ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

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

Previa a la obtención del título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: **ANDRÉS PATRICIO NAVEDA PAREDES**

SANGOLQUÍ, Marzo **del** 2012

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. Andrés Patricio Naveda Paredes como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

13 de Marzo del 2012.

_____

Eco. Gabriel Chiriboga.
Profesor Director.

CERTIFICACIÓN

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. Andrés Patricio Naveda Paredes como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA.

13 de Marzo del 2012.

_____

Ing. Mario Ron.
Profesor Codirector.

AUTORIZACIÓN

Yo, Andrés Patricio Naveda Paredes.

Autorizo a la ESCUELA POLITÉCNICA DEL EJÉRCITO la publicación, en la Biblioteca Virtual de la Institución, del trabajo "Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), utilizando el Estándar Internacional COBIT", cuyo contenido, ideas y criterios es de mi exclusiva responsabilidad y autoría.

13 de Marzo del 2012.

_____

Andrés Patricio Naveda Paredes.
Autor.

DEDICATORIA

Dedico esta tesis a mis padres, por su comprensión y ayuda en momentos bueno y malos, me han enseñado a encarar las adversidades sin perder nunca la dignidad ni desfallecer en el intento, gracias a ellos, me he formado como persona con valores y principios acompañados de una gran dosis de amor.

A mi madre, que estuvo, está y estará siempre a mi lado brindándome su mano amiga y protectora, dándome a cada instante una palabra de aliento para ser una mejor persona. A mi padre, por ser un apoyo a lo largo de mi formación profesional.

Y finalmente a mí dedicación, esfuerzo y perseverancia por cumplir un objetivo más en mi vida.

ANDRÉS NAVEDA P.

AGRADECIMIENTOS

Esta tesis pudo ser realizada gracias al apoyo de la Corporación HOLDINGDINE S.A., la cual me proporcionó la ayuda necesaria para ejecutar el proyecto.

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

Y finalmente, quiero expresar mi agradecimiento a Dios, a mis padres y a todos quienes estuvieron vinculados de alguna manera a la realización de mi tesis.

A todos, mi mayor reconocimiento y gratitud.

ANDRÉS NAVEDA P.

ÍNDICE DE CONTENDIO

LISTADO DE TABLAS

LISTADO DE CUADROS

LISTADO DE FIGURAS

LISTADO DE ANEXOS

Se adjuntan en formato digital, en el CD ANEXOS del proyecto de grado "Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), utilizando el Estándar Internacional COBIT".

ANEXOS .....CD ANEXOS

ANEXO A.docx
ANEXO B.docx
ANEXO C.docx
ANEXO D.docx
ANEXO E.docx
ANEXO F.docx
ANEXO G.docx
ANEXO H.docx

NOMENCLATURA UTILIZADA

AICPA: American Institute of Certified Public Accountants / Instituto Norteamericano de Contadores Públicos.

ANS: Acuerdo de nivel de servicio / Service Level Agreement.

ATM: Modo de Transferencia Asíncrona.

BMIS: Modelo de Negocio para la Información de Seguridad.

CICA: Instituto Canadiense de Contadores Certificados.

CISA: Certified Information Systems Auditor.

COBIT: Control de Objetivos para Información y Tecnología relacionada / Control Objectives for Information and related Technology.

COSO: Committee of Sponsoring Organizations of the treadway commission.

CPD: Centro de Proceso de Datos.

CPU: Unidad Central de Procesos.

DBA: Administrador de Base de Datos / Database Administrator.

DRP: Plan de Recuperación ante Desastres / Disaster Recovery Plan.

DTI: Dirección de Tecnologías de la Información.

HW: Hardware.

ISACA: Information Systems Audit and Control Association.

ISAF: Information Systems Audit and Control Foundation.

ISG: Consejo de Dirección de TI / IT Steering Group.

ISM: Gestión de la Seguridad de Información / Information Security Management.

ISO: International Organization for Standardization.

ITGI: Instituto de Gobierno de TI.

ITSCM: Gestión de Continuidad de los Servicio de TI / IT Service Continuity Management.

ITSM: Gestión de los Servicios de TI / IT Service Management.

KPI: Indicador Clave de Rendimiento / Key Performance Indicator.

MPLS: Multiprotocol Label Switching.

PC: Personal Computer.

PDA: Procesamiento automático de Datos.

PYMES: Pequeña y media empresa.

QA: Aseguramiento de la Calidad / Quality Assurance.

QMS: Quality Management System.

SGBD: Sistema de gestión de base de datos.

SGSI: Sistema de Gestión de la Seguridad de la Información.

SI: Sistema de Información.

SQL: Structured Query Language.

SW: Software.

TI: Tecnologías de la Información.

TIC: Tecnologías de la Información y Comunicacion.

TQM: Gestión Total de Calidad / Total Quality Management.

RESUMEN

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

Se definió el alcance de la auditoría, identificando los requerimientos de información relevantes del negocio y detallando los riesgos TI más críticos con el uso de una Matriz de Riesgos que permitió la selección de los procesos y actividades que fueron auditados, luego se elaboró el Plan de Investigación de Campo o Programa de Auditoría en base a recursos de evidencia e información recopilados en la Corporación. Se desarrolló la auditoría 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 detalle de los principales hallazgos encontrados como parte de la Evaluación Técnica Informática, terminando con un planteamiento de conclusiones y recomendaciones generales hacia la mejora continua de la Corporación.

PRÓLOGO

En la actualidad los temas relativos a la auditoría informática cobran cada vez más relevancia, debido a que la información se ha convertido en el activo más importante de las empresas y representa su principal ventaja estratégica, por lo que éstas invierten enormes cantidades de dinero y tiempo en la creación de sistemas de información, con el fin de obtener la mayor productividad y calidad posibles.

Para hacer una adecuada planeación de una auditoría informática, hay que seguir una serie de pasos previos que permitan dimensionar el tamaño y los requerimientos del área clave dentro de la organización a auditar.

El Capítulo 1, detalla los objetivos y el alcance del presente proyecto debidamente justificados.

El Capítulo 2, expone algunos conceptos y parámetros que definen a la Evaluación Técnica Informática, relacionados con los Sistemas de Información, Tecnologías de Información y Comunicaciones, Control Interno, Técnicas y Herramientas de Auditoría Informática, fases de la Auditoría Informática y Auditoría basada en Riesgos. De igual manera el presente capítulo cuanta con un análisis detallado del Modelo COBIT 4.1.

El Capítulo 3, describe la aplicación del Estándar Internacional COBTI 4.1 en la Corporación HOLDINGDINE S.A. (Matriz).

El Capítulo 4, presenta el informe detallado y resultados del caso práctico, describiendo las debidas observaciones, recomendaciones y puntos de vista de la Evaluación Técnica Informática.

El Capítulo 5, detalla las conclusiones y recomendaciones obtenidas a lo largo del presente trabajo.

CAPÍTULO 1

GENERALIDADES

1.1. Introducción

En la actualidad, los negocios buscan soluciones de información que les permita competir en un mercado cada vez más globalizado, es aquí en 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.

Son múltiples las aplicaciones tecnológicas que están incidiendo sobre los procesos de trabajo y sobre las propias organizaciones de hoy día, por lo que las nuevas tecnologías afectan todos los aspectos de la vida laboral.

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.

Por ello ante la necesidad de contar con un adecuado marco de administración y control, la Corporación HOLDINGDINE S.A. (Matriz), desde hace algunos años, ha venido ejecutando proyectos que han permitido una centralización del sistema de tecnologías de información, mediante un ERP (Planificación de Recursos Empresariales).

HOLDINGDINE S.A. (Matriz) cuenta con una unidad de apoyo, Gerencia de TI, que centraliza la información para la administración, gestión de actividades TI e implantación de sistemas requeridos por la Corporación y se preocupa por el adecuado funcionamiento de las aplicaciones existentes, bases de datos, redes y comunicaciones, software aplicativo adquirido y otros.

Por ello se ha considerado la necesidad de realizar una Evaluación Técnica Informática desde un punto de vista externo, en su matriz, a los controles establecidos por la Gerencia de TI, 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.

1.2. Antecedentes

Originalmente dentro de la Corporación HOLDINGDINE S.A. (Matriz), la informática cubrió las áreas de negocio por medio de productos y servicios variados, proliferaron el uso de computadoras personales e irrumpiendo de lleno las redes locales, sin unidades de apoyo establecidas y un sinnúmero de desventajas que afectaban al principal activo de la Corporación, la información.

De este modo, los responsables de tecnologías de información se vieron desbordados por estos acontecimientos y les imposibilitó continuar con los métodos utilizados hasta ese entonces. Así surgió la necesidad de la integración de la información, a través del establecimiento de una unidad de apoyo clave, Gerencia de TI, donde su misión es facilitar la planificación de todos los recursos tecnológicos de la Corporación y sus subsidiarios.

Entre los cambios más significativos fue la implementación de un sistema de ERP y sin duda, la centralización de la información, de este modo se tiene un monitoreo en tiempo real, lo que trae como consecuencia una toma de decisiones más rápida y segura.

La Corporación HOLDINGDINE S.A. (Matriz), tiene un incremento constante de las expectativas y necesidades relacionadas con la auditoría informática, al igual que la actualización continua de los elementos que componen la tecnología de este campo obligándola a disponer controles, realizar evaluaciones periódicas y completas de los sistemas de información a cargo de personal con el conocimiento adecuado.

1.3. Justificación

El desarrollo y la evolución tecnológica que enfrenta HOLDINGDINE S.A. (Matriz) con el manejo de diversos sistemas de información y automatización en sus procesos y actividades, necesita detectar y corregir errores mediante una Evaluación Técnica Informática, realizada y ejecutada por personal capacitado, que proponga soluciones efectivas para minimizar riesgos y mejorar el empleo de la tecnología de información dentro de la Corporación.

La Evaluación Técnica Informática que se aplicará como un ente externo a la Corporación HOLDINGDINE S.A. (Matriz), debe evaluar y analizar el sistema de información y emitir una opinión independiente sobre los mismos. Esta evaluación permitirá recoger, agrupar e indagar evidencias para determinar si el sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos tecnológicos.

La evaluación, permitirá tener una visión más clara en el control de la función informática, en el análisis de la eficiencia de los sistemas informáticos, en la verificación del cumplimiento de la normativa, en este ámbito, y la revisión de la eficacia de la gestión de los recursos informáticos. De esta forma HOLDINGDINE S.A. (Matriz), ganará eficiencia, eficacia, rentabilidad y seguridad en cada uno de sus procesos y actividades.

Todo esto se realizará bajo los lineamientos y herramientas del Estándar Internacional COBIT 4.1.

1.4. Objetivos

1.4.1. Objetivo General

- Realizar una Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), utilizando el Estándar Internacional COBIT, a fin de identificar debilidades y emitir recomendaciones dentro del ambiente informático, que permitirá eliminar o minimizar los riesgos más críticos en los procesos y actividades TI.

1.4.2. Objetivos Específicos

- Elaborar el plan de investigación de campo o programa de auditoría.
- Determinar los instrumentos para la investigación de campo o programa de auditoría.
- Recopilar información detalla de la situación actual del sistema de información de la Corporación HOLDINGDINE S.A. (Matriz).
- Realizar el análisis de la información.
- Determinar los niveles de madurez.
- Verificar las observaciones.
- Elaborar el informe detallado.
- Validar el informe detallado.
- Elaborar y entregar el informe final/ejecutivo.

1.5. Alcance

El proyecto de tesis consiste en una Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), localizada en la Av. Coruña E25-58 y San Ignacio, Edificio Altana Plaza, 6to y 7mo piso, en la ciudad de Quito.

Se hará uso de una matriz de riesgo, esta herramienta de control y de gestión se utilizará para identificar los riesgos más críticos de los procesos y actividades de la Corporación. Igualmente, la matriz de riesgo permitirá evaluar la efectividad de una adecuada gestión y administración de los riesgos que pudieran impactar los resultados y por ende al logro de los objetivos organizacionales.

Se utilizará el Estándar Internacional Objetivos de Control para la Información y Tecnologías relacionadas (COBIT), como un medio de control de TI, basado en criterios de negocios, documentado por objetivos de control, organizado en dominios, procesos y actividades TI. Provee 32 objetivos de control agrupados en cuatro dominios:

- Planificación y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Monitoreo y Evaluación.

1.6. Modelo de Aplicación

COBIT (Objetivos de Control para la Información y Tecnologías relacionadas) es un estándar generalmente aceptado para buenas prácticas en seguridad tecnológica, en administración y control de la tecnología de la información; COBIT tiene su base en los objetivos de control de ISACF, actualmente conocida como ISACA (Asociación para el Control y Auditoría de Sistemas de la Información), que han sido mejorados de acuerdo a los actuales estándares internacionales profesionales y específicos a la industria, este modelo de referencia tiene la facilidad de adaptarse a cualquier tipo de negocio y los objetivos de control que se han definido, pueden ser aplicados independientemente del ambiente, plataformas y madurez tecnológica de la organización.

COBIT, es una herramienta desarrollada para ayudar a los administradores de negocios a entender y administrar los riesgos asociados con la implementación de nuevas tecnologías y demostrar a las entidades reguladoras e inversionistas, que tan efectiva es su tarea.

Se ha definido a COBIT como: "una estructura de relaciones y procesos para direccionar y controlar la organización para lograr la consecución de los objetivos del negocio, entregando valor agregado mientras se administra el riesgo en función del ambiente de sistemas y sus procesos".

CAPÍTULO 2

MARCO TEÓRICO

2.1. Sistemas de Información

Antes de entrar a una definición concreta de lo que es un sistema de información, es necesario conocer conceptos básicos como:

- **Sistema:** Es un conjunto de partes o elementos organizados y relacionados que interactúan entre sí para lograr un objetivo. Los sistemas reciben (entrada) datos, energía o materia del ambiente y proveen (salida) información, energía o materia. Un sistema puede ser físico o concreto (una computadora, un televisor, un humano) o puede ser abstracto o conceptual (un software). Cada sistema existe dentro de otro más grande, por lo tanto un sistema puede estar formado por subsistemas y partes, y a la vez puede ser parte de un supersistema[1][1]. Aunque existe una gran variedad de sistemas, la mayoría de ellos pueden representarse a través de un modelo formado por cinco bloques básicos: elementos de entrada, elementos de salida, sección de transformación, mecanismos de control y objetivos, tal y como muestra en la figura 2.1.

[1] Definición de Sistema: http://www.alegsa.com.ar/Dic/sistema.php

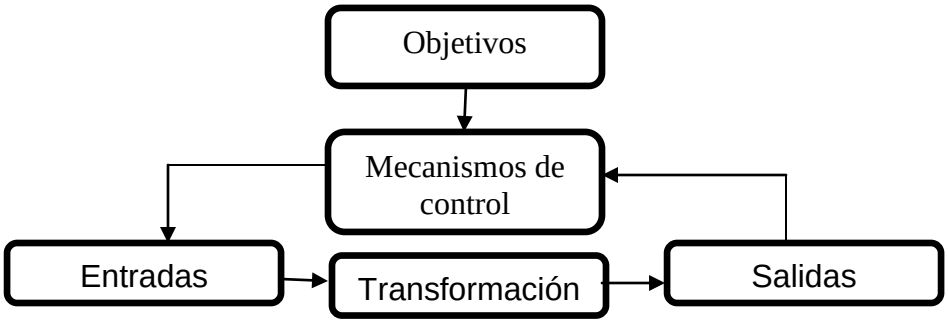


Figura 2.1. Modelo General de un Sistema.

Los recursos acceden al sistema a través de los elementos de entrada para ser modificados en la sección de transformación, este proceso es controlado por el mecanismo de control con el fin de lograr el objetivo marcado. Una vez se ha llevado a cabo la transformación, el resultado sale del sistema a través de los elementos de salida.

- **Información:** "Es un conjunto de datos con un significado, que reduce la incertidumbre o que aumenta el conocimiento de algo. En verdad, la información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a nuestras decisiones" (Idalberto Chiavenato)[2][2]. Para Ferrell y Hirt, la información "comprende los datos y conocimientos que se usan en la toma de decisiones" [3][3].

[2] Chiavenato Idalberto (2006). Introducción a la Teoría General de la Administración. Séptima Edición. McGraw-Hill Interamericana. Pág. 110.
[3] Ferrell O. C. y Hirt Geoffrey (2004). Introducción a los Negocios en un Mundo Cambiante. Cuarta Edición. McGraw-Hill Interamericana. Pág. 121.

Según Czinkota y Kotabe la información "consiste en datos seleccionados y ordenados con un propósito específico"[4][4]. En Wikipedia, la enciclopedia libre, en un sentido general información es "un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno"[5][5]. Teniendo en cuenta las anteriores ideas y definiciones, se puede decir que la información es un conjunto de datos acerca de algún suceso, hecho o fenómeno, que organizados en un contexto determinado tienen su significado, cuyo propósito puede ser el de reducir la incertidumbre o incrementar el conocimiento acerca de algo. Para la informática, la información es el conjunto de datos organizados y procesados que constituyen mensajes, instrucciones, operaciones, funciones y cualquier tipo de actividad que tenga lugar en relación con un ordenador.

En la actualidad, la expresión sistema de información se utiliza de forma común y habitual en las organizaciones; sin embargo, existen tantas definiciones y matices para ella como escuelas o autores del tema. Kenneth C. Laudon y Jane P. Laudon, definen los sistemas de información como "un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar la toma de decisiones y el control de una organización. Además de apoyar la toma de decisiones, la coordinación y el control, los sistemas de información también pueden ayudar a los gerentes y trabajadores a analizar problemas, a visualizar asuntos complejos y a crear productos nuevos"[6][6].

[4] Czinkota Michael y Kotabe Masaaki (2001). Administración de Mercadotecnia. Segunda Edición. International Thompson Editores. Pág. 115.
[5] Definición de Sistema de Información: http://www.alegsa.com.ar/Dic/sistema.php
[6] Kenneth C. Laudon y Jane P. Laudon (2004). Sistemas de Información Gerencial. Octava Edición. Pearson.

Alejandro Peña Ayala dice que "un sistema de información es un conjunto de elementos interrelacionados con el propósito de prestar atención a las demandas de información de una organización, para elevar el nivel de conocimientos que permitan un mejor apoyo a la toma de decisiones y desarrollo de acciones"[7][7].

De una manera más acertada se puede definir sistema de información como un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio, teniendo muy en cuenta el equipo computacional necesario para que pueda operar y el recurso humano, el cual debe estar formado por personal capacitado.

2.1.1. Actividades de los Sistemas de Información

Entre las actividades básicas de un SI[8][8], podemos tener:

- **Entrada de Información:** Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información, las entradas pueden ser manuales o automáticas.

  Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos, esto último se denomina interfaces automáticas[9][9].

[7] Ingeniería de Software: Una Guía para Crear Sistemas de Información (2006). Primera Edición. Instituto Politécnico Nacional México.
[8] SI: Sistema de Información.
[9] Entrada de Información: http://www.mitecnologico.com/Main/ElementosDeSistemaDeInformacion

- **Almacenamiento de Información:** El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM)[10][10].

- **Procesamiento de Información:** Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados[11][11].

- **Salida de Información:** La salida es la capacidad de un Sistema de Información para sacar la información procesada. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo[12][12]. (Figura 2.2.)

[10] Almacenamiento de Información: http://www.monografias.com/trabajos7/sisinf/sisinf.shtml
[11] Procesamiento de Información: http://www.mitecnologico.com/Main/ElementosDeSistemaDeInformacion
[12] Salida de Información: http://www.monografias.com/trabajos7/sisinf/sisinf.shtml

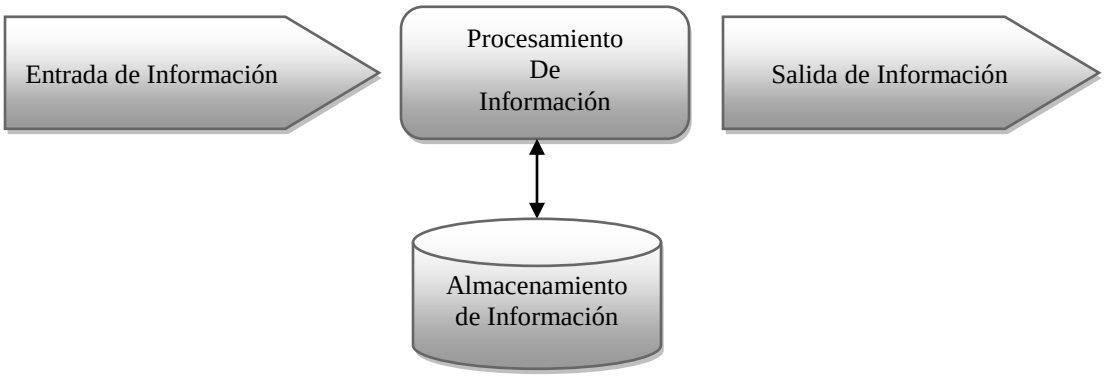


Figura 2.2. Actividades de un Sistema de Información.

2.1.2. Importancia de los Sistemas de Información

En la actualidad muchas organizaciones tienen éxito en sus objetivos por la implantación y uso de los Sistemas de Información. Muchas veces, las organizaciones no han entrado en la etapa de cambio hacía la era de la información, sin saber que es un riesgo muy grande de fracaso debido a las amenazas del mercado y su incapacidad de competir.

Así la función de los SI representa un área funcional dentro de las organizaciones que es tan importante para el éxito empresarial ,como para, las funciones de contabilidad, finanzas, administración, marketing, recursos humanos, entre otros. SI se consideran una colaboración significativa para le eficiencia operacional, la productividad y la moral del empleado, y el servicio y satisfacción del cliente. También es una fuente de información y respaldo importante para la toma de decisiones efectivas, por parte de los gerentes, como un ingrediente indispensable para el desarrollo de productos y servicios competitivos que den a las organizaciones una ventaja estratégica en el mercado global[13][13].

[13] Importancia de los Sistemas de Información: http://www.gestiopolis.com/Canales4/mkt/simparalas.htm

2.1.3. Sistemas de Información en las Organizaciones

Trabajadores de todos los niveles, clase de compañías e industrias utilizan en la actualidad Sistemas de Información para acrecentar su efectividad. Son muy pocos los empleados que no hacen uso de una computadora personal al menos una vez a la semana, si no es que a diario, para tener acceso a una red, elaborar expedientes, redactar un memorándum o crear una hoja de cálculo para efectos de análisis.

En el nivel corporativo, los tipos de Sistemas de Información de uso más común en las organizaciones son los sistemas de procesamiento de transacciones y comercio electrónico, de información administrativa, los sistemas de apoyo para la toma de decisiones y los sistemas expertos; en conjunto, auxilian a los empleados de las organizaciones en la ejecución de tareas tanto rutinarias como especiales, desde un registro de ventas hasta el procesamiento de la nómina; el apoyo para la toma de decisiones de varios departamentos y la propuesta de alternativas a proyectos y oportunidades de gran escala[14][14].

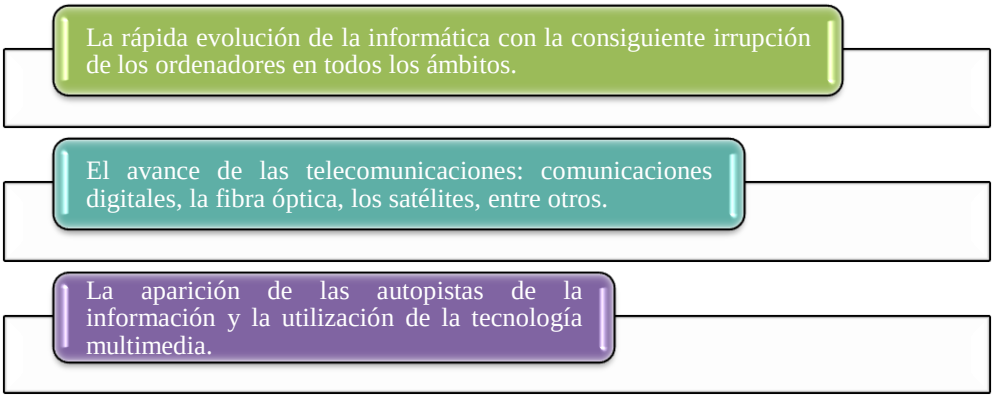
2.2. Tecnologías de la Información y la Comunicación

Se denominan Tecnologías de la Información y la Comunicación (TIC) al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de información[15][15].

[14] Ralph M. Stair y George W. Reynolds (1999). Sistemas de Información: Enfoque Administrativo. Cuarta Edición. International Thompson Editores.
[15] Tecnologías de la Información y la Comunicación: http://www.cibersociedad.net/archivo/articulo.php?art=218

Las TIC son todos aquellos medios electrónicos que almacenan, recuperan y transmiten información en grandes cantidades y a gran velocidad, incluyen a la informática, a la microelectrónica y a las telecomunicaciones. En la actualidad se está viviendo una revolución tecnológica y las Tecnologías de la Información están presentes en cualquier acción habitual por sencilla que sea. Ésta espectacular expansión de las nuevas TI se asienta en tres pilares que se observa en el cuadro 2.1. [16][16]

Cuadro 2.1. Pilares TI.



2.2.1. La Tecnología de la Información Hoy

Hoy, la Tecnología de la Información se ha expandido para abarcar muchos aspectos de computadora y de la tecnología, y el término es más reconocible que antes. El paraguas de la tecnología de información puede ser absolutamente grande, cubriendo muchos campos.

[16] Tecnologías de la Información y la Comunicación : http://iescapdellevant.org/departaments/tecno/1rbtx/tic/temas_iniciales/1_Introduccion_TIC.pdf

Los profesionales realizan una variedad de deberes que se extienden desde instalar, a diseñar redes de ordenadores y bases de datos complejas de información. Algunos de los deberes que los profesionales realizan pueden incluir:

- Gerencia de datos y/o de sistemas.
- Establecimiento de una red de la computadora.
- Diseño de los sistemas de la base de datos y de software.
- Sistemas de información de gerencia[17][17].

2.2.2. Características de las TIC

- **Inmaterialidad:** Con la posibilidad de digitalizar, las TIC convierten la información, tradicionalmente sujeta a un medio físico, en inmaterial. Mediante la digitalización es posible almacenar grandes cantidades de información en dispositivos físicos de pequeño tamaño (discos, CD, memorias USB, etc.). Esta característica, ha venido a definir lo que se ha denominado como "realidad virtual", esto es, realidad no real.
- **Instantaneidad:** Podemos transmitir la información instantáneamente a lugares muy alejados físicamente, mediante las denominadas "autopistas de la información".
- **Aplicaciones Multimedia:** Desarrollados para facilitar el acceso a las TIC, una de las características más importantes de estos entornos es la interactividad, la cual proporciona una comunicación bidireccional.[18][18].

[17] La tecnología de la Información Hoy: http://es.wikipedia.org/wiki/Tecnolog%C3%ADa_de_la_informaci%C3%B3n

[18] Características de las Tecnologías de la Información y la Comunicación: http://www.cibersociedad.net/archivo/articulo.php?art=218

2.2.3. Importancia de las TIC

Las TIC optimizan el manejo de la información y el desarrollo de la comunicación, permiten actuar sobre la información y generar mayor conocimiento e inteligencia. Están en todas partes y modifican los ámbitos de la experiencia cotidiana: el trabajo, las modalidades para comprar y vender, los trámites, el aprendizaje, entre otros.

El comercio electrónico, que tiene que ver con el intercambio de bienes y servicios realizado gracias a un soporte de protocolos y plataformas digitales estandarizadas, permite llegar a acuerdos sin tener que estar presente, un gran ahorro en dinero y tiempo. También se constituye en una herramienta que permite el acceso a información sobre precios, oferta y demanda, para que compradores y productores obtengan los mejores precios[19][19].

Las Tecnologías de la Información y la Comunicación (TIC) han revolucionado las relaciones de la empresa con su entorno, ya sea por obligación, por devoción o por ambos motivos, lo cierto es que cada vez hay más empresas que asoman la cabeza en este complicado mundo, que a veces, a quien carece de cualquier conocimiento sobre la materia, le puede parecer más árido de lo que en realidad es. Además, estas tecnologías pueden llegar a cualquier empresa sin importar su actividad o tamaño. No hay una solución universal para todas las empresas y cada una debe estudiar la situación en función de sus propios objetivos y buscar la mejor solución o herramienta que le permita llevar a cabo con éxito su plan de negocio[20][20].

[19] Importancia de las TIC: http://consuelomblog.blogspot.com/2007/04/qu-son-las-tics.html
[20] Importancia de las TIC: http://www.measurecontrol.com/la-importancia-de-las-tic/

2.2.4. TIC como herramienta de Gestión Empresarial

Las TIC agregan valor a las actividades operacionales y de gestión empresarial en general y permite a las empresas obtener ventajas competitivas, permanecer en el mercado y centrarse en su negocio. La instrumentación tecnológica es una prioridad en la comunicación de hoy en día, este importante cambio tecnológico marcan la diferencia entre una civilización desarrollada y otra en vías de. Es imposible hoy día ignorar el potencial de las TIC y especialmente del Internet[21][21].

La introducción de las TIC ha provocado cambios importantes en la organización, tanto interna como externa. El cambio más significativo es la capacidad de la empresa para interconectar los departamentos y cada uno de los trabajadores (y así poder compartir información, coordinar actividades, realizar operaciones en tiempo real), para trabajar en red con otras empresas.

Las TIC facilitan la descentralización del trabajo y la coordinación de tareas en una red interactiva de comunicación en tiempo real, ya sea entre continentes o entre plantas de un mismo edificio. La tecnología también contribuye a aumentar la competencia, ya que condensa el tiempo y el espacio. Las TIC contribuyen a aumentar la eficacia de las empresas, ya que ayudan a llevar un control más ajustado de los inventarios y de la entrega de los productos. Las entradas y salidas justo a tiempo han reducido enormemente los costes de intereses[22][22].

[21] TIC como herramienta de Gestión Empresarial: http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html
[22] TIC como herramienta de Gestión Empresarial: http://www.masterdopina.es/?p=141

2.2.5. Plan TIC dentro de las Organizaciones

Toda organización debe considerar un plan TIC que actúe en cada uno de los siguientes aspectos:

- **Dirigir:** Alineamiento con los objetivos del negocio para poder construir los mecanismos necesarios para entregar valor.
- **Crear:** Retorno del valor de la inversión realizada por TIC.
- **Proteger:** Gestión de riesgos para preservar el valor de los activos.
- **Actuar:** Gestión de recursos y desarrollo del plan TIC.
- **Monitorizar:** Evaluación de la ejecución y desempeño del plan establecido para realinear el gobierno de las TIC con el del negocio si es necesario.

La gerencia y los altos ejecutivos, han de ser conscientes del impacto de las TIC en la organización, ser capaces de conocer su rendimiento (retorno de valor/coste) y estar preparados para comprender y gestionar los riesgos inherentes a su utilización.

Mientras aquellas organizaciones cuyos directivos no comprenden, ni se preparan para los nuevos tiempos, estarán poniendo en peligro su capacidad de adaptación y, por consiguiente, estarán corriendo un riesgo de extinción muy elevado[23][23].

[23] Plan TIC dentro de las Organizaciones: http://www.tecnobiz.com/el-papel-de-las-tic-en-las-empresas

2.2.6. Ventajas de las TIC dentro de las Organizaciones

Las TIC son esenciales para mejorar la productividad de las empresas, la calidad, el control y facilitar la comunicación entre otros beneficios, aunque su aplicación debe llevarse a cabo de forma inteligente. El hecho de introducir tecnología en los procesos empresariales no es garantía de gozar de sus ventajas.

Para que la implantación de nueva tecnología produzca efectos positivos hay que cumplir varios requisitos: tener un conocimiento profundo de los procesos de la empresa, planificar detalladamente las necesidades de tecnología de la información e incorporar los sistemas tecnológicos paulatinamente, empezando por los más básicos.

Se ha investigado por qué fracasan algunos proyectos de implantación de TIC y se ha descubierto que el 90% de las veces el fracaso no es debido al software ni a los sistemas, sino al hecho de que la gente no tiene suficientes conocimientos sobre su propia empresa o sus procesos empresariales.

Entre las ventajas más importantes que se pueden mencionar con la implementación de las TIC son las siguientes:

- Apoyar a las PYMES[24][24] y a los empresarios locales para presentar y vender sus productos a través de Internet.
- Permitir el aprendizaje interactivo y la educación a distancia para los empleados.
- Impartir nuevos conocimientos para la empleabilidad que requieren muchas competencias (integración, trabajo en equipo, motivación, disciplina, etc.).

[24] PYMES: pequeñas y medianas empresas.

- Ofrecer nuevas formas de trabajo y de inclusión laboral, como teletrabajo.
- Dar acceso al flujo de conocimientos e información para empoderar y mejorar las vidas de las personas, facilidades, exactitud, menores riesgos, menores costos, etc.[25][25].

2.2.7. Estrategias Competitivas gracias a las TIC

Con frecuencia, el uso de las TIC para la globalización y la reingeniería de procesos empresariales da como resultado el desarrollo de sistemas de información que ayudan a una empresa a darle ventaja competitiva en el mercado, utilizándolos para desarrollar productos, servicios, procesos y capacidades que dan a una empresa una ventaja estratégica sobre las fuerzas competitivas que enfrenta[26][26].

Estrategias de diferenciación, como desarrollar maneras de utilizar las TIC para diferenciar productos o servicios de una empresa, de manera que los clientes perciban los productos o servicios como poseedores de atributos o beneficios únicos, por ejemplo, suministrar servicios rápidos y completos de soporte al cliente por medio de un sitio Web en Internet, o utilizar sistemas de marketing como objetivo para ofrecer a clientes individuales los productos y servicios que le atraen.

[25] Ventajas de las TIC dentro de las Organizaciones: http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html
[26] Estrategias Competitivas con gracias a las TIC: http://www.gestiopolis.com/Canales4/mkt/simparalas.htm

2.2.8. Gestión y Control de las TIC

La principal pregunta en toda organización es: ¿Cómo mejorar la gestión y el control de las TIC?; para ello es necesario que las organizaciones puedan disponer de:

- Una función de Auditoría Informática independiente.
- Una utilización correcta de la informática en la práctica de los distintos tipos de auditoría.
- La definición de unos objetivos de control de las TIC[27][27].

De esa manera el alcance en la Gestión y Control de las TIC, estará presente en:

- Monitoreo, gestión o administración de toda la plataforma de informática y/o de Telecomunicaciones.
- Administración total de usuarios en cualquier sistema y subsistema (directorio de servicios, mensajería, Intranet, etc.).

- Monitoreo, gestión o administración de la infraestructura de la red (enrutadores, switches, puntos de acceso inalámbrico, enlaces de última milla, conmutadores ATM[28][28], MPLS[29][29], Infraestructura telefónica entre otros).
- Operación y auditoría de copias de respaldo.
- Monitoreo de servicios de Internet (http, smtp, ftp).
- Gestión del rendimiento de aplicaciones.
- Administración de inventarios de Hardware y Software.
- Gestión Interna por incidentes[30][30].

[27] Gestión y Control de las TIC: http://www.eici.ucm.cl/Academicos/ygomez/descargas/Aud_Seg.../auditoria2.ppt
[28] ATM: Modo de Transferencia Asíncrona.
[29] MPLS: Multiprotocol Label Switching.

2.3. Introducción a la Auditoría Informática

2.3.1. Concepto de Auditoría

Existe una gran distorsión sobre la conceptualización de la Auditoría, en razón de que muchas veces el ejercicio de la misma se ha ceñido al modelo tradicional, por lo cual se hace necesario construir un concepto universal.

William Thomas Portero y John C. Burton definen la Auditoría como "el examen de la información por una tercera persona distinta de quien la preparó y del usuario, con la intención de establecer su veracidad; y el dar a conocer los resultados de este examen, con la finalidad de aumentar la utilidad de tal información para el usuario"[31][31]. Arthur W. Holmes obtiene como conclusión en su concepto moderno que la Auditoría es "el examen crítico y sistemático de la actuación y los documentos financieros y jurídicos en que se refleja, con la finalidad de averiguar la exactitud, integridad y autenticidad de los mismos"[32][32]. American Accounting Association define: "La Auditoría es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados. El fin del proceso consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como determinar si dichos informes se han elaborado observando principios establecidos para el caso"[33][33].

---

[30] Gestión y Control de las TIC: http://www.compuredes.com.co/gestionTICs.htm
[31] Concepto de Auditoría: http://members.tripod.com/~Guillermo_Cuellar_M/uno.html
[32] Arthur W. Holmes (2008). Auditoría: principios y procedimiento. Novena Edición. UTEHA
[33] Concepto de Auditoría: http://aaahq.org/

De las definiciones transcritas se puede definir que la Auditoría implica una reconstrucción de acontecimientos económicos del pasado para determinar su apego a la realidad y darles o no validez. Para lograr este cometido se requiere entonces recurrir en gran medida a la interpretación de los documentos escritos, por lo que, se puede afirmar que la Auditoría implica una "búsqueda de la verdad" de los hechos económicos producidos por una organización, los cuales afectan sus sistemas de información para darles autenticidad[34][34].

2.3.1.1. Clasificación de la Auditoría

2.3.1.1.1. Auditoría Interna

La estructura organizativa es la base sobre la cual una empresa planifica, ejecuta y controla actividades que contribuyen al logro de sus metas y objetivos, es así como la Auditoría Interna pretende realizar un examen completo y constructivo de la estructura organizativa de una organización y de sus métodos de operación, y velar por el empleo que se da a sus recursos humanos y materiales[35][35].

También considerado como un proceso cuya responsabilidad parte de la Alta Gerencia de las compañías, y se encuentra diseñado para proporcionar una seguridad razonable sobre el logro de los objetivos de la organización. Estos objetivos han sido clasificados en:

[34] Concepto de Auditoría: http://members.tripod.com/~Guillermo_Cuellar_M/uno.html
[35] Auditoría Interna: http://www.proyectosfindecarrera.com/auditoria-interna-externa.htm

- Establecimiento de estrategias para toda la empresa.
- Efectividad y eficiencia de las operaciones.
- Cumplimiento con las leyes, reglamentos, normas y políticas[36][36].

2.3.1.1.2. Auditoría Externa

La Auditoría Externa se puede definir como los métodos empleados por una firma externa de profesionales para averiguar la exactitud del contenido de los estados financieros presentados por una empresa[37][37].

Aplicando el concepto general, se puede decir que la Auditoría Externa es el examen crítico, sistemático y detallado de un sistema de información de una unidad económica, realizado por un Contador Público sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento. Una Auditoría Externa debe hacerla una persona o firma independiente de capacidad profesional reconocidas, esta persona o firma debe ser capaz de ofrecer una opinión imparcial y profesionalmente experta a cerca de los resultados de auditoría, basándose en el hecho de que su opinión ha de acompañar el informe presentado al término del examen y concediendo que pueda expresarse una opinión basada en la veracidad de los documentos y de los estados financieros y en que no se imponga restricciones al auditor en su trabajo de investigación[38][38].

[36] Auditoría Interna: http://www.deloitte.com/view/es_PE/pe/servicios/enterprise-risk-services/auditoria-interna/index.htm
[37] Auditoría Externa: http://www.soloeconomia.com/presupuesto/externa-auditoria.html
[38] Auditoría Externa: http://www.gerencie.com/auditoria-externa.html

2.3.2. Concepto de Auditoría Informática

Es el proceso de recoger, agrupar y evaluar evidencias para determinar si los sistemas de la organización trabajan adecuadamente en base a los parámetros, previamente establecidos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos[39][39].

José Antonio Echenique conceptualiza así la Auditoría Informática: "Es la revisión y evaluación de los controles, sistemas, procedimientos de informática, de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para la adecuada toma de decisiones"[40][40].

Dicho en otras palabras, la Auditoría Informática es un examen que se realiza a los sistemas de información, con el fin, de evaluar la eficacia y eficiencia de los mismos. Esta se lleva a cabo en base a diferentes, técnicas, procedimientos y herramientas, que son de gran apoyo para, analizar, evaluar , verificar y recomendar posibles mejoras, trayendo consigo seguridad y un trabajo informático de calidad en la empresa.

[39] Concepto de Auditoría Informática: http://culturaempresarialparatodos.blogspot.com/2009/02/62-auditoria-informatica.html
[40] José Antonio Echenique (2001).Auditoría en Informática. Segunda Edición. McGraw Hill.

2.3.2.1. Tipos de Auditoría Informática

- **Auditoría de Explotación:** Para realizar la Explotación Informática se dispone de los datos como materia prima, los cuales es necesario transformar, y que se someten previamente a controles de integridad y calidad. La transformación se realiza por medio de un proceso informático, el cual está dirigido por programas, una vez obtenido el producto final, los resultados son sometidos a controles de calidad, y finalmente son distribuidos al cliente y/o usuario. Se analiza cómo se prepara, se lanza y se sigue la producción diaria de los procesos Batch[41][41], o en tiempo real (Teleproceso)[42][42].
- **Auditoría de la Seguridad Física:** Se refiere a la protección de hardware y los soportes de datos, así también como la seguridad de los edificios y las instalaciones que lo albergan. Esto contempla situaciones de incendios, inundaciones, sabotajes, robos, catástrofes naturales, etc.[43][43].
- **Auditoría Ofimática:** Sistema informatizado que genera, procesa, almacena, recupera, comunica y presenta datos relacionados con el funcionamiento de la oficina, como por ejemplo, aplicaciones específicas a la gestión de tareas como hojas de cálculo o procesadores de texto, herramientas para la gestión de documentos, almacenamiento óptico de información, agendas y bases de datos personales.[44][44].

[41] Procesos Batch: Llevar a cabo una operación particular de forma automática en un grupo de archivos todos de una vez, en lugar de "manualmente" abrir, editar y guardar cada archivo por vez.
[42] Auditoría de Explotación: http://es.scribd.com/doc/18646089/TIPOS-Y-CLASES-DE-AUDITORIAS-INFORMATICAS
[43] Auditoría de la Seguridad Física: http://auditoria3.obolog.com/auditoria-seguridad-fisica-876557
[44] Auditoría Ofimática: http://www.ganimides.ucm.cl

- **Auditoría de Gestión:** El objetivo primordial de la auditoría de gestión consiste en descubrir deficiencias o irregularidades en algunas de las partes de la empresa y apuntar sus probables correcciones. La finalidad es ayudar a la dirección a lograr la administración más eficaz. Su intención es examinar y valorar los métodos y desempeño en todas las áreas[45][45].
- **Auditoría de Mantenimiento del Software:** Podemos decir que la mantenibilidad es un factor determinante para la auditoría informática del mantenimiento del software, es frecuente que las organizaciones busquen la máxima productividad en el desarrollo de sus productos, dejando en un segundo lugar a la etapa de mantenimiento. Si la productividad en la etapa del mantenimiento es baja, puede suceder que el equipo humano que desarrolle el producto tenga que dedicarse a tiempo completo a su mantenimiento. Por otro lado se requiere una labor de formación del nuevo equipo hasta adquirir el conocimiento necesario sobre los métodos y herramientas utilizadas por parte de área de desarrollo de software de las organizaciones[46][46].
- **Auditoría de Base de Datos:** Es el control y registro de una selección de las acciones del usuario de base de datos. Puede ser sobre la base de acciones individuales, tales como el tipo de sentencia SQL ejecutada, o en combinaciones de factores que pueden incluir el nombre de usuario, la aplicación, el tiempo, y así sucesivamente[47][47].

[45] Auditoría de Gestión: http://members.tripod.com/~Guillermo_Cuellar_M/gestion.html
[46] Auditoría de Mantenimiento del Software: http://www.innovavirtual.org
[47] Auditoría de Base de Datos: http://translate.google.com.ec/translate?hl=es&langpair=en|es&u=http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/auditing.htm

- **Auditoría de Sistemas:** Es la verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia, esta actividad está dirigida a verificar y juzgar la información[48][48].
- **Auditoría de Calidad:** La norma ISO 9000: 2000 define una Auditoría de Calidad como un proceso sistemático, independiente y documentado para obtener evidencias y evaluarlas de manera objetiva con el fin de determinar el alcance al que se cumplen los criterios de auditoría[49][49].
- **Auditoría de Redes y Comunicaciones:** Como en otros casos, la auditoría de este sector requiere un equipo de especialistas, expertos simultáneamente en Comunicaciones y en Redes Locales (no hay que olvidarse que en entornos geográficos reducidos, algunas empresas optan por el uso interno de Redes Locales, diseñadas y cableadas con recursos propios). El auditor de Comunicaciones deberá indagar sobre los índices de utilización de las líneas contratadas con información abundante sobre tiempos de desuso. Deberá proveerse de la topología de la red de comunicaciones, actualizada, ya que la desactualización de esta documentación significaría una grave debilidad[50][50].
- **Auditoría de Aplicaciones:** Se audita aplicaciones en funcionamiento en cuanto al grado de cumplimiento de los objetivos para los que fueron creadas. Los principales objetivos de las aplicaciones son:

[48] Auditoría de Sistemas: http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/
[49] Auditoría de Calidad: http://informandodecalidad.wordpress.com/2008/04/09/definicion-de-auditoria-de-calidad/
[50] Auditoría de Redes y Comunicaciones: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

- Registro de las operaciones.
- Procesos de cálculo y edición.
- Almacenamiento de la información.
- Dar respuesta a consultas de usuarios.
- Generar informes de interés para la organización.

Se pueden presentar posibles amenazas como:

- Posibilidades de fallo:
  - Software.
  - Hardware.
  - Redes y telecomunicaciones.
- Confidencialidad e integridad.
  - Gran uso de internet en las aplicaciones[51][51].

- **Auditoría Jurídica de Entornos Informáticos:** El objeto de la Auditoría Jurídica es comprobar que la utilización de la Informática se ajusta a la legislación vigente. Es esencialmente importante para evitar posibles reclamaciones de cualquier clase contra el sujeto a auditar. La Auditoría Jurídica dentro de la Auditoría Informática es la revisión independiente del uso del material, de la información y de sus manipuladores desde la perspectiva de la normativa legal (civil, penal, laboral), efectuada por un jurista experto independiente con la finalidad de emitir un dictamen sobre su adecuación a la legalidad vigente[52][52].

[51] Auditoría de Aplicaciones: http://www.wiziq.com/tutorial/38314-auditoria-de-aplicaciones

[52] Auditoría Jurídica de Entornos Informáticos http://www.innovavirtual.org

2.3.3. Importancia de la Auditoría Informática

A pesar de ser una disciplina cuya práctica ha aumentado en nuestro país durante los últimos años, la Auditoría Informática, es importante en las organizaciones por las siguientes razones:

- Se pueden difundir y utilizar resultados o información errónea si la calidad de datos de entrada es inexacta o los mismos son manipulados, lo cual abre la posibilidad de que se provoque un efecto dominó y afecte seriamente las operaciones, toma de decisiones e imagen de la empresa.
- Las computadoras, servidores y los Centros de Procesamiento de Datos se han convertido en blancos apetecibles para fraudes, espionaje, delincuencia y terrorismo informático.
- La continuidad de las operaciones, la administración y organización de la empresa no deben descansar en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.
- Las bases de datos pueden ser propensas a atentados y accesos de usuarios no autorizados o intrusos.
- La vigencia de la Ley de Derecho de Autor, la piratería de software y el uso no autorizado de programas, con las implicaciones legales y respectivas sanciones que esto puede tener para la empresa.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- En el Departamento de Sistemas se observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.

- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- El uso inadecuado de la computadora para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor y el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos[53][53].

2.3.4. Alcance de la Auditoría Informática

El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la Auditoría Informática, se complementa con los objetivos de ésta. Ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas[54][54].

El alcance de la Auditoría expresa los límites de la misma. Debe existir un acuerdo muy preciso entre auditores y clientes sobre las funciones, los procesos y las organizaciones a auditar. A los efectos de acotar el trabajo, resulta muy beneficioso para ambas partes expresar las excepciones de alcance de la Auditoría, es decir cuales procesos, funciones u organizaciones no van a ser auditadas; tanto los alcances como las excepciones deben figurar al comienzo del Informe Final.

[53] Importancia de la Auditoría Informática: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml

[54] Alcance de la Auditoría Informática: http://www.123innovationgroup.info/index.htm

Las personas que realizan la Auditoría Informática han de conocer con la mayor exactitud posible los objetivos a los que su tarea debe llegar. Deben comprender los deseos y pretensiones del cliente, de forma que las metas fijadas puedan ser cumplidas.

Una vez definidos los objetivos (objetivos específicos), éstos se añadirán a los objetivos generales y comunes de a toda Auditoría Informática: La operatividad de los Sistemas y los Controles Generales de Gestión Informática[55][55].

2.4. Control Interno

Se entiende por Control Interno al sistema integrado por el esquema de organización y el conjunto de los planes, métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por una entidad, con el fin de procurar que todas las actividades, operaciones y actuaciones, así como la administración de la información y los recursos, se realicen de acuerdo con las normas constitucionales y legales vigentes dentro de las políticas trazadas por la dirección y en atención a las metas u objetivos previstos.

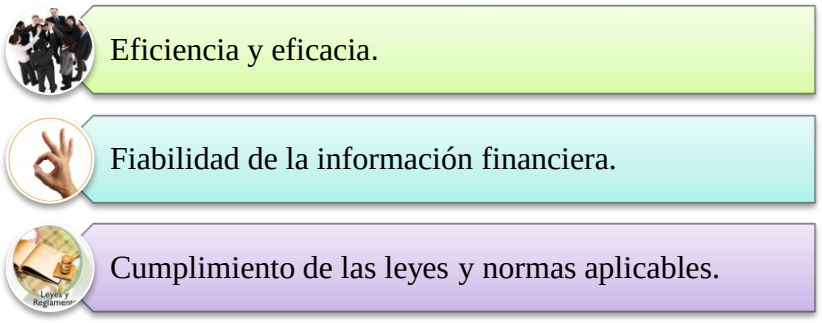
El ejercicio del Control Interno debe consultar los principios de igualdad, moralidad, eficiencia, economía, celeridad, imparcialidad, publicidad y valoración de costos ambientales. En consecuencia, deberá concebirse y organizarse de tal manera que su ejercicio sea intrínseco al desarrollo de las funciones de todos los cargos existentes en la entidad, y en particular de las asignadas a aquellos que tengan responsabilidad del mando.

[55] Alcance de la Auditoría Informática: http://archivosauditoria.blogspot.com/2009/11/alcance-y-objetivos-de-la-auditoria.html

El Control Interno se expresará a través de las políticas aprobadas por los niveles de dirección y administración de las respectivas entidades y se cumplirá en toda la escala de la estructura administrativa, mediante la elaboración y aplicación de técnicas de dirección, verificación y evaluación de regulaciones administrativas, de manuales de funciones y procedimientos, de sistemas de información y de programas de selección, inducción y capacitación de personal[56][56].

El Control Interno como proceso, es llevado a cabo por las personas de una organización, diseñado con el fin de proporcionar un grado de seguridad "razonable" para la consecución de sus objetivos, dentro de las siguientes categorías que se presentan en el cuadro 2.2. [57][57].

Cuadro 2.2. Control Interno.



[56]Control Interno: http://www.leticia-amazonas.gov.co/apc-aa-files/39613036666138353036316365656633/control.pdf
[57] Control Interno: http://www.mercadotendencias.com/informe-coso-definicion-de-control-interno/

2.4.1. Tipos de Controles Internos

- **Controles preventivos:** para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema.
- **Controles detectivos:** cuando fallan los preventivos para tratar de conocer cuanto antes el evento.
- **Controles correctivos:** facilitan la vuelta a la normalidad cuándo se han producido incidencias.

La Auditoría Informática debe ser respaldada por un proceso formal que asegure su previo entendimiento por cada uno de los responsables de llevar a la práctica dicho proceso en la organización[58][58].

2.4.2. Implantación de un Sistemas de Control Interno

La implementación de un Sistema de Control Interno implica que cada uno de sus componentes estén aplicados a cada categoría esencial de la organización, convirtiéndose en un proceso integrador y dinámico permanentemente, como paso previo cada entidad debe establecer los objetivos, políticas y estrategias relacionadas entre sí con el fin de garantizar el desarrollo organizacional y el cumplimiento de las metas corporativas.

[58] Tipos de Controles Internos: http://www.eumed.net/libros/2008a/351/Definicion%20y%20tipos%20de%20controles%20internos.htm

Aunque el Sistema de Control Interno debe ser intrínseco a la administración de la entidad y busca que esta sea más flexible y competitiva en el mercado, se producen ciertas limitaciones inherentes que impiden que el sistema como tal sea 100% confiable y donde cabe un pequeño porcentaje de incertidumbre, por esta razón se hace necesario un estudio adecuado de los riesgos internos y externos con el fin de que el control provea una seguridad razonable para la categoría a la cual fue diseñado.

Estos riesgos pueden ser atribuidos a fallas humanas como la toma de decisiones erróneas, simples equivocaciones o confabulaciones de varias personas, es por ello que es muy importante la contratación de personal con gran capacidad profesional, integridad y valores éticos, así como la correcta asignación de responsabilidades bien delimitadas donde se interrelacionan unas con otras con el fin de que no se rompa la cadena de control fortaleciendo el ambiente de aplicación del mismo.

La comprensión del Control Interno puede así ayudar a cualquier entidad pública o privada a obtener logros significativos en su desempeño con eficiencia, eficacia y economía, indicadores indispensables para el análisis, toma de decisiones y cumplimiento de metas. Aunque la tecnología y la información representan un gran factor para el desarrollo empresarial, existen muchas compañías en las cuales estos nuevos enfoques de control son desconocidos totalmente, lo que deja a la organización rezagada frente a la competitividad mundial que se exige permanentemente[59][59].

[59] Implantación de un Sistema de Control Interno: http://www.monografias.com/trabajos12/coso/coso.shtml

2.4.3. La Información como Recurso Crítico

Estudios realizados en diversas universidades revelan que en los sectores financieros, fabricación y distribución, una caída total del ordenador de tres o cuatro días puede dar lugar a la pérdida del negocio. Igualmente, la pérdida de confidencialidad en las bases de datos de investigación o en el plan estratégico, puede proporcionar a los competidores una ventaja definitiva.

Es por eso que no está de más que las organizaciones se formule preguntas como: ¿Están la Información y los Sistemas de Información suficientemente protegidos?, así la organización planteará un plan de recuperación de desastres y una protección de instalaciones físicas y control de acceso de la información. Con relación a los planes de recuperación de desastres, muchas organizaciones no desean describir su estado de preparación para estos casos, por otro lado, con relación a la protección de las instalaciones físicas y el control de acceso a los sistemas de información, hay pocas estadísticas disponibles sobre el uso del software de control de acceso en cuanto a sus políticas de utilización y calidad de su administración.

El valor de la información, algunas veces activo irremplazable y más valioso que muchos de los otros activos, puede solamente ser estimado indirectamente por el impacto que su pérdida, destrucción o distribución no autorizada puede tener sobre las organizaciones. La respuesta es que la información no se reconoce como un recurso crítico en los informes de las empresas[60][60].

[60] La información como Recurso Crítico: http://www.eici.ucm.cl/Academicos/ygomez/descargas/Aud_Seg.../auditoria2.ppt

2.4.3.1. Valor de la Información en las Organizaciones

El nuevo escenario socio-económico ha conllevado infinitos cambios, pero quizás el mayor se sitúa en la información y en los datos. El crecimiento de la información durante la última década ha sido exponencial y así seguirá siendo en el futuro.

Esto indica la obligatoriedad de disponer no ya de unos eficaces sistemas de almacenamiento, sino de establecer una estrategia concreta que marque pautas perfectamente definidas sobre la gestión de esa información. No se trata de almacenar, sino de gestionar, es algo crucial; no hay que olvidar que son muchos los valores que definen a una compañía, pero por encima de todos está la información.

La información, esto es algo asumido por todos, es el valor más preciado de cualquier organización, de su correcta gestión depende la viabilidad de la propia empresa u organización. Es verdad que la complejidad tecnológica es importante, pero también lo es el que la mayoría de empresas comprometidas con este segmento de almacenamiento son capaces de gestionar esa complejidad haciéndola prácticamente invisible para el usuario, y además, permitir la generación de eficiencias organizacionales.

Es lo que ya se define como almacenamiento inteligente, un concepto que articula la criticidad de los datos en base a una jerarquía concreta y específica según las necesidades de la organización[61][61].

[61] Valor de la Información en la Organizaciones:
http://www.idg.es/computerworld/El-valor-de-la-informacion/seccion-op/articulo-153382

2.5. Aplicación de la Auditoría Informática

2.5.1. Metodología de la Auditoría Informática

La metodología empleada en la Auditoría Informática es similar a las fases que componen una 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 las auditorías, con el fin de reportar las sugerencias correspondientes a las oportunidades de mejora encontradas y finalmente, se efectúa el seguimiento para evaluar el nivel del cumplimiento y el impacto de las recomendaciones hechas.

Para que las organizaciones puedan asegurar que construyen proyectos de tecnología de información que cubren de manera adecuada las necesidades del cliente en forma eficiente y oportuna, y dentro del presupuesto contemplado, existe una asociación internacional denominada Information Systems Audit and Control Association (ISACA), cuya misión es la de mejorar el reconocimiento de la profesión de auditoría y control de las TI mediante la elaboración de estándares y prácticas internacionales.

De igual forma, existe un 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 observa en la Figura 2.3.:

Figura 2.3. Dominios COBIT.

Se puede afirmar que el éxito de un organismo 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[62][62].

[62] Metodología de la Auditoría Informática: http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm

2.5.2. Justificación de la Auditoría Informática

Existen varias razones para justificar la implementación de una Auditoría Informática, como:

- La información es un recurso clave en la empresa para:
    - Planear el futuro, controlar el presente y evaluar el pasado.
- Las operaciones de la empresa dependen cada vez más de la sistematización.
- Los riesgos tienden a aumentar, debido a:
    - Pérdida de información.
    - Pérdida de activos.
    - Pérdida de servicios/ventas.
- La sistematización representa un costo significativo para la empresa en cuanto a: hardware, software y personal.
- Los problemas se identifican sólo al final.
- El permanente avance tecnológico.
- Aumento considerable e injustificado del presupuesto del PAD (Departamento de Procesamiento de Datos).
- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Falta total o parcial de seguridades lógicas y físicas que garanticen la integridad del personal, equipos e información.
- Descontento general de los usuarios por incumplimiento de plazos y mala calidad de los resultados[63][63].

[63] Justificativo de la Auditoría Informática: http://www.gestiopolis.com/finanzas-contaduria/auditoria-interna-de-la-informacion.htm

2.5.3. Normas de Auditoría

Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de este trabajo.

Las normas se pueden clasificar en:

- **Normas personales,** son cualidades que el auditor debe tener para ejercer sin fraude una auditoría, basados en un sus conocimientos profesionales así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.
- **Normas de ejecución del trabajo,** son la planificación de los métodos y procedimientos, tanto como papeles de trabajo a aplicar dentro de la auditoría.
- **Normas de información,** son el resultado que el auditor debe entregar a los interesados para que se den cuenta de su trabajo, también es conocido como informe o dictamen[64][64].

2.5.4. Técnicas y Herramientas de la Auditoría Informática

Se define a las Técnicas de Auditoría como los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio según las circunstancias. Al aplicar su conocimiento y experiencia, el auditor podrá conocer los datos de la empresa u organización a ser auditada que pudieran necesitar una mayor atención.

[64] Normas y Procedimientos de Auditoría. Instituto Mexicano de Contadores Públicos (IMCP).

Las técnicas o procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas así como los procedimientos de auditoría tienen una gran importancia para el auditor. Algunas técnicas efectivas cuando se va a implementar una Auditoría Informática, son:

- **Estudio General**, es la apreciación y juicio de las características generales de la empresa, las cuentas o las operaciones, a través de sus elementos más significativos para concluir se ha de profundizar en su estudio y en la forma que ha de hacerse.
- **Análisis**, es el estudio de los componentes de un todo para concluir con base en aquellos respecto de este. Esta técnica se aplica concretamente al estudio de las cuentas o rubros genéricos de los estados financieros.
- **Inspección**, es la verificación física de las cosas materiales en las que se tradujeron las operaciones, se aplica a las cuentas cuyos saldos tienen una representación material, (efectivos, mercancías, bienes, etc.).
- **Confirmación**, es la ratificación por parte de una persona ajena a la empresa, de la autenticidad de un saldo, hecho u operación, en la que participo y por la cual está en condiciones de informar válidamente sobre ella.
- **Investigación**, es la recopilación de información mediante pláticas con los funcionarios y empleados de la empresa.
- **Observación**, es una manera de inspección, menos formal, y se aplica generalmente a operaciones para verificar como se realiza en la práctica.

- **Entrevistas**, el auditor comienza a continuación las relaciones personales con el auditado. Lo hace de tres formas:
    - Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.
    - Mediante entrevistas en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.
    - Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

  La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.
- **Pruebas de Auditoría,** técnicas o procedimientos que utiliza el auditor para la obtención de evidencia comprobatoria, las pruebas pueden ser de tres tipos:
    - **Las pruebas de control,** están relacionadas con el grado de efectividad del control interno imperante.
    - **Las pruebas analíticas,** se utilizan haciendo comparaciones entre dos o más estados financieros o haciendo un análisis de las razones financieras de la entidad para observar su comportamiento.
    - **Las pruebas sustantivas,** son las que se aplican a cada cuenta en particular en busca de evidencias comprobatorias.

En sí, para poner en ejecución dichas técnicas todo auditor debe tener en cuenta y utilizar herramientas de apoyo como:

- **Cuestionarios,** es lo habitual comenzar solicitando la respuesta de cuestionarios pre impresos que se envían a las personas concretas que el auditor cree adecuadas, sin que sea obligatorio que dichas personas sean las responsables oficiales de las diversas áreas a auditar. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.
- **Checklist,** el auditor conversará y hará preguntas, que en realidad servirán para cumplir sistemáticamente con sus cuestionarios, de sus Checklist, estos deben ser contestados oralmente, ya que superan en riqueza y generalización a cualquier otra forma. Según la claridad de las preguntas y el talento del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable, por lo que hay que tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas. Los Checklist responden fundamentalmente a dos tipos de "filosofía" de calificación:
    - **Checklist de rango:** Contiene preguntas que el auditor debe puntuar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo).

      Son adecuados si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones.
    - **Checklist Binarios:** Es constituido por preguntas con respuestas única y excluyente: Si o No. Aritméticamente, equivalen a 1 (uno) o 0 (cero), respectivamente.

- **Software de Auditoría**, hasta hace ya algunos años se han utilizado productos software llamados genéricamente paquetes de auditoría, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático. Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación. En la actualidad, los productos Software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada. Estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación[65][65].

2.6. Fases de la Auditoría Informática

2.6.1. Evaluación de Sistemas de acuerdo al Riesgo

Se entiende como riesgo a la incertidumbre que ocurra un evento que podría tener un impacto en el logro de los objetivos. Los riesgos cuando se materializan, se denominan errores, irregularidades u omisiones, los cuales pueden generar una pérdida monetaria, en la imagen de la empresa o incumplimiento de normativa externa.

Riesgo = Impacto * Probabilidad

- **Impacto:** es el efecto o consecuencia cuando el riesgo se materializa
- **Probabilidad:** representa la posibilidad que un evento dado ocurra.

[65] Víctor Manuel Mendívil Escalante (2002). Elementos de Auditoría. Quinta Edición. Thomson Editores.

El riesgo inherente, son aquellos riesgos propios de la materia y/o componentes de ésta. Se entiende que una materia por su naturaleza tiene riesgos que surgen por diversas fuentes, como los errores, irregularidades o fallas que pudieran ser importantes en forma individual o en conjunto con otros riesgos.

Los riesgos inherentes a la materia pueden tener o no controles elaborados por la dirección para mitigar su probabilidad o su impacto. Los riesgos inherentes a la materia de bajo análisis pueden ser relativos al entorno, ambiente interno, procesos, información, etc. Algunos riesgos inherentes que se pueden dar dentro de la organización, son:

- Riesgo de Crédito.
- Riesgo Financiero.
- Riesgo Operacional.
- Riesgo de Tecnología de la Información.

2.6.1.1. Riesgo en la Integridad de la Información

Agrupa todos los riesgos asociados con la autorización, integridad, y exactitud de las transacciones según se ingresan, se procesan, se resumen y se informan en los sistemas computacionales de una organización, manifestándose en los siguientes componentes de un sistema:

- **Interfaz usuaria;** se refiere a si existen restricciones que hagan que los trabajadores de una organización estén autorizados a desarrollar funciones de negocio sobre necesidad del negocio y la necesidad de lograr una segregación de funciones razonable.

- **Procesamiento;** se relacionan a la existencia de controles que aseguran que el procesamiento de datos se ha completado y realizado a tiempo.
- **Administración del Cambio;** los riesgos en esta área pueden ser generalmente considerados parte del Riesgo de Infraestructura, pero ellos impactan significativamente sobre los sistemas de aplicación. Estos riesgos están asociados con procesos inadecuados de administración del cambio incluyendo tanto la participación y entrenamiento del usuario como el proceso por el cual los cambios de cualquier aspecto del sistema de aplicación son comunicados e implementados.
- **Error de Procesamiento;** se refiere a si existen procesos adecuados que aseguren que todas las excepciones de entrada y procesamiento de datos que se capturan, son corregidas y reprocesadas en forma precisa, íntegra y oportuna.
- **Datos;** se relacionan a la existencia de controles de administración de datos inadecuados que incluyen seguridad/integridad de los datos procesados.

La integridad se puede perder por errores en la programación, errores de procesamiento, errores de administración de sistemas.

2.6.1.2. Aspectos a considerar en la Gestión del Riesgo Informático

La gestión de riesgo debe considerar los siguientes aspectos:

- Identificación del Sistema o Proceso.
- Identificación de la Amenazas.
- Identificación de las Vulnerabilidades.
- Controles.

- Determinar la Probabilidad de ocurrencia.
- Análisis de Impacto.
- Determinación del Riesgo.
- Recomendación de Controles.
- Documentar los Resultados.

Desde el punto de vista de los servidores:

- Análisis de Vulnerabilidad de los servidores que darán el servicio.
- Antivirus instalado y actualizado en los servidores que darán el servicio.
- Parches de seguridad evaluados e instalados según corresponda en los servidores que darán el servicio.

Desde el punto de vista de la transferencia de información:

- Encriptación de la comunicación entre la organización y la empresa prestadora de servicios.

Desde el punto de la continuidad operacional:

- Servidores de respaldo.
- Máquinas especializadas de respaldo.
- Pruebas de contingencia[66][66].

[66] Mario Piattini & Emilio del Peso (2001). Auditoría Informática: Un enfoque práctico. Segunda Edición. Editorial RAMA.

2.6.2. Planeación de la Auditoría Informática

Para hacer una adecuada planeación de la Auditoría Informática hay que tener un profundo conocimiento y comprensión de la entidad a la que se aplicará la Auditoría Informática, de esta forma, permitirá dimensionar el tamaño y características del área dentro del organismo a auditar, sus sistemas, organización y equipo. Con ello podemos determinar el número y características del personal de auditoría, las herramientas necesarias, el tiempo y costo, así como definir los alcances de la auditoría para, en caso necesario, poder elaborar el contrato de servicios.

Dentro de la Auditoría Informática, la planeación es uno de los pasos más importantes, ya que una inadecuada planeación provocará una serie de problemas que pueden impedir que se cumpla con la auditoría o bien hacer que no se efectúe con el profesionalismo que debe tener cualquier auditor. El trabajo de auditoría debería incluir la planeación de la auditoría, el examen y la evaluación de la información, la comunicación de los resultados y el seguimiento. La planeación deberá ser documentada e incluirá:

- El establecimiento de los objetivos y el alcance del trabajo.
- La obtención de información de apoyo sobre las actividades que se auditarán.
- La determinación de los recursos necesarios para realizar la auditoría.
- El establecimiento de la comunicación necesaria con todos los que estarán involucrados en la auditoría.

- La realización, en la forma más apropiada, de una inspección física para familiarizarse con las actividades y controles a auditar, así como identificación de las aéreas en las que se deberá hacer énfasis al realizar la auditoría y promover comentarios y la promoción de los auditados.
- La preparación por escrito del plan de trabajo de la auditoría.
- La determinación de cómo, cuándo y a quién, se le comunicara los resultados de la auditoría.
- La obtención de la aprobación del plan de trabajo de la auditoría.
- Evaluación administrativa del área de procesos electrónicos.
- Evaluación de los sistemas y procedimientos.
- Evaluación de los equipos de cómputo.
- Evaluación del proceso de datos, de los sistemas y de los equipos de computo (software, hardware, redes, base de datos, comunicaciones).
- Seguridad y confidencialidad de la información.
- Aspectos legales de los sistemas y de la información.

Para lograr una adecuada planeación, lo primero que se requiere es obtener información general sobre la organización y sobre la función de la información a evaluar, para ello es preciso hacer una investigación preliminar y algunas entrevistas previas, con base en esto planear el programa de trabajado, el cual deberá incluir tiempos, costos, personal necesario y documentos auxiliares a solicitar o formular durante el desarrollo de la auditoría.

2.6.2.1. Conocimiento y Comprensión de la Organización

2.6.2.1.1. Recopilación de Información Organizacional

Una vez elaborada la planeación de la Auditoría Informática, la cual servirá como plan maestro de los tiempos, costos y prioridades, y como medio de control de la auditoría, se debe empezar la recolección de la información. Para ello se precederá a efectuar la revisión sistematizada del are, a través de los siguientes elementos:

- Revisión de la estructura orgánica:
    - Jerarquías (definición de la autoridad lineal, funcional y de asesoría).
    - Estructura orgánica.
    - Funciones.
    - Objetivos.
- Se deberá revisar la situación de los recursos humanos.
- Entrevistas con el persona de procesos electrónicos:
    - Jefatura.
    - Análisis.
    - Programadores.
    - Operadores.
    - Personal de base de datos.
    - Personal de comunicación y redes.
    - Personal de mantenimiento.
    - Personal administrativo.
    - Responsable de comunicaciones.

    - Responsable de internet e Intranet.
    - Responsable de redes locales o nacionales.
    - Responsable de sala de usuarios.
    - Responsable de capacitación.
- Se deberá conocer la situación en cuanto a:
    - Presupuesto.
    - Recursos financieros.
    - Recursos materiales.
    - Mobiliario y equipo.
    - Costos.
- Se hará un levantamiento del censo de recursos humanos y análisis de situación en cuanto a:
    - Número de personas y distribución por áreas.
    - Denominación de puestos y persona de confianza de base.
    - Capacitación.
    - Experiencia profesional.
- Por último, se deberá revisar el grado de cumplimiento de los documentos administrativos:
    - Organización.
    - Normas y políticas.
    - Controles.
    - Estándares.
    - Procedimientos.

La organización debe estar estructurada de tal forma que permita lograr eficiente y eficazmente los objetivos, y que esto se logre a través de una adecuada toma de decisiones. Una forma de evaluar la forma en que la gerencia de informática se está desempeñando es mediante la evaluación de las funciones que la alta gerencia debe realizar:

- **Planeación.** Determinar los objetivos del área y la forma en que se van a lograr estos objetivos.
- **Organización.** Proveer de las facilidades, estructura, división del trabajo, responsabilidades, actividades de grupo y personal necesario para realizar las metas.
- **Recursos humanos.** Seleccionando, capacitando y entrenando al personal requerido para realizar las metas.
- **Dirección.** Coordinando las actividades, proveyendo liderazgo y guía, y motivando al personal.
- **Control.** Comprando lo real contra lo planeado, como base para realizar los ajustes necesarios[67][67].

2.6.2.1.2. Evaluación del Talento Humano

Dentro de la Auditoría Informática es vital la evaluación de recursos humanos, ya que su propósito principal es mostrar cómo está funcionado el programa, localizando prácticas y condiciones que son perjudiciales para la empresa o que no están justificando su costo, o prácticas y condiciones que deben incrementarse. La evaluación es un sistema de revisión y control para informar a la administración sobre la eficiencia y la eficacia del programa que lleva a cabo.

[67] José Antonio Echenique (2001).Auditoría en Informática. Segunda Edición. McGraw Hill.

La evaluación del Talento Humano se encarga de planear, organizar y controlar las actividades relacionadas con la vida del personal en la empresa. La función de auditoría no es solo señalar las fallas y los problemas, sino también presentar sugerencias y soluciones[68][68].

2.6.2.1.3. Recursos Financieros y Herramientas para una Auditoría Informática

La elección de los recursos financieros ha de considerarse de forma global, no sólo consiste en determinar qué equipos físicos, programas o realizaciones cuestan más o menos, sino también abarca otros aspectos, además del económico, tales como: fiabilidad, velocidad de procesamiento, rentabilidad, etc.

Aspectos a tener en cuenta:

- Los métodos de control de gestión y contabilidad presupuestaria clásicos sirven para prever y posteriormente controlar la adecuación a los objetivos.
- La evolutividad implica un presupuesto no sólo flexible, sino modulado en el tiempo, ya que los costes son importantes.
- Los métodos clásicos de la contabilidad analítica permiten establecer los estándares de homogeneidad de los medios financieros.
- También es muy útil verificar periódicamente si los costes imputados son todavía competitivos con relación a un servicio exterior.
- Para elaborar un sistema equitativo sería preciso que dos servicios semejantes diera lugar a una misma valoración.

[68] Evaluación del Talento Humano: http://www.mitecnologico.com/Main/EvaluacionRecursosHumanos

- Los costos deben ser registrados de forma fiable, completa y pertinente, y los cálculos y agrupaciones efectuados deben ser legítimos. El trabajo del personal debe ser registrado o repartido según conceptos para que las cifras conserven algún sentido.
- La seguridad financiera se obtiene por una rentabilidad duradera de la financiación de hardware y el software.
- A la hora de la entrega de los equipos informáticos, el contrato debe recoger un plan y un informe de gastos que condujo a su elección. La garantía de fiabilidad material reside en una cláusula que fija el plazo de intervención, en caso de avería, y el grado de fiabilidad de los componentes.
- También puede contratarse un seguro para una garantía eficaz de los equipos.
- Tanto los contratos de adquisición y seguro como los documentos contables comprenden la documentación sobre los medios financieros[69][69].

2.6.2.2. Revisión preliminar de la Auditoría Informática

El objetivo de esta fase es revisar la aplicación de la Auditoría Informática para obtener información sobre cómo llevarla a cabo. Al finalizarla, el auditor puede proceder de tres maneras:

- No continuar con la auditoría, por ejemplo por problemas de independencia, si el auditor no tuviera capacidad técnica para realizar la auditoría y necesitara ayuda del propio auditado.

[69] Recursos Financieros y Herramientas para una Auditoría Informática: http://html.rincondelvago.com/auditoria-informatica_1.html

- Pasar a la fase de una revisión más detallada, para realizar la revisión de los controles internos, esperando poder confiar en ellos, y reducir los Test de Apoyo.
- Pasa directamente a la fase de pruebas de apoyo, si no se confía en los controles internos, puede ser menos costoso realizar directamente los Test de Apoyo. También puede ocurrir que los controles de Auditoría Informática sean iguales que los controles del usuario, en cuyo caso puede ser mejor revisar estos últimos.

2.6.2.3. Revisión detallada de la Auditoría Informática

El objetivo de esta fase es obtener información necesaria para tener un conocimiento detallado (profundo) de los controles utilizados en la aplicación de la auditoría.

Al finalizarla, el auditor puede tomar una de las siguientes decisiones:

- No continuar con la auditoría.
- Pasar a la fase de Pruebas de Comportamiento, esperando poder confiar en los controles internos.
- Pasar directamente a la fase de Pruebas de Apoyo.

En esta fase se revisan de nuevo los controles de Gerencia y de Aplicación, se identifican las causas de las perdidas y los controles para reducirlas y al final de la fase, se decide si estos controles reducen las causas de las perdidas a un nivel aceptable. Dado que aun no se sabe lo bien que funcionan dichos controles, se asume que lo harán bien, a menos que se tenga evidencias que demuestren lo contrario.

En esta fase pueden existir diferencias en el modo de conducir la auditoría, dependiendo de quien la esté realizando. En el caso de ser un auditor interno, este buscara causas que afecten principalmente a la eficiencia y a la efectividad del sistema, y tratara de que no se produzca un control excesivo del mismo, buscando el juego de controles mínimo necesario. Si se trata de un auditor externo, lo más probable es que busque controles para garantizar la salvaguarda de bienes y la integridad de los datos, principalmente.

2.6.2.4. Pruebas de Comportamiento

El objetivo de esta fase es comprobar que los controles internos funcionan como lo deben de hacer, es decir, que los controles que se suponía que existían, existen realmente y funcionan bien.

Las técnicas utilizadas, además de la recogida manual de evidencias ya descrita, contemplan el uso del ordenador para verificar los controles. Al final de la fase, el auditor puede decidir evaluar de nuevo el sistema de controles internos, de acuerdo con la fiabilidad que han mostrado los controles individuales. El procedimiento de evaluación y la elección de nuevos procedimientos de auditoría son los mismos que los de las fases anteriores.

2.6.2.5. Pruebas Controles de Usuario

El auditor puede decidir que no hace falta confiar en los controles internos porque existen controles del usuario que los sustituyen o compensan.

Para un auditor externo, revisar estos controles del usuario puede resultar más costoso que revisar los controles internos. Para un auditor interno, es importante hacerlo para eliminar posibles controles duplicados, bien internos o bien del usuario, para evitar la redundancia.

2.6.2.6. Pruebas de Apoyo

El objetivo de esta fase es obtener evidencias suficientes para tomar la decisión final sobre si pueden ocurrir o no pérdidas materiales durante el procesamiento de los datos.

Por ejemplo, un auditor externo podrá formarse una opinión sobre si existen o no discrepancias sobre el estado de cuentas de la empresa, mientras que un auditor interno deberá de tener una perspectiva más amplia y se cuestionara si se está de acuerdo o no con los controles internos, si han ocurrido perdidas o pueden ocurrir en el futuro, etc.

Se puede mencionar cinco tipos de pruebas de apoyo:

- Para identificar procesos erróneos.
- Para garantizar la calidad de los datos.
- Para identificar datos inconsistentes.
- Para comparar datos y cuentas físicas.
- De confirmación de datos con fuentes externas.

2.6.2.7. Finalización de la Auditoría Informática

El informe de Auditoría debe contener:

- Dictamen sobre los procesos de TI o del área administrativa auditada.
- Informe sobre la estructura del Control Interno de la entidad.
- Conclusiones y recomendaciones resultantes de la Auditoría.
- Deben detallarse en forma clara y sencilla, los hallazgos encontrados.

Si en el transcurso del trabajo de auditoría surgen hechos o se encuentran algunos o algún hallazgo que a juicio del auditor es grave, se deberá hacer un informe especial, dando a conocer el hecho en forma inmediata, con el propósito de que sea corregido o enmendado a la mayor brevedad. Así mismo, si al analizar el sistema de control interno se encuentran serias debilidades en su organización y contenido, se debe elaborar por separado un informe sobre la evaluación del control interno. El informe final del auditor, debe estar elaborado de forma sencilla y clara, ser constructivo y oportuno[70][70].

2.7. Auditoría de la Seguridad Informática

2.7.1. Función de la Seguridad en los Sistemas Informáticos

Garantiza que los recursos informáticos de una compañía estén disponibles para cumplir sus propósitos, es decir, que no estén dañados o alterados por circunstancias o factores externos, es una definición útil para conocer lo que implica el concepto de seguridad informática.

[70] Fases de la Auditoría Informática: http://blogs.vandal.net/3996/vm/1035432792006

En términos generales, la seguridad puede entenderse como aquellas reglas técnicas y/o actividades destinadas a prevenir, proteger y resguardar lo que es considerado como susceptible de robo, pérdida o daño, ya sea de manera personal, grupal o empresarial.

En este sentido, es la información el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales, para ello, resulta importante establecer políticas de seguridad, las cuales van desde el monitoreo de la infraestructura de red, los enlaces de telecomunicaciones, la realización del respaldo de datos y hasta el reconocimiento de las propias necesidades de seguridad, para establecer los niveles de protección de los recursos.

Las políticas deberán basarse en los siguientes pasos:

- Identificar y seleccionar lo que se debe proteger (información sensible).
- Establecer niveles de prioridad e importancia sobre esta información.
- Conocer las consecuencias que traería a la compañía, en lo que se refiere a costos y productividad, la pérdida de datos sensibles.
- Identificar las amenazas, así como los niveles de vulnerabilidad de la red.
- Realizar un análisis de costos en la prevención y recuperación de la información, en caso de sufrir un ataque y perderla.
- Implementar respuesta a incidentes y recuperación para disminuir el impacto.

Este tipo de políticas permitirá desplegar una arquitectura de seguridad basada en soluciones tecnológicas, así como el desarrollo de un plan de acción para el manejo de incidentes y recuperación para disminuir el impacto, ya que previamente habremos identificado y definido los sistemas y datos a proteger [71][71].

2.7.1.1. Seguridad de Entornos Físicos

Cuando se habla de seguridad informática existe una clara tendencia a hacer el siguiente razonamiento de forma más o menos inconsciente:

- Queremos proteger bienes de carácter informático (por ejemplo, datos confidenciales).
- Las amenazas que dichos bienes pueden sufrir proceden del medio informático (por ejemplo, copia no autorizada de esos datos).
- Por tanto, los mecanismos de protección también deben ser informáticos (por ejemplo, restricciones de acceso a dichos datos).

Así, asociamos el concepto de seguridad exclusivamente a mecanismos relativamente sofisticados de control informático, como pueden ser entrada restringida al sistema, denegación de privilegios de lectura y modificación de ficheros, cifrado de las comunicaciones, o protección de las redes mediante cortafuegos.

[71] Función de la Seguridad en los Sistemas de Información: http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm

Como consecuencia de esta manera de pensar los sistemas informáticos quedan a merced de amenazas que no dependen para nada de su configuración: ¿de qué nos sirve tener los mejores mecanismos de control de acceso a nuestros ordenadores, o disponer de los sistemas de cifrado más actuales e invulnerables, si un simple accidente del personal de limpieza de nuestra oficina puede hacer que el equipo acabe por el suelo y que la información en él contenida quede irrecuperable? ¿O si alguna de las personas que operan en ellos se lleva a su casa ficheros con información confidencial para trabajar sobre ellos y es víctima de un robo?

La seguridad física se ocupa precisamente de los problemas de seguridad informática que, por su origen, son ajenos a los equipos y no pueden ser previstos o evitados utilizando la programación de los mismos. Es decir, de los daños que se pueden producir sin necesidad de acceder al ordenador (y muchas veces sin necesidad de enchufarlo siquiera).

Las medidas de seguridad física servirán para proteger nuestros equipos e información frente a usos inadecuados, fallos de instalación eléctrica, accidentes, robos, atentados, desastres naturales, y cualesquiera otros agentes que atenten directamente contra su integridad física[72][72].

[72] Garfinkel y G. Spafford (1996). Practical Unix & Internet security. O'Reilly & Associates.

2.7.1.2. Seguridad Lógica

Luego de ver como los sistemas de información puede verse afectados por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos, sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren, estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo. Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean en la Seguridad Lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información[73][73].

2.7.2. Plan de Contingencia para recuperación de desastres informáticos

Para proteger información vital ante la posible pérdida, destrucción, robo y otras amenazas una empresa debe preparar un completo plan de contingencia informático. Un DRP (Plan de Recuperación ante Desastres - Disaster Recovery Plan) informático debe tener los siguientes componentes: Emergencia, Back-Up, Recuperación, Simulación y Mantenimiento.

El plan de emergencia indica las acciones que deben tomarse inmediatamente tras el desastre, un importante aspecto de este plan es el diagrama de organización de la contingencia, en el que se muestran los nombres del responsable de la contingencia y los principales coordinadores de la contingencia; las responsabilidades del gestor de la contingencia y los principales coordinadores deben explicarse de forma clara.

[73] Seguridad Lógica: http://www.4shared.com/document/-Q26VFvX/cap3_Seguridad_Lgica.html

El segundo aspecto crítico de un plan de contingencia es la preparación de un plan de backup, este documento es un elemento primordial y necesario para la recuperación, la selección de un backup alternativo requiere una cuidadosa preparación. La compañía debe considerar todas las alternativas tecnológicas y de servicios disponibles en el mercado.

El tercer aspecto es la preparación de un plan de recuperación, la organización debe establecer su capacidad real para recuperar información contable crítica en un periodo de tiempo aceptable, una parte importante del plan de recuperación es el equipo de recuperación. Es necesario por tanto la identificación previa de cuáles de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión, ese tipo de decisiones se realizan de forma más simple teniendo en cuenta los centros de trabajo alternativos, planes de trabajo, instalaciones de backup, necesidades de software, necesidades de personal, seguridad y requerimientos de documentación.

El DRP informático debe ser comprobado de forma periódica para detectar y eliminar problemas; muchas dificultades potenciales pueden ser eliminados mediante el desarrollo de una estrategia de testeo, la manera más efectiva de comprobar si un DRP funciona correctamente, es la de programar simulaciones de desastres reales. Finalmente, la empresa u organización debería asegurar procedimientos que permitan mantener la vigencia permanente del DRP [74][74].

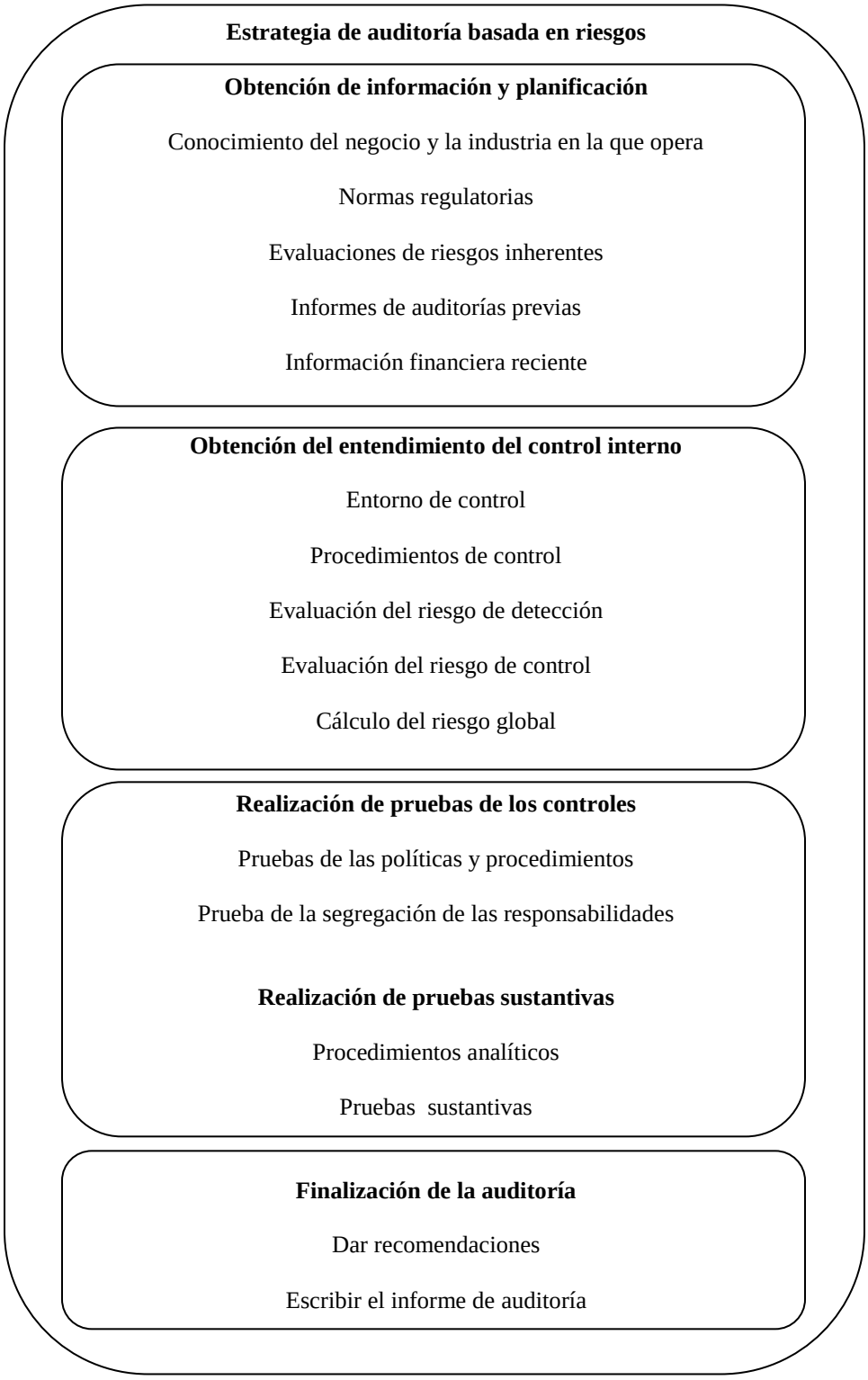
[74] José Salvador Sánchez Garreta (2003). Ingeniería de Proyectos Informáticos: Actividades y Procedimientos. Universitat Jaume.

2.8. Auditoría Basada en Riesgos

Cada vez más organizaciones se deciden por una estrategia de auditoría basada en la evaluación de riesgos para desarrollar y mejorar el proceso de auditoría continua, esto ayuda a tomar la decisión de si realizar pruebas de los controles o ir directamente a realizar pruebas sustantivas. Los riesgos de negocio son los temas acerca de los efectos probables de un evento incierto en la consecución de los objetivos de negocio establecidos, la naturaleza de estos riesgos puede ser financiera, regulatoria u operacional.

Entendiendo la naturaleza del negocio se puede identificar y categorizar los tipos de riesgos que mejor determinarán el modelo o estrategia de riesgos para realizar la auditoría. De una más práctica y entendible se expone la estrategia de auditoría basada en riesgos en el cuadro 2.3.

Cuadro 2.3. Estrategia de la Auditoría Basada en Riesgos.



2.8.1. Análisis del Riesgo

El análisis de riesgos es parte de la planificación de una auditoría, ya que ayuda a identificar los riesgos y vulnerabilidades para que el auditor pueda determinar los controles que son necesarios para mitigar esos riesgos.

Para evaluar los procesos de negocio basados en la utilización de TI de una organización, es importante entender la relación entre riesgo y control, concretamente, los tipos de riesgos y los controles que se utilizan para mitigarlos. La evaluación de riesgos sirve para poner el foco de la auditoría en las áreas que tengan mayor riesgo y planificar, en consecuencia, el trabajo de auditoría.

Hay muchas definiciones de riesgo, quizás una de las más concisas utilizada en el mundo de la seguridad de la información es la que se da en Guías para la Gestión de la seguridad de la TI de la International Organization for Standardization (ISO), donde expresa que riesgo es: "El potencial de que una amenaza dada pueda explotar las vulnerabilidades de un activo o grupo de activos y cause pérdida o daño a los activos. El impacto o severidad relativa del riesgo es proporcional al valor que para el negocio tiene la pérdida/daño y la frecuencia estimada de la amenaza".

Los riesgos tienen los siguientes elementos:

- Amenazas a, y vulnerabilidades de, los procesos y/o los activos, tanto activos físicos como lógicos.
- Probabilidad de las amenazas (combinación de la probabilidad y la frecuencia de ocurrencia).

Los riesgos de negocio son aquellas amenazas que pueden impactar los activos, o procesos u objetivos de una organización, la naturaleza de estas amenazas puede ser financiera, reglamentaria u operacional. Una clase particular de riesgos asociados con la información y los SI que la soportan es la que está definida por el potencial de pérdida de la confidencialidad, disponibilidad o integridad de la información.

En una auditoría también se puede pedir que se evalúe el proceso de gestión de riesgos que utiliza una organización para identificar, evaluar y gestionar los riesgos que tiene que hacer frente, ya que la gestión de riesgos es el proceso de identificar los riesgos de la seguridad de un sistema e identificar la probabilidad de ocurrencia, el impacto resultante y las salvaguardas que podrían mitigar el impacto en caso de ocurrencia, esto abarca a tres procesos:

- Identificación de riesgos,
- Mitigación de riesgos y,
- Evaluación de riesgos.

El proceso de gestión de riesgos comienza con la identificación de los objetivos de negocio, los activos de información y los sistemas o recursos de información que generan, almacenan, utilizan o manipulan los activos (hardware, software, bases de datos, redes, instalaciones, personal, etc.) que sean críticos para alcanzar dichos objetivos.

El mayor esfuerzo en la gestión de riesgos se debe centrar en los activos más críticos, una vez que se han identificado estos activos críticos, se evalúan las amenazas y el impacto en caso de que se materialicen estas amenazas frente a las vulnerabilidades que tienen dichos activos. El siguiente paso es identificar y evaluar los controles establecidos como medidas para mitigar el impacto de las amenazas, estas medidas pueden prevenir o reducir la probabilidad de que un riesgo ocurra, detectar la ocurrencia de un riesgo y minimizar el impacto o transferir el riesgo a otra organización.

Esto se puede conseguir:

- Identificando todos los controles que existen para minimizar el riesgo.
- Determinando y evaluando todo control nuevo o adicional que se identifique durante el análisis del riesgo de negocio.
- Priorizando todos los riesgos identificados, identificando aquellos controles que sean más eficaces y eficientes en la mitigación del riesgo.

La selección de los controles más eficaces/eficientes dependerá de:

- El coste del control comparado con el benefició que reporta su implantación.
- El nivel de riesgo que la organización está preparada para aceptar.
- Los métodos de reducción de riesgos preferidos por la dirección (eliminar el riesgo, minimizar la probabilidad de ocurrencia, minimizar el impacto, transferencia el riesgo).

2.8.2. Técnicas de Evaluación del Riesgo

Cuando se tenga que determinar las áreas que deben ser auditadas entre una variedad de ellas, se deberán evaluar los riesgos de cada una de ellas para seleccionar las que tengan más alto riesgo.

La utilización de la evaluación de riesgos para determinar las áreas a auditar:

- Permite la asignación eficaz de los recursos limitados de auditoría.
- Establece una base para gestionar de forma eficaz la función de auditoría.
- Asegura que se ha obtenido información relevante de todos los niveles de la gestión, incluyendo el comité de dirección, las áreas funcionales de la gestión y los auditores de SI. Generalmente, la información ayuda a que los gestores deleguen sus responsabilidades y asegura que las actividades de auditoría se dirijan hacia las áreas de negocio con más alto riesgo.
- Da un resumen de cómo está relacionado un tema individual de auditoría con la organización global así como con los planes de negocio.

Hay varios métodos que se emplean para realizar una evaluación de riesgos, uno de ellos es el de un sistema de puntuación, que es útil para priorizar las auditorías basándose en una evaluación de los factores de riesgo. Para ello se consideran variables como la dificultad técnica, nivel de los procedimientos de control establecidos y nivel de pérdidas financieras.

Otra forma es realizando juicios de valor, en donde la decisión se hace basándose en el conocimiento del negocio, directrices de la dirección ejecutiva, perspectivas históricas, objetivos de negocio y factores del entorno[75][75].

2.9. Análisis del Modelo COBIT

2.9.1. Introducción

Un elemento crítico para el éxito y la supervivencia de las organizaciones, es la administración efectiva de las TIC, ya que la sociedad global actual tiene una creciente dependencia de los datos, información y de sus sistemas. Para muchas organizaciones, la información y la tecnología que la soporta representan los activos más valiosos, es más, en el cambiante mundo actual, dichas organizaciones han incrementado sus expectativas con la entrega de servicios relacionados a las TIC. Desde un punto de vista empresarial, se reconocen los beneficios potenciales que la tecnología puede proporcionar, sin embargo, también comprende y conlleva riesgos asociados con la implementación de nuevas tecnologías, donde las organizaciones deben tener un entendimiento básico de los riesgos y limitantes del empleo de la Tecnologías de la Información para proporcionar una dirección efectiva y controles adecuados.

[75] Thimothy Bell, Mark E. Peecher, Ira Solomon, Frank O. Marrs y Howard Thomas (2007). Auditoría Basada en Riesgos, perspectiva estratégica de sistemas. Primera Edición. ECOE Ediciones.

COBIT (Objetivos de Control para la Información y Tecnologías relacionadas) ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos, proporcionando "buenas prácticas" a través de un Marco Referencial de dominios y procesos, donde se presentan actividades en una estructura manejable y lógica.

El impacto en los recursos TIC es enfatizado en el Marco Referencial de COBIT conjuntamente a los requerimientos de información del negocio que deben ser alcanzados con efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad. La orientación a negocios es el tema principal de COBIT, ya que este modelo está diseñado no solo para ser utilizado por usuarios y auditores, sino que en forma más importante, está diseñado para ser utilizado como una lista de verificación (*check list*) detallada para los propietarios de los procesos de negocio.

Con el fin de proporcionar la información que la empresa necesita para alcanzar sus objetivos, los recursos tecnológicos deben ser administrados por un conjunto de procesos agrupados en un conjunto de 34 Objetivos de Control de alto nivel, agrupados en cuatro dominios: *Planeación y Organización*, *Adquisición e Implementación*, *Entrega y Soporte*, *Monitoreo y Evaluación*. COBIT habilita el desarrollo de una política clara y de buenas prácticas de control de TI a través de organizaciones a nivel mundial, por lo que, el objetivo de COBIT es proporcionar estos objetivos de control, dentro del marco referencial definido, y obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo, por lo tanto, COBIT está orientado a ser la herramienta de gobierno de TI que ayude al entendimiento y a la administración de riesgos asociados con Tecnologías de la Información y con tecnologías relacionadas dentro de una organización.

2.9.2. Antecedentes

El proyecto COBIT se emprendió por primera vez en el año 1995, con el fin de crear un producto global que pudiese tener un impacto duradero sobre el campo de visión de los negocios, así como sobre los controles de los sistemas de información implantados. La primera edición de COBIT, fue publicada en 1996 y fue vendida a 98 países de todo el mundo, la segunda edición fue publicada en Abril de 1998, desarrolla y mejora lo que poseía la anterior mediante la incorporación de un mayor número de documentos de referencia fundamentales, nuevos y revisados (de forma detallada) objetivos de control de alto nivel, intensificando las líneas maestras de auditoría e introduciendo un conjunto de herramientas de implementación.

A partir de la segunda edición, se marcó una época en la que la orientación principal de las organizaciones era el Control Interno y la Auditoría de Sistemas, como tales, manteniendo una clara fidelidad a los orígenes de la entidad. En el 2000 se publica la tercera edición, la cual vino acompañada por vez primera de las "Directrices de Gestión", marcando un nuevo alcance, hacia la gestión de las TI[76][76].

La actual cuarta edición (2005) supone la culminación de la estrategia de ISACA[77][77] iniciada con la creación del ITGI[78][78] en 1998, de convertirse en el referente en Gobierno de TI, cuyo reflejo se materializa en la publicación de un elevado número de documentos, tales como:

[76] Historia del Modelo COBIT: http://ds5-andre-ortega-5a.host56.com/componentes.html.
[77] ISACA: Information Systems Audit and Control Association.
[78] ITGI: El Instituto de Gobierno de TI.

- “IT Governance Executive Summary”, “IT Strategy Committee”,
- “Board Briefing on IT Governance” (2001, 2003),
- “IT Governance Implementation Guide” (2003),
- “IT Alignment: Who is in charge?” (2005),
- “Governance of Outsourcing” (2005),
- “The CEO’s Guide to IT Value at Risk” (2005).

Paralelamente, en los últimos tiempos existe una intención de simplificación y acercamiento de COBIT a los usuarios, mediante iniciativas como COBIT Quickstart, COBIT On-line, COBIT in Academia, etc., así como otros cursos y material puestos a disposición por ISACA/ITGI para la difusión del modelo, entre los que destaca el inicio de las COBIT User Conventions[79][79].

En los últimos 5 años ISACA, una asociación mundial de más de 86.000 profesionales TI de aseguramiento, de seguridad y de gobierno, recibió casi 3.000 comentarios de más de 600 empresarios y profesionales de TI durante el período de la primera exposición pública del documento del diseño del proyecto de COBIT 5, que será una evolución importante del marco de trabajo COBIT. COBIT 5 será una extensión estratégica de la versión existente, proporcionando la siguiente generación de lineamientos ISACA sobre el manejo empresarial de las TI, basado en más de 15 años de uso práctico y la utilización de COBIT en empresas de todo el mundo, COBIT 5 se alineará con lo último en cuanto a la gestión y las técnicas de administración de TI.

[79] Historia del Modelo COBIT: http://www.borrmart.es/articulo_redseguridad.php?id=1145&numero=24.

La importancia de la información y la tecnología relacionada es cada vez más reconocida en todos los aspectos de los negocios y la vida pública. Como resultado, la necesidad de dar más valor a las inversiones en TI y administrar un abanico creciente de riesgos tecnológicos.

COBIT 5 proporcionará una guía completa y de fácil navegación para ayudar a las empresas administrar eficazmente sus TI, así como cumplir con el incremento de las obligaciones legales, reglamentarias y contractuales; además consolidará e integrará los marcos de trabajo COBIT 4.1y también sacará del marco de trabajo de aseguramiento de TI de ISACA y de BMIS[80][80].

Esta reciente versión tocará temas muy valiosos:

- Alineamiento estratégico de TI.
- Administración de la información.
- Medición del rendimiento.

El proceso de desarrollo de colaboración y la contribución de líderes de TI y de negocios de todo el mundo, son una parte muy importante de lo que hace a la Norma COBIT tan útil y respetado[81][81].

[80] BMIS: Modelo de Negocio para la Información de Seguridad.
[81] Historia del Modelo COBIT: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/COBIT5-ultimas-noticias.aspx

2.9.3. Misión del Modelo COBIT

La misión principal es investigar, desarrollar, hacer público y promover un marco de control de gobierno TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento[82][82].

2.9.4. Función Básica y Orientación COBIT

COBIT, es una herramienta de gobierno de las Tecnologías de la Información que ha cambiado de igual forma que lo ha hecho el trabajo de los profesionales de TI, ISACF organización creadora de COBIT, han diseñado este producto principalmente como una fuente de instrucción para los profesionales dedicados a las actividades de control. Este modelo 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.

[82] Misión del Modelo COBIT: http://cgi-pe.com/cursos/ptcob.html

En suma, cada uno de los 34 objetivos de control de alto nivel correspondiente, es una directiva de revisión y/o seguridad para permitir la inspección de los procesos de las tecnologías de la información en contraste con los 302 objetivos de control detallados en COBIT para el suministro de una gestión de seguridad, así como de un aviso para la mejora. El Modelo COBIT contiene un conjunto de herramientas de implementación el cual aporta una serie de lecciones de aprendizaje, con las que las organizaciones podrán aplicar de forma rápida y satisfactoria esta norma a sus entornos de trabajo[83][83]. (Figura 2.4.)

[83] Función Básica y Orientación COBIT: http://alarcos.inf-cr.uclm.es/per/fruiz/cur/mso/comple/Cobit.pdf

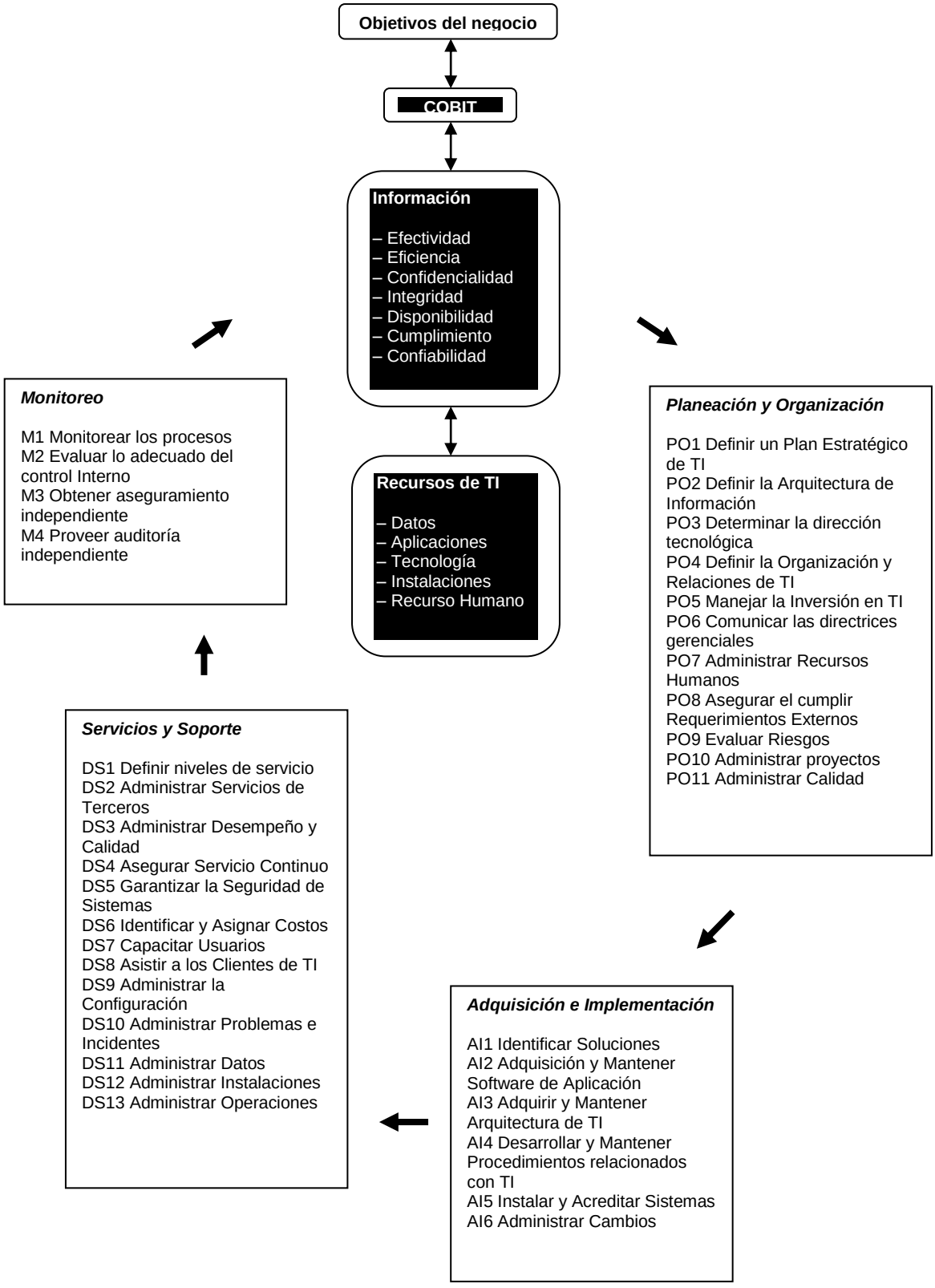


Figura 2.4. Marco de Trabajo COBIT.

2.9.5. Componentes del Modelo COBIT

- Un **Resumen Ejecutivo** (Executive Sumary), el cual consiste en una síntesis ejecutiva que proporciona a la alta gerencia entendimiento y concientizando sobre los conceptos clave y principios de COBIT;
- Un **Marco Referencial** (Framework), el cual 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;
- Los **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;
- Las **Guías de Auditoría** (Audit Guidelines), las cuales contienen los pasos de auditoría correspondientes a cada uno de los 34 objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los 302 objetivos detallados de control recomendados para proporcionar a la gerencia certeza o unas recomendaciones para mejorar[84][84].

[84] Componentes del Modelo COBIT: http://ds5-andre-ortega-5a.host56.com/componentes.html

2.9.6. Marco Referencial

2.9.6.1. La necesidad de control en Tecnologías de la Información

Hoy en día uno de los aspectos más importantes para el éxito y la supervivencia de cualquier organización, es la gestión efectiva de la información así como de las tecnologías relacionadas con ella. Por lo general, la Gerencia de Tecnologías debe decidir la inversión razonable en seguridad y control tecnológico, y cómo lograr un balance entre riesgos e inversiones en un ambiente de TI frecuentemente impredecible.

La gerencia, necesita un Marco Referencial de prácticas de seguridad y control de TI generalmente aceptadas para medir comparativamente su ambiente, desde el punto de vista tecnológico, tanto el existente como el planeado. Existe una creciente necesidad entre los usuarios en cuanto a la seguridad en los servicios de TI, a través de la acreditación y la auditoría de servicios de TI proporcionados internamente o por terceras partes, que aseguren la existencia de controles adecuados. Actualmente, es confusa la implementación de buenos controles de TI en sistemas de negocios por parte de entidades comerciales, entidades sin fines de lucro o entidades gubernamentales.

Esta confusión proviene de los diferentes métodos de evaluación, tal como, la evaluación ISO9000[85][85], nuevas evaluaciones de control interno, COSO, etc.; como resultado, los usuarios necesitan una base general para ser establecida como primer paso.

[85] ISO 9000: Describe los fundamentos y especifica la terminología para los sistemas de gestión de calidad.

Frecuentemente, los auditores han tomado el liderazgo en estos esfuerzos internacionales de estandarización, debido a que ellos enfrentan continuamente la necesidad de sustentar y apoyar frente a la gerencia su opinión acerca de los controles internos. Sin contar con un Marco Referencial, ésta se convierte en una tarea demasiado complicada. Esto ha sido mostrado en varios estudios recientes acerca de la manera en la que los auditores evalúan situaciones complejas de seguridad y control en TI, estudios que fueron dados a conocer casi simultáneamente en diferentes partes del mundo.

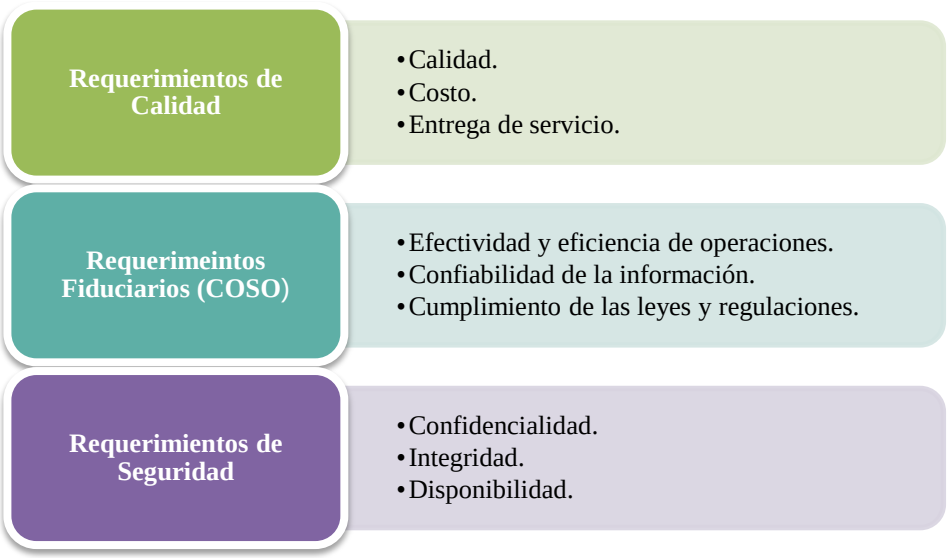
2.9.6.2. Principios del Marco Referencial COBIT

Existen dos clases distintas de modelos de control disponibles actualmente, aquéllos de la clase del modelo de control de negocios, por ejemplo COSO, y los modelos más enfocados a TI, por ejemplo, DTI[86][86].

COBIT intenta cubrir la brecha que existe entre los dos, debido a esto, se posiciona como una herramienta completa para operar a un nivel superior que los estándares de tecnología y de la administración de sistemas de información. Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información, al establecer la lista de requerimientos COBIT resalta los siguientes: (Cuadro 2.4.)

[86] DTI: Dirección de Tecnologías de la Información.

Cuadro 2.4. Requerimientos de Negocio COBIT.



Comenzando un análisis a partir de los requerimientos de Calidad, Fiduciarios y de Seguridad, se extrajeron siete puntos importantes que muestran las definiciones del trabajo de COBIT:

- **Efectividad:** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- **Eficiencia:** Se refiere a la provisión de información a través de la utilización óptima, más productiva y económica, de recursos.
- **Confidencialidad:** Se refiere a la protección de información sensible contra divulgación no autorizada.
- **Integridad:** Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

- **Disponibilidad:** Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro.
- **Cumplimiento:** Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- **Confiabilidad de la información:** Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Otra forma de ver la relación de los recursos de TI con respecto a la entrega de servicios se describe a continuación en la figura 2.5.

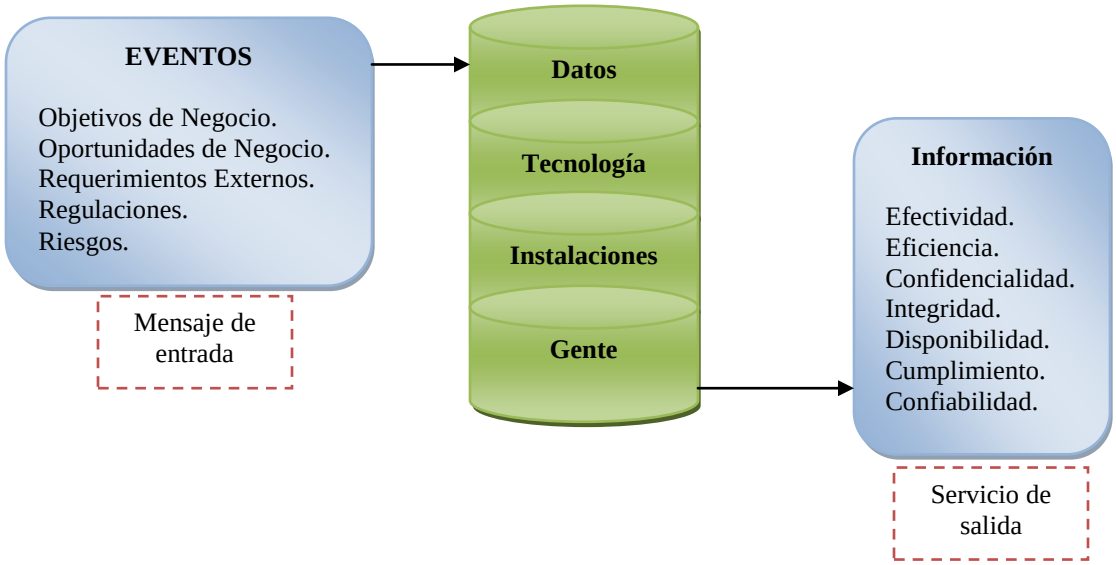


Figura 2.5. Relación de los Recursos TI.

La información que los procesos de negocio necesitan, es proporcionada a través del empleo de recursos de TI, con el fin de asegurar que los requerimientos de negocio sean una información satisfactoria.

El Marco Referencial consta de Objetivos de Control de TI de alto nivel y de 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 dominios 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.

Por lo tanto, 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 2.6.[87][87].

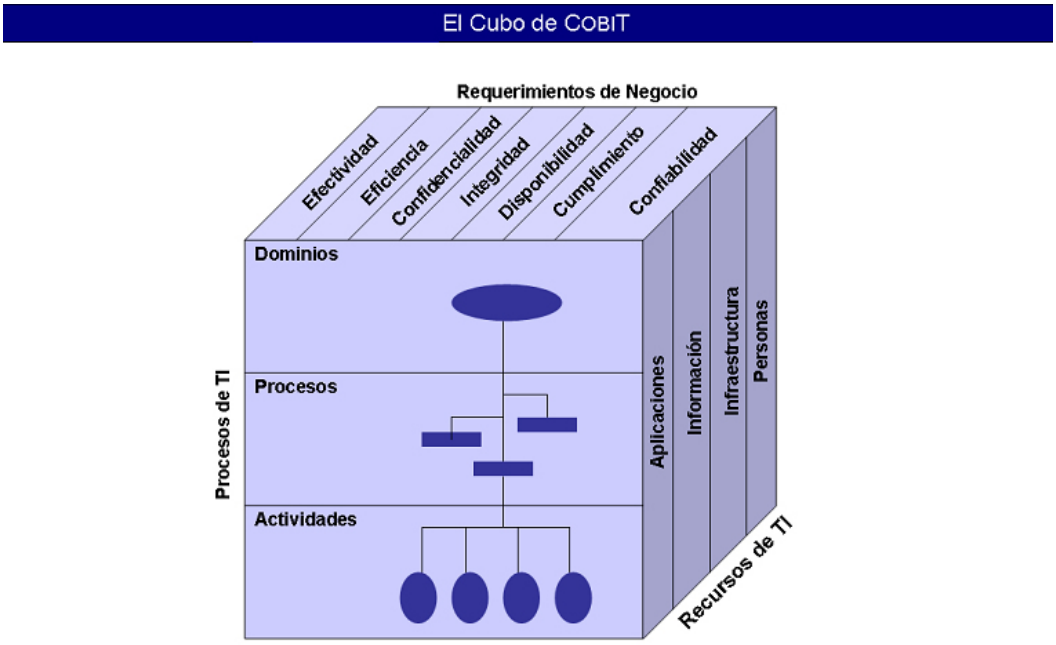


Figura 2.6. Cubo COBIT[88][88].

2.9.7. Objetivos de Control

Los Objetivos de Control dentro del Modelo COBIT muestran una relación clara y distintiva con los objetivos de negocio con el fin de apoyar su uso dentro de toda la organización y más allá del uso exclusivo de los auditores. Además, están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios.

[87] Marco Referencial: http://www.piramidedigital.com/Documentos/ICT/pdictcobitmarcoreferencial.pdf
[88] Figura 4.4. Cubo COBIT: http://www.overti.es/procesos-itsm/cobit.aspx.

Han sido organizados por proceso / actividad, pero también se facilita la entrada a partir de cualquier punto de vista estratégico, además para lograr enfoques combinados o globales, tales como instalación / implementación de un proceso, responsabilidades gerenciales globales para un proceso y utilización de recursos de tecnología informática por un proceso. El Marco de Referencia identifica un conjunto de 34 Objetivos de Control de alto nivel, uno para cada uno de los procesos de tecnología informática, agrupados en cuatro dominios, donde el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información[89][89].

2.9.8. 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 plan, 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.

[89] Objetivos de Control: ftp://200.60.110.5/Docentes/Mario_Ramos/CURSOS/PIURA%20AUDITORIA/OBLIGATORIOS/COBIT/COBIT_03.PDF

- **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[90][90].

2.9.9. Aceptabilidad general de COBIT

COBIT resulta de interés a distintos usuarios: dirección ejecutiva, gerencia del negocio, gerencia de TI y auditores por estar orientado a los objetivos y al alcance del gobierno de TI, asegurando que su marco de control sea integral, que esté alineado con los principios de Gobierno Corporativo, y por tanto, que sea aceptable para los consejos directivos, para la dirección ejecutiva, para los auditores y reguladores.

Las organizaciones antes de implementar el Modelo COBIT deben entender ¿qué hacer?, ¿cómo hacerlo? y ¿porqué es importante hacerlo?, para de esta forma garantizar la utilización las mejores prácticas.

Para lograr la alineación de las mejores prácticas con los requerimientos del negocio, se recomienda que COBIT se utilice al más alto nivel, brindando así un marco de control general basado en un modelo de procesos de TI que debe ser aplicable en toda la organización[91][91].

[90] COBIT orientado a Procesos: http://www.overti.es/procesos-itsm/cobit.aspx
[91] Aceptabilidad de COBIT: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf

CAPÍTULO 3

ELABORACIÓN DEL PLAN DE INVESTIGACIÓN DE CAMPO O PROGRAMA DE AUDITORÍA EN LA CORPORACIÓN HOLDINGDINE S.A. (MATRIZ)

3.1. Institución Sujeto de Estudio

Figura 3.1. Logotipo Corporación Industrial y Comercial HOLDINGDINE S.A.[92][92].

3.1.1. Conocimiento y Compresión de la Corporación HOLDINGDINE S.A.

HOLDINGDINE S.A. es una Corporación Industrial y Comercial que se constituyó en el año 2000, como una sociedad anónima, al amparo de lo previsto en el artículo 429 de la Ley de Compañías **(Ver CD Anexos → Documento "ANEXO A.docx")**, para administrar corporativamente las empresas de la Dirección de Industrias del Ejército, institución adscrita a la Fuerza Terrestre y estructurada a un Grupo Empresarial.

[92] Figura 3.1. Logotipo Corporación Industrial y Comercial HOLDINGDINE S.A.: http://www.holdingdine.com.

Diez años más tarde, por efecto de la cesión de todas las acciones de la Dirección de Industrias del Ejército en HOLDINGDINE S.A., a favor del Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA), se generó una trascendental conversión legal y empresarial en la conceptualización así como en la formulación de nuevos objetivos estratégicos de la Corporación y de las compañías que integran el Grupo Empresarial, sin generar modificación alguna en su naturaleza jurídica ni en el giro de sus negocios. El actual esquema jurídico empresarial derivado de la presencia del ISSFA como nuevo y único accionista de la Corporación.

Figura 3.2. Logotipo Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA)[93][93].

DINE (Dirección de Industrias del Ejército), a partir del año 1995, incorpora en su desarrollo organizacional, herramientas gerenciales y de gestión modernas, como planificación estratégica, cultura de la calidad, sistemas de calidad, sistemas integrados de gestión y tableros de comando, entre los más importantes.

[93] Figura 3.2. Logotipo Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA): www.issfa.mil.ec.

En el año 2000, la Dirección de Industrias del Ejército, en un paso decisivo para direccionar su actividad institucional, adopta un nuevo modelo de conglomerado empresarial, mediante la conformación de la compañía HOLDINGDINE S.A. Corporación Industrial y Comercial, como una organización supraempresarial que planifica, lidera, norma y evalúa corporativamente la gestión de las empresas en las que es accionista, armonizando monolíticamente las diferencias que se venían advirtiendo originalmente, por la coexistencia de figuras empresariales disímiles, en su estructura jurídica.

La compañía HOLDINGDINE S.A. se constituye como una sociedad anónima, cuyo único accionista es la Dirección de Industrias del Ejército, al amparo del Artículo 429 de la Ley de Compañías, que establece la existencia de los Grupos Empresariales, bajo la conducción de una Organización Superior (Matriz), que tiene por objeto la propiedad; adquisición y tenencia de acciones de las compañías (subsidiarias), con la finalidad de vincularlas e integrarlas jurídicamente, ejercer su control y administración superior como un centro de decisiones, con facultades para regular su gestión gerencial, financiera, crediticia, administrativa, y de resultados, en especial; por efecto de lo cual se busca maximizar su rentabilidad, evitando duplicidad en la ejecución de tareas y minimizando la carga fiscal.

La Corporación HOLDINGDINE S.A. para optimizar su gestión, productividad y competitividad, posee una estructura organizacional conformada por tres divisiones vinculadas a los sectores manufactura, agroindustrial y servicios[94][94].

[94] Conocimiento y Comprensión de la Corporación HOLDINGDINE S.A.: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.

El giro de sus negocios (objeto social) apunta hacia las siguientes actividades:

- Asumir la tendencia y propiedad de sociedades comerciales para vincularlas, ejercer su control y supraadministración.
- Otorgar consultoría, asesoría y asistencia técnica en los diferentes ámbitos de la gestión empresarial.
- Identificar, promover e instalar nuevas industrias y otras actividades productivas conexas conformando nuevas compañías mercantiles.

El Grupo Empresarial se integra por las denominadas compañías subsidiarias en las que HOLDINGDINE S.A. posee la mayoría accionarial, legalmente incorporadas por decisión unánime de sus accionistas e identificadas, en el argot corporativo, como Unidades Estratégicas de Negocios. La adecuada y legal supervisión, la administración corporativa, más aún la plena identificación del quehacer empresarial entre la Corporación y las Unidades Estratégicas de Negocio, descansan en la proclama corporativa: subordinación con coordinación.

3.1.2. Filosofía Corporativa

- **Visión:** ser una Corporación consolidada dentro de los cinco grupos empresariales de mayor rentabilidad en el país:
    - Generando negocios sustentables que incursionen en el mercado internacional.
    - Aprovechando nuevas oportunidades de negocios de rápida implementación, con riesgos aceptables.
    - Promoviendo la responsabilidad social empresarial.

- **Misión:** administrar corporativamente al Grupo Empresarial, optimizando recursos y agregando valor a clientes, colaboradores y accionistas, para apoyar al fortalecimiento del patrimonio de la seguridad social militar y contribuir al desarrollo nacional.

- **Principios y Valores Corporativos:**
    - Enfoque hacia el cliente.
    - Compromiso y lealtad institucional.
    - Ética profesional.
    - Iniciativa y creatividad.
    - Trabajo en equipo.
    - Orientación a resultados.
    - Responsabilidad social y ambiental.
    - Liderazgo e innovación empresarial[95][95].

3.1.3. Estructura Organizacional

En el nuevo esquema jurídico-empresarial originado por efecto de la titularidad del 100% de las acciones del HOLDINGDINE S.A., que posee en la actualidad el ISSFA, se advierten las siguientes situaciones:

[95] Filosofía Corporativa: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.

- En la Corporación se generó un cambio en su estructura accionarial. La Dirección de Industrias del Ejército dejó de ser accionista y el ISSFA es el nuevo y único accionista.
- En las compañías subsidiarias y en las compañías filiales se mantiene inalterable su estructura accionarial. En efecto, el HOLDINGDINE S.A. continúa manteniendo su participación en los mismos porcentajes y para todos los efectos legales y estatutarios.

Adicionalmente y respecto de la estructura de los Órganos de Gobierno y Administración, es importante considerar que:

- El Órgano Supremo del HOLDINGDINE S.A. es la Junta General de Accionistas, con capacidad privativa, legal y estatutaria, para decidir sobre su existencia, funcionamiento y destino.
- La Junta General de Accionistas se integra únicamente por el ISSFA, representado por el Director General, a quien le corresponde emitir, en esta instancia, las pertinentes instrucciones y adoptar las acciones que correspondieren, para la aplicación y ejecución de las políticas, directrices y resoluciones que dicte el Consejo Directivo del ISSFA.
- La Junta Directiva es el Órgano colegiado de administración, que desarrolla sus actividades con sujeción al Estatuto Social, las políticas y las directrices de la Junta General de Accionistas (ISSFA).

La supervisión y el control del manejo empresarial del HOLDINGDINE S.A. corresponden directamente a la Junta General (ISSFA), sin perjuicio de las que realicen, por mandato legal, las auditorías, los órganos de fiscalización societaria, la Superintendencia de Compañías y la Contraloría General del Estado.

El control y la administración de las compañías subsidiarias corresponden directamente al HOLDINGDINE S.A., como Centro Corporativo y de Alta Dirección, en observancia de la Ley de Compañías y del Estatuto Social[96][96].

[96] Estructura Organizacional: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.

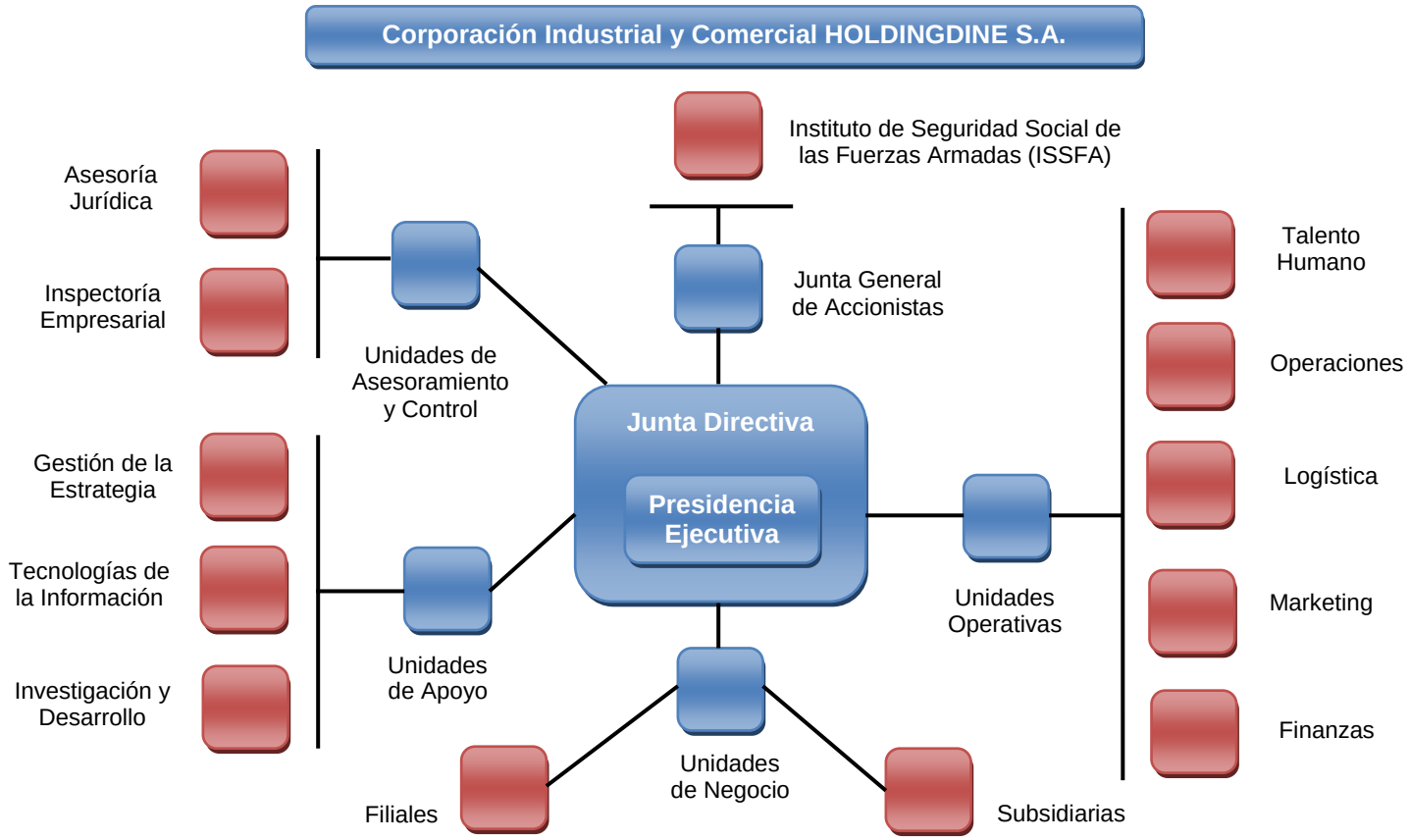


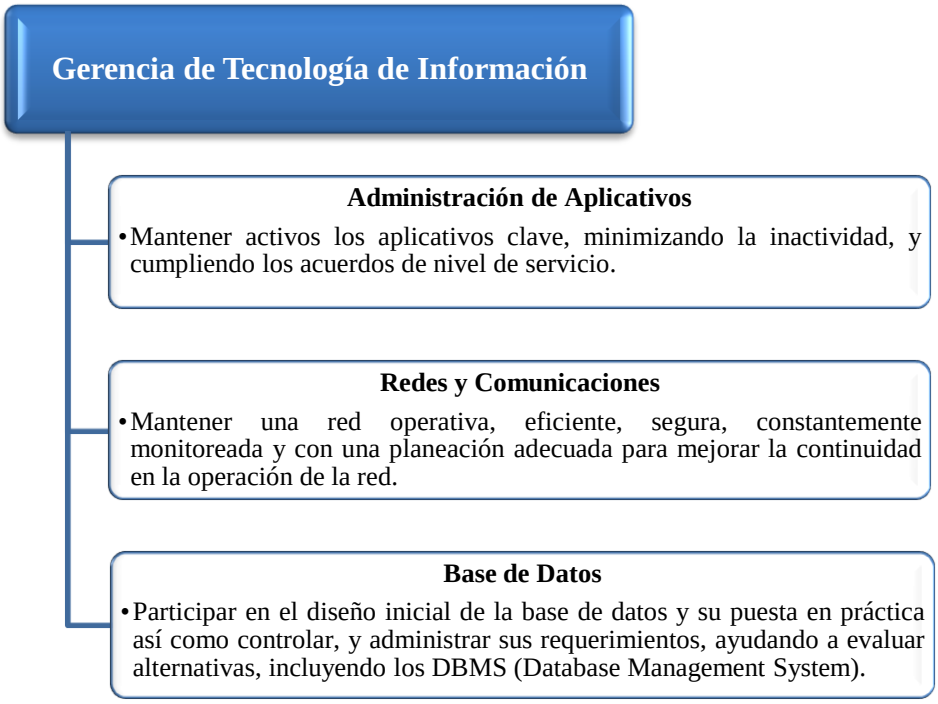
Figura 3.3. Estructura Organizacional de la Corporación HOLDINGDINE S.A.[97][97]

[97] Figura 3.3. Estructura Organizacional de la Corporación HOLDINGDINE S.A.: Fuente, Vicepresidencia de la Corporación HOLDINGDINE S.A.

3.1.4. Conocimiento y Compresión de la Gerencia TI de la Corporación HOLDINGDINE S.A. (Matriz)

La misión de la unidad de apoyo, Gerencia TI, se enfoque en objetivos fundamentales y prioritarios para mantener una infraestructura tecnológica adecuada y competente, tanto en la matriz de la Corporación como en cada una de las empresas subsidiarias con sus tres áreas claves que se detallan en el cuadro 3.1.[98][99].

Cuadro 3.1. Áreas claves de la Gerencia TI.



[98] Conocimiento y Compresión de la Gerencia de TI de la CORPORACIÓN HOLDINGDINE S.A. (Matriz): Fuente, Gerencia TI de la Corporación HOLDINGDINE S.A.

3.1.5. Composición Funcional de la unidad de apoyo Gerencia de TI

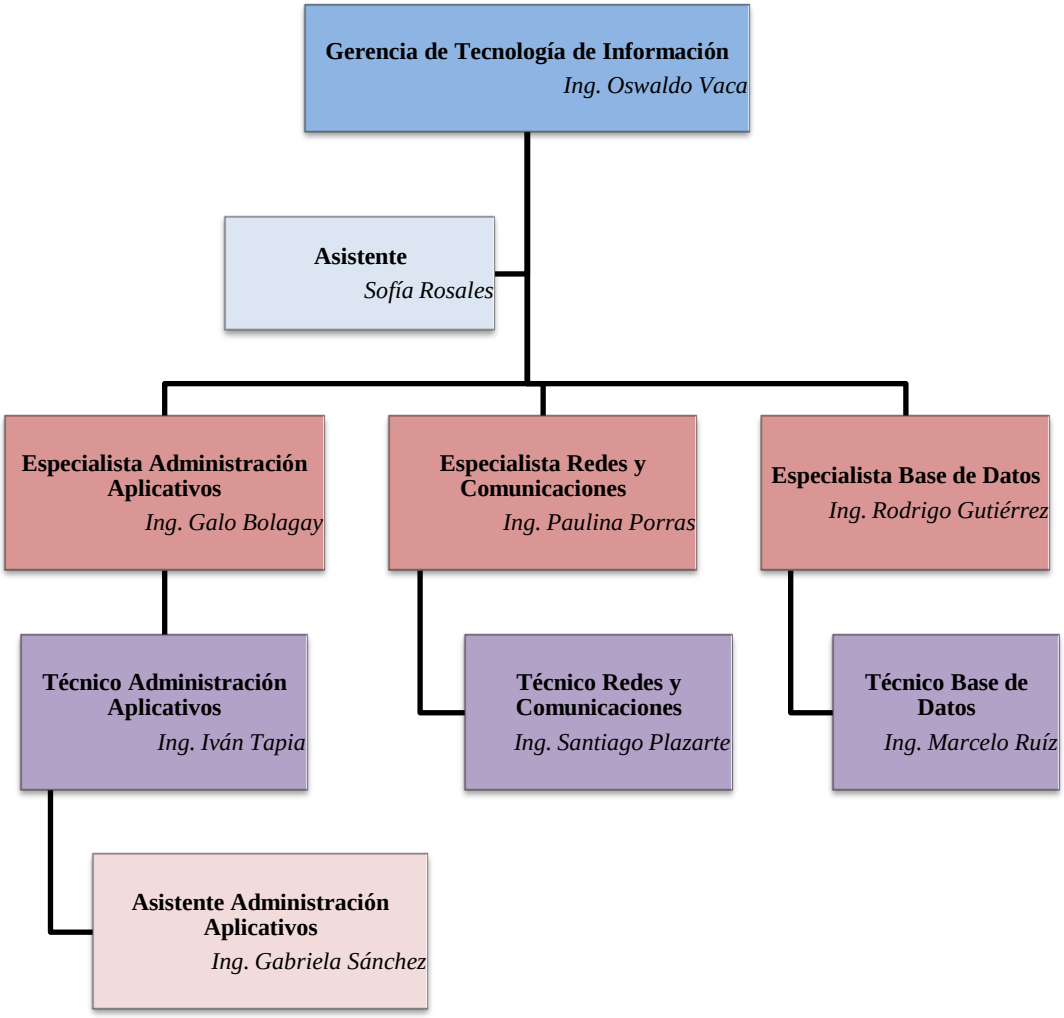


Figura 3.4. Composición Funcional de la Gerencia TI.

En base a la figura 3.4., a continuación se detalla las funciones que actualmente desempeña el personal dentro de la Gerencia de TI:

- **Gerente de Tecnología de la Información:**
    - Dirigir y controlar la gestión del área de Tecnología de la Información de HOLDINGDINE y sus empresas.
    - Evaluar y garantizar la implementación de los procesos, planes y proyecto tecnológicos en el Grupo Empresarial HOLDINGDINE.
    - Proponer políticas para los procesos informáticos de HOLDINGDINE y sus empresas.
    - Proporcionar soporte técnico al Grupo Empresarial HOLDINGDINE.
    - Elaborar la planificación estratégica del área de Tecnología de la Información del HOLDINGDINE y sus empresas.
    - Asesorar al Grupo Empresarial HOLDINGDINE, en la toma de decisiones, a través de la provisión de información.

- **Asistente Técnico:**
    - Proporcionar servicio de Service Desk al HOLDINGDINE Matriz y sus empresas.
    - Controlar y dar seguimiento de los soportes técnicos del área de T.I.
    - Coordinar actividades del Área de Tecnología de la Información.
    - Elaborar, controlar y dar seguimiento a la documentación interna y externa del departamento de Tecnología de la Información.
    - Registrar y coordinar la agenda de la Gerencia.
    - Mantener y organizar el archivo físico del área.
    - Tramitar los procedimientos logísticos administrativos del área.

- **Especialista de Administración de Aplicativos:**
    - Administrar y realizar soporte de los aplicativos del Grupo Empresarial HOLDINGDINE: ADAM (Todas las empresas), SIAF (Sepriv), SIAF (ENERGYHDINE), Evaluación Desempeño (Todas las empresas), Evaluación de competencias (Todas las empresas), STRATEGYLINK (Todas las empresas), 9000DOC (Todas las empresas), INSOFT (SSFT Y COSSFA).
    - Coordinar la implementación y mantenimiento de los aplicativos del Grupo Empresarial HOLDINGDINE.
    - Dirigir planes y proyectos necesarios para el funcionamiento de los aplicativos del Grupo Empresarial HOLDINGDINE.
    - Coordinar y organizar la ejecución de manuales, procedimientos, normativas y políticas de seguridad de aplicativos.
    - Coordinar y controlar los servicios recibidos de los diferentes proveedores de aplicativos.
    - Recomendar y asesorar en soluciones tecnológicas en aplicativos a las autoridades y Grupo Empresarial HOLDINGDINE.
    - Realizar planes de contingencia, políticas corporativas del proceso de aplicativos.
    - Dirigir y supervisar las actividades del equipo a su cargo en los planes y proyectos a ejecutarse.

- **Técnico de Aplicativos:**
    - Administrar, soporte, analizar y configurar los aplicativos del Grupo Empresarial HOLDINGDINE: BAAN Módulos Logística, Inventarios, Ventas (FabrilFame, Fmsb Santa Bárbara, ANDEC y HOLDINGDINE).
    - Administrar y coordinar el mantenimiento de los aplicativos acorde con el avance del negocio.
    - Brindar soporte técnico a los aplicativos del Grupo Empresarial HOLDINGDINE.
    - Ejecutar y documentar planes de contingencia, políticas corporativas del proceso de aplicativos.
    - Realizar y mantener un esquema de implementación de aplicativos.
    - Detectar y analizar requerimientos de aplicativos para la implementación en el Grupo Empresarial HOLDINGDINE.

- **Asistente de Administración de Aplicativos:**
    - Webmaster.
    - Desarrollar, administrar y mantener los sitios WEB, portales, intranet de todas las empresas del Grupo.
    - Ejecutar las políticas de respaldos de información de los aplicativos WEB.
    - Administrar, soporte, analizar y configurar los aplicativos del Grupo Empresarial HOLDINGDINE: ASINFO (Aychapicho Agro's, Dinmob).

- **Especialista de Redes y Comunicaciones:**
    - Evaluar y organizar la red corporativa de comunicaciones.
    - Coordinar la implementación y mantenimiento de las en redes y Comunicaciones del grupo empresarial HOLDINGDINE.
    - Administrar la infraestructura Corporativa Tecnológica.
    - Diseñar y controlar planes y proyectos necesarios para el funcionamiento del Servicio de Comunicaciones del grupo empresarial HOLDINGDINE.
    - Dirigir e integrar planes de contingencia, políticas corporativas del proceso de redes y Comunicaciones para difusión al grupo empresarial HOLDINGDINE.
    - Recomendar y asesorar en soluciones Tecnológicas en redes y comunicaciones a las autoridades y al grupo empresarial HOLDINGDINE.
    - Gerenciar planes y proyectos de redes y comunicaciones en el Grupo HOLDINGDINE.
    - Gestión de administración de Seguridades (Todas las empresas).
    - Gestión de administración de Video Conferencia.
    - Brindar soporte técnico en redes y comunicaciones al grupo empresarial HOLDINGDINE.
    - Administrar el Sistema de control de correspondencia del HOLDINGDINE.
    - Administrar el aplicativo XASS Y BANAXASS (Hdineagro's).
    - Administrar el servicio de "HELP DESK" de todas las empresas del Grupo.

- **Técnico de Redes y Comunicaciones:**
    - Analizar, configurar y actualizar los equipos y redes de comunicación del grupo empresarial HOLDINGDINE.
    - Ejecutar actividades de instalación en redes y comunicaciones.
    - Detectar, reportar y controlar riesgos a los que está expuesto la infraestructura de telecomunicaciones y redes.
    - Brindar soporte técnico en redes y comunicaciones al grupo empresarial HOLDINGDINE.
    - Realizar y controlar los inventarios de los equipos y dispositivos de comunicación del grupo empresarial HOLDINGDINE.
    - Realizar, ejecutar y documentar planes de contingencia, políticas corporativas del proceso de redes y comunicaciones.
    - Garantizar la disponibilidad de los servicios de datos e internet.

- **Especialista de Base de Datos:**
    - Administrar y controlar el desempeño de las Bases de Datos de la Corporación.
    - Diseñar y controlar planes y proyectos necesarios para el funcionamiento del servicio de base de datos del Grupo Empresarial HOLDINGDINE.
    - Liderar e integrar planes de contingencia, políticas corporativas para difusión al grupo empresarial HOLDINGDINE.

- Liderar y supervisar las actividades del equipo a su cargo en los planes y proyectos a ejecutarse.
- Administrar, soporte, analizar y configurar los aplicativos del Grupo Empresarial HOLDINGDINE: BAAN Módulos: Producción, Planificación y Proyectos (FabrilFame, Fmsb Santa Bárbara, ANDEC y HOLDINGDINE).

- **Técnico de Base de Datos:**
  - Supervisar, analizar y configurar las bases de datos del Grupo Empresarial HOLDINGDINE.
  - Coordinar y ejecutar actividades de respaldos de las bases de datos.
  - Brindar soporte técnico en administración de la base de datos al Grupo Empresarial HOLDINGDINE.
  - Realizar y mantener un esquema de seguridades de la base de datos.
  - Administrar, soporte, analizar y configurar los aplicativos del Grupo Empresarial HOLDINGDINE: BAAN Módulos: Contabilidad, Tesorería, Presupuesto (FabrilFame, Fmsb Santa Bárbara, ANDEC y HOLDINGDINE), Venture (Explocen)[99][100].

[99] Composición Funcional de la unidad de apoyo Gerencia de TI: Fuente, Gerencia TI de la Corporación HOLDINGDINE S.A.

3.1.6. Características de los Sistemas y Ambiente Computarizado

El 02 de mayo de 2008 arrancó en tiempo real el ***Proyecto Integración Tecnológica Corporativa (ITC)***, con su slogan "Comprometidos con la Excelencia Empresarial", en el HOLDINGDINE S.A.; a fin de contar con información oportuna y en línea de las áreas: Financieras, Manufactureras, Logísticas, Comercialización, Talento Humano y Mantenimiento. Para la ejecución del ITC, el HOLDINGDINE S.A., implementó el Enterprise Resource Planning (ERP) llamado ***Baan 5***, que se complementó con dos software empresariales: el ***Qlik View*** y el ***ADAM 3.0.***; facilitando la planificación de los recursos, el control y la gestión de la Corporación.

El ***Baan 5*** es una herramienta de recursos empresariales que integra las funciones y automatiza los procesos del negocio: finanzas (contabilidad general, cuentas por cobrar y por pagar, administración de activos, tesorería, presupuestos, facturación); manufactura (listas de materiales, rutas, cálculo de costos, procesos, requerimientos de herramientas y clasificación de productos); logística (clasificación de proveedores, cotizaciones, licitaciones, contratos, calendarios de compra); ventas (precios, contratos, calendarios de venta); gestión de la calidad; proyectos; entre otros.

El ***Baan 5*** es una solución flexible, con una arquitectura tecnológica compatible con otras plataformas; también contribuye a que toda transacción efectuada se registre desde su captura en una sola base de datos, viabilizando la consulta en línea de información relevante: capacidad de producción, relación entre lo elaborado y los medios empleados, ahorro en costos operativos, atención a clientes, gestión administrativa; más aún, posibilita visualizar y controlar las operaciones.

En este sentido, la información que suministra el ***Baan 5*** permite examinar atentamente el estado de las empresas y tomar decisiones en el momento apropiado. La implementación del ***Bann 5*** fue un proceso largo, de alto riesgo y complejo, porque implicó rediseñar los esquemas de trabajo optimizar los recursos existentes, invertir en un sistema de soporte de negocio y capacitar a los usuarios claves y finales en el uso de las nuevas herramientas tecnológicas, a fin de obtener ventajas competitivas frente a otras compañías. Además, demandó el involucramiento permanente de los técnicos tanto de las empresas participantes como de la consultora Novatech.

El ***Qlik View*** es una herramienta de inteligencia de negocios orientado a ejecutar reportes de resultados consolidados en forma gráfica. El aplicativo favorece el acceso a la información inmediata y apoya a la realización de los análisis respectivos para la toma de decisiones.

El ***ADAM 3.0.***, es un sistema que contribuye a la función estratégica de la Gerencia de Talento Humano para una eficiente administración del personal en la Corporación. Está desarrollado en una plataforma tecnológica conformada por dos módulos:

- ***Módulo de Operación Básica:*** optimiza al máximo los recursos económicos y facilita las funciones técnicas de la Gerencia de Talento Humano en los procesos y actividades que intervienen para el manejo de nómina, préstamos, planificación de vacaciones de los colaboradores, reportes con respecto al pago del Impuesto a la Renta, aportes personales al Seguro Social Ecuatoriano, entre otros.

- ***Módulo de Operación de gestión:*** está orientado a la administración del talento humano desde la selección, contratación, ingreso de los colaboradores hasta la trayectoria laboral (desempeño, capacitación, evaluación, entre otros). Este modulo está compuesto de ocho aplicativos: Inventario de Recursos Humanos, Estructura Organizacional, Capacitación, Selección de personal, Administración de sueldos y salarios, Valuación de puestos y Desarrollo del personal.

También dentro de la Corporación HOLDINGDINE S.A., se cuenta con aplicativos corporativos de gestión como:

- ***Balanced Scoredcard***

  BSC (Balanced Scorecard) es una sigla que se traduce al español como "Indicadores Balanceados de Desempeño", esta metodología se deriva de la gestión estratégica del Grupo Empresarial y acepta una elección de indicadores que no debe ser restringida al área económico – financiera. Así como no es posible comandar un avión controlando apenas la velocidad, los indicadores financieros no son suficientes para garantizar que el Grupo Empresarial se dirija en la dirección correcta. Por estos motivos, será necesario monitorear, junto a los indicadores económicos – financieros, el desempeño de mercado, los procesos internos, la innovación y la tecnología. De este modo, los resultados financieros serán fruto de la sumatoria de acciones generadas por personas a través del uso de las mejores tecnologías, vinculación a las mejores prácticas y los procesos internos de la organización, todo esto en armonía con la Propuesta de Valor ofrecida al cliente, esto proceso se denomina "crear valor a través de activos intangibles".

Balanced Scorecard ofrece una visión integrada y balanceada de la empresa y permite desarrollar la estrategia en forma clara. Esto se logra a través de objetivos estratégicos identificados en 4 perspectivas: financiera, clientes, procesos internos y aprendizaje e innovación. Cada una de las perspectivas se vincula con las demás mediante relaciones de causa y efecto. BSC promueve, además, el alineamiento de los objetivos estratégicos con indicadores de desempeño, metas y planes de acción para hacer posible la generación de estrategias en forma integrada y garantizar que los esfuerzos de la organización se encuentren en línea con las mismas. (Figura 3.5.)

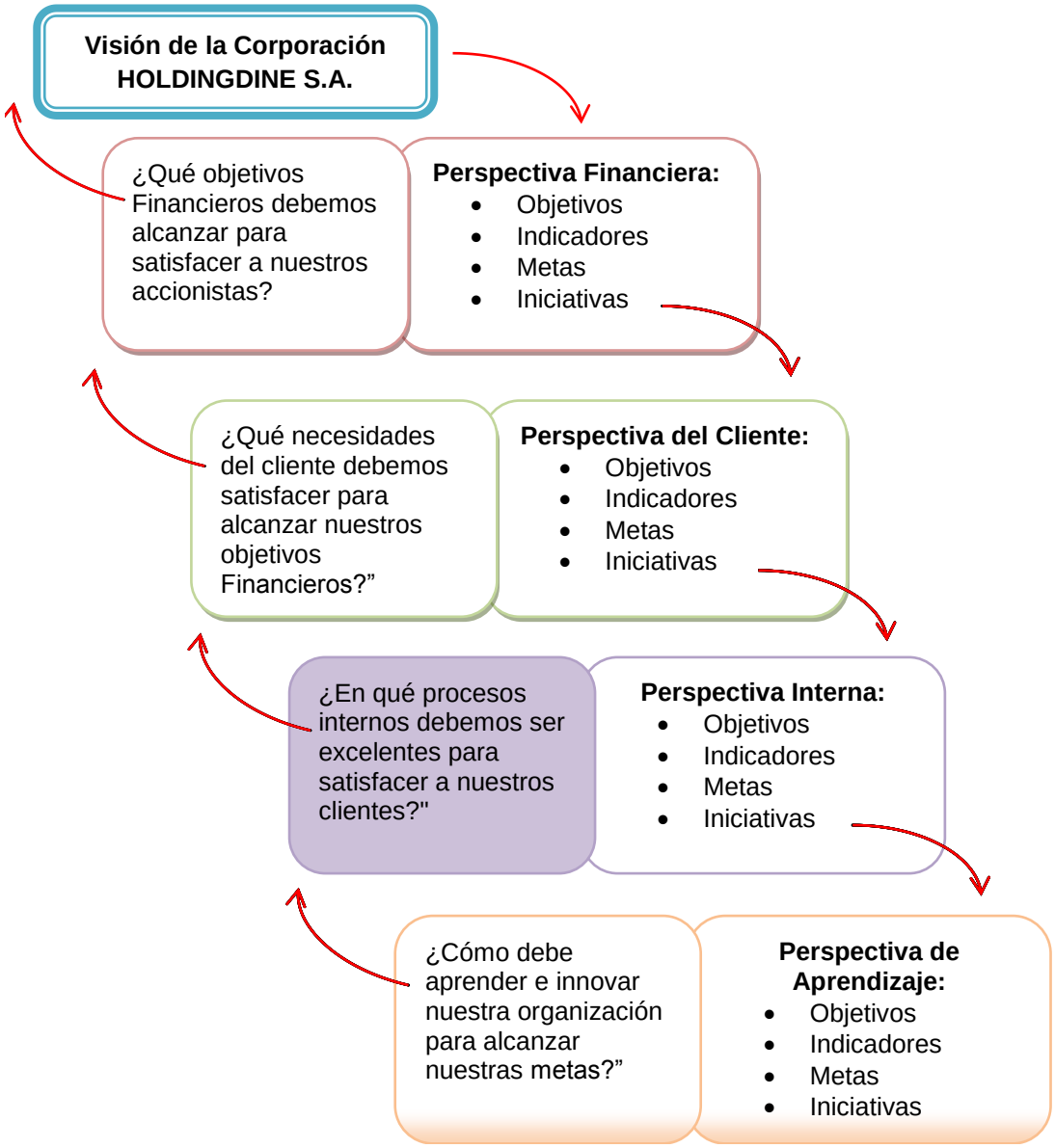


Figura 3.5. Las cuatro perspectivas del negocio.

- ***DOC9000***

  Es un software de control de documentos, parte de la familia JKT9000 de la calidad de los módulos de software de gestión, este se presenta como una solución rentable y eficiente a un problema complejo de papeleo; DOC9000 se implementó en la Corporación para ayudar a cumplir con las normas de gestión tales como ISO 9000, ISO 14000, ISO 27000.

- ***StrategyLink***

  Es una solución de ERM, Employee Relationship Management, este software han sido diseñado para ayudar a alinear el desempeño y esfuerzo del recurso humano de la Corporación con la estrategia y objetivos empresariales, a través del uso del método de Balanced Scorecard y mediante el desarrollo de destrezas y comportamiento clave permitiendo administrar los tres fundamentos del desempeño del recurso humano: alineamiento, productividad y satisfacción. StrategyLink provee una solución que cubre todos los aspectos gerenciales de Recursos Humanos, incluyendo la administración de desempeño, competencias, evaluaciones de 360 grados, verificaciones técnicas, capacitación, reclutamiento y contratación, planeación de carrera, satisfacción del empleado y satisfacción del cliente.

En cuanto al ambiente computarizado dentro de la Corporación HOLDINGDINE S.A. (Matriz) está presente una tecnología cliente/servidor con el uso de software propietario, mas no se utiliza en ninguna área software libre, se maneja versiones de Windows XP, Windows 7, base de datos SQL Server 2005, Oracle 10.5g y Oracle 11g.

3.2. Aplicación del Modelo COBIT 4.1., en la Corporación HOLDINGDINE S.A. (Matriz)

3.2.1. Justificación

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 deberá optimizar el empleo de sus recursos disponibles, los cuales incluyen: 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 las actividades van por el camino equivocado.

La Gerencia TI debe asegurar que los sistemas de control interno o el marco referencial están funcionando y soportan los procesos del negocio, y debe de ser consciente de cómo cada actividad individual de control satisface los requerimientos de información e impacta los recursos de TI.

El impacto sobre los recursos de TI son resaltados en el Marco de Referencia de COBIT 4.1., junto con los requerimientos del negocio que deben ser alcanzados con: eficiencia, efectividad, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de la información.

3.2.2. Planificación de la Evaluación Técnica Informática en la Corporación HOLDINGDINE S.A. (Matriz)

En la tabla 3.1., se detalla cada una de las tareas y el tiempo estimado para la realización del plan de investigación de campo o programa de auditoría.

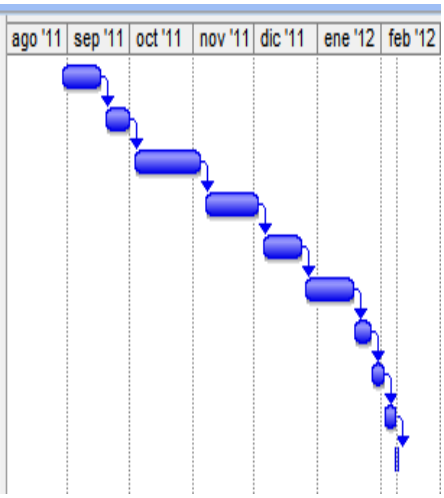
Tabla 3.1. Plan de Investigación de Campo

	Nombre de tarea	Duración	Comienzo	Fin
1	Elaboración plan de investigación de campo	15 días	lun 29/08/11	vie 16/09/11
2	Determinación de instrumentos de investigación de campo	10 días	lun 19/09/11	vie 30/09/11
3	Recopilación info. Sistema de infromación	25 días	lun 03/10/11	vie 04/11/11
4	Análisis de la información	20 días	lun 07/11/11	vie 02/12/11
5	Determinación de los niveles de madurez	15 días	lun 05/12/11	vie 23/12/11
6	Verificación de observaciones	18 días	lun 26/12/11	mié 18/01/12
7	Elaboración del informe detallado	6 días	jue 19/01/12	jue 26/01/12
8	Validación del informe detallado	5 días	vie 27/01/12	jue 02/02/12
9	Elaboración informe final/ejecutivo	3 días	vie 03/02/12	mar 07/02/12
10	Entrega de los informes detallado y final/ejecutivo	1 día	mié 08/02/12	mié 08/02/12

En la tabla 3.2., mediante el diagrama de Gantt, se presenta el cronograma de tareas y la duración total del desarrollo del plan de investigación de campo o programa de auditoría.

Tabla 3.2. Diagrama de Gantt.

	Nombre de tarea	Duración	Comienzo	Fin
1	Elaboración plan de investigación de campo	15 días	lun 29/08/11	vie 16/09/11
2	Determinación de instrumentos de investigación de campo	10 días	lun 19/09/11	vie 30/09/11
3	Recopilación info. Sistema de infromación	25 días	lun 03/10/11	vie 04/11/11
4	Análisis de la información	20 días	lun 07/11/11	vie 02/12/11
5	Determinación de los niveles de madurez	15 días	lun 05/12/11	vie 23/12/11
6	Verificación de observaciones	18 días	lun 26/12/11	mié 18/01/12
7	Elaboración del informe detallado	6 días	jue 19/01/12	jue 26/01/12
8	Validación del informe detallado	5 días	vie 27/01/12	jue 02/02/12
9	Elaboración informe final/ejecutivo	3 días	vie 03/02/12	mar 07/02/12
10	Entrega de los informes detallado y final/ejecutivo	1 día	mié 08/02/12	mié 08/02/12



3.2.3. Objetivos

- Realizar una Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), utilizando el Estándar Internacional COBIT, a fin de identificar debilidades y emitir recomendaciones dentro del ambiente informático, que permitirá eliminar o minimizar los riesgos más críticos en los procesos y actividades TI.

- Utilizar el Marco de Referencia del Modelo COBIT 4.1., para:
    - Elaborar un plan de investigación de campo o programa de auditoría.
    - Determinar los instrumentos necesarios para la investigación de campo o programa de auditoría.
    - Recopilar información detalla de la situación actual del sistema de información de la Corporación HOLDINGDINE S.A. (Matriz).
    - Realizar el análisis de la información.

- Determinar los niveles de madurez.
- Verificar las observaciones.
- Elaborar el informe detallado.
- Validar el informe detallado.
- Elaborar un informe final/ejecutivo.

3.2.4. Alcance

El plan de investigación de campo tiene por objetivo una Evaluación Técnica Informática al Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), localizada en la Av. Coruña E25-58 y San Ignacio, Edificio Altana Plaza, 6to y 7mo piso, en la ciudad de Quito.

Para iniciar, se realizará un estudio general de la situación actual de la Gerencia TI de la Corporación, para identificar las normas, políticas, estructuras y funciones que se manejan internamente, así como la manera en la que éstas se apoyan para cumplir con los objetivos organizacionales. Posteriormente se analizará de forma minuciosa con el gerente y especialistas de TI, cuales son los procesos y actividades más críticos que necesitan ser auditados y/o evaluados, mediante la elaboración de una Matriz de Riesgos TI teniendo como marco de referencia al Modelo COBIT 4.1., para así satisfacer las necesidades actuales y vigentes de la Corporación, a fin de proporcionar una información real y apropiada al staff ejecutivo de manera eficiente, efectiva y eficaz.

La Matriz de Riesgos TI se utilizará como herramienta de control y de gestión, para identificar el nivel de riesgo, nivel de impacto y documentación referente de los procesos y actividades más críticos dentro del Sistema de Información de la Corporación.

A continuación se desarrollará el plan de investigación de campo, utilizando el Estándar Internacional Objetivos de Control para la Información y Tecnologías (COBIT), como un medio de control de TI, ya que está basado en criterios de negocios, documentado por objetivos de control, organizado en dominios, procesos y actividades TI.

COBIT provee 34 objetivos de control agrupados en cuatro dominios:

- Planificación y Organización.
- Adquisición e Implementación.
- Entrega y Soporte.
- Monitoreo y Evaluación.

En base al Modelo COBIT 4.1., se examinará los procesos y actividades más críticos, objetivas de control seleccionados para cada dominio y se evaluará las funciones del Sistema de Información de la Corporación en función a cada objetivo de control. Al finalizar, se entregará un informe en donde se detalla conclusiones y recomendaciones orientadas a una mejora continua por parte del auditor/evaluador.

3.2.5. Elaboración del Plan de Investigación de Campo

3.2.5.1. Matriz de Riesgos Críticos TI

La tabla 3.3., que se observa a continuación, resume los procesos y actividades más críticos por dominio en base al Modelo COBIT 4.1., que se han identificado en la Matriz de Riesgos del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz). **Ver CD Anexos → Documento "ANEXO B.docx"**

Los procesos y actividades más críticos fueron discutidos y puestos en conocimiento al tutor designado por la Gerencia TI, Ing. Paulina Porras – Especialista de Redes y Comunicaciones. A continuación consta el Acta de Reunión.

Tabla 3.3. Matriz de Riesgos Críticos TI del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz).

MATRIZ DE RIESGOS CRÍTICOS TI DEL SISTEMA DE INFORMACIÓN DE LA CORPORACIÓN HOLDINGDINE S.A. (MATRIZ)										
PROCESOS Y ACTIVIDADES	**Nivel de Riesgo**			**Nivel de Impacto**			**Auditable**		**Documentación Actualizada**	
	Alto	Medio	Bajo	Alto	Medio	Bajo	SI	NO	SI	NO
Dominio: Planear y Organizar (PO)										
PO1 Definir un plan estratégico de TI										**Fuente: Gerencia TI**
PO1.4 Plan estratégico de TI	X			X			X			X
PO1.5 Planes tácticos de TI	X			X			X			X
PO2 Definir la arquitectura de la información										**Fuente: Área de Redes y Comunicaciones TI**
PO2.1 Modelo de arquitectura de información empresarial	X			X			X			X
PO2.4 Administración de la integridad	X			X			X			X
PO3 Determinar la dirección tecnológica										**Fuente: Gerencia TI**
PO3.1 Planeación de la dirección tecnológica	X			X			X			X
PO3.2 Plan de infraestructura tecnológica	X			X			X			X
PO4 Definir los procesos, organización y relaciones de TI										**Fuente: Gerencia TI**
PO4.3 Comité directivo de TI	X				X		X			X
PO4.4 Ubicación organizacional de la función de TI	X				X		X		X	
PO5 Administrar la inversión en TI										**Fuente: Gerencia TI**
PO5.1 Marco de trabajo para la administración financiera	X				X		X			X
PO5.4 Administración de costos de TI	X			X			X			X
PO6 Comunicar las aspiraciones y la dirección de la gerencia										**Fuente: Gerencia TI**

PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI	X			X			X			X
PO6.5 Comunicación de los objetivos y la dirección de TI	X			X			X			X
PO7 Administrar recursos humanos de TI										**Fuente: Gerencia TI**
PO7.2 Competencias del personal	X			X			X			X
PO7.4 Entrenamiento del personal de TI	X			X			X			X
PO7.7 Evaluación del desempeño del empleado	X			X			X			X
PO8 Administrar la calidad										**Fuente: Gerencia TI**
PO8.1 Sistema de administración de calidad	X			X			X			X
PO9 Evaluar y administrar los riesgos de TI										**Fuente: Gerencia TI**
PO9.1 Marco de trabajo de administración de riesgos	X			X			X			X
PO10 Administrar proyectos										**Fuente: Gerencia TI**
P010.2 Marco de trabajo para la administración de proyectos	X			X			X			X
Dominio: Adquirir e Implementar (AI)										
AI1 Identificar soluciones automatizadas										**Fuente: Área de Redes y Comunicaciones TI**
AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales de negocio	X			X			X			X
AI1.2 Reporte de Análisis de Riesgos	X			X			X			X
AI2 Adquirir y mantener software aplicativo										**Fuente: Área de Aplicativos TI**
AI2.5 Configuración e implantación de software aplicativo adquirido	X			X			X			X
AI2.8 Aseguramiento de la calidad del software	X			X			X			X
AI3 Adquirir y mantener infraestructura tecnológica										**Fuente: Área de Redes y Comunicaciones TI**
AI3.1 Plan de adquisición de infraestructura tecnológica		X		X			X			X
AI3.3 Mantenimiento de la Infraestructura	X			X			X			X
AI4 Facilitar la operación y el uso										**Fuente: Área de BD TI**
AI4.1 Plan para soluciones de operación	X			X			X			X
AI4.2 Transferencia de conocimiento a la gerencia del negocio		X		X			X			X
AI5 Adquirir recursos de TI										**Fuente: Área de BD TI**

AI5.1 Control de adquisición		X			X		X			X
Dominio: Entregar y Dar Soporte (DS)										
DS1 Definir y administrar los niveles de servicio										**Fuente: Área de Redes y Comunicaciones TI**
DS1.2 Definición de servicios	X			X			X			X
DS2 Administrar los servicios de terceros										**Fuente: Área de Redes y Comunicaciones TI**
DS2.1 Identificación de todas las relaciones con proveedores		X			X		X			X
DS3 Administrar el desempeño y la capacidad										**Fuente: Área de Redes y Comunicaciones TI**
DS3.1 Planeación del desempeño y la capacidad		X		X			X			X
DS3.5 Monitoreo y reporte		X		X			X			X
DS4 Garantizar la continuidad del servicio										**Fuente: Área de Redes y Comunicaciones TI**
DS4.1 Marco de trabajo de continuidad de TI	X			X			X			X
DS4.3 Recursos críticos de TI	X			X			X			X
DS5 Garantizar la seguridad de los sistemas										**Fuente: Área de Redes y Comunicaciones TI**
DS5.2 Plan de seguridad de TI	X			X			X			X
DS6 Identificar y asignar costos										**Fuente: Gerencia TI**
DS6.1 Definición de servicios		X			X		X			X
DS6.3 Modelación de costos y cargos		X			X		X			X
DS8 Administrar la mesa de servicio y los incidentes										**Fuente: Área de Redes y Comunicaciones TI**
DS8.1 Mesa de servicios	X			X			X			X
DS8.5 Análisis de tendencias	X			X			X			X
DS10 Administración de problemas										**Fuente: Área de Redes y Comunicaciones TI**
DS10.1 Identificación y clasificación de problemas	X			X			X			X
DS10.2 Rastreo y resolución de problemas	X			X			X			X
DS11 Administrar los datos										**Fuente: Área de BD TI**
DS11.1 Requerimientos del negocio para administración de datos		X		X			X			X
DS11.2 Acuerdos de almacenamiento y conservación	X			X			X			X

DS12 Administración del ambiente físico									**Fuente: Área de Redes y Comunicaciones TI**	
DS12.2 Medidas de seguridad física	X			X			X			X
Dominio: Monitorear y Evaluar (ME)										
ME1 Monitorear y evaluar el desempeño de TI									**Fuente: Gerencia TI**	
ME1.3 Método de monitoreo	X			X			X			X
ME1.5 Reportes al consejo directivo y a ejecutivos	X			X			X			X
ME2 Monitorear y evaluar el control interno									**Fuente: Gerencia TI**	
ME2.1 Monitoreo del marco de trabajo de control interno		X		X			X			X
ME2.2 Revisiones de Auditoría	X			X			X			X
ME2.4 Auto evaluación del control		X			X		X			X
ME3 Garantizar el cumplimiento con requerimientos externos									**Fuente: Gerencia TI**	
ME3.3 Evaluación del cumplimiento con requerimientos externos	X			X			X			X
ME4 Proporcionar gobierno de TI									**Fuente: Gerencia TI**	
ME4.1 Establecimiento de un marco de gobierno de TI	X			X			X			X

Partiendo de la Matriz de Riesgos Críticos TI, se va estructurando el plan de investigación de campo que se observa en la sección 3.2.5.3.

3.2.5.2. Determinación de Recursos a utilizar para el desarrollo del Plan de Investigación de Campo

Para el plan de investigación de campo o programa de auditoría se utilizó recursos humanos, de evidencia y tecnológicos como:

- **Recurso Humano:** Auditor/Evaluador, persona que recopila, sistematiza y analiza la información, debe conocer la metodología de auditoría como también el modelo COBIT y su aplicación. Para este plan de investigación de campo se ha designado al Sr. Andrés Patricio Naveda Paredes como único evaluador.
- **Recursos 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. **Ver CD Anexos → Documento "ANEXO C.docx".**
    - **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. **Ver CD Anexos → Documento "ANEXO D.docx".**
    - **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. **Ver CD Anexos → Documento "ANEXO E.docx".**

- **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. **Ver CD Anexos → Documento "ANEXO F.docx".**
- **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. **Ver CD Anexos → Documento "ANEXO G.docx".**

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

3.2.5.3. Plan de Investigación de Campo

Tabla 3.4. Plan de Investigación de Campo del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz).

Plan de Investigación de Campo del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz)							
Dominio: Planear y Organizar (PO)		**Pruebas de Control**					
Objetivos de Control / Procesos de Control	**Actividades de Control**	**Revisión del Control**	**Ambiente del Control**	**Documentación de Referencia**	**Criterio de la Prueba de Control**	**Instrumento Investigación de Campo**	**Fuente**
PO1 Definir un plan estratégico de TI							
PO1.4 Plan estratégico de TI	Crear un plan estratégico, en cooperación con la TI, que contribuirá a los objetivos estratégicos de la empresa así como los costos y riesgos relacionados.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO1.4	Cuestionario No.1	Gerente TI
PO1.5 Planes tácticos de TI	Crear un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por TI.	No existe revisión	No existe actividad de control	No	Verificar PO1.5	Cuestionario No.2	Gerente TI
PO2 Definir la arquitectura de la información							
PO2.1 Modelo de arquitectura de información empresarial	Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO2.1	Cuestionario No.3	Especialista de Redes y Comunicaciones TI

PO2.4 Administración de la integridad	Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico.	Anualmente	Manual	No	Verificar PO2.4	Prueba de Cumplimiento No.1	Especialista TI de Redes y Comunicaciones TI
PO3 Determinar la dirección tecnológica							
PO3.1 Planeación de la dirección tecnológica	Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO3.1	Cuestionario No.4	Gerente TI
PO3.2 Plan de infraestructura tecnológica	Crear y mantener un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO3.2	Cuestionario No.5	Gerente TI
PO4 Definir los procesos, organización y relaciones de TI							
PO4.3 Comité directivo de TI	Establecer un comité directivo compuesto por la gerencia ejecutiva del negocio y de TI para determinar las prioridades de los programas de inversión de TI.	Trimestralmente	Manual	No	Verificar PO4.3	CheckList No.1	Gerente TI
PO4.4 Ubicación organizacional de la función de TI	Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa.	Anualmente	Manual	En formato digital	Verificar PO4.4	CheckList No.2	Gerente TI
PO5 Administrar la inversión en TI							
PO5.1 Marco de trabajo para la administración financiera	Establecer un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos.	Semestralmente	Manual	No	Verificar PO5.1	Cuestionario No.6	Gerente TI

PO5.4 Administración de costos de TI	Implantar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO5.4	Prueba Sustantiva No.1	Gerente TI
PO6 Comunicar las aspiraciones y la dirección de la gerencia							
PO6.2 Riesgo Corporativo y Marco de Referencia de Control Interno de TI	Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno.	Semestralmente	Manual	No	Verificar PO6.2	Cuestionario No.7	Gerente TI
PO6.5 Comunicación de los objetivos y la dirección de TI	Asegurar de que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización.	Anualmente	Manual	No	Verificar PO6.5	Observación Directa No.1	Gerente TI
PO7 Administrar recursos humanos de TI							
PO7.2 Competencias del personal	Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia.	Anualmente	Manual	En formato digital e impreso, está desorganizada	Verificar PO7.2	Prueba de Cumplimiento No.2	Gerente TI
PO7.4 Entrenamiento del personal de TI	Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO7.4	Prueba de Cumplimiento No.3	Gerente TI
PO7.7 Evaluación del desempeño del empleado	Evaluar el desempeño del empleado periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto.	Anualmente	Manual	En formato digital e impreso, está desorganizada	Verificar PO7.7	Observación Directa No.2	Gerente TI
PO8 Administrar la calidad							

PO8.1 Sistema de administración de calidad	Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio.	No existe revisión	No existe actividad de control	No	Verificar PO8.1	CheckList No.3	Gerente TI
PO9 Evaluar y administrar los riesgos de TI							
PO9.1 Marco de trabajo de administración de riesgos	Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar PO9.1	CheckList No.4	Gerente TI
PO10 Administrar proyectos							
P010.2 Marco de trabajo para la administración de proyectos	Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos.	Anualmente	Manual	Escasa	Verificar PO10.2	CheckList No.5	Gerente TI

Plan de Investigación de Campo de la Corporación HOLDINGDINE S.A.							
Dominio: Adquirir e Implementar (AI)		**Pruebas de Control**					
Objetivos de Control / Procesos de Control	**Actividades de Control**	**Revisión del Control**	**Ambiente del Control**	**Documentación de Referencia**	**Criterio de la Prueba de Control**	**Instrumento Investigación de Campo**	**Fuente**
AI1 Identificar soluciones automatizadas							
AI1.1 Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio	Identificar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar AI1.1	Cuestionario No.8	Técnico de Redes y Comunicaciones TI

AI1.2 Reporte de Análisis de Riesgos	Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos.	Anualmente	Manual	No	Verificar AI1.2	CheckList No.6	Técnico de Redes y Comunicaciones TI
AI2 Adquirir y mantener software aplicativo							
AI2.5 Configuración e implantación de software aplicativo adquirido	Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar AI2.5	Prueba Sustantiva No.2	Especialista de Administración de Aplicativos TI
AI2.8 Aseguramiento de la calidad del software	Desarrollar, implantar y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en los requerimientos y en las políticas de la organización.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar AI2.8	Cuestionario No.9	Especialista de Administración de Aplicativos TI
AI3 Adquirir y mantener infraestructura tecnológica							
AI3.1 Plan de adquisición de infraestructura tecnológica	Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar AI3.1	Cuestionario No.10	Técnico de Redes y Comunicaciones TI
AI3.3 Mantenimiento de la Infraestructura	Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar AI3.3	Cuestionario No.11	Técnico de Redes y Comunicaciones TI
AI4 Facilitar la operación y el uso							
AI4.1 Plan para soluciones de operación	Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar AI4.1	CheckList No.7	Técnico de BD TI

AI4.2 Transferencia de conocimiento a la gerencia del negocio	Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos, y ejercer la responsabilidad por la entrega y calidad del servicio.	No existe revisión	No existe actividad de control	No	Verificar AI4.2	Prueba de Cumplimiento No.4	Técnico de BD TI
AI5 Adquirir recursos de TI							
AI5.1 Control de adquisición	Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar AI5.1	Prueba Sustantiva No.3	Técnico de BD TI

Plan de Investigación de Campo de la Corporación HOLDINGDINE S.A.							
Dominio: Entregar y Dar Soporte (DS)		**Pruebas de Control**					
Objetivos de Control / Procesos de Control	**Actividades de Control**	**Revisión del Control**	**Ambiente del Control**	**Documentación de Referencia**	**Criterio de la Prueba de Control**	**Instrumento Investigación de Campo**	**Fuente**
DS1 Definir y administrar los niveles de servicio							
DS1.2 Definición de servicios	Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar DS1.2	Cuestionario No.12	Técnico de Redes y Comunicaciones TI
DS2 Administrar los servicios de terceros							
DS2.1 Identificación de todas las relaciones con proveedores	Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar DS2.1	Prueba Sustantiva No.4	Especialista de Redes y Comunicaciones TI
DS3 Administrar el desempeño y la capacidad							

DS3.1 Planeación del desempeño y la capacidad	Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño.	No existe revisión	No existe actividad de control	No	Verificar DS3.1	Prueba de Cumplimiento No.5	Especialista de Redes y Comunicaciones TI
DS3.5 Monitoreo y reporte	Monitorear continuamente el desempeño y la capacidad de los recursos de TI.	Trimestralmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS3.5	CheckList No.8	Técnico de Redes y Comunicaciones TI
DS4 Garantizar la continuidad del servicio							
DS4.1 Marco de trabajo de continuidad de TI	Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización.	No existe revisión	No existe actividad de control	No	Verificar DS4.1	Cuestionario No.13	Técnico de Redes y Comunicaciones TI
DS4.3 Recursos críticos de TI	Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación.	No existe revisión	No existe actividad de control	No	Verificar DS4.3	Cuestionario No.14	Técnico de Redes y Comunicaciones TI
DS5 Garantizar la seguridad de los sistemas							
DS5.2 Plan de seguridad de TI	Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar DS5.2	CheckList No.9	Técnico de Redes y Comunicaciones TI
DS6 Identificar y asignar costos							
DS6.1 Definición de servicios	Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar DS6.1	CheckList No.10	Gerente TI

DS6.3 Modelación de costos y cargos	Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar DS6.3	CheckList No.11	Gerente TI
DS8 Administrar la mesa de servicio y los incidentes							
DS8.1 Mesa de servicios	Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS8.1	Prueba Sustantiva No.5	Especialista de Redes y Comunicaciones TI
DS8.5 Análisis de tendencias	Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta.	Trimestralmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS8.5	Prueba de Cumplimiento No.6	Especialista de Redes y Comunicaciones TI
DS10 Administración de problemas							
DS10.1 Identificación y clasificación de problemas	Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS10.1	CheckList No.12	Técnico de Redes y Comunicaciones TI
DS10.2 Rastreo y resolución de problemas	El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS10.2	CheckList No.13	Técnico de Redes y Comunicaciones TI
DS11 Administrar los datos							
DS11.1 Requerimientos del negocio para administración de datos	Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS11.1	Observación Directa No.3	Técnico de BD TI

DS11.2 Acuerdos de almacenamiento y conservación	Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS11.2	Observación Directa No.4	Técnico de BD TI
DS12 Administración del ambiente físico							
DS12.2 Medidas de seguridad física	Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio.	Anualmente	Automatizado	En formato digital, está incompleta y desactualizada	Verificar DS12.2	CheckList No.14	Técnico de Redes y Comunicaciones TI

Plan de Investigación de Campo de la Corporación HOLDINGDINE S.A.							
Dominio: Monitorear y Evaluar (ME)		**Pruebas de Control**					
Objetivos de Control / Procesos de Control	**Actividades de Control**	**Revisión del Control**	**Ambiente del Control**	**Documentación de Referencia**	**Criterio de la Prueba de Control**	**Instrumento Investigación de Campo**	**Fuente**
ME1 Monitorear y evaluar el desempeño de TI							
ME1.3 Método de monitoreo	Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa.	Semestralmente	Automatizado	En formato digital	Verificar ME1.3	Prueba de Cumplimiento No.7	Gerente TI
ME1.5 Reportes al consejo directivo y a ejecutivos	Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas.	Semestralmente	Manual	En formato digital, está incompleta y desactualizada	Verificar ME1.5	Cuestionario No.15	Gerente TI
ME2 Monitorear y evaluar el control interno							

ME2.1 Monitoreo del marco de trabajo de control interno	Monitorear de forma continua el ambiente de control y el marco de control de TI.	No existe revisión	No existe actividad de control	No	Verificar ME2.1	Prueba Sustantiva No.6	Gerente TI
ME2.2 Revisiones de Auditoría	Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo, por ejemplo, el cumplimiento de políticas y estándares.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar ME2.2	CheckList No.15	Gerente TI
ME2.4 Auto evaluación del control	Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar ME2.4	CheckList No.16	Gerente TI
ME3 Garantizar el cumplimiento con requerimientos externos							
ME3.3 Evaluación del cumplimiento con requerimientos externos	Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos legales y regulatorios.	Anualmente	Manual	En formato digital, está incompleta y desactualizada	Verificar ME3.3	CheckList No.17	Gerente TI
ME4 Proporcionar gobierno de TI							
ME4.1 Establecer un marco de gobierno de TI	Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales.	Trimestralmente	Manual	En formato digital, está incompleta y desactualizada	Verificar ME4.1	Cuestionario No.16	Gerente TI

3.2.6. Documentación a entregar

- **Informe Detallado**

  El Informe Detallado, que consta en el Capítulo 4, fue presentado para su revisión el día miércoles 08 de febrero del 2012 al el Ing. Oswaldo Vaca - Gerente de Tecnología de Información y a la Ing. Paulina Porras – Especialista de Redes y Comunicaciones de la Corporación HOLDINGDINE S.A. (Matriz).

- **Informe Final/Ejecutivo**

  Una vez revisado el Informe Detallado y aceptadas las respectivas recomendaciones y puntos de vista, se procederá a presentar el Informe Final/Ejecutivo a la Alta Gerencia de la Corporación HOLDINGDINE S.A. (Matriz). Esto queda a cargo de la Gerencia TI.

  A continuación consta el acta de reunión.

CAPÍTULO 4

INFORME DETALLADO Y RESULTADOS DEL CASO PRÁCTICO

4.1. Introducción

Después de identificar y analizar los riesgos TI más críticos (procesos, actividades y documentación referente) de acuerdo a la Matriz de Riesgos TI y al Plan de Investigación de Campo basados en el Modelo COBIT 4.1., se pudo obtener un conjunto de observaciones y recomendaciones los cuales se indican en el Informe Detallado, el cual fue presentado y analizado con el Sr. Ing. Oswaldo Vaca, MBA – Gerente TI y la Sra. Ing. Paulina Porras – Especialista de Redes y Comunicaciones TI, de lo cual se obtuvo las justificaciones respectivas de la Evaluación Técnica Informática al Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz).

Posteriormente se elaboró el Informe Ejecutivo que incluye un resumen gerencial y las conclusiones y recomendaciones para una mejora continua en el Sistema de Información de la Corporación HOLDINGDINE S.A (Matriz). **Ver CD Anexos → Documento "ANEXO H.docx".**

4.2. Descripción del trabajo efectuado

Una vez analizada y conocida la situación actual de la organización y de la Gerencia TI, el enfoque de auditoría externa se justificó en la realización de 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.
- Recopilación de información referente a la entidad, Gerencia TI y al Sistema de Información.
- 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 Tl, con la finalidad de conocer más a detalle las actividades y procesos existentes en la corporación.
- Una vez obtenida la información, realizar su respectivo análisis 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 al Gerente y Especialista de Redes y Comunicaciones de la Gerencia TI, donde se incluye todas oportunidades de mejora, con la finalidad de conocer su opinión al respecto.

- Después de discutidas las recomendaciones con el Gerente y la Especialista de Redes y Comunicaciones de la Gerencia TI, indicar en el informe su punto de vista.
- Finalmente emitir el Informe Ejecutivo de auditoría.
- El Informe Ejecutivo, a cargo de la Gerencia TI, se entregará al staff ejecutivo de la Corporación HOLDINGDINE S.A. (Matriz).

4.3. Informe Detallado

En conformidad con el plan de tesis "Evaluación Técnica Informática del Sistema de Información de la CORPORACIÓN HOLDINGDINE S.A. (Matriz), utilizando el Estándar Internacional COBIT", realizado por el Sr. Andrés Patricio Naveda Paredes, se ha evaluado los procesos y actividades de control más críticos que afectan a la Corporación, referentes a los cuatro dominios del Estándar Internacional COBIT 4.1., de la que se detalla a continuación las observaciones y recomendaciones resultantes.

PLANEAR Y ORGANIZAR (PO)

Este dominio cubre las estrategias y las tácticas de la organización, y tiene que ver con identificar la manera en que TI pueda contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una tecnológica apropiada.

Este dominio cubre los siguientes objetivos de control:

PO1. Definir un plan estratégico de TI.

PO2. Definir la arquitectura de la información.

PO3. Determinar la dirección tecnológica.

PO4. Definir los procesos, organización y relaciones de TI.

PO5. Administrar la inversión en TI.

PO6. Comunicar las aspiraciones y la dirección de la gerencia.

PO7. Administrar recursos humanos de TI.

PO8. Administrar la calidad.

PO9. Evaluar y administrar los riesgos de TI.

PO10. Administrar proyectos.

PO1. Definir un plan estratégico de TI

PO1.4. Plan estratégico de TI

Observación PO1.4.

La Gerencia TI cuenta con un plan estratégico TI, el cual cumple parcialmente con los objetivos estratégicos del negocio.

Criterio PO1.4.

"Establecer un plan estratégico que defina, en cooperación con los interesados relevantes, cómo la TI contribuirá a los objetivos estratégicos de la empresa (metas) así como los costos y riesgos relacionados. Incluye cómo la TI dará soporte a los programas de inversión facilitados por TI y a la entrega de los servicios operacionales. Define cómo se cumplirán y medirán los objetivos y recibirá una autorización formal de los interesados. El plan estratégico de TI debe incluir el presupuesto de la inversión / operativo, las fuentes de financiamiento, la estrategia de procuración, la estrategia de adquisición, y los requerimientos legales y regulatorios. El plan estratégico debe ser lo suficientemente detallado para permitir la definición de planes tácticos de TI".

Condición PO1.4.

El plan estratégico TI solo incluye el presupuesto de inversión / operativo, más no: fuentes de financiamiento, estrategia de obtención, estrategia de adquisición, requerimientos legales y regulatorios. No existen planes tácticos TI.

Evidencia PO1.4.

Cuestionario No.1, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO1.4.

- Desactualización de la información.
- Información incompleta.
- Falencias en el plan estratégico TI referentes a los programas de presupuesto de inversión**.**

Efecto PO1.4.

- La desactualización del plan estratégico TI contribuirá al no cumplimiento de los objetivos estratégicos del negocio (metas).
- El plan estratégico no cuenta con planes táctico TI.

- El plan estratégico TI no cuenta con fuentes de financiamiento, estrategia de obtención, estrategia de adquisición, requerimientos legales y regulatorios.

Recomendación PO1.4.

El Gerente de TI debe actualizar y completar información del plan vinculado con fuentes de financiamiento, estrategia de obtención, estrategia de adquisición, requerimientos legales y regulatorios; además de incluir planes tácticos TI. Se debe archivar en formato digital e impreso el plan estratégico TI.

Punto de Vista PO1.4. Se acepta la observación.

PO1.5. Planes tácticos de TI

Observación PO1.5.

No existe un portafolio de planes tácticos TI.

Criterio PO1.5.

"Establecer un portafolio de planes tácticos de TI que se deriven del plan estratégico de TI. Estos planes tácticos describen las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Los planes tácticos deben tener el detalle suficiente para permitir la definición de planes proyectados. Administrar de forma activa los planes tácticos y las iniciativas de TI establecidas por medio del análisis de los portafolios de proyectos y servicios. Esto incluye el equilibrio de los requerimientos y recursos de forma regular, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados, y tomando las medidas necesarias en caso de desviaciones".

Condición PO1.5.

No se cuanta con un portafolio de planes tácticos que se derive del plan estratégico TI.

Evidencia PO1.5.

Cuestionario No.2, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO1.5.

Falta de planes tácticos TI en la unidad de Apoyo, Gerencia TI.

Efecto PO1.5.

Al no contar con un portafolio de planes tácticos, no se detalla las iniciativas y los requerimientos de recursos requeridos por TI, y cómo el uso de los recursos y el logro de los beneficios serán monitoreados y administrados. Existe un desequilibrio de los requerimientos y recursos, comparándolos con el logro de metas estratégicas y tácticas y con los beneficios esperados.

Recomendación PO1.5.

El Gerente de TI debe considerar la creación de planes tácticos derivados del plan estratégico TI, para guiar las actividades a corto plazo sirviendo de vínculo entre estas acciones y los objetivos organizacionales a largo plazo.

Punto de Vista PO1.5. Se acepta la observación.

PO2. Definir la arquitectura de la información

PO2.1. Modelo de arquitectura de información empresarial

Observación PO2.1.

No se detalla cómo está compuesto el modelo de arquitectura de información empresarial.

Criterio PO2.1.

"Establecer y mantener un modelo de información empresarial que facilite el desarrollo de aplicaciones y las actividades de soporte a la toma de decisiones, consistente con los planes de TI. El modelo facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera que conserva la integridad y es flexible, funcional, rentable oportuna segura y tolerante a fallas".

Condición PO2.1.

- No se pone en práctica una mejora y actualización del modelo de información empresarial.
- Teóricamente la actualización y/o modificaciones del modelo de arquitectura de información empresarial se realiza anualmente.

Evidencia PO2.1.

Cuestionario No.3, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO2.1.

Existe escasa información referente al modelo de arquitectura de información empresarial y no se establece una mejora y actualización de dicho modelo.

Efecto PO2.1.

Con la carencia de información, no se puede detallar cómo está compuesto el modelo de arquitectura de información empresarial y sin la debida mejora y actualización, se dificulta el desarrollo de aplicaciones y de actividades de soporte a la toma de decisiones consistente con los planes TI.

Recomendación PO2.1.

El Especialista y Técnicos de Redes y Comunicaciones de TI deben obtener y completar información relevante del modelo de información empresarial, para sí saber con detalle cómo está compuesta. Realizar una mejora continua del modelo para facilitar el desarrollo de aplicaciones y de actividades de soporte en la toma de decisiones, al igual que facilita la creación, uso y compartición óptimas de la información por parte del negocio de una manera íntegra, flexible, funcional, rentable, oportuna, segura y tolerante a fallas. Archivar la documentación en formato digital e impreso.

Punto de Vista PO.2.1. Se acepta la observación.

PO2.4. Administración de la integridad

Observación PO2.4.

Procedimientos ineficientes que no garantizan la integridad y consistencia de todos los datos almacenados en formato electrónico.

Criterio PO2.4.

"Definir e implantar procedimientos para garantizar la integridad y consistencia de todos los datos almacenados en formato electrónico, tales como bases de datos, almacenes de datos y archivos".

Condición PO2.4.

- No existe documentación referente a procedimientos de integridad y consistencia de datos almacenados en formato electrónico.
- No existe una clasificación adecuada de datos, de niveles de seguridad, de los niveles de acceso y "defaults".

- La clasificación de datos no defina claramente: quién puede tener acceso, quién es responsable de determinar el nivel de acceso apropiado, la aprobación específica requerida para el acceso, los requerimientos especiales para el acceso (por ejemplo, acuerdo de confidencialidad).

Evidencia PO2.4.

Prueba de Cumplimiento No.1, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa PO2.4.

Falta de procedimientos y normatividad para garantizan la integridad y consistencia de todos los datos almacenados en formato electrónico.

Efecto PO2.4.

- Inconsistencias en el modelo de datos corporativo, en los sistemas de información asociados y en los planes a largo y corto plazo de tecnología de información.
- Elementos de datos en los que la propiedad no haya sido claramente y/o apropiadamente determinada.
- Clases de datos que hayan sido definidos de manera no apropiada.
- Niveles de seguridad de datos inconsistentes con la regla de "necesidad de acceso"

Recomendación PO2.4.

El Especialista y Técnicos de Redes y Comunicaciones de TI deben realizar una revisión detallada de los procedimientos de administración de la integridad y de los niveles de seguridad definidos para datos delicados, con el fin de verificar que se haya obtenido la autorización apropiada para el acceso, y que el acceso sea consistente con los niveles de seguridad definidos en las políticas y procedimientos de la función de servicios de información. Archivar la información en formato digital e impreso.

Punto de vista PO2.4. Se acepta la observación.

PO3. Determinar la dirección tecnológica

PO3.1. Planeación de la dirección tecnológica

Observación PO3.1.

La Gerencia TI en teoría cuenta con un plan decisivo, que no está estructurado.

Criterio PO3.1.

"Analizar las tecnologías existentes y emergentes y planear cuál dirección tecnológica es apropiado tomar para materializar la estrategia de TI y la arquitectura de sistemas del negocio. También identificar en el plan qué tecnologías tienen el potencial de crear oportunidades de negocio. El plan debe abarcar la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura".

Condición PO3.1.

- El plan decisivo no incluye la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura.
- El plan decisivo no aporta con respuestas oportunas a cambios en el ambiente competitivo, así como tampoco con la interoperabilidad mejorada de las plataformas y de las aplicaciones.
- En teoría se debería actualizar el plan decisivo anualmente, pero no se pone en práctica ni la actualización y ni la legalización de la información.

Evidencia PO3.1.

Cuestionario No.4, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO3.1.

Presencia de información incompleta y desactualizada del plan decisivo e inoperancia a respuestas en el ambiente competitivo.

Efecto PO3.1.

El plan decisivo lleva a una vulnerabilidad competitiva empresarial por falta de respuestas oportunas y por la carencia de información referente a la arquitectura de sistemas, dirección tecnológica, estrategias de migración y aspectos de contingencia de los componentes de la infraestructura.

Recomendación PO3.1.

El Gerente de TI debe ejecutar una reestructuración del plan decisivo para analizar las tecnologías existentes y emergentes en la creación de oportunidades de negocio. Incluir en el plan la arquitectura de sistemas, la dirección tecnológica, las estrategias de migración y los aspectos de contingencia de los componentes de la infraestructura. Cumplir con la actualización anual y archivar la documentación en formato digital e impreso.

Punto de vista PO3.1. Se acepta la observación.

PO3.2. Plan de infraestructura tecnológica

Observación PO3.2.

La Gerencia TI cuenta con un plan de infraestructura tecnológica que se ajusta parcialmente a los planes estratégicos y de manera nula a los planes tácticos TI, ya que no existe planificación táctica.

Criterio PO3.2.

"Establecer un plan de infraestructura tecnológica que esté de acuerdo con los planes estratégicos y tácticos de TI. El plan se basa en la dirección tecnológica e incluye acuerdos para contingencias y orientación para la adquisición de recursos tecnológicos. También toma en cuenta los cambios en el ambiente competitivo, las economías de escala en la obtención de equipo de sistemas de información, y la mejora en la interoperabilidad de las plataformas y las aplicaciones".

Condición PO3.2.

- El plan de infraestructura tecnología no está orientado a la adquisición de recursos tecnológicos.
- El plan de infraestructura tecnología abarca únicamente las estrategias de migración y contingencias, dejando de lado a la arquitectura de sistemas, dirección tecnológica, planes de adquisición y estándares

Evidencia PO3.2.

Cuestionario No.5, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO3.2.

Se cuenta con documentación escasa y desactualizada, lo que ocasiona falencias en el plan de infraestructura tecnológica.

Efecto PO3.2.

Planes de adquisición de hardware y software que no reflejen las necesidades del plan de infraestructura tecnológica. El plan, en el aspecto de adquisición de recursos tecnológicos, no es consistente con los estándares de tecnología.

Recomendación PO3.2.

El Gerente de TI debe evaluar y administra la utilización de tecnología actual y futura, y así ajustar y mejorar la información para cumplir con los planes a corto y largo plazo de tecnología de información. Se debe cumplir con los estándares de tecnología y que éstos sean agregados e incorporados como parte del proceso de desarrollo tecnológico. Archivar la documentación en formato digital e impreso.

Punto de vista PO3.2. Se acepta la observación.

PO4. Definir los procesos, organización y relaciones de TI

PO4.3. Comité directivo de TI

Observación PO4.3.

La Gerencia TI no cuenta con un comité directivo reglamentariamente formado.

Criterio PO4.3.

"Establecer un comité directivo de TI (o su equivalente) compuesto por la gerencia ejecutiva, del negocio y de TI para: determinar las prioridades de los programas de inversión de TI alineadas con la estrategia y prioridades de negocio de la empresa, hacer seguimiento al estatus de los proyectos y resolver los conflictos de recursos y monitorear los niveles de servicio y las mejoras del servicio".

Condición PO4.3.

- No se establecen procesos para incrementar el conocimiento, la conciencia, la comprensión y la habilidad para identificar y resolver problemas de administración de la información.

Evidencia PO4.3.

CheckList No.1, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa PO4.3.

No existe documentación que evidencie la creación de un Comité Directivo TI.

Efecto PO4.3.

Al no estar reglamentariamente definido un Comité Directivo TI, se propagará debilidades en la función de servicios de información y sus actividades ocasionadas por una vigilancia no efectiva por parte del comité de planeación de dicha función.

Recomendación PO4.3.

El Gerente de TI debe legalizar y mantener el Comité Directivo TI actual, formado por el gerente y por los especialistas de las tres áreas claves (Redes y Comunicaciones, Aplicativos y Base de Datos), para determinar las prioridades de los programas de inversión TI alineadas con la estrategia y prioridades de negocio; además recaudar información que justifique la existencia de dicho comité. Archivar la información en formato digital e impreso.

Punto de vista PO4.3. Se acepta la observación.

PO4.4. Ubicación organizacional de la función de TI

Observación PO4.4.

La Gerencia TI se ubica como Unidad de Apoyo dentro de la estructura organizacional, pero la unidad en sí, posee pocas áreas claves para el aporte al cumplimiento de las estrategias del negocio.

Criterio PO4.4.

"Ubicar a la función de TI dentro de la estructura organizacional general con un modelo de negocios supeditado a la importancia de TI dentro de la empresa, en especial en función de que tan crítica es para la estrategia del negocio y el nivel de dependencia operativa sobre TI".

Condición PO4.4.

- Las políticas y los comunicados de la gerencia TI no aseguran la independencia y la autoridad de la función de los servicios de información.
- La gerencia TI se asegura parcialmente de las funciones y responsabilidades que se están siendo llevadas a cabo dentro de la unidad de apoyo.

Evidencia PO4.4.

CheckList No.2, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa PO4.4.

No existen políticas y procedimientos que consideren la necesidad de evaluar y modificar la composición funcional de la unidad de apoyo, para satisfacer objetivos y circunstancias cambiantes de la corporación.

Efecto PO4.4.

Composición funcional inapropiadas, funciones faltantes, personal insuficiente, deficiencias en competencia, funciones y responsabilidades no apropiadas, confusión en la propiedad de datos y sistemas, problemas de supervisión, falta de segregación de funciones, etc.

Recomendación PO4.4.

El Gerente de TI debe poner en ejecución una evaluación detallada de la composición funcional, las aptitudes del personal, las funciones y responsabilidades asignadas, la propiedad de datos y sistemas, supervisión, segregación y anexión de funciones, etc., así la unidad de apoyo tendrá una mejora continua y responderá con eficiencia y eficacia a los requerimientos del negocio.

Punto de vista PO4.4. Se acepta la observación.

PO5. Administrar la inversión en TI

PO5.1. Marco de trabajo para la administración financiera

Observación PO5.1.

La Gerencia TI carece de un marco de trabajo para la administración financiera.

Criterio PO5.1.

"Establecer un marco de trabajo financiero para TI que impulse el presupuesto y el análisis de rentabilidad, con base en los portafolios de inversión, servicios y activos. Dar mantenimiento a los portafolios de los programas de inversión de TI, de servicios y de activos de TI, los cuales forman la base para el presupuesto corriente de TI. Brindar información de entrada hacia los casos de negocio de nuevas inversiones, tomando en cuenta los portafolios actuales de activos y servicios de TI. Las nuevas inversiones y el mantenimiento a los portafolios de servicios y de activos influenciarán el futuro presupuesto de TI.

Comunicar los aspectos de costo y beneficio de estos portafolios a los procesos de priorización de presupuestos, administración de costos y administración de beneficios".

Condición PO5.1.

- La Gerencia Financiera es la encargada de dar mantenimiento a los portafolios de los programas de inversión, servicios y activos TI.
- La Gerencia Financiera tiene mayor influencia decisiva al momento de dar a conocer nuevas inversiones tecnológicas.

Evidencia PO5.1.

Cuestionario No.6, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO5.1.

No existe un marco de trabajo financiero TI.

Efecto PO5.1.

La Gerencia TI al no establecer un marco de trabajo financiero propio, se hace dependiente de la Gerencia Financiera con relación a los programas de inversión, servicios y activos TI.

Recomendación PO5.1.

El Gerente de TI debe analizar e implantar un marco de trabajo financiero propio de la Gerencia TI, para poner en marcha mediciones ("Benchmarking") de presupuestos y costos contra organizaciones similares y realizar revisiones detalladas del presupuesto actual y del año inmediato anterior contra los resultados reales, variaciones y acciones correctivas aplicadas.

Punto de vista PO5.1. Se acepta la observación.

PO5.4. Administración de costos de TI

Observación PO5.4.

No se realiza una revisión detallada del presupuesto actual y del año inmediato anterior, para hacer una estadística de resultados reales, variaciones y acciones correctivas.

Criterio PO5.4.

"Implantar un proceso de administración de costos que compare los costos reales con los presupuestados. Los costos se deben monitorear y reportar.

Cuando existan desviaciones, estas se deben identificar de forma oportuna y el impacto de esas desviaciones sobre los programas se debe evaluar y, junto con el patrocinador del negocio para estos programas, se deberán tomar las medidas correctivas apropiadas y, en caso de ser necesario, el caso de negocio del programa de inversión se deberá actualizar".

Condición PO5.4.

- Existe documentación en formato digital de reportes y monitoreo de costos de años anteriores, pero está incompleta y desactualizada.
- No se cumple con los tiempos de compras, debido a problemas con procesos internos de las unidades operativas.
- El soporte en el presupuesto de la función de servicios de información no es el adecuado para justificar el plan operativo anual de dicha función.
- Las categorías de gastos de la función de servicios de información no son suficientes y no han sido clasificadas adecuadamente.

Evidencia PO5.4.

Prueba Sustantiva No.1, **Ver CD Anexos → Documento "ANEXO F.docx".**

Causa PO5.4.

Falta de procedimientos y normatividad en una administración adecuada de los costos TI.

Efecto PO5.4.

Presupuestos de la función de sistemas de información que no estén en línea con el presupuesto y los planes a corto y largo plazo de la organización y con los planes a corto y largo plazo de tecnología de información.

Recomendación PO5.4.

El Gerente de TI debe realizar una revisión detallada del presupuesto actual y del año inmediato anterior contra los resultados reales, variaciones y acciones correctivas aplicadas. Fortalecer los procedimientos de administración de costos TI pata tener un monitoreo y reporte real. Archivar la información en formato digital e impreso.

Punto de vista PO5.4. Se acepta la observación.

PO6. Comunicar las aspiraciones y la dirección de la gerencia

PO6.2. Riesgo Corporativo y Marco de referencia de control interno de TI

Observación PO6.2.

No se cuenta con documentación que evidencie la elaboración de un marco de trabajo con enfoque empresarial general hacia los riesgos y el control interno TI.

Criterio PO6.2.

"Elaborar y dar mantenimiento a un marco de trabajo que establezca el enfoque empresarial general hacia los riesgos y hacia el control interno para entregar valor mientras al mismo tiempo se protegen los recursos y sistemas de TI. El marco de trabajo debe estar integrado al sistema de administración de calidad, y debe cumplir los objetivos generales de la empresa. Debe tener como meta maximizar el éxito de la entrega de valor mientras minimiza los riesgos para los activos de información por medio de medidas preventivas, la identificación oportuna de irregularidades, la limitación de pérdidas y la oportuna recuperación de activos del negocio".

Condición PO6.2.

- El marco de enfoque empresarial general hacia los riesgos y control interno no está integrado al marco de procesos de TI.
- El marco de enfoque empresarial no está integrado a un sistema de administración de calidad, ya que no existe dicho sistema.

Evidencia PO6.2.

Cuestionario No. 7, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa PO6.2.

Falta de políticas y procedimientos para establecer un marco de enfoque empresarial general hacia los riesgos y control interno TI.

Efecto PO6.2.

La falta de un marco referencial de control, pone en duda el compromiso de la administración de la Gerencia TI, en cuanto al fomento de un ambiente de control interno positivo a través de la organización.

Recomendación PO6.2.

El Gerente de TI debe implantar políticas de seguridad y control interno TI para aportar con la formación de un marco de enfoque empresarial solido que identifique componentes de control tales como: ambiente de control, reevaluación de riesgos, actividades de control, información y comunicación, monitoreo, etc.

Punto de vista PO6.2. Se acepta la observación.

PO6.5. Comunicación de los objetivos y la dirección de TI

Observación PO6.5.

No se comunica los objetivos y la dirección del negocio y de TI a toda la corporación.

Criterio PO6.5.

"Garantizar que la conciencia y el entendimiento de los objetivos y la dirección del negocio y de TI se comunican a toda la organización. La información comunicada debe abarcar una misión claramente articulada, los objetivos de servicio, la seguridad, los controles internos, la calidad, el código de ética y conducta, políticas y procedimientos, etc., y se deben incluir dentro de un programa de comunicación continua, apoyado por la alta dirección con acciones y palabras. La dirección debe dar especial atención a comunicar la conciencia sobre la seguridad de TI y el mensaje de que la seguridad de TI es responsabilidad de todos".

Condición PO6.5.

- No existe documentación de referencia.
- No se comunica los objetivos TI a toda la corporación.
- Es evidente las fallas en la administración para comunicar efectivamente políticas relacionadas con el ambiente de control interno de la organización y de la Gerencia TI.
- Deficiencias en la función de servicios de información en su compromiso con la calidad o en su habilidad para definir, documentar, mantener y comunicar efectivamente una filosofía, políticas y objetivos de calidad.

Evidencia PO6.5.

Observación Directa No.1, **Ver CD Anexos → Documento "ANEXO G.docx".**

Causa PO6.5.

Falta de procedimientos y normatividad en la divulgación y entendimiento de los objetivos y la dirección del negocio y de TI a toda la corporación.

Efecto PO6.5.

- Un marco referencial de control débil que ponga en duda el compromiso de la dirección del negocio y de TI, en cuanto al fomento de un ambiente de control interno positivo a través de la organización.
- Fallas en la administración para comunicar efectivamente sus políticas relacionadas con el ambiente de control interno de la organización.
- Deficiencias de la Gerencia TI en su compromiso en su habilidad para definir, documentar, mantener y comunicar efectivamente una filosofía, políticas y objetivos de calidad.

Recomendación PO6.5.

El Gerente de TI debe poner en marcha mediciones "Benchmarking" del marco referencial de control de la información y del programa de conocimiento y conciencia de los objetivos del negocio y TI contra organizaciones similares, para detectar y analizar cuáles son los mejores procedimientos y ponernos en práctica. Archivar la información en formato digital e impreso.

Punto de vista PO6.5. Se acepta la observación.

PO7. Administrar recursos humanos de TI

PO7.2. Competencias del personal

Observación PO7.2.

La Unidad de Talento Humano no realiza los correctivos necesarios en las competencias del personal.

Criterio PO7.2.

“Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso”.

Condición PO7.2.

Existe documentación en formato digital e impresa que está desorganizada e incompleta referente a las competencias del personal.

Evidencia PO7.2.

Prueba de Cumplimiento No.2, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa PO7.2.

Los resultados negativos de las evaluaciones técnicas y no técnicas al personal, no son tomados en cuenta para hacer los correctivos necesarios.

Efecto PO7.2.

- Personal calificado no apropiadamente.
- Personal cuyas evaluaciones de desempeño no existen o no dan soporte a la posición ocupada y/o funciones llevadas a cabo.

Recomendación PO7.2.

La Unidad de Talento Humano con los resultados de las evaluaciones técnicas y no técnicas, debe tomar los correctivos inmediatos hacia el personal que no cumplen con las habilidades necesarias para cumplir con sus roles dentro de la corporación. Archivar la información en formato digital e impreso.

Punto de vista PO7.2. Se acepta la observación.

PO7.4. Entrenamiento del personal de TI

Observación PO7.4.

La Gerencia TI parcialmente proporciona la orientación necesaria a sus empleados.

Criterio PO7.4.

"Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales".

Condición PO7.4.

- Existe documentación en formato digital que está incompleta y desactualizada referente a los planes de capacitación.

- Las oportunidades de entrenamiento y desarrollo no están ligadas a las brechas de competencia.
- Presupuestos y tiempos inadecuados asignados al entrenamiento y desarrollo del personal.

Evidencia PO7.4.

Prueba de Cumplimiento No.3, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa PO7.4.

Falta de procedimientos y normatividad en el entrenamiento adecuado para el personal de TI.

Efecto PO7.4.

- Inadecuada continuidad de los entrenamientos al personal de TI.
- Dependencia de la Unidad de Talento Humano en los planes de capacitación.

Recomendación PO7.4.

El Gerente de TI en conjunto con la Unidad de Talento Humano deben realizar una revisión detallada de las actividades de la administración del personal de la función de servicios de información, para mejorar el entrenamiento continuo, teniendo en cuanta los controles internos y conciencia sobre la seguridad al nivel requerido para alcanzar las metas organizacionales. Archivar la información en formato digital e impreso referente a los planes de capacitación.

Punto de vista PO7.4. Se acepta la observación.

PO7.7. Evaluación del desempeño del empleado

Observación PO7.7.

La evaluación del desempeño del empleado no está orientada a las metas organizacionales.

Criterio PO7.7.

"Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario".

Condición PO7.7.

- Existe documentación en formato digital e impresa que está desorganizada referente al desempeño del personal.
- Se espera que el personal cuente con los conocimientos adecuados de las operaciones para la función de su posición o áreas de responsabilidad.
- Los expedientes del personal no contienen un reconocimiento en cuanto a la comprensión del programa general de educación, conciencia y conocimiento de la organización.
- El personal de seguridad de la información no ha recibido el entrenamiento apropiado en procedimientos y técnicas de seguridad.

Evidencia PO7.7.

Observación Directa No.2, **Ver CD Anexos → Documento "ANEXO G.docx".**

Causa PO7.7.

El conocimiento de los objetivos del negocio por parte del personal asignado a las funciones críticas incluye parcialmente la filosofía de los controles internos.

Efecto PO7.7.

- Personal cuyo desempeño no han sido llevadas a cabo.
- Insuficiencias en los programas de entrenamiento y en las actividades de desarrollo personal.

Recomendación PO7.7.

El Gerente de TI conjuntamente con la Unidad de Talento Humano deben fortalecer las evaluaciones de desempeño de los empleados, para que cuenten con los conocimientos adecuados de las operaciones para la función de su posición o áreas de responsabilidad. Realizar un proceso de entrenamiento y educación continua para el personal asignado a funciones críticas. Archivar la información en formato digital e impreso.

Punto de vista PO7.7. Se acepta la observación.

PO8. Administrar la calidad

PO8.1. Sistema de administración de calidad

Observación PO8.1.

La Gerencia TI no cuenta con un Sistema de Administración de la Calidad (QMS).

Criterio PO8.1.

"Establecer y mantener un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio. El QMS identifica los requerimientos y los criterios de calidad, los procesos claves de TI, y su secuencia e interacción, así como las políticas, criterios y métodos para definir, detectar, corregir y prever las no conformidades. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y las responsabilidades. Todas las áreas clave desarrollan sus planes de calidad de acuerdo a los criterios y políticas, y registran los datos de calidad. Monitorear y medir la efectividad y aceptación del QMS y mejorarla cuando sea necesario".

Condición PO8.1.

- No existe documentación que respalde a un Sistema de Administración de la Calidad.
- A pesar que la organización tiene una fuerte dependencia de la función TI, se ha dejado a un lado la implementación de un Sistema de Administración de la Calidad.
- Teóricamente las áreas clave (Redes y Comunicación, Aplicativos y Base de Datos) desarrollan sus planes de calidad de acuerdo a los criterios y políticas, que vagamente se pone en práctica.

Evidencia PO8.1.

CheckList No.3, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa PO8.1.

No existe un Sistema de Administración de la Calidad (QMS).

Efecto PO8.1.

La Gerencia TI al no tener un Sistema de Administración de la Calidad (QMS), no proporciona un enfoque estándar, formal y continuo, con respecto a la administración de la calidad, que esté alineado con los requerimientos del negocio.

Recomendación PO8.1.

El Gerente de TI conjuntamente con los Especialistas de Áreas Claves deben realizar un análisis e implantación de un QMS que proporcione un enfoque estándar, formal y continuo, con respecto a la administración de la calidad. El QMS debe definir la estructura organizacional para la administración de la calidad, cubriendo los roles, las tareas y responsabilidades.

Punto de vista PO8.1. Se acepta la observación.

PO9. Evaluar y administrar los riesgos de TI

PO9.1. Marco de trabajo de administración de riesgos

Observación PO9.1.

La Gerencia TI no cuenta con un marco referencial para la administración de riesgos.

Criterio PO9.1.

"Integrar el gobierno, la administración de riesgos y el marco de control de TI, al marco de trabajo de administración de riesgos de la organización. Esto incluye la alineación con el apetito de riesgo y con el nivel de tolerancia al riesgo de la organización".

Condición PO9.1.

- Existe documentación en formato digital que está desactualizada e incompleta referente al plan de acción contra riesgos.
- No existen procedimientos de evaluación e identificación de riesgos.
- No se considera urgente la realización de auditorías externas para la determinación de riesgos críticos en el sistema de información.
- El plan de acción contra riesgos no incluye controles económicos y medidas de seguridad para mitigar la exposición al riesgo.

Evidencia PO9.1.

CheckList No.4, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa PO9.1.

Los objetivos de toda la organización no están incluidos en el proceso de identificación de riesgos.

Efecto PO9.1.

Riesgos no identificados, riesgos no considerados/manejados a un nivel aceptable, evaluaciones de riesgos obsoletos, medidas incorrectas cuantitativas y/o cualitativas de riesgos, amenazas y exposiciones. Planes de acción contra riesgos que no aseguren controles económicos y medidas de seguridad.

Recomendación PO9.1.

El Gerente de TI conjuntamente con los Especialistas de Áreas Claves deben primeramente actualizar e integrar un marco de trabajo de administración de riesgos de la organización al actual plan de acción contra riesgos, además incluir procedimientos enfocados a la evaluación para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual. Archivar la información en formato digital e impreso. Se debe considerar como una opción de mejora la puesta en ejecución de auditorías informáticas externas.

Punto de vista PO9.1. Se acepta la observación.

PO10. Administrar proyectos

PO10.2. Marco de trabajo para la administración de proyectos

Observación PO10.2.

Se cuenta con un marco de trabajo para la administración de proyectos que no está estructurado.

Criterio PO10.2.

"Establecer y mantener un marco de trabajo para la administración de proyectos que defina el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas a cada proyecto emprendido. Las metodologías deben cubrir, como mínimo, el inicio, la planeación, la ejecución, el control y el cierre de las etapas de los proyectos, así como los puntos de verificación y las aprobaciones. El marco de trabajo y las metodologías de soporte se deben integrar con la administración del portafolio empresarial y con los procesos de administración de programas".

Condición PO10.2.

- La documentación referente al marco de trabajo para la administración de proyectos es muy escasa.

- El marco referencial de administración de proyectos únicamente define el alcance y no toma en cuenta las limitaciones del proyecto.
- El marco referencial de administración de proyectos no asegura que las demandas del proyecto sean revisadas, en cuanto a su consistencia con el plan operativo aprobado.
- El marco referencial de administración de proyectos no define las responsabilidades y la autoridad de los miembros del equipo del proyecto.
- El marco referencial de administración de proyectos no proporciona un documento inicial de definición del proyecto que incluya estatutos claros sobre la naturaleza y alcance del proyecto.

Evidencia PO10.2.

CheckList No.5, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa PO10.2.

El marco de referencia de administración de proyectos tiene carencias en su estructuración.

Efecto PO10.2.

Proyectos que sean administrados inadecuadamente, que hayan excedido fechas claves, excedido costos, sean obsoletos, no sean técnicamente factibles, no otorguen los beneficios planeados, no satisfagan los requerimientos de control interno y seguridad y que no eliminen o mitiguen los riesgos.

Recomendación PO10.2.

El Gerente de TI debe reestructurar el marco de referencia de administración de proyectos e incluir aspectos generales para la definición, autorización y ejecución de proyectos, como: definición de las funciones del sistema, factibilidad, dar la limitaciones del proyecto, determinación de los costos y beneficios del sistema, compromiso de recursos (de personal y económicos) por parte del propietario/patrocinador, definición de responsabilidades y autoridad de los participantes en el proyecto y puntos de revisión y verificación en la autorización de las diferentes fases del proyecto. Archivar la información en formato digital e impreso.

Punto de vista PO10.2. Se acepta la observación.

ADQUIRIR E IMPLEMENTAR (AI)

Para llevar a cabo la estrategia de TI, las soluciones TI necesitan ser identificadas, desarrolladas o adquiridas así como la implementación e integración en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.

Este dominio cubre los siguientes objetivos de control:

AI1. Identificar soluciones automatizadas.

AI2. Adquirir y mantener software aplicativo.

AI3. Adquirir y mantener infraestructura tecnológica.

AI4. Facilitar la operación y el uso.

AI5. Adquirir recursos de TI.

AI1. Identificar soluciones automatizadas

AI1.1. Definición y mantenimiento de los requerimientos técnicos y funcionales del negocio

Observación AI1.1.

La Gerencia TI parcialmente define criterios de aceptación de los requerimientos técnicos y funcionales del negocio.

Criterio AI1.1.

"Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI. Definir los criterios de aceptación de los requerimientos. Estas iniciativas deben incluir todos los cambios requeridos dada la naturaleza del negocio, de los procesos, de las aptitudes y habilidades del personal, su estructura organizacional y la tecnología de apoyo".

Condición AI1.1.

- Existe documentación en formato digital que está incompleta y desactualizada referente a los requerimientos técnicos y funcionales.
- No existen políticas y procedimientos para analizar los requerimientos técnicos y funcionales en su desempeño, seguridad, confiabilidad, compatibilidad y legislación.

Evidencia AI1.1.

Cuestionario No.8, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa AI1.1.

Baja prioridad de los requerimientos funciones y técnicos hacia el cumplimiento de las expectativas de los programas de inversión TI.

Efecto AI1.1.

Los requerimientos técnicos y funcionales no toman en cuenta la dirección tecnológica y no garantizan integridad, exactitud y validez de los requerimientos del negocio, como base para el control de la adquisición y el desarrollo continuo de sistemas.

Recomendación AI1.1.

El Especialista y Técnicos de Redes y Comunicaciones de TI deben implantar políticas y procedimientos para que los requerimientos técnicos y funcionales toman en cuenta la dirección tecnológica, el desempeño, el costo, la confiabilidad, la compatibilidad, la auditoría, la seguridad, la disponibilidad y continuidad, la ergonomía, la funcionalidad, la seguridad y la legislación de la empresa. Establecer procesos para garantizar y administrar la integridad, exactitud y la validez de los requerimientos del negocio, como base para el control de la adquisición y el desarrollo continuo de sistemas. Estos requerimientos deben ser propiedad del patrocinador del negocio. Archivar la documentación en formato digital e impreso.

Punto de vista AI1.1. Se acepta la observación.

AI1.2. Reporte de análisis de riesgos

Observación AI1.2.

No se cuanta con un análisis de riesgos apropiado de los procesos del negocio.

Criterio AI1.2.

"Identificar, documentar y analizar los riesgos asociados con los procesos del negocio como parte de los procesos organizacionales para el desarrollo de los requerimientos. Los riesgos incluyen las amenazas a la integridad, seguridad, disponibilidad y privacidad de los datos, así como el cumplimiento de las leyes y reglamentos".

Condición AI1.2.

- No se cuenta con documentación referente a la verificación, identificación y análisis de los riesgos asociados con los procesos del negocio.
- No existen políticas y procedimientos a los proyectos de desarrollo, implementación o modificación de sistemas propuestos, para un análisis de las amenazas a la seguridad y eliminación del riesgo identificado.
- No existen mecanismos para asignar o mantener los atributos de seguridad para la exportación e importación de datos para interpretarlos correctamente.

Evidencia AI1.2.

CheckList No.6, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa AI1.2.

No se emplea un análisis solido de riesgos referentes a los procesos del negocio.

Efecto AI1.2.

No se identifican adecuadamente riesgos (incluyendo amenazas, vulnerabilidades e impactos potenciales), controles internos y de seguridad para reducir o eliminar los riesgos asociados con los procesos del negocio.

Recomendación AI1.2.

El Especialista y los Técnicos de Redes y Comunicaciones de TI deben fortalecer el análisis de riesgos para identificar, documentar y analizar las amenazas asociados con los procesos organizacionales del negocio. Archivar la información en formato digital e impreso.

Punto de vista AI1.2. Se acepta la observación.

AI2. Adquirir y mantener software aplicativo

AI2.5. Configuración e implementación de software aplicativo adquirido

Observación AI2.5.

Las simulaciones al software aplicativo adquirido se realizan con datos no reales.

Criterio AI2.5.

"Personalizar e implantar la funcionalidad automatizada adquirida con el uso de procedimientos de configuración, aceptación y prueba. Los aspectos a considerar incluyen la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema".

Condición AI2.5.

- Existe documentación en formato digital que está incompleta y desactualizada referente a los reportes de errores y aciertos de los aplicativos adquiridos.
- Algunas especificaciones de diseño del software aplicativo no reflejan los requerimientos del usuario.
- No se realiza una revisión detallada de los estándares de prueba de la organización y la implementación de los planes de software aplicativo adquirido.

- No se realiza una revisión detallada de la satisfacción del usuario final con el sistema, sus reportes, la documentación y material de referencia, las instalaciones de ayuda, etc.

Evidencia AI2.5.

Prueba Sustantiva No.2, **Ver CD Anexos → Documento "ANEXO F.docx".**

Causa AI2.5.

Falta de normatividad y procedimientos de configuración, aceptación y prueba.

Efecto AI2.5.

- Especificaciones de diseño que no reflejen los requerimientos del usuario.
- Deficiencias en la integridad de los datos en software de programas de simulación.

Recomendación AI2.5.

El Especialista y Técnicos de la Administración de Aplicativos de TI deben realizar una revisión detallada de la efectividad de los estándares de prueba de la corporación y de la implementación de planes de pruebas al software aplicativo adquirido. Además de una revisión detallada de la satisfacción del usuario final con el sistema, sus reportes, la documentación y material de referencia, las instalaciones de ayuda, etc. Archivar la información en formato digital e impreso.

Punto de vista AI2.5. Se acepta la observación.

AI2.8. Aseguramiento de la calidad del software

Observación AI2.8.

La Gerencia TI no establece los recursos necesarios para una ejecución óptima del plan de aseguramiento de calidad del software.

Criterio AI2.8.

"Desarrollar, implantar los recursos y ejecutar un plan de aseguramiento de calidad del software, para obtener la calidad que se especifica en la definición de los requerimientos y en las políticas y procedimientos de calidad de la organización. Los asuntos a considerar en el plan de aseguramiento de calidad incluyen el especificar el criterio de calidad y los procesos de validación y verificación, incluyendo inspección, revisión de algoritmos y código fuente y pruebas".

Condición AI2.8.

- Existe documentación en formato digital que está incompleta y desactualizada referente al plan de aseguramiento de la calidad del software.
- En el plan de aseguramiento de calidad no se incluyen los procesos de validación, verificación, inspección, revisión de algoritmos y código fuente.
- La Gerencia de Tecnología de Información no cuenta con un área dedicada al Desarrollo de Software, dependen directamente de terceros para la adquisición del producto software final.
- En teoría el porcentaje de importancia que se le da a la calidad de un producto software es del 100%, pero en la práctica no llega a su totalidad.

Evidencia AI2.8.

Cuestionario No.9, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa AI2.8.

Carencia de un área de Desarrollo de Software.

Efecto AI2.8.

Falta de procesos de validación, verificación, inspección, revisión de algoritmos y código fuente en el producto software final.

Recomendación AI2.8.

El Especialista de la Administración de Aplicativos de TI debe realizar un análisis de viabilidad sobre la implantación de un área de Desarrollo de Software, poniendo en claro los pros y los contra; y si al final no se considera la creación de dicha área, definir un grupo o comité especializado de Pruebas de Software Adquirido para así reajustar el plan de aseguramiento de calidad en procesos de validación, verificación, inspección, revisión de algoritmos y código fuente del producto final software. Archivar la información en formato digital e impreso.

Punto de vista AI2.8. Se acepta la observación.

AI3. Adquirir y mantener infraestructura tecnológica

AI3.1. Plan de adquisición de infraestructura tecnológica

Observación AI3.1.

La Gerencia TI cuenta con un plan de adquisición de infraestructura tecnológica que parcialmente satisface los requerimientos del negocio.

Criterio AI3.1.

"Generar un plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la dirección tecnológica de la organización. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Evaluar los costos de complejidad y la viabilidad comercial del proveedor y el producto al añadir nueva capacidad técnica".

Condición AI3.1.

Existe documentación en formato digital pero está incompleta y desactualizada referente al plan de adquisición de infraestructura tecnológica.

Evidencia AI3.1.

Cuestionario No. 10, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa AI3.1.

Falta de procesos y normatividad en del plan de adquisición de infraestructura tecnológica.

Efecto AI3.1.

Riesgo en la continuidad de las operaciones.

Recomendación AI3.1.

El Especialista de Redes y Comunicaciones de TI debe ajustar el plan actual para adquirir, implementar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio, y que esté de acuerdo con la Gerencia TI de la corporación. Archivar la información en formato digita e impreso.

Punto de vista AI3.1. Se acepta la observación.

AI3.3. Mantenimiento de la infraestructura

Observación AI3.3.

La Gerencia TI cuenta con un plan de mantenimiento de la infraestructura que no está estructurado.

Criterio AI3.3.

"Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad".

Condición AI3.3.

- Existe documentación en formato digital incompleta y desactualizada referente a la estrategia y/o un plan de mantenimiento de la infraestructura.
- En el calendario de mantenimiento preventivo, no garantiza que el mantenimiento de la infraestructura tecnológica programado no tendrá ningún impacto negativo sobre aplicaciones críticas o sensibles.

Evidencia AI3.3.

Cuestionario No.11, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa AI3.3.

Falta de políticas y procesos en el plan que permitan la realización de mantenimiento de la infraestructura.

Efecto AI3.3.

Impacto en la infraestructura tecnológica y bajo desempeño de los requerimientos del negocio.

Recomendación AI3.3.

El Especialista de Redes y Comunicaciones de TI debe implantar procesos enfocados mantener y proteger la infraestructura de acuerdo con las estrategias tecnológicas convenidas y la disposición del ambiente de desarrollo y pruebas. Esto garantiza que exista un soporte tecnológico continuo para las aplicaciones del negocio. Archivar la información en formato digital e impreso.

Punto de vista AI3.3. Se acepta la observación.

AI4. Facilitar la operación y el uso

AI4.1. Plan para soluciones de operación

Observación AI4.1.

La Gerencia TI cuenta con un plan para soluciones de operación que no está estructurado.

Criterio AI4.1.

"Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operacionales, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura".

Condición AI4.1.

- Existe documentación en formato digital que está desactualizada e incompleta referente al plan para soluciones de operación.
- El nivel de servicio y las expectativas de desempeño no están lo suficientemente detallados para permitir el seguimiento, la emisión de reportes y las oportunidades de mejora.
- Los requerimientos operativos y los niveles de servicio no están utilizando mediciones o "benchmarks".

Evidencia AI4.1.

CheckList No.7, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa AI4.1.

Falta de procedimientos y normatividad en el plan para soluciones de operación.

Efecto AI4.1.

- El plan o manual de operación no incluye a la definición de los nombres de todos los archivos de entrada, de salida y del formato del medio.
- Parcialmente se realiza el entrenamiento y el mantenimiento continuo de la documentación de aplicación, planes o manuales de operación y de usuario.

Recomendación AI4.1.

El Especialista de Base de Datos de TI debe realizar una revisión detallada de la documentación seleccionada de sistemas operacionales, para determinar si los requerimientos formales de desempeño de hardware y software son óptimos. Ejecutar un mantenimiento del sistema y controles de cambio para asegurar el cumplimiento adecuado de la infraestructura tecnológica. Archivar la información en formato digital e impreso.

Punto de vista AI4.1. Se acepta la observación.

AI4.2. Transferencia de conocimiento a la gerencia del negocio

Observación AI4.2.

No existen procedimientos para la transferencia de conocimiento a la gerencia ejecutiva de la corporación referente a los datos, entrega y calidad del servicio.

Criterio AI4.2.

"Transferir el conocimiento a la gerencia de la empresa para permitirles tomar posesión del sistema y los datos y ejercer la responsabilidad por la entrega y calidad del servicio, del control interno, y de los procesos administrativos de la aplicación. La transferencia de conocimiento incluye la aprobación de acceso, administración de privilegios, segregación de tareas, controles automatizados del negocio, respaldo/recuperación, seguridad física y archivo de la documentación fuente".

Condición AI4.2.

- No se transfiere el conocimiento a la gerencia ejecutiva de la corporación para permitirles tomar posesión del sistema y los datos, y ejercer la responsabilidad por la entrega y calidad del servicio.
- No hay documentación de respaldo.

Evidencia AI4.2.

Prueba de Cumplimiento No.4, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa AI4.2.

Falta de normatividad y procedimientos en transferir el conocimiento a la gerencia ejecutiva de la corporación.

Efecto AI4.2.

- Insuficiente conocimiento por parte de la gerencia ejecutiva de los sistemas, datos y responsabilidad por la entrega y calidad del servicio y del control interno TI.
- Fallas en la administración para comunicar efectivamente sus políticas relacionadas con el ambiente de control interno de la organización.

Recomendación AI4.2.

El Especialista de Base de Datos de TI debe poner en marcha programas y procedimientos de conocimiento y conciencia de los objetivos TI a la gerencia ejecutiva de la corporación, para permitirles tomar posesión del sistema, de los datos y ejercer la responsabilidad por la entrega y calidad del servicio y del control interno. Archivar la información en formato digital e impreso.

Punto de vista AI4.2. Se acepta la observación.

AI5. Adquirir recursos de TI

AI5.1. Control de adquisición

Observación AI5.1.

La Gerencia TI cuenta con un plan de adquisición que no está estructurado.

Criterio AI5.1.

"Desarrollar y seguir un conjunto de procedimientos y estándares consistente con el proceso general de adquisiciones de la organización y con la estrategia de adquisición, para garantizar que la adquisición de infraestructura, instalaciones, hardware, software y servicios relacionados con TI, satisfagan los requerimientos del negocio".

Condición AI5.1.

- Existe documentación en formato digital que está incompleta y desactualizada referente al plan de adquisiciones.
- Se cumple parcialmente con los objetivos del plan de adquisiciones.
- La adquisición de servicios y/o bienes TI, está alineado con los procesos corporativos de adquisición de la corporación en forma general.

Evidencia AI5.1.

Prueba Sustantiva No.3, **Ver CD Anexos → Documento "ANEXO F.docx".**

Causa AI5.1.

Falta de procedimientos y estándares consistentes con el proceso general de estrategia de adquisiciones de la organización.

Efecto AI5.1.

- No contar un soporte tecnológico para las aplicaciones del negocio.
- No proporcionar plataformas adecuadas en el momento oportuno para las aplicaciones del negocio, de acuerdo con la arquitectura definida de TI y los estándares de tecnología.

Recomendación AI5.1.

El Especialista de Base de Datos debe reestructurar y fortalecer el plan para adquirir, implantar y mantener la infraestructura tecnológica que satisfaga los requerimientos establecidos funcionales y técnicos del negocio. El plan debe considerar extensiones futuras para adiciones de capacidad, costos de transición, riesgos tecnológicos y vida útil de la inversión para actualizaciones de tecnología. Este Plan de Adquisiciones de Tecnología debe estar alineado al Plan de Infraestructura Tecnológica. Archivar la información en formato digital e impreso.

Punto de vista AI5.1. Se acepta la observación.

ENTREGAR Y DAR SOPORTE (DS)

Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operacionales.

Por lo general abarca los siguientes objetivos de control:

DS1. Definir y administrar los niveles de servicio.

DS2. Administrar los servicios de terceros.

DS3. Administrar el desempeño y la capacidad.

DS4. Garantizar la continuidad del servicio.

DS5. Garantizar la seguridad de los sistemas.

DS6. Identificar y asignar costos.

DS8. Administrar la mesa de servicio y los incidentes.

DS10. Administración de problemas.

DS11. Administrar los datos.

DS12. Administración del ambiente físico.

DS1. Definir y administrar los niveles de servicio

DS1.2. Definición de servicios

Observación DS1.2.

La Gerencia TI cuenta con documentación incompleta y desactualizada referente al catalogo o portafolio de servicios TI.

Criterio DS1.2.

"Definiciones base de los servicios de TI sobre las características del servicio y los requerimientos de negocio, organizados y almacenados de manera centralizada por medio de la implantación de un enfoque de catálogo/portafolio de servicios".

Condición DS1.2.

- Existe documentación en formato digital incompleta y desactualizada referente al catalogo o portafolio de servicios TI.
- No existen políticas y procedimientos generales para la organización asociadas a las relaciones proveedor/usuario.
- No existen políticas y procedimientos de la función de servicios de información relacionadas con acuerdos de nivel de servicio y métodos de seguimiento de desempeño.
- Los usuarios apropiados están parcialmente conscientes del acuerdo de nivel de servicio del portafolio de servicios TI.
- Para reportar la disponibilidad de los servicios TI hacia los objetivos del negocio, se trabaja con contratos informales más no con ANS.

Evidencia DS1.2.

Cuestionario No.12, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa DS1.2.

Se cuenta con documentación incompleta de la función de servicios de información relacionada con el reporte de desempeño de nivel de servicio y programas de mejora del servicio.

Efecto DS1.2.

Uso de contratos informales, más no el uso correcto de ANS (acuerdos de nivel de servicio).

Recomendación DS1.2.

El Especialista de Redes y Comunicaciones de TI debe analizar y poner en uso los ANS (acuerdos de nivel de servicios) para determinar que se definen y alcancen las provisiones cualitativas y cuantitativas que confirman las obligaciones del acuerdo de nivel de servicio seleccionado para confirmar que los procedimientos de solución de problemas, específicamente el desempeño bajo sean incluidos y llevados a cabo. Archivar la información en formato digital e impreso.

Punto de vista DS1.2. Se acepta la observación.

DS2. Administrar los servicios de terceros

DS2.1. Identificación de todas las relaciones con proveedores

Observación DS2.1.

No se cataloga a los proveedores por: tipo de proveedor, importancia y/o criticidad.

Criterio DS2.1.

"Identificar todos los servicios de los proveedores y catalogarlos de acuerdo con el tipo de proveedor, la importancia y la criticidad. Mantener documentación formal de las relaciones técnicas y organizacionales incluyendo los roles y responsabilidades, metas, expectativas, entregables esperados y credenciales de los representantes de estos proveedores".

Condición DS2.1.

- Existe documentación en formato digital que está incompleta y desactualizada referente a los servicios de proveedores.
- Informalidad de las relaciones con los proveedores y la existencia de contratos.
- El desempeño del proveedor no es controlado por indicadores de cumplimiento en cuanto a desempeño, fechas límite y especificaciones de costos.

Evidencia DS2.1.

Prueba Sustantiva No.4, **Ver CD Anexos → Documento "ANEXO F.docx".**

Causa DS2.1.

Falta de normatividad y procedimientos en los servicios de proveedores.

Efecto DS2.1.

- Provisiones que no describen, coordinan y comunican la relación entre el proveedor y el usuario de los servicios de información.
- La no aprobación de todos los contratos por parte de la administración y el consejo legal.

Recomendación DS2.1.

El Especialista de Redes y Comunicaciones de TI debe realizar una revisión detallada de cada uno de los contratos de proveedores para determinar provisiones cualitativas y cuantitativas que confirmen la definición de las obligaciones. Mejorar la base y su clasificación de datos existe. Archivar la información en formato digital e impreso.

Punto de vista DS2.1. Se acepta la observación.

DS3. Administrar el desempeño y la capacidad

DS3.1. Planeación del desempeño y la capacidad

Observación DS3.1.

No se cuenta con un proceso, plan o marco de trabajo definido para la revisión del desempeño de los recursos TI.

Criterio DS3.1.

"Establecer un proceso de planeación para la revisión del desempeño y la capacidad de los recursos de TI, para asegurar la disponibilidad de la capacidad y del desempeño, con costos justificables, para procesar las cargas de trabajo acordadas tal como se determina en los ANS (acuerdos de nivel de servicios). Los planes de capacidad y desempeño deben hacer uso de técnicas de modelado apropiadas para producir un modelo de desempeño, de capacidad y de rendimiento de los recursos de TI, tanto actual como pronosticado".

Condición DS3.1.

- El desempeño de los recursos TI se revisa en base a los proyectos cumplidos.
- No hay documentación de respaldo.

Evidencia DS3.1.

Prueba de Cumplimiento No.5, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa DS3.1.

Falta de normatividad y procedimientos para el desempeño de los recursos TI.

Efecto DS3.1.

- Falta de reportes de desempeño en cuanto a oportunidades de mejora o solución de debilidades.
- Las expectativas de desempeño de los recursos TI no satisfacen las necesidades de los usuarios.
- Problemas específicos encontrados y el aseguramiento de la efectividad del proceso de solución de problemas débilmente puesto en marcha.

Recomendación DS3.1.

El Especialista y Técnicos de Redes y Comunicaciones de TI deben realizar pruebas de las necesidades del negocio, para asegurar que los términos y requerimientos de disponibilidad de los recursos TI reflejan adecuadamente una ayuda oportuna a estas necesidades. Además implantar procedimientos para la medición continua del desempeño de los recursos TI, para tener periódicamente un reporte de desempeño producido y revisado por la Gerencia TI. Archivar la información en formato digital e impreso.

Punto de vista DS3.1. Se acepta la observación.

DS3.5. Monitoreo y reporte

Observación DS3.5.

No se trabaja con ANS (acuerdos de nivel de servicio) para reportar la disponibilidad del los servicios TI.

Criterio DS3.5.

"Monitorear continuamente el desempeño y la capacidad de los recursos de TI. La información reunida sirve para dos propósitos:

- Mantener y poner a punto el desempeño actual dentro de TI y atender temas como resiliencia, contingencia, cargas de trabajo actuales y proyectadas, planes de almacenamiento y adquisición de recursos.
- Para reportar la disponibilidad hacia el negocio del servicio prestado como se requiere en los ANS (acuerdos de nivel de servicio). Acompañar todos los reportes de excepción con recomendaciones para llevar a cabo acciones correctivas".

Condición DS3.5.

- Existe documentación en formato digital que está desactualizada e incompleta referente al monitoreo continuo del desempeño y la capacidad de los recursos de TI.
- Para reportar la disponibilidad de los servicios TI hacia los objetivos del negocio, se trabaja con contratos informales más no con ANS.

Evidencia DS3.5.

CheckList No.8, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS3.5.

Falta de documentación y procesos referente al tema.

Efecto DS3.5.

Reportes de desempeño erróneos en cuanto a oportunidades de mejora o solución de debilidades. Problemas específicos no encontrados para el aseguramiento de la efectividad del proceso.

Recomendación DS3.5.

La Gerencia de TI debe trabajar de manera regular con ANS para verificar y asegurar que las expectativas de desempeño están siendo alcanzadas en lo referente a capacidad, respuesta y disponibilidad de los recursos TI. Realizar verificación periódica del reporte de desempeño producido. Archivar la información en formato digital e impreso.

Punto de vista DS3.5. Se acepta la observación.

DS4. Garantizar la continuidad del servicio

DS4.1. Marco de trabajo de continuidad de TI

Observación DS4.1.

La Gerencia TI no cuenta con un marco de trabajo de continuidad TI.

Criterio DS4.1.

"Desarrollar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. El objetivo del marco de trabajo es ayudar en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias.

El marco de trabajo debe tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI. El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación".

Condición DS4.1.

- No se toma en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes; así como las reglas y estructuras para documentar, probar y ejecutar la recuperación de desastres y los planes de contingencia de TI.
- No se considera puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación.
- Teóricamente se cuenta con un plan de contingencia, pero no se pone en práctica.

Evidencia DS4.1.

Cuestionario No.13, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa DS4.1.

Falta de procesos y normatividad para la creación de un plan de continuidad TI.

Efecto DS4.1.

La Gerencia TI no ayuda en la determinación de la resistencia requerida de la infraestructura y de guiar el desarrollo de los planes de recuperación de desastres y de contingencias.

Recomendación DS4.1.

La Especialista de Redes y Comunicaciones de TI debe implantar un marco de trabajo de continuidad de TI para soportar la continuidad del negocio con un proceso consistente a lo largo de toda la organización. Tomar en cuenta la estructura organizacional para administrar la continuidad, la cobertura de roles, las tareas y las responsabilidades de los proveedores de servicios internos y externos, su administración y sus clientes.

El plan debe también considerar puntos tales como la identificación de recursos críticos, el monitoreo y reporte de la disponibilidad de recursos críticos, el procesamiento alternativo y los principios de respaldo y recuperación. Archivar la información en formato digital e impreso.

Punto de vista DS4.1. Se acepta la observación.

DS4.3. Recursos críticos de TI

Observación DS4.3.

La Gerencia TI no centraliza la atención en puntos determinados como los más críticos, para construir resistencia y establecer prioridades en situaciones de recuperación.

Criterio DS4.3.

"Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio".

Condición DS4.3.

- No existe documentación que respalde la centralización de la atención de puntos determinados como los más críticos en el plan de continuidad de TI.
- Al no contar con un plan de continuidad TI, no se centra la atención en puntos determinados como los más críticos, para construir resistencia y establecer prioridades en situaciones de recuperación.
- No existen planes de recuperación de desastre/contingencia, que sean actuales y que sea comprendido por todas las partes afectadas.
- Teóricamente existe planes de contingencia, pero no están desarrollados tomando como base la no disponibilidad de los recursos físicos para llevar a cabo procesamientos críticos manuales y computarizados.

Evidencia DS4.3.

Cuestionario No.14, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa DS4.3.

Falta de procesos y normatividad para centralizar la atención en puntos determinados como los más críticos**.**

Efecto DS4.3.

No existe procedimientos de resistencia y de establecimiento de prioridades en situaciones de recuperación.

Recomendación DS4.3.

El Especialista de Redes y Comunicaciones de TI debe implantar un plan de continuidad TI y ejecutar una revisión detallada de los objetivos del plan para asegurar una centralización de los puntos más críticos y la creación de una estrategia apropiada para garantizar la continuidad general del negocio.

Punto de vista DS4.3. Se acepta la observación.

DS5. Garantizar la seguridad de los sistemas

DS5.2. Plan de seguridad de TI

Observación DS5.2.

La Gerencia TI cuenta con un plan de seguridad TI que no contiene los suficientes procedimientos y políticas de seguridad.

Criterio DS5.2.

"Trasladar los requerimientos de información del negocio, la configuración de TI, los planes de acción del riesgo de la información y la cultura sobre la seguridad en la información a un plan global de seguridad de TI. El plan se implementa en políticas y procedimientos de seguridad en conjunto con inversiones apropiadas en servicios, personal, software y hardware. Las políticas y procedimientos de seguridad se comunican a los interesados y a los usuarios".

Condición DS5.2.

- Existe documentación en formato digital referente al plan de seguridad estratégico TI que está incompleta y desactualizada.

- La Gerencia TI no cuenta con una unidad de apoyo de seguridad centralizada responsable de asegurar el acceso apropiado a los recursos del sistema.
- No se cuenta con reportes de violaciones a la seguridad y procedimientos formales de solución de problemas.

Evidencia DS5.2.

CheckList No.9, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS5.2.

Falta de procesos y normatividad para fortalecer el plan de seguridad TI.

Efecto DS5.2.

Accesos inapropiados por parte de los usuarios a los recursos del sistema, empleados no verificados como usuarios legítimos o antiguos empleados que cuenten aún con acceso, la falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones.

Recomendación DS5.2.

El Especialista de Redes y Comunicaciones de TI debe reforzar el contenido del plan de seguridad TI y realizar una revisión detallada de la seguridad de los sistemas de información, incluyendo evaluaciones de penetración de la seguridad física y lógica de los recursos computacionales, de comunicación, etc. Realizar un análisis de viabilidad sobre la implantación de un área de Seguridad Centralizada, poniendo en claro los pros y los contra. Archivar la información en formato digital e impreso.

Punto de vista DS5.2. Se acepta la observación.

DS6. Identificar y asignar costos

DS6.1. Definición de servicios

Observación DS6.1.

La Gerencia TI tiene escasa información referente a la identificación y asignación de costos.

Criterio DS6.1.

"Identificar todos los costos de TI y equipararlos a los servicios de TI para soportar un modelo de costos transparente. Los servicios de TI deben vincularse a los procesos del negocio de forma que el negocio pueda identificar los niveles de facturación de los servicios asociados".

Condición DS6.1.

- Existe documentación en formato digital que está incompleta y desactualizada referente a los costos y servicios TI.
- No existe una metodología de asignación de costos, que los usuarios están de acuerdo en cuanto a su equidad.

Evidencia DS6.1.

CheckList No.10, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS6.1.

Falta de procesos y normatividad en la asignación de costos.

Efecto DS6.1.

Pocas oportunidades para una mayor efectividad y propiedad de la metodología de facturación.

Recomendación DS6.1.

El Gerente de TI debe hacer uso de una metodología de asignación de costos, llevando a cabo una revisión detalla de la distribución de reportes en cuanto a utilización e información de costos. Archivar la información en formato digital e impreso.

Punto de vista DS6.1. Se acepta la observación.

DS6.3. Modelación de costos y cargos

Observación DS6.3.

La Gerencia TI no cuanta con un modelo solido de costos.

Criterio DS6.3.

"Con base en la definición del servicio, definir un modelo de costos que incluya costos directos, indirectos y fijos de los servicios, y que ayude al cálculo de tarifas de reintegros de cobro por servicio. El modelo de costos debe estar alineado con los procedimientos de contabilización de costos de la empresa.

El modelo de costos de TI debe garantizar que los cargos por servicios son identificables, medibles y predecibles por parte de los usuarios para propiciar el adecuado uso de recursos. La gerencia del usuario debe poder verificar el uso actual y los cargos de los servicios".

Condición DS6.3.

- Existe documentación en formato digital que está incompleta y desactualizada referente al modelo de costos de los servicios de TI.
- Dentro de los elementos de la función de servicios de información no se cuenta con metodología o algoritmo de asignación de costos.

Evidencia DS6.3.

CheckList No.11, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS6.3.

Falta de procesos y normatividad en el modelo de costos.

Efecto DS6.3.

Inconsistencias dentro del modelo de costos, pocas oportunidades para el usuario con el fin de aplicar de una mejor manera los recursos de servicios de información para alcanzar los requerimientos de negocios.

Recomendación DS6.3.

El Gerente de TI debe ejecutar un fortalecimiento del modelo de costos y que cuente con un algoritmo real para compilar y asignar costos a facturación. Se lleven a cabo revisiones de consistencia de la facturación entre los diferentes usuarios. Archivar la información en formato digital e impreso.

Punto de vista DS6.3. Se acepta la observación.

DS8. Administrar la mesa de servicios y los incidentes

DS8.1. Mesa de servicios

Observación DS8.1.

Se cumple parcialmente con la función de mesa de servicios.

Criterio DS8.1.

"Establecer la función de mesa de servicio, la cual es la conexión del usuario con TI, para registrar, comunicar, atender y analizar todas las llamadas, incidentes reportados, requerimientos de servicio y solicitudes de información. Deben existir procedimientos de monitoreo y escalamiento basados en los niveles de servicio acordados en los ANS (acuerdo de nivel de servicios), que permitan clasificar y priorizar cualquier problema reportado como incidente, solicitud de servicio o solicitud de información. Medir la satisfacción del usuario final respecto a la calidad de la mesa de servicios y de los servicios de TI".

Condición DS8.1.

- Existe documentación en formato digital que está incompleta y desactualizada referente a la mesa de servicios.
- Ocurre interacciones inadecuadas de las actividades del buró de ayuda con respecto a otras funciones dentro de la función de servicios de información, así como a las organizaciones usuarias.
- Se cuenta con procedimientos y actividades insuficientes relacionadas con problemas en el reporte de recepción, registro, seguimiento, escalamiento y solución de incidentes.

Evidencia DS8.1.

Prueba Sustantiva No.5, **Ver CD Anexos → Documento "ANEXO F.docx".**

Causa DS8.1.

No se aplica un marco de referencia para definir Acuerdos de Niveles de Servicio.

Efecto DS8.1.

- Ineficiencia en el uso de recursos.
- Atención deficiente a los usuarios.
- La falta de registro y control de todos los problemas e incidentes, puede ocasionar que existan problemas que no se hayan resuelto debidamente y a tiempo.
- El no realizar una medición de satisfacción de usuarios da lugar a que se pierda la cultura de autocontrol y de que las oportunidades de mejora del procedimiento no se materialicen.

Recomendación DS8.1.

El Especialista de Redes y Comunicaciones de TI debe definir y poner en práctica cronogramas de revisiones periódicas de los incidentes reportados para determinar que todos los incidentes fueron solucionados correctamente, en el tiempo oportuno. Archivar la información en formato digital e impreso.

Punto de vista DS8.1. Se acepta la observación.

DS8.5. Análisis de tendencias

Observación DS8.5.

No se hace un reporte estadístico del desempeño de los servicios y tiempos de respuesta referentes a las actividades de la mesa de servicios.

Criterio DS8.5.

"Emitir reportes de la actividad de la mesa de servicios para permitir a la gerencia medir el desempeño del servicio y los tiempos de respuesta, así como para identificar tendencias de problemas recurrentes de forma que el servicio pueda mejorarse de forma continua".

Condición DS8.5.

- Existe documentación en formato digital que está incompleta y desactualizada referente a las mediciones de desempeños y tiempo de respuesta de las actividades de la mesa de servicios.
- La Gerencia TI maneja una bitácora de soporte, la cual emite reportes de incidentes proporcionado información básica como hora de inicio y final del incidente.
- Se maneja de manera muy general los reportes de la actividad de la mesa de servicios.

Evidencia DS8.5.

Prueba de Cumplimiento No.6, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa DS8.5.

Falta de normatividad y procedimientos en los reportes de la mesa de servicios para poder medir su desempeño y tiempos de respuesta.

Efecto DS8.5.

- Interacciones inadecuadas de las actividades del buró de ayuda con respecto a otras funciones dentro de la función de servicios de información, así como a las organizaciones usuarias.
- Procedimientos y actividades insuficientes relacionadas con problemas en el reporte de recepción, registro, seguimiento, escalamiento y solución de preguntas.
- Oportunidad inadecuada en el reporte de problemas o insatisfacción del usuario en cuanto al proceso de reporte de problemas.

Recomendación DS8.5.

El Especialista de Redes y Comunicaciones de TI debe realizar una revisión de la competencia y capacidad del personal del buró de ayuda con respecto a la realización de sus tareas, además de una revisión de los reportes de tendencias y posibles oportunidades de mejoras de desempeño en la mesa de servicios. Archivar la información en formato digital e impreso.

Punto de vista DS8.5. Se acepta la observación.

DS10. Administración de problemas

DS10.1. Identificación y administración de problemas

Observación DS10.1.

No se cuanta con un área clave de administración de incidentes.

Criterio DS10.1.

"Implementar procesos para reportar y clasificar problemas que han sido identificados como parte de la administración de incidentes. Los pasos involucrados en la clasificación de problemas son similares a los pasos para clasificar incidentes; son determinar la categoría, impacto, urgencia y prioridad. Los problemas deben categorizarse de manera apropiada en grupos o dominios relacionados (por ejemplo, hardware, software, software de soporte). Estos grupos pueden coincidir con las responsabilidades organizacionales o con la base de usuarios y clientes, y son la base para asignar los problemas al personal de soporte".

Condición DS10.1.

- Teóricamente se cuenta con un grupo de trabajo encargado de detectar incidentes, pero no está legalizado dentro del organigrama de la Gerencia TI.
- Existe documentación en formato digital que está incompleta y desactualizada referente a la detección de incidentes TI.
- No existen procedimientos para seguir las tendencias de incidentes críticos para maximizar recursos TI.

Evidencia DS10.1.

CheckList No.12, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS10.1.

Falta de procesos y normatividad en el manejo de incidentes.

Efecto DS10.1.

Ocurrencias de problemas reconocidos pero no resueltos por proceso de manejo de problemas, variaciones entre los eventos de procesos reales y formales con respecto a la solución de problemas y deficiencias de los usuarios en el proceso de manejo, comunicación y solución de problemas.

Recomendación DS10.1.

El Especialista de Redes y Comunicaciones conjuntamente con la aprobación del Gerente de TI deben conformar reglamentariamente un grupo o área clave de administración de incidentes para manejar correctamente la identificación de problemas reportados, pruebas que aseguren que los procedimientos de manejo de problemas fueron seguidos para todas las actividades no-estándar, incluyendo:

- Registro de todos los eventos no-estándar por proceso.
- Seguimiento y solución de todos y cada una de los eventos.
- Nivel apropiado de respuesta tomando como base la prioridad del evento.
- Escalamiento de problemas para eventos críticos.
- Reporte apropiado dentro de la función de servicios de información y grupos usuarios.
- Revisiones regulares de efectividad y eficiencia de procesos en cuanto a mejoras.
- Expectativas y éxito de programa de mejoras del desempeño.

Archivar la información en formato digital e impreso.

Punto de vista DS10.1. Se acepta la observación.

DS10.2. Rastreo y resolución de problemas

Observación DS10.2.

La Gerencia TI no cuenta con un sistema de administración de problemas.

Criterio DS10.2.

"El sistema de administración de problemas debe mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados considerando: • Todos los elementos de configuración asociados • Problemas e incidentes sobresalientes • Errores conocidos y sospechados. Identificar e iniciar soluciones sostenibles indicando la causa raíz, incrementando las solicitudes de cambio por medio del proceso de administración de cambios establecido. En todo el proceso de resolución, la administración de problemas debe obtener reportes regulares de la administración de cambios sobre el progreso en la resolución de problemas o errores. La administración de problemas debe monitorear el continuo impacto de los problemas y errores conocidos en los servicios a los usuarios. En caso de que el impacto se vuelva severo, la administración de problemas debe escalar el problema".

Condición DS10.2.

- Existe documentación en formato digital que está incompleta y desactualizada, para en un futuro definir e implementar un sistema de manejo de problemas.
- No se realiza un monitoreo continuo del impacto de los problemas y errores en los servicios a los usuarios.
- No existen procedimientos de manejo de problemas que aseguren la suficiencia del alcance de una auditoría informática para incidentes TI.
- No existen procedimientos de manejo de problemas para: registrar, analizar y resolver de manera oportuna todos los eventos no-estándar.

Evidencia DS10.2.

CheckList No.13, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS10.2.

No existe un sistema de administración de problemas.

Efecto DS10.2.

Ocurrencias de problemas no controlados formalmente por el proceso de manejo de problemas.

Recomendación DS10.2.

El Especialista de Redes y Comunicaciones de TI debe realizar un análisis de viabilidad sobre la implantación de un sistema de administración de problemas, poniendo en claro los pros y los contra. El sistema ayudará a mantener pistas de auditoría adecuadas que permitan rastrear, analizar y determinar la causa raíz de todos los problemas reportados. Realizar un monitoreo continuo del impacto de los problemas y errores conocidos en los servicios TI. Archivar la información en formato digital e impreso.

Punto de vista DS10.2. Se acepta la observación.

DS11. Administrar los datos

DS11.1. Requerimientos del negocio para administración de datos

Observación DS11.1.

Falta de mecanismos para garantizar que el negocio reciba los documentos originales que espera.

Criterio DS11.1.

"Establecer mecanismos para garantizar que el negocio reciba los documentos originales que espera, que se procese toda la información recibida por parte del negocio, que se preparen y entreguen todos los reportes de salida que requiere el negocio y que las necesidades de reinicio y reproceso estén soportadas".

Condición DS11.1.

- Existe documentación en formato digital que está incompleta y desactualizada referente a mecanismos para la entrega de documentación
- Existen formas de entrada y salida sensibles de documentación no protegida.
- Existen reportes de salidas de documentación no útiles a los usuarios.

Evidencia DS11.1.

Observación Directa No.3, **Ver CD Anexos → Documento "ANEXO G.docx".**

Causa DS11.1.

Falta de normatividad y procedimientos para garantizar que el negocio reciba los documentos originales que espera**.**

Efecto DS11.1.

- Reportes de salidas no útiles a los usuarios.
- Datos transmitidos sin controles adicionales, incluyendo:
    - Accesos de envío/recepción de transmisiones limitados
    - Autorización e identificación apropiadas del emisor y del receptor.
    - Medios seguros de transmisión.

Recomendación DS11.1.

El Especialista de Base de Datos de TI debe implantar nuevos procedimientos y fortalecer las actuales referentes a garantizar que el negocio reciba la documentación esperada. Realizar pruebas específicas durante la preparación de datos, el procesamiento de entradas, el procesamiento de datos, la salida, distribución o integración, el manejo de errores en todas las fases del procesamiento, la integridad de los datos a través del manejo de errores en todas las fases del procesamiento, la retención y destrucción de la información.

Punto de vista DS11.1. Se acepta la observación.

DS11.2. Acuerdos de almacenamiento y conservación

Observación DS11.2.

No se realiza respaldos continuos de los datos.

Criterio DS11.2.

"Definir e implementar procedimientos para el archivo y almacenamiento de los datos, de manera que los datos permanezcan accesibles y utilizables. Los procedimientos deben considerar los requerimientos de recuperación, la rentabilidad, la integridad continua y los requerimientos de seguridad. Para cumplir con los requerimientos legales, regulatorios y de negocio, establecer mecanismos de almacenamiento y conservación de documentos, datos, archivos, programas, reportes y mensajes (entrantes y salientes), así como la información (claves, certificados) utilizada para encripción y autenticación".

Condición DS11.2.

- Existe documentación escasa referente a procedimientos para el archivo y almacenamiento de los datos.
- Existe procedimientos para el archivo y almacenamientos de datos, pero no están definidos.
- La estrategia de respaldos y restauración de medios no es la apropiada.
- Los sitios de almacenamiento de medios son seguros físicamente, pero no se lleva un inventario actualizado.

Evidencia DS11.2.

Observación Directa No.4, **Ver CD Anexos → Documento "ANEXO G.docx".**

Causa DS11.2.

Falta de normatividad y procedimientos para el archivo y almacenamiento de los datos.

Efecto DS11.2.

Perdida de datos importantes para la corporación.

Recomendación DS11.2.

El Especialista de Base de Datos de TI debe implantar procedimientos para el archivo y almacenamiento de datos de toda la corporación. Además respaldar la información continuamente.

Punto de vista DS11.2. Se acepta la observación.

DS12. ADMINISTRACIÓN DEL AMBIENTE FÍSICO

DS12.2. Medidas de seguridad física

Observación DS12.2.

No se implanta las medidas de seguridad físicas necesarias.

Criterio DS12.2.

"Definir e implementar medidas de seguridad físicas alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción.

En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física".

Condición DS12.2.

- Existe documentación en formato digital que está incompleta y desactualizada referente a la implementación de medidas de seguridad físicas alineadas con los requerimientos del negocio.
- Existe documentación en forma digital que está incompleta y desactualizada referente al plan de recuperación/contingencia en caso de desastre.
- No existe una copia del documento de planeación de recuperación/contingencia en caso de desastre.
- Los procedimientos de acceso lógico y físico no son suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones.
- No se lleva a cabo una revisión de los procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma para los diferentes niveles de emergencias ambientales.

Evidencia DS12.2.

CheckList No.14, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa DS12.2.

Falta de procesos y normatividad en la implementación de medidas de seguridad.

Efecto DS12.2.

Insuficiencia de extinguidores de incendios, sistemas de aspersión, UPS y drenaje. Discrepancias en la bitácora de visitantes y en los gafetes de visitantes.

Recomendación DS12.2.

El Especialista y Técnicos de Redes y Comunicaciones de TI deben analizar e implantar las medidas de seguridad faltantes como: procedimientos de acceso lógico y físico suficientes, incluyendo perfiles de seguridad de acceso para empleados, proveedores, equipo y personal de mantenimiento de las instalaciones y procedimientos de aviso contra incendio, cambios de clima, problemas eléctricos y procedimientos de alarma para los diferentes niveles de emergencias ambientales.

Desarrollar un plano físico contra bosquejos del edificio y dispositivos de seguridad. Tener una copia actualizada del documento de planeación de recuperación/contingencia en caso de desastre. Archivar la información en formato digital e impreso.

Punto de vista DS12.2. Se acepta la observación.

MONITOREAR Y EVALUAR (ME)

Todos los procesos de TI deben evaluarse de forma regular en el tiempo en cuanto a su calidad y cumplimiento de los requerimientos de control. Este dominio abarca la administración del desempeño, el monitoreo del control interno, el cumplimiento de requerimientos externos y la aplicación del gobierno.

Por lo general abarca los siguientes objetivos de control:

ME1. Monitorear y evaluar el desempeño de TI.

ME2. Monitorear y evaluar el control interno.

ME3. Garantizar el cumplimiento con requerimientos externos.

ME4. Proporcionar gobierno de TI.

ME1. Monitorear y evaluar el desempeño de TI

ME1.3. Método de monitoreo

Observación ME1.3.

Bajo nivel de conocimiento por parte de las unidades de la corporación referente al método de monitoreo implantado, BalancedScoreCard.

Criterio ME1.3.

"Garantizar que el proceso de monitoreo implante un método (ej. Balanced Scorecard), que brinde una visión sucinta y desde todos los ángulos del desempeño de TI y que se adapte al sistema de monitoreo de la empresa".

Condición ME1.3.

- El BSC mezcla los indicadores estratégicos y operativos.
- Falta de referencia al rol de los proveedores.
- No se enfatiza el papel del benchmarking para validar la excelencia de los indicadores.
- No diagnostica la situación inicial de la organización.
- No se consideran de forma sistemática variables externas como el entorno y el impacto en la sociedad.

Evidencia ME1.3.

Prueba de Cumplimiento No.7, **Ver CD Anexos → Documento "ANEXO D.docx".**

Causa ME1.3.

Poco conocimiento sobre las desventajas que podría ocasionar BSC en la corporación, por más mínimas que estas sean.

Efecto ME1.3.

- Falta de comprensión de que el BSC es un medio, no un fin, de ahí la cantidad de problemas que puede generar en la corporación.
- Las estrategias sin acción no conducen a nada concreto, por lo tanto algunos resultados del BSC no muestran lo que la alta gerencia debe conocer y medir.
- No todas las áreas de la empresa se involucran adecuadamente y menos aún se comprometen decididamente con el programa.

Recomendación ME1.3.

El Gerente de TI debe realizar mediciones "Benchmarking" referente al monitoreo del desempeño respecto a organizaciones similares. Además permanentemente poner en ejecución una revisión de la relevancia de los datos dentro de los procesos que se están monitoreando y del desempeño real contra lo planeado en todas las áreas de la función de servicios de información. Analizar el grado de cumplimiento de las metas de desempeño e iniciativas de mejoramiento para así evitar cualquier aspecto desfavorable para la corporación. Archivar la información en formato digital e impreso.

Punto de vista ME1.3. Se acepta la observación.

ME1.5. Reportes al consejo directivo y a ejecutivos

Observación ME1.5.

La Gerencia TI cuenta no cuenta con procedimientos establecidos para reportes al Consejo Directivo y a ejecutivos.

Criterio ME1.5.

"Proporcionar reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI, niveles de servicio de programas individuales y la contribución de TI a ese desempeño. Los reportes de estatus deben incluir el grado en el que se han alcanzado los objetivos planeados, los entregables obtenidos, las metas de desempeño alcanzadas y los riesgos mitigados. Durante la revisión, se debe identificar cualquier desviación respecto al desempeño esperado y se deben iniciar y reportar las medidas administrativas adecuadas".

Condición ME1.5.

- Existe documentación en formato digital que está incompleta y desactualizada referente a los reportes administrativos en formato digital.
- Dentro de los reportes de las actividades de la función de servicios de información no se incluye reportes de auditorías internas, reportes de auditorías externas, encuestas de satisfacción de los usuarios y minutas del comité de auditoría.

- Se trata parcialmente que los reportes internos de la utilización de los recursos de la función de servicios de información (gente, instalaciones, aplicaciones, tecnología y datos) sean adecuados.
- No es suficiente confiabilidad y utilidad de los reportes de desempeño para no usuarios, tales como auditor externo, comité de auditoría y alta administración de la organización.

Evidencia ME1.5.

Cuestionario No.15, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa ME1.5.

Falta de políticas y procedimientos para proporcionar reportes a ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño del portafolio empresarial de programas de inversión habilitados por TI.

Efecto ME1.5.

No existe una evaluación técnica del desempeño real contra lo planeado en todas las áreas de la función de servicios de información.

Recomendación ME1.5.

El Gerente de TI debe fortalecer los reportes administrativos para ser revisados por la alta dirección sobre el avance de la organización hacia metas identificadas, específicamente en términos del desempeño de servicios TI. Dentro de los reportes de las actividades de la función de servicios de información incluir reportes de auditorías internas, reportes de auditorías externas, encuestas de satisfacción de los usuarios y minutas del comité de auditoría. Además brindar la suficiente confiabilidad y utilidad de los reportes de desempeño para no usuarios, tales como auditores externos. Archivar la información en formato digital e impreso.

Punto de vista ME1.5. Se acepta la observación.

ME2. Monitorear y evaluar el control interno

ME2.1. Monitoreo del marco de trabajo de control interno

Observación ME2.1.

La Gerencia TI no realiza un monitoreo continuo del marco de control interno.

Criterio ME2.1.

"Monitorear de forma continua el ambiente de control y el marco de control de TI. Se debe realizar la evaluación usando mejores prácticas de la industria y se debería utilizar benchmarking para mejorar el ambiente y el marco de trabajo de control de TI".

Condición ME2.1.

No existe evidencia de que la corporación haya implementado un proceso de monitoreo y seguimiento para el ambiente de control TI, que garantice que las acciones implementadas por recomendaciones de auditorías y exámenes especiales hayan sido desarrolladas en términos de eficiencia y efectividad.

Evidencia ME2.1.

Prueba Sustantiva No.6, **Ver CD Anexos → Documento "ANEXO F.docx".**

Causa ME2.1.

Falta de involucramiento de Auditoría Informática externa e interna.

Efecto ME2.1.

No proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

Recomendación ME2.1.

El Gerente de TI debe implementar un procedimiento para el monitoreo del marco de trabajo de control interno TI, cuyo objetivo sea una revisión permanente de los controles internos de toda la organización y en particular de la función de servicios de información para asegurar la suficiencia de la cobertura y de los diversos niveles de detalle para los responsables del proceso. Dar importancia a la ejecución de Auditorías Informáticas tanto externas como internas, para tener un análisis del grado de cumplimiento de las metas de control interno e iniciativas de mejoramiento, al igual del nivel de implantación de las recomendaciones dadas por dichas auditorías y exámenes especiales. Archivar la información en formato digital e impreso.

Punto de vista ME2.1. Se acepta la observación.

ME2.2. Revisiones de auditoría

Observación ME2.2.

La Gerencia TI no cuenta con los procedimientos necesarios para un debido reporte de los controles internos TI mediante revisiones de auditoría.

Criterio ME2.2.

"Monitorear y reportar la efectividad de los controles internos sobre TI por medio de revisiones de auditoría incluyendo, por ejemplo, el cumplimiento de políticas y estándares, seguridad de la información, controles de cambios y controles establecidos en acuerdos de niveles de servicio".

Condición ME2.2.

- Existe documentación en formato digital que está incompleta y desactualizada referente al monitoreo y reporte de la efectividad de los controles internos TI.
- Los reportes de los datos de control interno de la función de servicios de información no son adecuados.
- La respuesta de la organización a las recomendaciones de mejoramiento del control de calidad, auditoría interna y externa no es apropiada.
- No es suficiente la confiabilidad y utilidad de los reportes de control interno para auditores externos a la organización.

Evidencia ME2.2.

CheckList No. 15, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa ME2.2.

Falta de políticas y procedimientos para reportes de los controles internos TI.

Efecto ME2.2.

No existen iniciativas para implantar revisiones de auditoría y de resultados de mejoramiento del control interno TI deseable. No se cuanta con reportes adecuados de monitoreo del control interno.

Recomendación ME2.2.

El Gerente de TI debe incentivar la ejecución de revisiones de auditoría tanto internas como externas, así habrá un fortalecimiento de los reportes para que permitan una respuesta rápida ante las excepciones o incumplimientos identificados en el control interno TI. Archivar la información en formato digital e impreso.

Punto de vista ME2.2. Se acepta la observación.

ME2.4. Auto evolución del control

Observación ME2.4.

La Gerencia TI no realiza un análisis del control interno real contra lo planeado.

Criterio ME2.4.

"Evaluar la completitud y efectividad de los controles internos de la administración de los procesos, políticas y contratos de TI por medio de un programa continuo de auto-evaluación".

Condición ME2.4.

- Existe documentación en formato digital que está incompleta y desactualizada referente al programa de autoevaluación de los controles internos de la administración de los procesos, políticas y contratos de TI.
- Los datos identificados para monitorear los controles internos de la función de servicios de información no son los apropiados.
- La información concerniente a errores, inconsistencias y excepciones de control interno no se mantiene de manera sistemática y tampoco se reporta a la Gerencia TI.
- Los empleados conocen de manera general las políticas y procedimientos relativos al monitoreo del control interno.
- La alta gerencia no está satisfecha con los reportes sobre la seguridad y control interno.

Evidencia ME2.4.

CheckList No.16, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa ME2.4.

Falta de políticas y procedimientos organizacionales relacionadas con la planeación, administración, monitoreo y reporte de los controles internos.

Efecto ME2.4.

No se analiza el grado de cumplimiento de las metas de control interno e iniciativas de mejoramiento.

Recomendación ME2.4.

El Gerente de TI debe realizar revisiones continuas de la relevancia de los datos dentro de los procesos que se están monitoreando y en el reporte de los controles internos. Revisión del control interno real contra lo planeado en todas las áreas de la función de servicios de información. Archivar la información en formato digital e impreso.

Punto de vista ME2.4. Se acepta la observación.

ME3. Garantizar el cumplimiento con requerimientos externos

ME3.3. Evaluación del cumplimiento con requerimientos externos

Observación ME3.3.

No existe evidencia de supervisión efectiva para el cumplimiento de los requerimientos externos que rige a la Corporación.

Criterio ME3.3.

"Evaluar de forma eficiente el cumplimiento de las políticas, estándares y procedimientos de TI, incluyendo los requerimientos externos, con base en la supervisión del gobierno de la gerencia de TI y del negocio y la operación de los controles internos".

Condición ME3.3.

- Existe documentación en formato digital que está incompleta y desactualizada referente a la evaluación del cumplimiento de las políticas, estándares y procedimientos de TI.
- La Gerencia TI y la alta dirección, no buscan el involucramiento de auditoría, antes de decidir sobre soluciones del servicio de tecnología de Información.
- La Gerencia TI carece de un área de apoyo referente a la Auditoría Informática.

Evidencia ME3.3.

CheckList No.17, **Ver CD Anexos → Documento "ANEXO E.docx".**

Causa ME3.3.

Falta de políticas y procedimientos para garantizar la respuesta de los requerimientos externos.

Efecto ME3.3.

Indeterminación en la suficiencia y oportunidad de las certificaciones/acreditaciones. Bajo involucramiento de auditoría.

Recomendación ME3.3.

El Gerente de TI debe fortalecer las políticas y procesos para una revisión detallada que verifique los contratos de aseguramiento independiente respecto a certificaciones/acreditaciones, suficiencia y oportunidad de las revisiones de cumplimiento de requerimientos externos y de compromisos contractuales. Verificar el involucramiento proactivo de auditoría informática. Archivar la información en forma digital e impreso.

Punto de vista ME3.3. Se acepta la observación.

ME4. Proporcionar gobierno de TI

ME4.1. Establecer un marco de gobierno de TI

Observación ME4.1.

La Gerencia TI técnicamente cuenta con un Consejo Directivo formado por el gerente y por los especialistas de las tres áreas claves (Redes y Comunicaciones, Aplicativos y Base de Datos), pero no está reglamentariamente establecido dentro de la Corporación.

Criterio ME4.1.

"Trabajar con el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles y responsabilidades, requerimientos de información, y estructuras organizacionales para garantizar que los programas de inversión habilitados por TI de la empresa ofrezcan y estén alineados con las estrategias y objetivos empresariales. El marco de trabajo debería proporcionar vínculos claros entre la estrategia empresarial, el portafolio de programas de inversiones habilitadas por TI que ejecutan la estrategia, los programas de inversión individual y los proyectos de negocio y de TI que forman los programas.

El marco de trabajo debería definir una rendición de cuentas y prácticas incontrovertibles para evitar fallas de control interno y de supervisión. El marco de trabajo debería ser consistente con el ambiente completo de control empresarial y con los principios de control generalmente aceptados y estar basado en el proceso y en el marco de control de TI".

Condición ME4.1.

- El Comité Estratégico TI está formado por los integrantes del Consejo Directivo (gerente y los tres especialistas de área), pero no está legalmente establecido dentro de la Gerencia TI.
- Se cuenta con un marco de trabajo TI, pero en sí solo proporciona directrices para una buena administración, mas de son directrices de gobierno.
- Existe documentación en formato digital referente a un marco de trabajo, pero está incompleta, desactualizada y con una visión escasa a un gobierno TI.

Evidencia ME4.1.

Cuestionario No.16, **Ver CD Anexos → Documento "ANEXO C.docx".**

Causa ME4.1.

Falta de procesos y normatividad para establecer un Consejo Directivo formal.

Efecto ME4.1.

Se asegura parcialmente un vínculo e integración de las reglas del negocio con los planes de TI.

Recomendación ME4.1.

El Gerente de TI debe formalizar el consejo directivo para definir y establecer un marco de trabajo para el gobierno de TI, incluyendo liderazgo, procesos, roles, responsabilidades, requerimientos de información y estructuras organizacionales para garantizar el cumplimiento de los objetivos empresariales. Archivar la información en formato digital e impreso.

Punto de vista ME4.1. Se acepta la observación.

A continuación se presenta el certificado de la culminación de la Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), utilizando el Estándar Internacional COBIT 4.1.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- La auditoría informática se conforma obteniendo información y documentación de los riesgos críticos que tiene una organización, con el fin de elaborar informes detallados para analizar situaciones de debilidad en las que se involucran recursos informáticos.
- El trabajo del auditor consiste en lograr obtener toda la información necesaria para emitir recomendaciones orientadas a la mejora de los procesos y actividades de Tecnologías de Información, siempre amparado de las evidencias comprobatorias.
- Toda organización que posean Sistemas de Información medianamente complejos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia. Hoy en día, la mayoría de las empresas tienen toda su información estructurada en sistemas informáticos, de aquí, la vital importancia que funcionen correctamente.
- Es primordial la aplicación de un modelo de control reconocido internacionalmente, como lo es COBIT, que en la actualidad, es una herramienta para mantener el control de los procesos y actividades de TI. Este modelo exige que todos las actividades estén documentadas, aprobadas, en conocimiento, aplicadas y evaluadas por los usuarios de la organización.

- Es de relevante importancia la utilización de una guía para la puesta en marcha de un plan de auditoría, en este caso, el Marco Referencial de COBIT 4.1., facilita la gestión del auditor, al tener de antemano un grupo de directrices orientadas hacia la implantación de buenas prácticas TI.
- Lo importante al utilizar un modelo de control, cualquiera que sea ésta, es la colaboración y predisposición del personal de toda la organización, ya que cualquier control que se implemente únicamente tendrá efecto en el momento en que la gente tome conciencia de su importancia y el aporte que éste brinda al desempeño organizacional.
- Con el marco de referencia COBIT 4.1., se identificó y evaluó los procesos y actividades TI más críticos de la Corporación HOLDINGDINE S.A. (Matriz), donde se pudo dar un conjunto de observaciones y recomendaciones las cuales pueden ayudar a alinear de mejor manera la Gerencia de TI con los requerimientos del negocio.

5.2. Recomendaciones

- Hoy en día, se recomienda a las organizaciones el involucramiento de la Auditoría Informática, tanto como ente interno y/o externo, para evaluar y analizar los sistemas de información que protegen el activo más importante, la información.
- Se recomienda la implantación de la Auditoría Informática ya que permitirá recoger, agrupar e indagar evidencias para determinar si el sistema de información de las organizaciones salvaguarda el activo empresarial, si se mantiene la integridad de los datos y si se utiliza eficientemente los recursos tecnológicos.

- Se espera que a partir de las observaciones planteadas a cada uno de los procesos y actividades TI que fueron parte de la Evaluación Técnica Informática del Sistema de Información de la Corporación HOLDINGDINE S.A. (Matriz), se tomen en cuenta las recomendaciones puntualizadas en los Informes: Detallado y Ejecutivo, desde un punto de vista a la mejora continua de la Corporación.
- Se recomienda que tanto la Corporación HOLDINGDINDE S.A., como matriz, y sus subsidiarias, se inicie un proceso de implantación de un modelo de control, que puede ser COBIT, ya que éste ayuda a salvar las brechas existentes entre riesgos de negocio, necesidades de control y aspectos técnicos, proporcionando buenas prácticas a través de un Marco Referencial pre establecido.
- Se recomienda hacer el uso del presente trabajo, con el fin de tomarlo como guía para futuras mejoras en TI, además de realizar evaluaciones periódicas con el fin de medir el avance de cada uno de los procesos y actividades de la Corporación.

REFERENCIAS BIBLIOGRÁFICAS

- **[1]** Definición de Sistema: http://www.alegsa.com.ar/Dic/sistema.php
- **[2]** Chiavenato Idalberto (2006). Introducción a la Teoría General de la Administración. Séptima Edición. McGraw-Hill Interamericana. Pág. 110.
- **[3]** Ferrell O. C. y Hirt Geoffrey (2004). Introducción a los Negocios en un Mundo Cambiante. Cuarta Edición. McGraw-Hill Interamericana. Pág. 121.
- **[4]** Czinkota Michael y Kotabe Masaaki (2001). Administración de Mercadotecnia. Segunda Edición. International Thompson Editores. Pág. 115.
- **[5]** Definición de Sistema de Información: http://www.alegsa.com.ar/Dic/sistema.php
- **[6]** Kenneth C. Laudon y Jane P. Laudon (2004). Sistemas de Información Gerencial. Octava Edición. Pearson.
- **[7]** Ingeniería de Software: Una Guía para Crear Sistemas de Información (2006).
- **[8]** Definición SI: http://es.wikipedia.org/wiki/Sistema_de_informaci%C3%B3n
- **[9]** Entrada de Información: http://www.mitecnologico.com/Main/ElementosDeSistemaDeInformacion
- **[10]** Almacenamiento de Información: http://www.monografias.com/trabajos7/sisinf/sisinf.shtml
- **[11]** Procesamiento de Información: http://www.mitecnologico.com/Main/ElementosDeSistemaDeInformacion
- **[12]** Salida de Información: http://www.monografias.com/trabajos7/sisinf/sisinf.shtml
- **[13]** Importancia de los Sistemas de Información: http://www.gestiopolis.com/Canales4/mkt/simparalas.htm

- **[14]** Ralph M. Stair y George W. Reynolds (1999). Sistemas de Información: Enfoque Administrativo. Cuarta Edición. International Thompson Editores.
- **[15]** Tecnologías de la Información y la Comunicación: http://www.cibersociedad.net/archivo/articulo.php?art=218
- **[16]** Tecnologías de la Información y la Comunicación: http://iescapdellevant.org/departaments/tecno/1rbtx/tic/temas_iniciales/1_Introduccion_TIC.pdf
- **[17]** La tecnología de la Información Hoy: http://es.wikipedia.org/wiki/Tecnolog%C3%ADa_de_la_informaci%C3%B3n
- **[18]** Características de las Tecnologías de la Información y la Comunicación: http://www.cibersociedad.net/archivo/articulo.php?art=218
- **[19]** Importancia de las TIC: http://consuelomblog.blogspot.com/2007/04/qu-son-las-tics.html
- **[20]** Importancia de las TIC: http://www.measurecontrol.com/la-importancia-de-las-tic/
- **[21]** TIC como herramienta de Gestión Empresarial: http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html
- **[22]** TIC como herramienta de Gestión Empresarial: http://www.masterdopina.es/?p=141
- **[23]** Plan TIC dentro de las Organizaciones: http://www.tecnobiz.com/el-papel-de-las-tic-en-las-empresas
- **[24]** Definición PYMES: http://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa

- **[25]** Ventajas de las TIC dentro de las Organizaciones: http://cibermundos.bligoo.com/content/view/145501/Las-TIC-como-herramienta-a-la-gestion-empresarial.html
- **[26]** Estrategias Competitivas con gracias a las TIC: http://www.gestiopolis.com/Canales4/mkt/simparalas.htm
- **[27]** Gestión y Control de las TIC: http://*www.eici.ucm.cl/Academicos/ygomez/descargas/Aud_Seg.../auditoria2.ppt*
- **[28]** Definición ATM: http://es.kioskea.net/contents/technologies/atm.php3
- **[29]** Definición MPLS: http://es.wikipedia.org/wiki/Multiprotocol_Label_Switching
- **[30]** Gestión y Control de las TIC: http://www.compuredes.com.co/gestionTICs.htm
- **[31]** Concepto de Auditoría: http://members.tripod.com/~Guillermo_Cuellar_M/uno.html
- **[32]** Arthur W. Holmes (2008). Auditoría: principios y procedimiento. Novena Edición. UTEHA.
- **[33]** Concepto de Auditoría: http://aaahq.org/
- **[34]** Concepto de Auditoría: http://members.tripod.com/~Guillermo_Cuellar_M/uno.html
- **[35]** Auditoría Interna: http://www.proyectosfindecarrera.com/auditoria-interna-externa.htm
- **[36]** Auditoría Interna: http://www.deloitte.com/view/es_PE/pe/servicios/enterprise-risk-services/auditoria-interna/index.htm
- **[37]** Auditoría Externa: http://www.soloeconomia.com/presupuesto/externa-auditoria.html
- **[38]** Auditoría Externa: http://www.gerencie.com/auditoria-externa.html

- **[39]** Concepto de Auditoría Informática: http://culturaempresarialparatodos.blogspot.com/2009/02/62-auditoria-informatica.html
- **[40]** José Antonio Echenique (2001).Auditoría en Informática. Segunda Edición. McGraw Hill.
- **[41]** Definición Procesos Batch: http://www.alegsa.com.ar/Dic/proceso%20batch.php
- **[42]** Auditoría de Explotación: http://es.scribd.com/doc/18646089/TIPOS-Y-CLASES-DE-AUDITORIAS-INFORMATICAS
- **[43]** Auditoría de la Seguridad Física: http://auditoria3.obolog.com/auditoria-seguridad-fisica-876557
- **[44]** Auditoría Ofimática: http://www.ganimides.ucm.cl
- **[45]** Auditoría de Gestión: http://members.tripod.com/~Guillermo_Cuellar_M/gestion.html
- **[46]** Auditoría de Mantenimiento del Software: http://*www.innovavirtual.org*
- **[47]** Auditoría Informática de Base de Datos: http://translate.google.com.ec/translate?hl=es&langpair=en|es&u=http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/auditing.htm
- **[48]** Auditoría de Sistemas: http://auditoriasistemas.com/auditoria-de-sistemas-informaticos/
- **[49]** Auditoría de Calidad: http://informandodecalidad.wordpress.com/2008/04/09/definicion-de-auditoria-de-calidad/
- **[50]** Auditoría Informática de Redes y Comunicaciones: http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

- **[51]** Auditoría de Aplicaciones: http://www.wiziq.com/tutorial/38314-auditoria-de-aplicaciones
- **[52]** Auditoría Jurídica de Entornos Informáticos http://www.innovavirtual.org
- **[53]** Importancia de la Auditoría Informática: http://www.monografias.com/trabajos12/fichagr/fichagr.shtml
- **[54]** Alcance de la Auditoría Informática: http://www.123innovationgroup.info/index.htm
- **[55]** Alcance de la Auditoría Informática: http://archivosauditoria.blogspot.com/2009/11/alcance-y-objetivos-de-la-auditoria.html
- **[56]** Control Interno: http://www.leticia-amazonas.gov.co/apc-aa-files/396130366661383530363163656566 33/control.pdf
- **[57]** Control Interno: http://www.mercadotendencias.com/informe-coso-definicion-de-control-interno/
- **[58]** Tipos de Controles Internos: http://www.eumed.net/libros/2008a/351/Definicion%20y%20tipos%20de%20controles%20internos.htm
- **[59]** Implantación de un Sistema de Control Interno: http://www.monografias.com/trabajos12/coso/coso.shtml
- **[60]** La información como Recurso Crítico: http://www.eici.ucm.cl/Academicos/ygomez/descargas/Aud_Seg.../auditoria2.ppt
- **[61]** Valor de la Información en la Organizaciones: http://www.idg.es/computerworld/El-valor-de-la-informacion/seccion-op/articulo-153382

- **[62]** Metodología de la Auditoría Informática: http://www.enterate.unam.mx/Articulos/2005/octubre/auditoria.htm
- **[63]** Justificativo de la Auditoría Informática: http://www.gestiopolis.com/finanzas-contaduria/auditoria-interna-de-la-informacion.htm
- **[64]** Normas y Procedimientos de Auditoría. Instituto Mexicano de Contadores Públicos (IMCP).
- **[65]** Víctor Manuel Mendívil Escalante (2002). Elementos de Auditoría. Quinta Edición. Thomson Editores.
- **[66]** Mario Piattini & Emilio del Peso (2001). Auditoría Informática: Un enfoque práctico. Segunda Edición. Editorial RAMA.
- **[67]** José Antonio Echenique (2001).Auditoría en Informática. Segunda Edición. McGraw Hill.
- **[68]** Evaluación del Talento Humano: http://www.mitecnologico.com/Main/EvaluacionRecursosHumanos
- **[69]** Recursos Financieros y Herramientas para una Auditoría Informática: http://html.rincondelvago.com/auditoria-informatica_1.html
- **[70]** Fases de la Auditoría Informática: http://blogs.vandal.net/3996/vm/1035432792006
- **[71]** Función de la Seguridad en los Sistemas de Información: http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm
- **[72**] Garfinkel y G. Spafford (1996). Practical Unix & Internet security. O'Reilly & Associates.
- **[73]** Seguridad Lógica: http://www.4shared.com/document/-Q26VFvX/cap3_Seguridad_Lgica.html

- **[74]** José Salvador Sánchez Garreta (2003). Ingeniería de proyectos informáticos: Actividades y Procedimientos. Universitat Jaume.
- **[75]** Thimothy Bell, Mark E. Peecher, Ira Solomon, Frank O. Marrs y Howard Thomas (2007). Auditoría Basada en Riesgos, perspectiva estratégica de sistemas. Primera Edición. ECOE Ediciones.
- **[76]** Historia del Modelo COBIT: http://ds5-andre-ortega-5a.host56.com/componentes.html
- **[77]** Definición ISACA: https://www.isaca.org/Pages/default.aspx
- **[78]** Definición ITGI: http://www.itgi.org/
- **[79]** Historia del Modelo COBIT: http://www.borrmart.es/articulo_redseguridad.php?id=1145&numero=24.
- **[80]** Definición BMIS: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/ISACA-Issues-Comprehensive-Business-Model-for-Information-Security-Spanish.aspx
- **[81]** Historia del Modelo COBIT: http://www.isaca.org/About-ISACA/Press-room/News-Releases/Spanish/Pages/COBIT5-ultimas-noticias.aspx
- **[82]** Misión del Modelo COBIT: http://cgi-pe.com/cursos/ptcob.html
- **[83]** Función Básica y Orientación COBIT: http://alarcos.inf-cr.uclm.es/per/fruiz/cur/mso/comple/Cobit.pdf
- **[84]** Componentes del Modelo COBIT: http://ds5-andre-ortega-5a.host56.com/componentes.html

- **[85]** Definición ISO 9000: http://www.tuveras.com/calidad/normalizacion/vocabulario.htm
- **[86]** Definición DTI: http://www.informatica.catamarca.gov.ar/
- **[87]** Marco Referencial: http://www.piramidedigital.com/Documentos/ICT/pdictcobitmarcoreferencial.pdf
- **[88]** Figura 4.4. Cubo COBIT: http://www.overti.es/procesos-itsm/cobit.aspx.
- **[89]**Objetivos de Control: ftp://200.60.110.5/Docentes/Mario_Ramos/CURSOS/PIURA%20AUDITORIA/OBLIGATORIOS/COBIT/COBIT_03.PDF
- **[90]** COBIT orientado a Procesos: http://www.overti.es/procesos-itsm/cobit.aspx
- **[91]** Aceptabilidad de COBIT: http://www.isaca.org/Knowledge-Center/Research/Documents/Alineando-Cobit-4.1,-ITIL-v3-y-ISO-27002-en-beneficio-de-la-empresa-v2,7.pdf
- **[92]** Figura 3.1. Logotipo Corporación Industrial y Comercial HOLDINGDINE S.A.: http://www.holdingdine.com
- **[93]** Figura 3.2. Logotipo Instituto de Seguridad Social de las Fuerzas Armadas (ISSFA): www.issfa.mil.ec.
- **[94]** Conocimiento y Comprensión de la Corporación HOLDINGDINE S.A.: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.
- **[95]** Filosofía Corporativa: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.

- **[96]** Estructura Organizacional: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.
- **[97]** Figura 3.3. Estructura Organizacional de la Corporación HOLDINGDINE S.A.: Fuente, Vicepresidencia de la Corporación HOLDINGDINE S.A.
- **[98]** Grupo Empresarial HOLDINGDINE S.A.: Fuente, Vicepresidencia Ejecutiva de la Corporación HOLDINGDINE S.A.
- **[99]** Conocimiento y Compresión de la Gerencia de TI de la CORPORACIÓN HOLDINGDINE S.A. (Matriz): Fuente, Gerencia TI de la Corporación HOLDINGDINE S.A.
- **[100]** Composición Funcional de la unidad de apoyo Gerencia de TI: Fuente, Gerencia TI de la Corporación HOLDINGDINE S.A.

BIOGRAFÍA

Nombres y Apellidos: Andrés Patricio Naveda Paredes.

Lugar y Fecha de Nacimiento: Quito, 26 de julio de 1987.

Formación Académica

Educación Primaria: De Primer a Sexto Grado.

Centro de Estudios: Borja #2 Los Andes - Quito. **Año:** 1993 – 1999.

Educación Secundaria: De Primer a Sexto Curso con especialidad Físico Matemáticas.

Centro de Estudios: Colegio Marista - Quito. **Año:** 1999 – 2005.

Educación Superior: Carrera de Ingeniería en Sistemas e Informática.

Centro de Estudios: ESPE - Sangolquí. **Año:** 2005 – 2011.

Títulos Obtenidos

Programación Estructurada y Lenguaje C: ESPE –Departamento de Ciencias de la Computación.

Horas: 80. **Año:** 2007.

3D Max y Dark Basic: ESPE – Departamento de Ciencias de la Computación.

Horas: 40. **Año:** 2008.

CISCO – CCNA1 Exploration: Network Fundamentals: ESPE.

Semanas: 6. **Año:** 2009.

CISCO – CCNA2 Exploration: Routing Protocols and Concepts: ESPE.

Semanas: 6. **Año:** 2009.

Suficiencia en el Idioma Inglés: En la ESPE - Departamento de Lenguas.

Niveles: 8 **Año:** 2011.

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA POR

_____

Sr. Andrés Patricio Naveda Paredes

COORDINADOR DE LA CARRERA

_____

Sr. Ing. Mauricio Campaña

Lugar y fecha: _____