EVALUACIÓN TÉCNICA INFORMÁTICA DEL SISTEMA DE INFORMACIÓN DE LA CORPORACIÓN HOLDINGDINE S.A. (MATRIZ), UTILIZANDO EL ESTÁNDAR INTERNACIONAL COBIT

Andrés Naveda Paredes; Eco. Gabriel Chiriboga B.; Ing. Mario Ron Egas MSc.

Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Ecuador, apnaveda@espe.edu.ec;
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Ecuador, gechiriboga@espe.edu.ec;
Departamento de Ciencias de la Computación, Escuela Politécnica del Ejército, Ecuador, mbron@espe.edu.ec;

RESUMEN

El presente proyecto tiene por objetivo realizar la Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), con el Estándar Internacional COBIT 4.1.

Se definió el alcance de la auditoría mediante la identificación de los requerimientos de información relevantes del negocio y el detalle de los riesgos TI más críticos con el uso de una Matriz de Riesgos, que permitió realizar la selección de los procesos y actividades que más adelante fueron auditados, luego se elaboró el Plan de Investigación de Campo o Programa de Auditoría, con el que se recopiló la información pertinente y las evidencias relacionadas. La auditoría se desarrolló cumpliendo las directrices establecidas por el Marco de Referencia COBIT 4.1.

Finalmente se presentó los informes resultantes de la auditoría realizada, incluyendo un resumen ejecutivo y el informe detallado con las evidencias correspondientes como parte de la Evaluación Técnica Informática de la Corporación.

Palabras Clave:

Auditoría, Informática, Sistema, Información, COBIT, HOLDINGDINE.

ABSTRACT

This project aims to perform the Technical Informatics Evaluation of the Corporation HOLDINGDINDE S.A. (Headquarters), for this propose it was used the International Standard COBIT 4.1.

First it was defined the range of the audit, identifying the main requirements of information of the Corporation, detailing the most critical IT risks using a Risk Matrix. Then it was made a selection of process and activities that were audit. Right away it was executed the Field Research Plan or Audit Program, based on the evidence and information collected inside the Corporation. The audit was developed in compliance with the guidelines established by the COBIT 4.1 framework.

Finally it was presented the audit report, including an executive summary and a detailed resume of main findings as part of the Technical Informatics Evaluation; in addition it was manifested conclusions and general recommendations for the continuous improvement of HOLDINGDINDE S.A. (Headquarters).

Key Words:

Audit, Informatics, Systems, Information, COBIT, HOLDINGDINE.

1. INTRODUCCIÓN

En la actualidad, los negocios buscan soluciones de información que les permita competir en un mercado cada vez más globalizado, es aquí donde aparece el rol de las tecnologías de la información, que forman parte de la estrategia competitiva de las organizaciones y de esta manera incrementan la eficiencia operacional, así como la mejora en los procesos y la calidad de los servicios que ofrecen.

El impacto de la tecnología en las organizaciones, ha obligado a tener en cuenta aspectos muy relevantes como políticas de seguridad, estrategias organizacionales, separación de funciones, impacto de los errores, ingresos no autorizados, sustracción y manipulación de información, etc. [1].

Ante la necesidad de contar con un adecuado marco de administración y control, la Corporación HOLDINGDINE S.A., ha considerado la necesidad de realizar una Evaluación Técnica Informática en su matriz desde un punto de vista externo, bajo los estándares de un marco referencial a nivel mundial como es COBIT.

COBIT define las actividades de TI de una organización, mediante un modelo genérico de procesos en cuatro dominios que son: Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar; lo que brinda un marco de trabajo para la medición y monitoreo del desempeño de las tecnologías de información e integra las mejores prácticas administrativas [2].

El presente proyecto presenta un Informe Detallado a la Gerencia TI, que describe las observaciones y hallazgos de los procesos y actividades TI, identificados como los más críticos dentro de la Corporación, proporcionando recomendaciones para una mejora continua. Además de un Informe Final/Ejecutivo que se puso en conocimiento del staff ejecutivo de HOLDINGDINDE S.A.

2. MATERIALES Y MÉTODOS

2.1. Materiales

Para el plan de investigación de campo o programa de auditoría se utilizó los siguientes materiales:

- **Material de Evidencia:** El programa de auditoría que se ha planificado, parte de la elaboración de una Matriz de Riesgos TI, para identificar los procesos y actividades más críticos y así dar paso al plan de investigación de campo que se respaldará con :

    - **Cuestionarios,** la información obtenida a través de él, nos permite adelantar un pre diagnóstico de la situación de la unidad y orienta el trabajo de campo.
    - **Pruebas de cumplimiento,** determinan si un sistema de control interno funciona adecuadamente según la documentación, según declaran los auditados y según las políticas y procedimientos de la organización.
    - **Checklist,** técnica muy utilizada en el campo de la auditoría informática, no es más que una lista de comprobación, que sigue unas pautas determinadas dependiendo de qué estemos evaluando o qué objetivos queramos alcanzar.
    - **Pruebas sustantivas,** aportan al auditor informático suficientes evidencias para que se pueda realizar un juicio imparcial, verificando asimismo la exactitud, integridad y validez de la información obtenida.

- **Observación directa,** técnica que permite captar la realidad de la organización y puede ser de dos tipos, no participante es aquella en que el auditor observa externamente el proceso sin interferir en ellos y participante es aquella en la que el auditor participa en los procesos de la unidad auditada, sea integrándose en el grupo y sus actividades [3].

- **Material Tecnológico:** Computadora portátil, utilizada para la documentación y almacenamiento de la información entregada por la Gerencia TI de la Corporación para la auditoría.

- **Material Tecnológico:** Software, los programas que servirán de apoyo para este trabajo de auditoría son los siguientes:
  - Microsoft Office Project 2007, para planificación y control de tareas.
  - Microsoft Office Excel, para la matriz de riegos.
  - Microsoft Office Word, para documentación.

2.2. Métodos

Los métodos empleados en el presente proyecto se fundamentan en la auditoría basada en riesgos; primero se planea para obtener y entender los procesos de negocio; en segundo lugar se analiza y evalúa el control interno establecido para determinar la probable efectividad y eficiencia del mismo; posteriormente, se aplican pruebas de auditorías para verificar la efectividad de los procedimientos de control (pruebas de cumplimiento), o de los productos de los procesos de trabajo (pruebas sustantivas). Después se informan los resultados de la auditoría, con el fin de reportar las sugerencias correspondientes a las oportunidades de mejora encontradas.

Para que la Corporación HOLDINGDINDE S.A. (Matriz) pueda asegurar que construye proyectos de tecnología de información que cubren de manera adecuada los requerimientos del negocio, se aplicará el estándar internacional conocido como Control Objetives for Information and Related Technology (COBIT), que sirve como guía para la buena práctica de la auditoría de las TI, emitido por la ISACA. Éste contempla los procesos típicos de la función de TI, agrupados en cuatro dominios, que se muestra en el **Figura 1.**

- **Planificación y Organización:** identificación de la forma en que las TI pueden contribuir de la mejor manera al logro de los objetivos institucionales, y al establecimiento de una organización e infraestructura tecnológica apropiada.
- **Adquisición e Implementación:** para llevar a cabo la estrategia de TI es necesario identificar, desarrollar o adquirir soluciones de TI adecuadas, así como implementarlas e integrarlas dentro del proceso del negocio. Además, cubre los cambios y el mantenimiento realizados a sistemas existentes.
- **Distribución y Soporte:** corresponde a la entrega de los servicios requeridos, desde las tradicionales operaciones sobre seguridad y continuidad, hasta la capacitación, así como los procesos de soporte necesarios.
- **Monitoreo:** todos los procesos necesitan ser evaluados de forma regular a través del tiempo, para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Figura 1. Dominios COBIT

Se puede afirmar que el éxito de una organización depende de los controles de evaluación, de la eficacia y eficiencia de sus sistemas de TI. Hoy en día, las organizaciones estructuran su información en sistemas de TI, debido a ello, es de vital importancia que éstos funcionen de forma correcta e ininterrumpida para la productividad y supervivencia futura de una organización. El trabajo que se realiza en la auditoría informática debe contar con un marco de referencia metodológico, así como con gente altamente capacitada, ya que una auditoría mal hecha puede acarrear consecuencias drásticas económicamente para la organización auditada [4].

2.3. Estándar COBIT 4.1.

Este estándar parte con una simple y pragmática premisa de "proporcionar la información que la organización necesita para llevar a cabo sus objetivos, los requisitos de las tecnologías de la información necesitan ser gestionados por un conjunto de procesos agrupados de forma natural" y cuenta con un conjunto de 34 objetivos de control de alto nivel para cada uno de los procesos de las tecnologías de la información, agrupados en cuatro dominios: planificación y organización, adquisición e implementación, soporte de entrega y monitorización. Mediante la dirección de estos 34 objetivos de control de alto nivel, los procesos propios de negocio pueden garantizar la existencia de un sistema de control adecuado para los entornos de las tecnologías de la información, que se observa en la **Figura 2.**

En suma, cada uno de los 34 objetivos de control de alto nivel, corresponde a una directiva de revisión y/o seguridad, que permite la inspección de los procesos de las tecnologías de la información, en contraste con los 302 objetivos de control detallados en COBIT en los que se especifica en forma explícita los controles necesarios para una gestión de calidad [5].

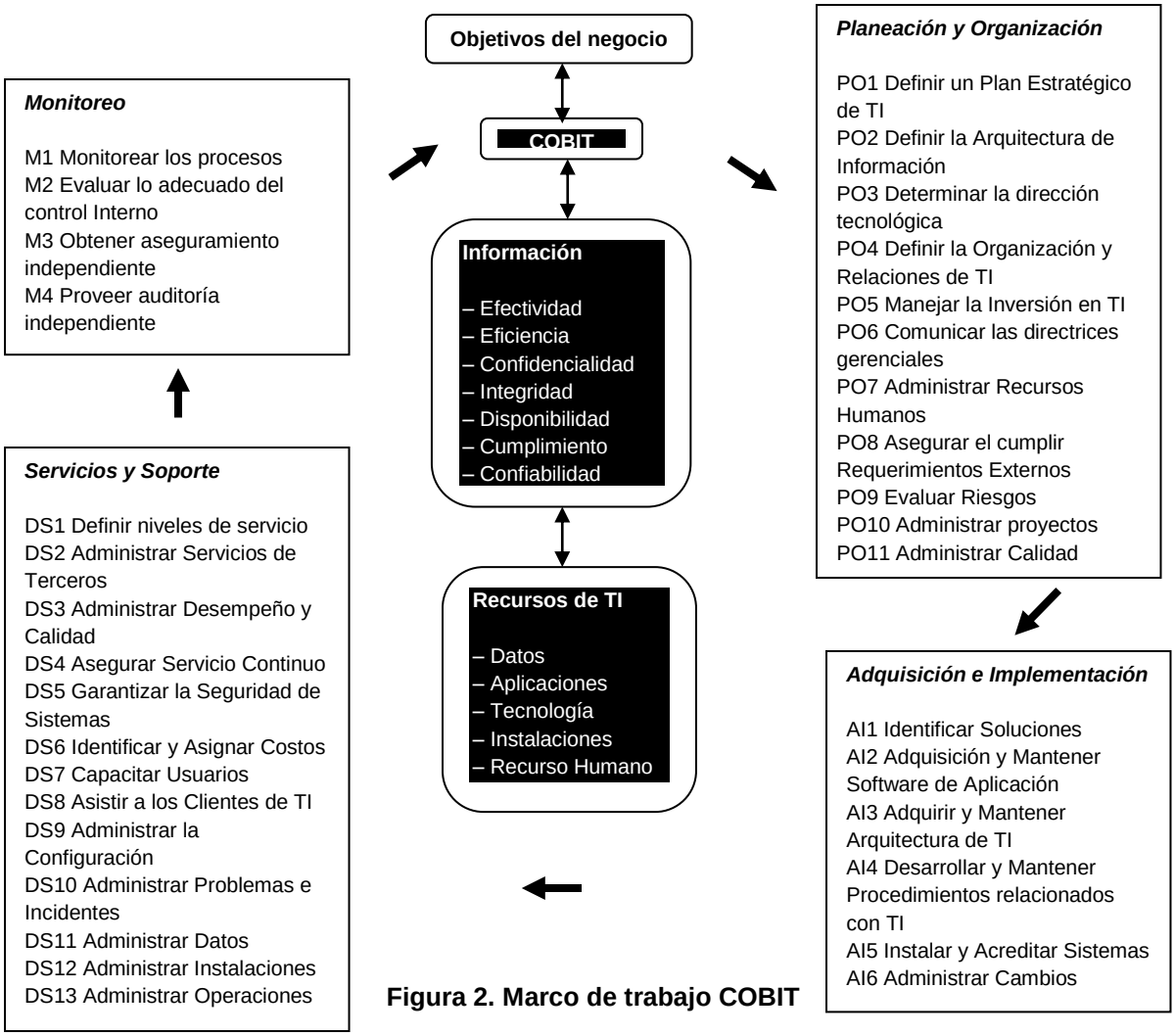

Figura 2. Marco de trabajo COBIT

2.3.1 Componentes de COBIT

- ***Resumen Ejecutivo*** (Executive Sumary), que consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y concientizando sobre los conceptos clave y principios de COBIT;
- ***Marco Referencial*** (Framework), que proporciona a la alta gerencia un entendimiento más detallado de los conceptos clave y principios de COBIT, e identifica los cuatro dominios en detalle, además, los 34 objetivos de control de alto nivel e identificando los requerimientos de negocio para la información y los recursos de las Tecnologías de la Información que son impactados en forma primaria por cada objetivo de control;
- ***Objetivos de Control*** (Control Objetives), los cuales contienen declaraciones de los resultados deseados o propósitos a ser alcanzados mediante la implementación de 302 objetivos de control detallados [6].

2.3.2 Marco Referencial

Contiene los Objetivos de Control de TI de alto nivel y una estructura general para su clasificación y presentación, consta de tres niveles de actividades de TI al considerar la administración de sus recursos. Comenzando por la base, encontramos las actividades y tareas necesarias para alcanzar un resultado medible, las actividades cuentan con un concepto de ciclo de vida, mientras que las tareas son consideradas más discretas. El concepto de ciclo de vida cuenta con requerimientos de control diferentes a los de actividades discretas, algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios.

La segunda categoría incluye tareas llevadas a cabo como soporte para la planeación estratégica de tecnologías de la información, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño. Los procesos se definen entonces en un nivel superior como una serie de actividades o tareas conjuntas. Al nivel más alto, los procesos son agrupados de manera natural en dominios, su agrupamiento natural es confirmado frecuentemente como dominio de responsabilidad en una estructura organizacional y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de tecnologías de la información.

El Marco Referencial conceptual puede ser enfocado desde tres puntos estratégicos: Recursos de TI, Requerimientos de negocio para la información y Procesos de TI. Estos puntos de vista diferentes permiten al Marco Referencial ser accedido eficientemente como se muestra en la **Figura 3.** [7].

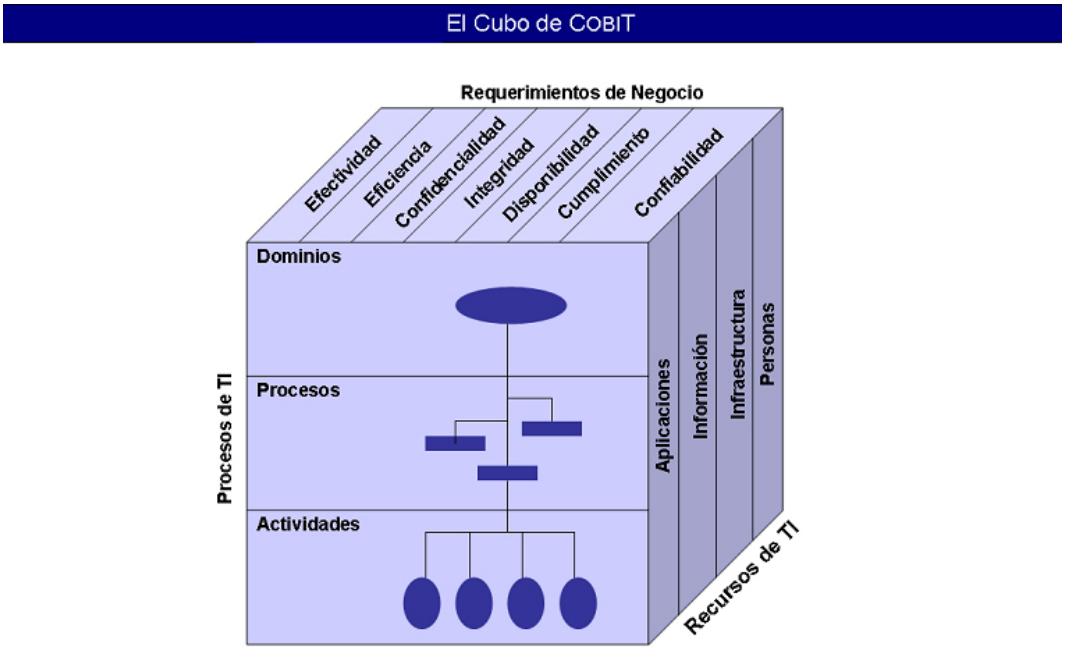

Figura 3. Cubo COBIT [7]

2.3.3 COBIT orientado a Procesos

El marco de trabajo COBIT proporciona un modelo de procesos de referencia y un lenguaje común para que todos en la empresa visualicen y administren las actividades de TI. Un modelo de procesos fomenta la propiedad de los procesos, permitiendo que se definan las responsabilidades.

Para gobernar efectivamente TI, es importante determinar las actividades y los riesgos que requieren ser administrados. Normalmente se ordenan dentro de dominios de responsabilidad de planificar, construir, ejecutar y monitorear.

- **Planear y Organizar (PO)** - Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicio (DS)
- **Adquirir e Implementar (AI)** - Proporciona las soluciones y las pasa para convertirlas en servicios.
- **Entregar y Dar Soporte (DS)** - Recibe las soluciones y las hace utilizables por los usuarios finales.
- **Monitorear y Evaluar (ME)** - Monitorear todos los procesos para asegurar que se sigue la dirección prevista [8].

3. ANÁLISIS Y DISEÑO

3.1. Análisis

La Corporación HOLDINGDINE S.A. (Matriz) debe cumplir con requerimientos de calidad, fiduciarios y de seguridad, tanto para su información, como para sus activos. La Gerencia TI debe optimizar el empleo de sus recursos disponibles, que incluye: personal, instalaciones, tecnología, sistemas de aplicación y datos. Para cumplir con esta responsabilidad, así como para alcanzar sus objetivos, la gerencia debe entender el estado de sus propios sistemas de TI y decidir el nivel de seguridad y control que deben proveer estos sistemas.

Los Objetivos de Control para la Información y las Tecnologías relacionadas (COBIT, versión 4.1.), ayudan a satisfacer las múltiples necesidades de la administración estableciendo un puente entre los riesgos del negocio, los controles necesarios y los aspectos técnicos. Provee buenas prácticas y presenta actividades en una estructura manejable y lógica. Las “Buenas prácticas” de COBIT ayudarán a optimizar la inversión de la información y proporcionarán un mecanismo de medición que permitirá juzgar cuando los procesos y actividades TI van por el camino equivocado.

3.2. Diseño

Una vez analizada y conocida la situación actual de la Corporación y de la Gerencia TI, la auditoría externa, aplicando COBIT 4.1., realizó las siguientes tareas:

- Elaboración de una Matriz de Riesgos TI, para identificar los riesgos más críticos de la Corporación.
- Preparación y desarrollo de un Plan de Investigación de Campo.
- Determinación de recursos e instrumentos para el Plan de Investigación de Campo.
- Planificación de cuestionarios, listas de chequeo, pruebas sustantivas, pruebas de cumplimiento y observaciones directas con el gerente y los especialistas de las tres áreas (Redes y Comunicaciones, Base de Datos y Administración de Aplicativos) de la Gerencia TI, con la finalidad de conocer más a detalle las actividades y procesos existentes en la corporación
- Recopilación de información referente a la entidad, Gerencia TI y al Sistema de Información.
- Análisis de la información y documentación, para emitir conclusiones para cada actividad de control.
- Elaboración de un Informe Detallado de auditoría, donde por cada Objetivo de Control se detallará:
    - Observaciones.
    - Evidencias.
    - Recomendaciones.
- Presentar y analizar el Informe Detallado a la Gerencia TI, donde se incluye todas oportunidades de mejora, con la finalidad de conocer su opinión al respecto.
- Finalmente emitir el Informe Ejecutivo de auditoría que será entregado al staff de la Corporación HOLDINGDINE S.A. (Matriz).

4. RESULTADOS

A continuación, en la **Tabla 1.**, se detalla los resultados del Grado de Madurez, de cada uno de los 34 procesos que recomienda COBIT 4.1., del Sistema de Información de la Corporación HOLDINGDINDE S.A. (Matriz).

MATRIZ DE PROCESOS DEL SISTEMA DE INFORMACIÓN DE LA CORPORACIÓN HOLDINGDINE S.A. (MATRIZ)	
PROCESOS	**GRADO DE MADUREZ**
Dominio: Planear y Organizar (PO)	
PO1 Definir un plan estratégico de TI	2
PO2 Definir la arquitectura de la información	2
PO3 Determinar la dirección tecnológica	2
PO4 Definir los procesos, organización y relaciones de TI	2
PO5 Administrar la inversión en TI	1
PO6 Comunicar las aspiraciones y la dirección de la gerencia	1
PO7 Administrar recursos humanos de TI	3
PO8 Administrar la calidad	0
PO9 Evaluar y administrar los riesgos de TI	1
PO10 Administrar proyectos	1
Dominio: Adquirir e Implementar (AI)	
AI1 Identificar soluciones automatizadas	1
AI2 Adquirir y mantener software aplicativo	3
AI3 Adquirir y mantener infraestructura tecnológica	2
AI4 Facilitar la operación y el uso	1
AI5 Adquirir recursos de TI	3
AI6 Administrar cambios	0
AI7 Instalar y acreditar soluciones y cambios	0
Dominio: Entregar y Dar Soporte (DS)	
DS1 Definir y administrar los niveles de servicio	2
DS2 Administrar los servicios de terceros	2
DS3 Administrar el desempeño y la capacidad	2
DS4 Garantizar la continuidad del servicio	1
DS5 Garantizar la seguridad de los sistemas	2
DS6 Identificar y asignar costos	3
DS7 Educar y entrenar a los usuarios	0
DS8 Administrar la mesa de servicio y los incidentes	2
DS9 Administrar la configuración	0
DS10 Administración de problemas	2
DS11 Administrar los datos	2
DS12 Administración del ambiente físico	3

DS13 Administrar las operaciones	0
Dominio: Monitorear y Evaluar (ME)	
ME1 Monitorear y evaluar el desempeño de TI	1
ME2 Monitorear y evaluar el control interno	1
ME3 Garantizar el cumplimiento con requerimientos externos	2
ME4 Proporcionar gobierno de TI	2

Tabla 1. Grado de Madurez de los procesos del Sistema de Información de la Corporación HOLDINGDINDE S.A. (Matriz)

Los resultados expuestos se basan en el Modelo Genérico de Madurez descrito por COBIT 4.1., donde:

- **0 No Existente:** Carencia completa de cualquier proceso reconocible. La empresa no ha reconocido siquiera que existe un problema a resolver.
- **1 Inicial:** Existe evidencia que la empresa ha reconocido que los problemas existen y requieren ser resueltos.
- **2 Repetible:** Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea.
- **3 Definido:** Los procedimientos se han estandarizado y documentado, y se han difundido a través de entrenamiento. Los procedimientos en sí no son sofisticados pero formalizan las prácticas existentes.
- **4 Administrado:** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva.
- **5 Optimizado**: Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de mejoras continuas y en un modelo de madurez con otras empresas.

5. AGRADECIMIENTOS

Este trabajo pudo ser realizado gracias al apoyo de la Corporación HOLDINGDINE S.A., la cual proporcionó la ayuda necesaria para ejecutar el proyecto.

Mi más amplio agradecimiento para el Ing. Mario Ron, por su valiosa orientación y apoyo, quién con su excelente respaldo e interés, hicieron posible la realización de esta Evaluación Técnica Informática.

También quisiera hacer patente mi agradecimiento al Ing. Oswaldo Vaca y a la Ing. Paulina Porras, integrantes de la Gerencia TI de la Corporación HOLDINGDINE S.A., por las valiosas aportaciones que me brindaron para mejorar la presente investigación.

A todos, mi mayor reconocimiento y gratitud.

6. CONCLUSIONES Y TRABAJO FUTURO

Se detectaron las debilidades de los procesos y actividades TI más críticos, de la Corporación HOLDINGDINDE S.A. (Matriz) y se han expuesto las recomendaciones tendientes a minimizar el impacto en el caso de que se llegaran a materializar los riesgos.

Existen riesgos que requieren la aplicación de acciones inmediatas para evitar una exposición de alto impacto.

La participación de la alta gerencia y la implementación del gobierno de TI, aún no ha sido comprendida por la mayor parte de las organizaciones, esto incluye a la Corporación, como entidad industrial y comercial, por lo que las oportunidades de mejora detectadas, requieren el involucramiento y el apoyo de la alta gerencia para su implementación.

TI permite potencializar todos los procesos y actividades de la organización, por lo que se requiere una adecuada coordinación de las diferentes áreas de la Corporación con la Gerencia TI para llegar a acciones eficientes y eficaces.

En un futuro inmediato se recomienda formular, ejecutar y evaluar un Plan de mejora y cumplimiento de las recomendaciones establecidas en el Informe Detallado de la Evaluación Técnica Informática, los informes especiales y la Matriz de Correlación de COBIT emitido por el evaluador.

7. REFERENCIAS BIBLIOGRÁFICAS

- **[1]** Gil Peuchan Ignacio, “Sistemas y Tecnologías de la Información para la Gestión”, Edit. McGraw Hill, Madrid España (1999).
- **[2]** Definición de COBIT: http://www.eici.ucm.cl/Academicos/ygomez/descargas/Aud_Seg.../auditoria2.ppt
- **[3]** Víctor Manuel Mendívil Escalante (2002). Elementos de Auditoría. Quinta Edición. Thomson Editores.
- **[4]** José Antonio Echenique García, “Auditoria Informatica”, Editorial McGraw-Hill. Segunda Edición.
- **[5]** Modelo COBIT 4.1: http://alarcos.inf-cr.uclm.es/per/fruiz/cur/mso/comple/Cobit.pdf
- **[6]** Componentes del Modelo COBIT: http://ds5-andre-ortega-5a.host56.com/componentes.html
- **[7]** Marco Referencial: http://www.piramidedigital.com/Documentos/ICT/pdictcobitmarcoreferencial.pdf
- **[8]** Glanser Services, “IT Governance Institute COBIT 4.0 Objetivo de Control, Directrices Gerenciales y Modelos de Madurez” 2007