6 de febrero. Consulta: 12 de setiembre del 2011. <http://news.bbc.co.uk/hi/spanish/news/newsid_1803000/1803224.stm>

[CIEC 2009] Centro Integral de Educación Continua (CIEC) Universidad de Lima
2009 Nuevos enfoques del control interno [diapositivas]. Lima

[COSO 1992] Committe of Sponsoring Organizations of the Treadway Commission
1992 Internal Control Integrated Framework. USA. COSO Publishing

[COSO ERM 2004] Committe of Sponsoring Organizations of the Treadway Commission
2004 Gestión de riesgos corporativos — ERM. USA. COSO Publishing

[COSO 2011] Committe of Sponsoring Organizations of the Treadway Commission
2011 Consulta: 28 de setiembre del 2011. <http://www.coso.org/>

[CGRP 1998] Contraloría General de la República de Panamá
1998 " Normas del Control Interno Gubernamenta".5 de mayo. Consulta 1 de octubre del 2011 <http://unpan1.un.org/intradoc/groups/public/documents/icap/unpan026373.pdf>

[CGRP 2011] Contraloría General de la Republica de Perú
2011 Consulta: 28 de setiembre del 2011. <http://www.contraloria.gob.pe/>

[COSO 2007] R. Moeller
2007 COSO Enterprise Risk Management: understanding the new integrated ERM framework.USA. Wiley&Sons

[ELN2000] Fabian O. Linares Chirinos
2000 Consulta;15 de setiembre 2012 <http://http://www.linareschirinos.com.ar/Biblioteca/Ley%20Sarbanes-Oxley/Ley_Sarbanes-Oxley_index.htm/>

[ISACA 2012] ISACA
2012 Cobit 5ta edición

[ISO19011 2002] ISO 19011
2002 ISO 1ra edición

[ISO 27000] The ISO 27000 Directory 2011
2011 Consulta: 28 de setiembre del 2011 <http://www.27000.org/>

[ISO24774 2010] ISO 24774
2010 ISO 1ra edición

[IES 2007] IES Antonio Machado
2007 Metodología PDCA [diapositivas]. Madrid-España

[Iñaki Díez 2010] Iñaki Díez
2010 “La justicia italiana condena al principal acusado del fraude de Parmalat a 18 años de cárcel”. rtve.9 de diciembre. Consulta: 12 de setiembre de 2011. <http://www.rtve.es/noticias/20101209/justicia-italiana-condena-principal-acusado-del-fraude-parmalat-a-18-anos-carcel/383760.shtml>

[ISACA 2012] ISACA

2012 "ISACA- Código de Ética Profesional".
Consulta: 3 de enero de 2012.
<http://www.isaca.org.pe/index.php/que-son-las certificaciones/etica-profesional.html>

[J. Lam 2003] J. Lam

2003 Enterprise Risk Management.
USA. Wiley&Sons.

[PMPS 2007] Pedro Manuel Pérez Solórzano

2007 "Los cinco componentes del Control Interno".
Consulta: 7 de setiembre del 2011.
<http://www.degerencia.com/articulo/los_cinco_componentes_del _control_interno>

[UPN2010] Vazallo Veneros Carlos Alberto.y Rodriguez Malaver.Beto Alonso

2010 "Implementacion de un sistema de administración del riesgo operativo en los procesos de créditos y cobranzas y su impacto en la eficiencia de las operaciones de la empresa Carrocerias Continental SAC"
Trujillo-Perú

[Tupia 2009] Tupia Anticona, Manuel

2009 Administración de la seguridad de información. Segunda edición.
Lima: Tupia Consultores y Auditores.