Universidad de Costa Rica

Sistema de Estudios de Postgrado

Auditoría del Plan Estratégico de Tecnologías de Información y Comunicaciones en la Compañía Nacional de Fuerza y Luz S.A.

Tesis sometida a la consideración del programa de estudio de posgrado en Auditoría de Tecnologías de Información para optar por el grado de Maestría

Ing. Gisela Fernández Guevara

Carné: A46850

Ciudad Universitaria “Rodrigo Facio”, Costa Rica, 2007

Dedicatoria

A mi padre Horacio Fernández Porras con el mismo amor con el que me dio la vida, por su inmensa e incondicional comprensión y por animarme siempre a seguir adelante.

Agradecimientos

A Dios que me permite servirle con los dones que me dado.

A mi abuelita Digna María Rodríguez González por su amor.

Al Máster Maximiliano Espinoza Jiménez por su amabilidad desde el primer momento en que le solicite la ayuda, su disponibilidad, dedicación y su gran aporte en la revisión final de este texto.

A la Máster Darling Picado Rodríguez por toda la ayuda brindada en este trabajo.

A todos mis profesores y amigos del posgrado de Auditoría de Tecnologías de Información, que gracias a ellos pude culminar los estudios a este trabajo.

Hoja de Aprobación del Trabajo Final de Investigación Aplicada

Esta Tesis fue aceptada por la Comisión del Programa de Estudios de Posgrado en Dirección de Empresas de la Universidad de Costa Rica, como requisito para optar por el grado de Magíster en Auditoría de Tecnologías de Información.

Máster Xiomar Delgado Rojas
Coordinador

Máster Maximiliano Espinoza Jiménez
Lector

Máster Darling Picado Rodríguez
Asistente de la Dirección de Tecnologías de Información,
Compañía Nacional de Fuerza y Luz, S.A.

Doctor Aníbal Barquero Chacón
Director de Programa de Estudios de Posgrado en Dirección de Empresas

---

Ingeniera Gisela Fernández Guevara
Sustentante

ÍNDICE

INTRODUCCIÓN ____ *vii*

CAPÍTULO I ____ *11*

MARCO TEÓRICO ____ *11*

¿QUÉ ES EL PETIC? ____ **12**

¿CÓMO SE CONCIBE UN PETIC? ____ **13**

¿QUÉ ELEMENTOS DEBE CONTENER UN PETIC? ____ **14**

CONSIDERACIONES PARA UNA AUDITORÍA DEL PETIC ____ **17**

NORMATIVA ____ 17
NORMATIVA INTERNACIONAL ____ 17
NORMATIVA GUBERNAMENTAL COSTARRICENSE ____ 19
OTRA NORMATIVA ____ 19

COMUNICACIÓN DE RESULTADOS ____ **21**

CAPÍTULO II ____ *22*

PLANIFICACIÓN PRELIMINAR EL PROCESO DE AUDITORÍA DE TI: LA PLANIFICACIÓN ____ *22*

EL PROCESO DE AUDITORÍA DE TI: LA PLANIFICACIÓN ____ *23*

PLANIFICACIÓN PRELIMINAR ____ **24**

PROCESO DE AUDITORÍA DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LA CNFL ____ 24
PROGRAMA PARA LA PLANIFICACIÓN PRELIMINAR DE LA AUDITORÍA DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN ____ 27
PROGRAMA PARA OBTENER EL CONOCIMIENTO DE LAS OPERACIONES DE LA ENTIDAD ____ 32
PROGRAMA PARA OBTENER EL CONOCIMIENTO ____ 35
DE LAS OPERACIONES DE TI ____ 35
INFORME SOBRE LA PLANIFICACIÓN PRELIMINAR DE LA AUDITORÍA ____ 37

CAPÍTULO III ____ *39*

PLANIFICACIÓN DETALLADA OBJETIVOS DE AUDITORÍA ____ *39*

OBJETIVOS DE AUDITORÍA ____ *40*

OBJETIVO GENERAL ____ 40
OBJETIVOS ESPECÍFICOS ____ 40
PLANIFICACIÓN DETALLADA ____ 41
PRUEBAS DE CONTROL ____ 44
PRUEBAS SUSTANTIVAS ____ 47
CUESTIONARIO DE CONTROL INTERNO ____ 49
LISTA DE CHEQUEO ____ 51
COMUNICACIÓN DE RESULTADOS ____ 54
INFORME A LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN DE LA COMPAÑÍA NACIONAL DE FUERZA Y LUZ S.A. ____ 55
HALLAZGOS DE AUDITORÍA ____ 56

CONCLUSIONES ____ *59*

BIBLIOGRAFÍA ____ *61*

ANEXOS ***63***
Glosario 64

INTRODUCCIÓN

La incorporación de Tecnologías de Información (TI) es uno de los temas principales que concierne, hoy en día, a los altos ejecutivos y organizaciones tanto privadas como gubernamentales. Esto ha producido una creciente demanda en el desarrollo de los Sistemas de Información (SI) y los componentes tecnológicos para soportar las actividades de una empresa.

Las tendencias actuales en el desarrollo de TI en el mercado se han caracterizado por su esfuerzo al automatizar el "desorden" y como detalla Hammer,[1] propulsor de la reingeniería de procesos, lo obtenido es un “desorden automatizado”. En la dirección de TI, se dedica poco esfuerzo en la especificación de la estrategia de negocios, y así también en construir un modelo de organización como precursores en la determinación de requerimientos de TI. Las aplicaciones son construidas para satisfacer metas a corto plazo o problemas inmediatos al producirse islas de TI, a lo largo y ancho en todas las áreas funcionales. La necesidad de un plan de TI es clara, pero el proceso para lograrlo no es obvio; en consecuencia, el riesgo por incorporar TI se ha incrementado en las organizaciones.

Bajo esta nueva realidad, se debe conocer y controlar el ambiente en donde incursionan las tecnologías, esto debido a la aparición de un nuevo campo de trabajo para la Auditoría conocido como Auditoría de tecnologías de información. Este ha tomado relevancia en los últimos años en Costa Rica y, en la actualidad son muchas las organizaciones privadas y públicas que han incorporado este elemento en su esquema organizacional e inclusive las mismas autoridades reguladoras como la Contraloría General de la República y la Superintendencia de Entidades Financieras están reglamentando lo relativo a las tecnologías de información y brindan una guía de criterios para efectuar las Auditorías informáticas.

[1] Harvard Review, May 1999, Reengineering New Process, page 8

Al ser la planeación estratégica un proceso fundamental en la buena administración de todo negocio o quehacer empresarial, existe en el concepto informático una Planeación Estratégica de Tecnologías de Información (PETI) el cual representa el eje transversal, que integra de manera dinámica las visiones estratégicas del negocio con la visión estratégica de TI, con el fin de conformar una visión única final.

De esta forma, el PETI o PETIC (Planeación Estratégica de Tecnologías de Información y Comunicación) representa un insumo sustancial para un auditor informático durante la labor de planeación de un esquema de trabajo, por tanto conocerlo desde su estructuración, le representará una ventaja estratégica para su propio conocimiento.

La Compañía Nacional de Fuerza y Luz, S.A., está consolidada como la principal empresa distribuidora y comercializadora de energía eléctrica de Costa Rica. Su servicio cubre 903 Km2 de la Gran Área Metropolitana, que representan el 2% del territorio nacional y es brindado a 480.000 clientes directos. Ubicada donde se concentra la mayor parte de la población nacional y la actividad comercial, productiva e institucional del país, CNFL tiene bajo su responsabilidad el suministro de energía eléctrica al 40% de los clientes del sistema eléctrico costarricense y comercializa el 46% del total de la electricidad del mercado de distribución nacional.

Es una empresa pública no financiera, cuya principal responsabilidad es contribuir al desarrollo económico del país, mediante la distribución de electricidad en la Gran Área Metropolitana. Legalmente está constituida como una sociedad anónima perteneciente al Grupo ICE, que es dueño del 98.6% de las acciones. El sustento jurídico lo constituye el Contrato Eléctrico emitido por decreto legislativo el 8 de abril de 1941, por un plazo de 25 años y prorrogado en dos oportunidades con la Ley No. 4197 del 20 de septiembre de 1968, por lo cual rige también hasta el año 2040.

La CNFL integra el Grupo ICE, junto con Radiográfica Costarricense, Racsa y el Instituto Costarricense de Electricidad, ICE.

La CNFL tiene una alta concentración de servicios. Con más de 499,800 clientes, que representan el 37 % del total nacional; y una gestión comercial que abarca el 46% del mercado eléctrico costarricense, la Compañía Nacional de Fuerza y Luz se caracteriza por tener también una alta densidad de carga en su área de servicio, la cual abarca el 1.8% del territorio nacional, con el 45% de la demanda eléctrica.

Para garantizar el suministro cuenta con un sistema de distribución formado por 32 subestaciones, 5,553 kilómetros de líneas en operación y 1351MVA de capacidad instalada en transformadores de distribución, con una cobertura del 99% de la zona servida.

El potencial de generación es de 88,1 MW de capacidad instalada en nueve plantas hidroeléctricas, las cuales generaron el 11% de la energía comercializada y el 89% restante se le compró al ICE.

El proyecto PETIC se inicio formalmente en la CNFL el 22 de Octubre del año 2006 con la firma del contrato con la empresa KPMG para el desarrollo del mismo, la encargada del proyecto es la Máster Darling Picado Rodriguez, el proyecto tiene como objetivo la creación del “Plan Empresarial de Tecnologías de Información y Comunicaciones, de la Compañía Nacional de Fuerza y Luz, S. A., para el período 2008 - 2012”, el cual quedará planteado en un documento como producto final que entre otros puntos contendrá: introducción y antecedentes, alineamiento estratégico institucional, los alcances y objetivos del plan, metas, etapas definidas, plazos e indicadores de gestión, responsables, así como la identificación y formulación planes de acción y de proyectos concretos, que permitan a la Compañía alcanzar resultados medibles, considerando todas las áreas prestatarias de servicios de tecnologías tanto centralizadas como descentralizadas.

Para obtener un producto final que sea un instrumento alineado con el Plan Estratégico Institucional y en concordancia con las fuentes de normativa internas tales como: recomendaciones de la Auditoría, las normativas institucionales y las externas tales como: de la Contraloría General de la República particularmente la versión vigente de *LAS NORMAS DE CONTROL INTERNO PARA LOS SISTEMAS DE INFORMACION COMPUTADORIZADOS* y entes reguladores entre otros.

Tomando en cuenta el entorno globalizado y el continuo cambio de las tecnologías y surgimiento de nuevas necesidades, los lineamientos del gobierno, los marcos normativos y las políticas de la institución, se establece que el plan contemple el desarrollo para un periodo de cinco años del 2008 al 2012.

CAPÍTULO I

MARCO TEÓRICO

¿QUÉ ES EL PETIC?

La Planeación Estratégica de Tecnología de Información y la Comunicación son ampliamente reconocidas como herramientas para ordenar los esfuerzos de incorporación de TI al engranaje del gobierno corporativo. Establecen, a su vez, las políticas requeridas para controlar la adquisición, el uso y la administración de los recursos de TI. Integra, también la perspectiva del negocio con el enfoque de TI, establece un desarrollo informático que responde a las necesidades de la organización y contribuye al éxito de la empresa. Su desarrollo está relacionado con la creación de un plan de transformación el cual, va del estado actual de la organización hasta su estado final esperado de automatización (determinación y análisis de brecha), en concordancia con la estrategia de negocios y con el propósito de crear una ventaja competitiva.

La planeación estratégica de tecnologías de información y comunicación es un proceso dinámico en el que las estrategias sufren una continua adaptación, innovación y cambio, el cual se refleja en los elementos funcionales quienes componen toda la organización. Trabajos relacionados con la construcción de un PETIC han sido desarrollados desde los años ochenta, pero presentan limitaciones importantes.

Un proceso de planeación de TI que integre las necesidades de información de una organización resulta una tarea compleja. Al mismo tiempo, contribuye a establecer una clara relación entre la planeación estratégica de negocios, el modelado de la organización y las TI. Su construcción está sustentada en un modelo conceptual, el cual propone una alternativa basada en la transformación de la estrategia de negocios en componentes operativos y de TI.

¿CÓMO SE CONCIBE UN PETIC?

Los criterios para definir el contenido de un PETIC particular dependen de muchos factores, tales como el ambiente organizacional, los recursos, la misión, la visión, entre otros.

La estructura que poseen en común un PETIC se puede dividir en cuatro grandes fases:

Todo el proceso inicia con un estudio de la situación actual en la fase I. En este paso, se evalúa el entendimiento de la estrategia de negocios, la eficiencia de los procesos operativos y la aceptación de TI en la organización. Se evalúa el riesgo de no contar con un PETIC y también se analiza el costo/beneficio de implementarlo.

La fase II, relacionada con la creación de un modelo de la organización, inicia con un análisis del entorno y del establecimiento de la estrategia de negocios (el proceso de planeación se basa en una transformación de dichas estrategias). Continúa con el diseño en detalle de los modelos operativos, que producen en parte los requerimientos de TI necesarios para mejorar la eficiencia y la productividad de la empresa, (ésta aproximación es soportada por una reingeniería de procesos o una automatización incremental que identifica deficiencias operativas con el propósito de rediseñarlas, modificarlas y automatizarlas). Posteriormente, se construye la estructura de la organización que especifica puestos, perfiles, habilidades, entre otras; necesarios para administrar la empresa. La fase termina con la construcción de una arquitectura informática que identifica las necesidades globales de la información en la empresa. El modelo es descrito con la utilización de términos y conceptos del negocio, independientemente del soporte computacional.

La fase III trata del desarrollo de un modelo de TI. En su primer módulo, tiene como objetivo la transformación de las estrategias de negocios en una estrategia de TI. Continúa con la construcción de la arquitectura de sistemas

que establece un marco para la especificación de las aplicaciones y la integración de la información.

Luego se definen los elementos clave y las características esenciales de la arquitectura tecnológica (“hardware” y comunicaciones), además establece la plataforma en la cual los sistemas van a funcionar. Continúa con el diseño en detalle de los modelos operativos de TI quienes describen el funcionamiento del área informática. Concluye con la definición sobre la estructura de la organización de TI, necesaria para administrar los requerimientos informáticos.

La fase IV se concentra en la elaboración de un modelo de planeación. Se realiza un estudio de administración del riesgo el cual se encarga de reconocer la existencia de amenazas que puedan poner en peligro el éxito del PETIC. Continúa con un estudio de la recuperación de la inversión a través de un análisis costo/beneficio. Finaliza con la definición de un plan de implementación con el propósito de determinar el orden de desarrollo de los proyectos de negocio y de TI.

¿QUÉ ELEMENTOS DEBE CONTENER UN PETIC?

Una vez realizadas las cuatro fases anteriores y basados en los resultados, se comienza a estructurar el PETIC bajo un modelo de esta estructura como la siguiente:

1. Marco referencial.
2. Descripción metodológica.
3. Declaración de valores e ideas rectoras relacionadas con TI.
   - **a)** Visión.
   - **b)** Misión.
   - **c)** Objetivos de largo plazo (estratégicos).
   - **d)** Función de TI en la organización (niveles de servicio acordados).
4. Análisis situacional de TI actuales (diagnóstico de la plataforma y recursos de TI existente, FODA).

5. Resumen de proyectos estratégicos de TI.

a) Por área de apoyo o proceso organizacional.

b) Costos estimados.

c) Prioridades de ejecución.

6. Detalle de los programas y los proyectos estratégicos de TI.

a) Proyectos estratégicos de sistemas de información organizacionales de TI considerando:

- Definiciones.
- Perfiles de los proyectos.
- Prioridades de ejecución.
- Costos estimados.
- Cronogramas.
- Responsables.

b) Plan estratégico de TI a nivel técnico.

i) Plan estratégico de la infraestructura de “hardware”

(1) Proyectos de la plataforma de “hardware”.

- Definiciones.
- Perfiles de los proyectos.
- Prioridades de ejecución.
- Costos estimados.
- Cronogramas.
- Responsables.

ii) Plan estratégico de la infraestructura de “software”.

(1) Proyectos de la plataforma de “software”.

- Definiciones.
- Perfiles de los proyectos.
- Prioridades de ejecución.
- Costos estimados.

- Cronogramas.
- Responsables.

iii) Plan estratégico de la infraestructura de las comunicaciones.

(1) Proyectos de la plataforma de comunicaciones.

- Definiciones.
- Perfiles de los proyectos.
- Prioridades de ejecución.
- Costos estimados.
- Cronogramas.
- Responsables.

iv) Plan estratégico de formación del “Talento Humano”.

(1) Proyectos de formación de competencias de “Talento Humano”.

- Definiciones.
- Perfiles de los proyectos.
- Prioridades de ejecución.
- Costos estimados.
- Cronogramas.
- Responsables.

Se debe establecer una relación biunívoca entre las cuatro fases del PETIC descritas anteriormente y ésta estructura de elementos del PETIC.

Teniendo claro la definición y el contenido de un PETIC, se forman los elementos de juicio pertinentes para proceder con el proceso de una auditoría informática en cualquiera de los elementos que lo componen.

CONSIDERACIONES PARA UNA AUDITORÍA DEL PETIC

Para llevar a cabo una auditoría de un Plan Estratégico de Tecnologías de Información y Comunicación es necesario conocer su contenido, la organización en donde se aplicará, su entorno de TI, sus planes estratégicos, políticas, procedimientos y normativa que regulan la actividad. Igualmente se requiere definir aquellos objetivos de la auditoría, su alcance y la metodología por utilizar. La información anterior, además de servir al auditor para conocer el ambiente sobre el cual desarrollará su trabajo, también constituye una fuente esencial para definir los criterios de auditoría utilizados para evaluar la actividad sujeto de estudio, definir los objetivos de la auditoría, concluir sobre ellos y emitir las recomendaciones pertinentes sobre aquellos hallazgos los cuales constituyen aspectos a ser mejorados.

NORMATIVA

Durante su intervención, el auditor debe considerar los diferentes tipos de normativa relacionada con la actividad como por ejemplo: la normativa gubernamental, la normativa internacional y toda aquella propia de la organización objeto de estudio.

NORMATIVA INTERNACIONAL

INTOSAI (International Organization of Supreme Audit Institution)

La Organización Internacional de las Entidades Fiscalizadoras Supremas (INTOSAI) ha emitido pautas para desarrollar una metodología de planificación estratégica de TI/SI de alcance general. El documento en idioma inglés, denominado "Guía para el Desarrollo de Estrategias de Informática (TI) en las Entidades Fiscalizadoras Superiores", señala varias etapas sobre planificación estratégica de sistemas de información, entre ellas la que se cita a continuación.

1) Desarrollar la estrategia del Plan de Tecnologías y Sistemas de Información.

- Trabajo preparatorio, en relación con el establecimiento de cronogramas y guías de control del avance del proyecto.
- Declaración del alcance y especificaciones del proyecto.
- Establecimiento de la metodología de trabajo.
- Determinación de asuntos relacionados con el comité de sistemas.
- Designación del equipo del proyecto de planificación.
- Establecimiento de los requerimientos de apoyo y logística.
- Definición de los factores críticos de éxito del proceso de planificación.

COBIT (Control Objectives for Information and Related Technologies)

COBIT está diseñado para ser la herramienta de gobierno de TIC que ayude al entendimiento y a la administración de los riesgos, así como de los beneficios asociados con la información y sus tecnologías relacionadas.

Consiste en un marco referencial con un conjunto de treinta y cuatro objetivos de Control de alto nivel, uno para cada uno de los procesos de TIC, agrupados en cuatro dominios: Planeación y Organización, Adquisición e Implementación, Entrega de Servicios y Soporte y Monitoreo. Planeación y la Organización deben ser considerados por el auditor al evaluar la etapa de formulación, mientras que los dominios restantes deben ser contemplados al evaluar la etapa de ejecución de un PETIC.

Con COBIT el auditor contará con un marco de referencia para evaluar si la organización dispone de los controles adecuados en el proceso de planeación, organización e implantación del PETIC.

NORMATIVA GUBERNAMENTAL COSTARRICENSE

En este momento, la Contraloría General de la República (CGR) cuenta con un Manual sobre Normas Técnicas para la Gestión y el control de las Tecnologías de Información[2].

También se encuentran las "*Normas Técnicas de control interno para la gestión de las tecnologías de Información (TI)*[3]*" que deben ser aplicadas por la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización* dentro de la cual ésta norma específica para el PETIC que se denomina "Norma: Planificación estratégica de las tecnologías de información".

A partir del año 2006, se solicita a las entidades y a los órganos sujetos a fiscalización de la CGR que incluyan en el PAO (Plan anual operativo) un resumen del PETIC de la organización.

OTRA NORMATIVA

Otra normativa importante por considerar es aquella la cual rige a la organización toda clase de políticas, procedimientos y reglamentos a su vez estos se encuentran debidamente documentados y aprobados por unidades facultadas para ello, por ejemplo:

- Normas para la implementación de programas antivirus en equipos de cómputo.
- Políticas estratégicas y objetivos para la Gestión de Tecnologías de Información y Comunicaciones.
- Normas para el uso del correo electrónico.
- Normas para uso de equipos de cómputo y programas informáticos.

---

2 Fecha de publicación: La gaceta Jueves 21 de junio de 2007.

3 Poder legislativo ley Nº 8292

- Normas para el uso de “Internet” por medio de la red institucional o por acceso remoto.
- Normas para el uso y administración del Sistema de Información Gerencial -SIGE-.
- Normas para el ingreso a las zonas de acceso restringido de la Dirección de Tecnologías de Información.
- Modificación en la red de comunicaciones de datos.
- Actualización de datos de transformadores en los sistemas SIGEL y SIT.
- Administración de programas y documentos fuente.
- Administración de clientes en el Sistema RIME.
- Administración de usuarios en el Sistema RIME.
- Desarrollo, actualización y publicación de los “sitios Web de Intranet” e “Internet”.
- Atención de averías del Sistema de administración y automatización de la distribución (SASS).
- Atención de averías y emergencias en el Sistema de Seguridad de la CNFL.
- Reparación de equipos de comunicación en SCAT.
- Atención de emergencias SCAT.
- Mantenimiento preventivo de equipos de comunicación.
- Plan de contingencias por suspensión del Sistema Sifras.
- Respaldo, resguardo y recuperación de los registros electrónicos.
- Trámite para atención de averías de soporte técnico, “intranet”, “internet”, correo electrónico, infraestructura y sistemas de información.
- Reparación de microcomputadoras y dispositivos periféricos.
- Gestión de mantenimiento de los sistemas de información.
- Guía para la administración de proyectos de tecnologías de información y comunicaciones.

- Normas para el uso y administración del Sistema de Información Gerencial -SIGE-.
- Certificación de la competencia del recurso humano.
- Planificación de la capacitación.
- Gestión de capacitación interna y externa.
- Instructivo para la elaboración del plan operativo anual institucional y presupuesto.
- Política para la Gestión Integral del Riesgo y directrices asociadas.
- Normas para la contratación de bienes y servicios.
- Contratación temporal de servicios profesionales.

COMUNICACIÓN DE RESULTADOS

Una vez realizada la ejecución de la auditoría y documentada en los "papeles de trabajo" respectivos, se procede a organizar, codificar y generar las referencias pertinentes (papeles de trabajo contra informe, informe contra papeles de trabajo, de papel a papel de trabajo) con el fin de sustentar los hallazgos[4] del estudio de auditoría.

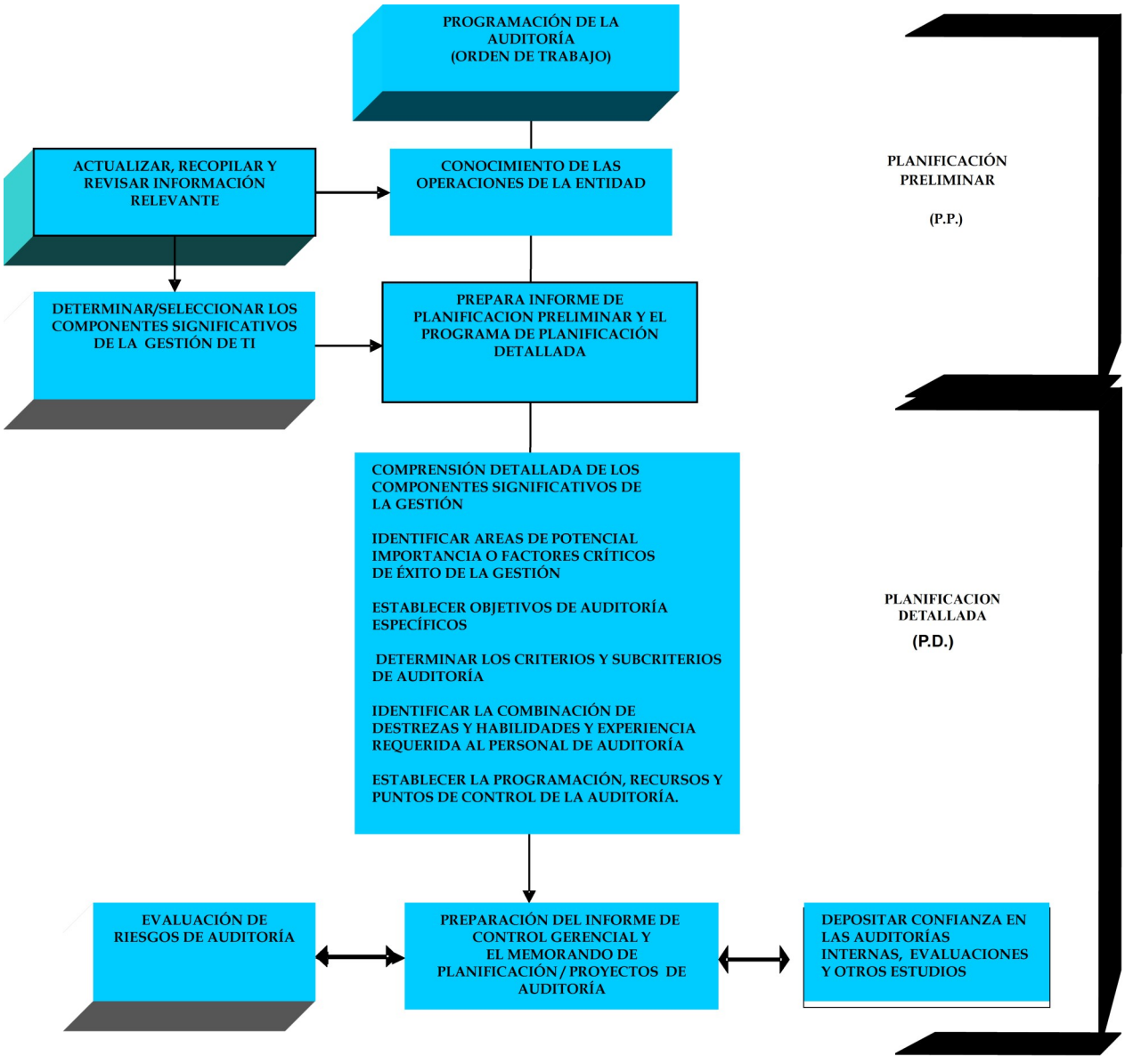
Se debe preparar una agenda para la presentación y discusión del informe preliminar con el auditado, proceder con los ajustes pertinentes que se deriven del proceso de discusión, validar el informe final y comunicar los resultados finales a la Administración.

4 Un hallazgo es un arreglo lógico de información en el que el auditor enmarca diferentes aspectos relacionados con las condiciones detectadas en su intervención.

CAPÍTULO II

PLANIFICACIÓN PRELIMINAR

EL PROCESO DE AUDITORÍA DE TI: LA PLANIFICACIÓN



PT-PP01

PLANIFICACIÓN PRELIMINAR

PROCESO DE AUDITORÍA DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES EN LA CNFL

1. OBJETIVO

Evaluar el plan estratégico de la Compañía Nacional de Fuerza y Luz, S.A., esto con el propósito de verificar que su contenido sea acorde con la misión, visión y las estrategias de negocio de la organización.

2. ALCANCE

El estudio comprenderá el análisis del plan estratégico de la Compañía Nacional de Fuerza y Luz, S.A. con un carácter preventivo y asesor. El estudio abarcará el período comprendido entre el 1º de Abril 2007 y el 15 de Agosto 2007.

3. LIMITACIONES

- Disponibilidad de los entrevistados.
- Confidencialidad de la información.

4. OBJETIVOS ESPECÍFICOS DE LA AUDITORÍA

- Verificar la existencia de estudios de factibilidad previos a la elaboración del Plan Estratégico de Tecnologías de Información y Comunicaciones para evaluar la pertinencia de su contenido.

- Verificar la existencia de procedimientos y políticas para el desarrollo del Plan Estratégico de Tecnologías de Información y Comunicaciones para garantizarse una guía de desarrollo.

- Verificar la existencia de metodologías para las modificaciones y las adaptaciones al Plan Estratégico de Tecnologías de Información y Comunicaciones para asegurar que los planes se adaptan a los posibles cambios de la organización.

- Verificar la comunicación del Plan Estratégico de Tecnologías de Información y Comunicaciones a todos los interesados en la organización, con el fin de garantizar el conocimiento del mismo en todos los niveles relevantes.

- Verificar la existencia, la pertinencia y la aplicación de los planes de monitoreo y de evaluación del Plan Estratégico de Tecnologías de Información y Comunicaciones para que la organización garantice su ejecución.

- Verificar que el Plan Estratégico de Tecnologías de Información y Comunicaciones esté alineado con la estrategia del negocio para que se cumpla eficiente y eficazmente con la misión, visión, objetivos y metas.

- Evaluar el Plan Estratégico de Tecnologías de Información y Comunicaciones para verificar que propicia un balance óptimo entre los requerimientos y las oportunidades acorde con los objetivos estratégicos institucionales, el cual debe formar parte del plan de acción empresarial.

5. METODOLOGÍA

Las técnicas por desarrollar en ésta auditoría son las siguientes:

- Entrevistas.
- Inspecciones oculares.
- Revisión de documentos existentes.
- Revisión de estándares internacionales.
- Aplicación de cuestionarios.
- Análisis de la información recopilada.
- Este trabajo se va a sustentar con lo estipulado en el dominio de Planificación y Organización del COBIT 4.0

PT-PP02

PROGRAMA PARA LA PLANIFICACIÓN PRELIMINAR DE LA AUDITORÍA DEL PLAN ESTRATÉGICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

01 ABRIL 2007

OBJETIVOS DE AUDITORÍA:

1. Obtener información general preliminar para desarrollar un conocimiento y comprensión general de la entidad y del área y operaciones de TI de la entidad.
2. Tomar las principales decisiones que regirán el trabajo en la fase planificación detallada de la auditoría de TI.
3. Considerar la pertinencia del objetivo general de la auditoría señalado en la orden de trabajo y proponer los cambios y ajustes que sean necesarios para definir un objetivo realista y alcanzable.

Fecha de Inicio			Fecha de Terminación						Días Laborables			Visto Bueno GFG
			Estimado			Real			Estimado	Real	Dif.	
01	04	2007	15	05	2007	15	05	2007	45 días	0	0	

No.	Descripción de los Procedimientos	Ref. P/T	Auditor	Fecha

Fecha de Inicio	Fecha de Terminación	Días Laborables		Visto Bueno
1	Obtener o actualizar el conocimiento de las operaciones de la CNFL[5], guiándose para tales efectos en el Programa para obtener/actualizar el conocimiento de las operaciones de la entidad. De ser posible que resuma todo el conocimiento obtenido o actualizado de la entidad en la ***"Hoja para Documentar el Conocimiento de las Operaciones de la Entidad Auditada".*** Complemente este conocimiento con el conocimiento del área de Tecnologías de Información al utilizar el programa, al mismo tiempo, tabule la información más relevante sobre TI en la entidad.	**PT-PP03**[6] **PP-PP04**[7] **PT-PP07**[8]	**GFG**[9] **GFG** **GFG**	**10-04-2007**
2	Analizar la información obtenida en el punto anterior para concebir un modelo gráfico que le permita entender y descomponer el área y la gestión de TI en componentes significativos, para un conocimiento mucho más detallado en la siguiente fase.	**PT-PP05**[10]	**GFG**	**20-04-2007**
3	Preparar una matriz de evaluación de los componentes significativos de la gestión de TI			

5 Compañía Nacional de Fuerza y Luz S.A

6 PT-PP003 Programa para obtener y actualizar el conocimiento de la entidad

7 PT-PP004 Hoja de trabajo para documentar el conocimiento de las operaciones de la entidad

8 PT-PP007 Programa para obtener el conocimiento de las operaciones de TI en la CNFL

9 GFG = acrónimo de Gisela Fernández Guevara

10 PT-PP005 Modelo de la Estructura de TI en la CNFL

Fecha de Inicio	Fecha de Terminación	Días Laborables		Visto Bueno
	para seleccionar aquellos que serán llevados a la planificación detallada. Adopte un método de asignación de puntos a cada uno de los factores, que le garantice objetivo del instrumento para la toma de decisiones.	**PT-PP06**[11]	**GFG**	
	Los factores son: ***el impacto sobre los resultados*** en términos de información válida y segura para la toma de decisiones acertadas, con cumplir con los objetivos institucionales. ***Riesgo de no auditarlo*** y que resulte eventualmente la causa de graves pérdidas para la entidad; ***recursos (insumos) involucrados*** de los cuales realmente se espera, una vez introducidos al proceso, determinados productos y resultados importantes para que la entidad logre alcanzar sus objetivos y metas***; oportunidad para mejorar el desempeño*** y que aumente valor al proceso productivo de la información***; factibilidad de la auditoría*** tomando en cuenta que algunas veces las circunstancias no permiten llevar a cabo los estudios por falta de recursos, por oportunidad de las pruebas, etc.			**30-04-2007**
4	Preparar un Informe de Planificación Preliminar con el fin de destacar los principales esfuerzos de auditoría hechos en esta fase, con la siguiente estructura o alguna otra conveniente.	**PT-**	**GFG**	**15-05-2007**

11 PT-PP006 Matriz de componentes significativos de la Gestión de Proyectos de la CNFL

Fecha de Inicio	Fecha de Terminación	Días Laborables		Visto Bueno
		PP08[12]		

- Introducción.
  - Referencia a la orden de trabajo.
  - Objetivo general de la auditoría.
  - Encargada de la auditoría.

- Resumen del conocimiento de las operaciones de la entidad y del área de TI.

- Componentes Significativos de la Gestión de TI.

  - Todos los componentes significativos de la gestión identificados con la información más importante que los describa.
  - Indica cuáles de ellos y por qué serán objeto de una planificación más detallada.
  - También se debe indicar las expectativas de auditoría del resto de los componentes significativos de la gestión identificados que no serían objeto de una planificación detallada en la presente auditoría.
  - Indica cómo la auditoría de tales

12 PT-PP008 Informe sobre la planificación preliminar de la auditoría en la CNFL

Fecha de Inicio	Fecha de Terminación	Días Laborables		Visto Bueno
	componentes seleccionados agregará valor al cumplimiento de los objetivos institucionales y marcará una diferencia para los principales usuarios de la información procesada con TI. ▪ Una descripción del enfoque de auditoría adoptado, las principales razones de por qué se adoptó tal enfoque y las razones de cualesquiera limitaciones al enfoque adoptado y los posibles riesgos de auditoría que pudieran existir. ▪ Una explicación de cómo se relacionan esos componentes con las prioridades de auditoría. • <u>Programa de Planificación Detallada.</u> ▪ La indicación de que la planificación detallada se realizará efectivamente al cumplir con el programa adjunto.			

Elaborado por: Gisela Fernández Guevara

Fecha: 01-04-2007

PT-PP03

PROGRAMA PARA OBTENER EL CONOCIMIENTO DE LAS OPERACIONES DE LA ENTIDAD

10 ABRIL 2007

OBJETIVOS DE AUDITORÍA:

1. Verificar en la entidad CNFL los requerimientos de los sistemas que los usuarios necesitan.
2. Adoptar decisiones preliminares de auditorías sobre los sistemas, fundamentadas en el conocimiento de la entidad.
3. Organizar el archivo permanente de la entidad, en documentos y en formatos electrónicos.

Fecha de Inicio			Fecha de Terminación						Días Laborables			Visto Bueno GFG
			Estimado			Real			Estimado	Real	Dif..	
10	04	07	20	04	07	20	04	07	10	10	0	

I. INFORMACIÓN A OBTENERSE DE LA CNFL

No.	Procedimientos	Ref. P/T	Iniciales Auditor	Fecha

Fecha de Inicio	Fecha de Terminación	Días Laborables		Visto Bueno
1.	Comprobar en las oficinas de la **CNFL** la existencia de un archivo permanente (AP) y el archivo corriente (AC) de la última auditoría; en caso de existir, revise y complemente: a. La ley de la entidad, sus reglamentos, decretos y otras disposiciones que regulan su funcionamiento y afines con las actividades. b. Confirmar con la Dirección Jurídica de la CNFL la vigencia de las disposiciones obtenidas u obtenga de la "Web" y otros medios una versión actualizada de las disposiciones. c. Revisar los planes estratégicos y otras formas de planificación de corto, mediano y largo plazo. d. Revisar el organigrama y las funciones de cada unidad administrativa. e. Revisar los manuales de administración de personal, contabilidad, de compras y otras relacionadas con la gestión financiera y administrativa de la entidad.	**PP-PP04**[13]		**10-04-2007**

13 PT-PP004 Hoja de trabajo para documentar el conocimiento de las operaciones de la entidad

14 GFG = acrónimo de Gisela Fernández Guevara

II. INFORMACIÓN A OBTENERSE EN LA ENTIDAD AUDITADA.				
No.	**Procedimientos**	**Ref. P/T**	**Iniciales Auditor**	**Fecha**
2.	Solicitar una cita con la **máxima autoridad de la entidad** para desarrollar la siguiente agenda: a. Explicación de los objetivos y el alcance de la auditoría. b. Metodología por utilizar. c. Solicitud de oficinas para el equipo y otras facilidades logísticas indispensables. d. Designación de un coordinador para tratar asuntos de la auditoría.	**PP-PP04**[15]	**GFG**	**10-04-2007**

Elaborado por: Gisela Fernández Guevara

Fecha: 10-04-2007

15 PT-PP004 Hoja de trabajo para documentar el conocimiento de las operaciones de la entidad

PT-PP07

PROGRAMA PARA OBTENER EL CONOCIMIENTO

DE LAS OPERACIONES DE TI

18 ABRIL 2007

OBJETIVOS:

1. Verificar en la CNFL la existencia de una base de datos sobre el funcionamiento y las operaciones realizadas en la Dirección de TI.
2. Adoptar decisiones preliminares de auditorías sobre las bases objetivas fundamentadas en el conocimiento la Dirección de TI.

Fecha de Inicio			Fecha de Terminación						Días Laborables			Visto Bueno GFG
			Estimado			Real			Estimado	Real	Dif.	
30	04	07	15	05	07	15	05	07	15	15	0	

III. INFORMACIÓN A OBTENERSE DE LA DIRECCIÓN DE TI

No.	Procedimientos	Ref. P/T	Auditor	Fecha
1.	Determinar el perfil de las tecnologías de información, para tal efecto revisar la documentación existente.	PT-PP07-1[16]	GFG	20-04-07
2.	Determinar las diferentes aplicaciones en producción como las aplicaciones en desarrollo.	PT-PP07-2[17]	GFG	25-04-07
3.	Determinar los costos globales en tecnologías y sistemas de información.	PT-PP07-3[18]	GFG	26-04-07

16 PT-PP07-1 Perfil de las Tecnologías de Información

17 PT-PP07-2 Sistemas de aplicación de producción

18 PT-PP07-3 Costos Globales de Tecnologías y Sistemas de Información

Fecha de Inicio	Fecha de Terminación	Días Laborables		Visto Bueno
4.	Determinar los costos anuales por cada unidad operacional de TI.	PT-PP07-4[19]	GFG	27-04-07
5.	Aplicar un cuestionario al Auditor Interno para determinar la existencia y el conocimiento del área de auditoría de TI/SI.	PT-PP07-5[20]	GFG	29-04-07
6.	Determinar las funciones realizadas por TI.	PT-PP07-6[21]	GFG	02-05-07
7.	Determinar el personal que labora en el área de TI.	PT-PP07-7[22]	GFG	05-05-07

Elaborado por: Gisela Fernández Guevara

Fecha: 18-04-2007

19 PT-PP07-4 Costos anuales de Tecnologías y Sistemas de Información por unidad Operacional

20 PT-PP07-5 Cuestionario de TI/SI para la auditoría interna

21 PT-PP07-6 Funciones y estructura organizativa de la dirección de Tecnologías de Información

22 PT-PP07-7 Personal que labora en la dirección de Tecnologías de Información

PT-PP08

INFORME SOBRE LA PLANIFICACIÓN PRELIMINAR DE LA AUDITORÍA

La presente planificación preliminar se efectuó en respuesta a la necesidad por evaluar el plan estratégico de la Compañía Nacional de Fuerza y Luz S.A. para verificar que su contenido sea acorde con la misión, visión y las estrategias de negocio de la organización. (Ref. PT-PP01[23]). Por lo tanto se considera lo siguiente:

- La creciente dependencia de la información y de los sistemas de información que la proporcionan.
- La creciente vulnerabilidad y las amenazas inherentes al desarrollo tecnológico.
- El elevado costo de las inversiones en tecnología de información.
- El potencial de las tecnologías para cambiar radicalmente las organizaciones y sus procesos internos, crear oportunidades y reducir costos.

En la fase de auditoría prelimar, se realizó un conocimiento de las operaciones de la entidad (Ref. PT-PP04[24]) y de la Dirección de Tecnologías de Información para determinar su estructura y áreas significativas de su gestión (Ref. PT-PP07[25], PT-PP05[26] y PT-PP06[27]).

23 PT-PP001 Proceso de auditoría del plan estratégico de las tecnologías de información y comunicaciones en la CNFL.

24 PT-PP004 Hoja de trabajo para documentar el conocimiento de las operaciones de la entidad

25 PT-PP007 Programa para obtener el conocimiento de las operaciones de TI en la CNFL

26 PT-PP005 Modelo de la Estructura de TI en la CNFL

27 PT-PP006 Matriz de componentes significativos de la Gestión de Proyectos de la CNFL

Para la siguiente fase, la cual pertenece a la planificación detallada de uno de los componentes significativos detectados, se realizará siguiendo el programa adjunto para tal fin (Ref. PT-PD01[28]).

Elaborado por: Gisela Fernández Guevara

Fecha: 15-05-2007

28 PT-PD01 Planificación detallada de la CNFL

CAPÍTULO III

PLANIFICACIÓN DETALLADA

OBJETIVOS DE AUDITORÍA

OBJETIVO GENERAL

Evaluar el proceso de planificación estratégica de TIC, con sus respectivas herramientas de gestión, para verificar si éste promueve y asegura un balance continuo y óptimo entre las oportunidades y los requerimientos de TI, en concordancia con la estrategia global de la organización.

OBJETIVOS ESPECÍFICOS

1. Confirmar la integración de Tecnología de Información como parte del plan a largo y corto plazo.
2. Evaluar que se hayan considerado los sistemas existentes.
3. Verificar la consideración de un modelo de arquitectura de la información.
4. Evaluar la determinación de la dirección tecnológica.
5. Comprobar que estén bien definidas las funciones y las responsabilidades.
6. Revisar que en el PETIC se haya considerado las inversiones requeridas en TIC.
7. Verificar que el PETIC haya considerado la administración del recurso humano relacionado con las TIC.
8. Comprobar si el PETIC incorporó un marco referencial para la evaluación sistemática de riesgos.
9. Verificar la existencia de políticas y procedimientos relacionados con la administración de proyectos.
10. Evaluar la consideración dentro del PETIC de las políticas y los procedimientos relacionados con el aseguramiento de la calidad, el ciclo de vida del desarrollo de sistemas y la documentación de sistemas.

PT-PD01

PLANIFICACIÓN DETALLADA

01 JULIO 2007

No.	Descripción de los Procedimientos	Ref.P/T	Auditor	Fecha
	EVALUACIÓN PRELIMINAR			
1.	Verificar que se enviaron los comunicados respectivos de solicitud de entrevistas.		**GFG**	**05-06-2007**
2.	Verificar que se aplicó un cuestionario de control interno el cual permita obtener información referente al ambiente de control en donde se desarrolla y aplicará el PETIC, así como identificar la existencia de cualquier debilidad que podría impactar en el proceso de implantación y ejecución del mismo	**PT-PD04**[29]	**GFG**	**12-06-2007**
3.	Verificar con el personal de alto nivel gerencial de la organización que exista lo siguiente: a. Políticas y procedimientos relacionados con el proceso de planificación estratégica. b. Papeles y responsabilidades directivas de la administración		**GFG**	**19-06-2007**

29

No.	Descripción de los Procedimientos	Ref.P/T	Auditor	Fecha
	EVALUACIÓN PRELIMINAR			
	superior en el proceso de planificación. c. Grado de participación de la administración superior en el proceso de planificación de TI. d. Objetivos organizacionales y los planes de largo y corto plazos. e. Objetivos de TI y los planes de largo y corto plazos. f. Relación entre los objetivos organizacionales y los de TI. g. Informes de avance y minutas de las reuniones de los comités de planificación organizacional, y del comité de informática.			
4.	Revisar los resultados de las entrevistas con el siguiente personal: a. Responsable máximo de la organización. b. Responsables de las operaciones sustantivas de la organización. c. Responsable del área financiera. d. Responsable de TIC. e. Miembros del comité de informática f. Personal de alto nivel de TIC. g. Personal de recursos humanos relacionado con actividades TIC. h. Auditoría Interna.		**GFG**	**20-06-2007**

No.	Descripción de los Procedimientos	Ref.P/T	Auditor	Fecha
	EVALUACIÓN PRELIMINAR			
5.2	Obtener copia de las políticas y de los procedimientos relacionados con el proceso de planificación estratégica.		**GFG**	**22-06-2007**
6.3	Solicitar el PETIC de la organización para el período sujeto de evaluación.		**GFG**	**23-06-2007**
7.	Solicitar la normativa que rige la actividad de la organización con respecto a la elaboración del PETIC.		**GFG**	**24-06-2007**
8.4	Indagar acerca del proceso de planificación estratégica para TIC, con el propósito de conocer: a. Metodología o práctica administrativa para la planificación de TI. b. Funcionarios participantes en el proceso. c. Dependencia administrativa responsable del proceso. d. Documentos resultantes. e. Procedimiento de trabajo.		**GFG**	**27-06-2007**
9.5	Obtener los objetivos y planes a corto y largo plazo organizacionales.		**GFG**	**28-06-2007**

Elaborado por: Gisela Fernández Guevara

Fecha: 30-06-2007

29 PT-PD04 Cuestionario de control interno

PT-PD02

PRUEBAS DE CONTROL

01 JULIO 2007

No.	Descripción de los Procedimientos	Ref. P/T	Auditor	Fecha
	PRUEBAS DE CONTROL			
1.	Elaborar y aplicar una lista de chequeo la cual considere los distintos elementos contenidos en el PETIC. Por medio de la misma se pueda determinar razonablemente el cumplimento de la organización de los puntos que constituyen áreas de potencial importancia del PETIC.	**PT-PD05**[30]	**GFG**	**01-07-2007**
2.	Verificar la existencia de un proceso formalmente documentado, divulgado, para la planificación estratégica de TI.		**GFG**	**11-07-2007**
3.	Investigar sobre los controles existentes que ha implantado la administración, aplicables al proceso de elaboración, control e implantación de la planificación estratégica de TI.		**GFG**	**12-07-2007**

30 PT-PD05 Lista de Chequeo

30

4.	Solicitar las Políticas y los Procedimientos existentes relacionadas con la administración de proyectos.		**GFG**	**13-07-2007**
5.	Revisar lo estrictamente adecuado en la asignación de responsabilidades y funciones en el proceso de elaboración del PETIC.		**GFG**	**14-07-2007**
6.	Comprobar y documentar la existencia de una relación entre las metas y los objetivos del PETIC con las estrategias organizacionales.		**GFG**	**15-07-2007**
7.	Investigar sobre la relación existente entre el plan estratégico de sistemas de información, los objetivos de corto plazo (PAO) y el presupuesto organizacional.		**GFG**	**16-07-2007**
8.	Verificar la existencia de los procedimientos de reporte periódicos y rendición de cuentas sobre el cumplimiento de los planes de TI y su aplicabilidad.		**GFG**	**17-07-2007**
9.	Comprobar la debida definición de indicadores claves de desempeño del proceso de planificación estratégica de Tecnologías y para el proceso de su ejecución.		**GFG**	**18-07-2007**
10.	Investigar sobre el proceso de planificación estratégica de TI utilizado por la organización.		**GFG**	**19-07-2007**
11.	Revisar la existencia de políticas para el proceso de divulgación del plan estratégico de TI y refiérase a lo		**GFG**	**20-07-2007**

	adecuado de su aplicación y resultados.			
12.	Evaluar el contenido de las minutas y verificar que estas reflejan el proceso de planeación.		**GFG**	**21-07-2007**
13.	Investigar acerca de los mecanismos de comunicación utilizados entre la administración superior y la unidad responsable del PETIC.		**GFG**	**22-07-2007**
14.	Indagar sobre la consideración en el PETIC de políticas y procedimientos para todas las actividades relacionadas con el ciclo de vida de desarrollo de sistemas, su mantenimiento y el nivel de comunicación al personal de la organización.		**GFG**	**23-07-2007**

Elaborado por: Gisela Fernández Guevara

Fecha: 24-07-2007

PT-PD03

PRUEBAS SUSTANTIVAS

25 JULIO 2007

No.	Descripción de los Procedimientos	Ref. P/T	Auditor	Fecha
1.	**PRUEBAS SUSTANTIVAS**	**PT-PD05**[31]	**GFG**	**25-07-2007**
2.	Elaborar un papel de trabajo mediante la cual se documente la relación e integración de TIC como parte de los objetivos a corto y largo plazo. (Acuerdos, minutas, planes y documentos que contienen dicha información).		**GFG**	**26-07-2007**
3.	Obtener el inventario de sistemas, "hardware" y "software" existente, seleccione una muestra significativa y coteje su consideración en el utilizado para la elaboración del PETIC.		**GFG**	**27-07-2007**
4.	Mediante un análisis de la documentación solicitada, identificar la dirección tecnológica contenida en el plan.		**GFG**	**28-07-2007**
5.	Solicitar, revisar y cuantificar las inversiones requeridas en TIC. Refiérase a su razonabilidad técnica y económica en relación con los objetivos propuestos en el plan estratégico de sistemas de información.		**GFG**	**29-07-2007**
6.	Con base en el inventario obtenido en		**GFG**	**30-07-2007**

31

	el punto 2, analizar dichas existencias, comparar con el detalle de inversiones requeridas en TIC para determinar la brecha tecnológica.			
7.	A la luz de los objetivos estratégicos y proyectos establecidos en el PETIC, comprobar la consideración del recurso humano idóneo, su ambiente, capacitación y motivación dentro del marco de las TIC.		**GFG**	**31-07-2007**
8.	Verificar la inclusión en el contenido del PETIC de un marco referencial para la evaluación sistemática de riesgos.		**GFG**	**01-08-2007**
9.	Comprobar y documentar la existencia dentro del PETIC de políticas y procedimientos relacionados con el aseguramiento de la calidad.		**GFG**	**02-08-2007**
10.	Comprobar y documentar la existencia dentro del PETIC de políticas y procedimientos relacionados con el ciclo de vida del desarrollo de sistemas.		**GFG**	**03-08-2007**
11.	Comprobar y documentar la existencia dentro del PETIC de políticas y procedimientos relacionados con la documentación de los sistemas.		**GFG**	**04-08-2007**

Elaborado por: Gisela Fernández Guevara

Fecha: 05-08-2007

PT-PD04

CUESTIONARIO DE CONTROL INTERNO

07 AGOSTO 2007

	REVISION PRELIMINAR			OBSERVACIONES
	S	N	N/A	
1. Las responsabilidades con respecto a la elaboración e implantación del PETIC se encuentran claramente definidas y documentadas.	X			
2. Es la estructura organizacional la adecuada.	X			
3. Se tienen definidos y documentados los objetivos y políticas de planeación de TI.	X			
4. Se cuenta con el recurso humano necesario que garantice la continuidad del PETIC.	X			
5. ¿Son los distintos planes organizacionales evaluados periódicamente?	X			
6. ¿Se cumple con los procedimientos y los controles establecidos por la administración?	X			
7. ¿Se realizan estudios de viabilidad técnica y económica para la adquisición de las TIC?	X			
8. ¿Existe compromiso de la alta dirección en lo que respecta a la	X			

	REVISION PRELIMINAR			OBSERVACIONES
adquisición y uso de TIC?				
9. ¿Existe algún documento debidamente autorizado referente al diccionario de datos que defina claramente: a) ¿Quién puede tener acceso? b) ¿Quién es responsable de determinar el nivel de acceso apropiado? c) La aprobación específica requerida para el acceso. d) Los requerimientos especiales para el acceso (por ejemplo, acuerdo de confidencialidad).	X			No esta actualizado.

Elaborado por: Gisela Fernández Guevara

Fecha: 07-08-2007

PT-PD05

LISTA DE CHEQUEO

10 AGOSTO 2007
ASPECTOS QUE DEBE CONTENER UN PETIC

Concepto	*SI*	*NO*	*Observaciones*
1.Marco referencial.	X		
2.Descripción metodológica.	X		
3. Declaración de valores e ideas rectoras relacionadas con TI. • Visión. • Misión. • Objetivos de largo plazo (estratégicos). • Función de TI en la organización (niveles de servicio acordados).	X		
4. Análisis situacional de TI actuales (diagnóstico de la plataforma y recursos de TI existente, FODA).	X		
5. Resumen de los proyectos estratégicos de TI. • Por área de apoyo o proceso organizacional. • Costos estimados. • Prioridades de implantación.	X		
6. Detalle de los programas y proyectos estratégicos de TI. **a)** Proyectos estratégicos de sistemas de información organizacionales de TI, en donde se consideran: • Definiciones.	X		

Concepto	*SI*	*NO*	*Observaciones*
• Perfiles de los proyectos. • Prioridades de ejecución. • Costos estimados. • Cronogramas. • Responsables.			
b) Plan estratégico de TI en el nivel técnico. i. Plan estratégico de la infraestructura de “hardware”. 1. Proyectos de la plataforma de “hardware”. ➢ Definiciones. ➢ Perfiles de los proyectos. ➢ Prioridades de ejecución. ➢ Costos estimados. ➢ Cronogramas. ➢ Responsables.	X		
ii. Plan estratégico de la infraestructura de “software de Base”. 1. Proyectos de la plataforma de software. ➢ Definiciones. ➢ Perfiles de los proyectos. ➢ Prioridades de ejecución. ➢ Costos estimados. ➢ Cronogramas. ➢ Responsables.			

Concepto	*SI*	*NO*	*Observaciones*
iii. Plan estratégico de la infraestructura de las comunicaciones. 1. Proyectos de la plataforma de comunicaciones. ➢ Definiciones. ➢ Perfiles de los proyectos. ➢ Prioridades de ejecución. ➢ Costos estimados. ➢ Cronogramas. ➢ Responsables.	X		
iv. Plan estratégico de formación del Talento Humano. 1. Proyectos de formación de competencias de Talento Humano. ➢ Definiciones. ➢ Perfiles de los proyectos. ➢ Prioridades de ejecución. ➢ Costos estimados. ➢ Cronogramas. ➢ Responsables.		X	Esto lo evalúa recursos humanos.

Elaborado por: Gisela Fernández Guevara

Fecha: 10-08-2007

PT-PD07

COMUNICACIÓN DE RESULTADOS

25 AGOSTO 2007

No.	Descripción de los Procedimientos	Ref. P/T	Auditor	Fecha
	COMUNICACIÓN DE RESULTADOS			
1.	Documentar y referenciar los resultados obtenidos a través de las pruebas de auditoría en los papeles de trabajo respectivos que permiten sustentar los hallazgos del estudio realizado.		GFG	30-08-2007
2.	Discutir el preliminar del informe con el auditado, documentar sus argumentos y evaluar y referenciar cualquier ajuste o modificación al contenido del informe.		GFG	04-09-2007
3.	Elaborar el documento del informe final y comunicar los resultados del estudio a la Administración mediante un proceso formal y documentado.	**PT-PD08**[32]	GFG	06-09-2007

Elaborado por: Gisela Fernández Guevara

Fecha: 10-09-2007

32 PT-PD08 Informe Final a la Dirección de Tecnologías de Información

32

PT-PD08

INFORME A LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN DE LA COMPAÑÍA NACIONAL DE FUERZA Y LUZ S.A.

11 SETIEMBRE 2007

Señor.
Óscar Cavallini Corrales.
Director de Tecnologías de Información
Compañía Nacional de Fuerza y Luz S.A.

He auditado el plan estratégico de la Compañía Nacional de Fuerza y Luz para verificar que su contenido sea acorde con la misión, visión y las estrategias de negocio de la organización y es mi responsabilidad expresar una opinión sobre las situaciones encontradas que podrían ocasionar la afectación del mismo.

La evaluación se basó en los criterios de COBIT 4.0 mediante la realización de pruebas selectivas, la obtención de evidencia y los cuestionarios.

En mi opinión, a la fecha de hoy, el proyecto se ha desarrollado eficazmente, sin embargo, adjunto con éste informe los hallazgos que se desprenden de mi evaluación.

Elaborado por: Gisela Fernández Guevara
Fecha: 11-09-2007

PT-PD06

HALLAZGOS DE AUDITORÍA

15 AGOSTO 2007

Hallazgo 1

TÍTULO: Carencia de un procedimiento oficializado para la realización del plan estratégico de tecnologías de información y brindarle el mantenimiento pertinente.
CONDICIÓN: Luego de entrevistas realizadas a la asistencia de Tecnologías de Información no se halló evidencia de la existencia de un proceso formalmente documentado para la realización del PETIC.
CRITERIO: COBIT 4.0 PO6.3 Administración de políticas para TI. Elaborar y dar mantenimiento a un conjunto de políticas que apoyen la estrategia de TI. Estas políticas deben incluir la intención de las políticas, funciones y responsabilidades, procesos de excepción, enfoque de cumplimiento y referencias a procedimientos, estándares y directrices. Las políticas deben incluir tópicos clave como calidad, seguridad, confidencialidad, controles internos y propiedad intelectual. Su relevancia se debe confirmar y aprobar de forma regular.
CAUSA: La administración no ha tenido los recursos necesarios con el fin de elaborar un procedimiento formal para realizar los PETIC periódicamente y nunca se había contratado a una empresa, la cual realizara un buen plan estratégico para TI.
EFECTO: La no existencia de un proceso formalmente documentado para la realización del PETIC puede incurrir en costos muy elevados, pérdidas de tiempo. De lo anterior se podría derivar: • No se realice el PETIC en forma adecuada. • No se le dé un mantenimiento para su actualización.

• No se cuente con un plan de divulgación en el nivel institucional para el cumplimiento de los objetivos.
RECOMENDACIÓN: A la administración: realizar un procedimiento para la realización del plan estratégico de tecnologías de información, divulgarlo a toda la compañía y mantenerlo actualizado en la intranet.

Elaborado por: Gisela Fernández Guevara

Fecha: 15-08-2007

Hallazgo 2

TÍTULO: Reprogramación en la entrega de productos.
CONDICIÓN: La empresa contratada ha presentado atrasos en la entrega de sus productos.
CRITERIO: COBIT 4.0 DS2.4 Monitoreo del desempeño del proveedor. Establecer un proceso para monitorear la prestación del servicio de esta forma asegurar que el proveedor cumpla con los requerimientos del negocio actuales; así mismo se apegue continuamente a los acuerdos del contrato y a los convenios de niveles de servicio, por último que el desempeño sea competitivo respecto a los proveedores alternativos y a las condiciones del mercado.
CAUSA: Al inicio del proyecto, el atraso se debió a la dificultad de participación en los talleres, en reuniones, disponibilidad de tiempo para entrevistas, para entrega de cuestionarios, etc. La información debe ser revisada y devuelta para que la contemplen o verifiquen, esto significa más tiempo de lo previsto en los cronogramas. Actualmente, la empresa contratada esta atrasada en la entrega de sus productos.
EFECTO: El atraso de los productos obedece a la entrega de los productos con sus requisitos establecidos y a la satisfacción de la administración lo cual ha originado que en conjunto se reprogramen las entregas de los productos. El cronograma se ha visto afectado en varias ocasiones, lo cual afecta los compromisos con la Contraloría.
RECOMENDACIÓN: a la administración: Velar por el cumplimiento adecuado de los niveles de servicio acordados.

Elaborado por: Gisela Fernández Guevara

Fecha: 15-08-2007

CONCLUSIONES

La aplicación de la auditoría a un PETIC es necesaria porque coadyuva a regular y minimizar los riesgos asociados con:

- Incapacidad de producir resultados.
- Incongruencia entre la estrategia organizacional y la estrategia de TI: insuficiente alineación estratégica.
- Objetivos poco claros, que dificultan la medición de la eficacia.
- Falta de dominio sobre los programas de cambio organizacional en TI; fragmentación de la toma de decisiones, unidades organizacionales las cuales operan divergentemente, decisiones conflictivas; problemas de prioridades para programas y proyectos.
- Incongruencia en el inventario de soluciones tecnológicas, instalaciones, proyectos de sistemas de información e infraestructura, así como previsiones de telecomunicaciones, con relación en las cambiantes necesidades de los usuarios.
- Obsolescencia tecnológica, motivada por insuficiente investigación y desarrollo.
- Insuficiente capacidad de adaptación a los ajustes y cambios organizacionales y del entorno, así como sus efectos sobre TI.
- Pérdidas por inversiones en proyectos sin estudios de factibilidad oportunos.
- Incapacidad de conocer las condiciones de servicio de las plataformas existentes y su contribución real para la organización.
- Falta de conocimiento de los niveles de exposición al riesgo operativo y de satisfacción de los requerimientos de usuarios.
- Pérdida de oportunidades para explotar nuevas formas de trabajo para beneficio de la organización.

- Incoherencia en la planificación de los recursos humanos.
- Imposibilidad de medir el aporte de Recurso Humanos de TIC para la contribución organizacional.
- Incapacidad para compartir recursos computacionales, información y servicios electrónicos con otros entes internos y externos.
- Incapacidad para el aprendizaje organizacional, debido a la repetición de fallas y a lecciones no aprendidas.
- Insuficiente “retroalimentación” gerencial.

En la Compañía Nacional de Fuerza y Luz se está en la etapa final del PETIC 2008-2012 y ese mismo contiene todo los aspectos mencionados en este trabajo como por ejemplo: introducción y antecedentes, alineamiento estratégico institucional, los alcances y objetivos del plan, metas, etapas definidas, plazos e indicadores de gestión, responsables, así como la identificación y formulación planes de acción y de proyectos concretos, que permitirán a la Compañía alcanzar resultados medibles, considerando todas las áreas prestatarias de servicios de tecnologías tanto centralizadas como descentralizadas. El PETIC es un instrumento alineado con el Plan Estratégico Institucional y en concordancia con las fuentes de normativa internas tales como: recomendaciones de la Auditoría, las normativas institucionales y las externas tales como: de la Contraloría General de la República particularmente la versión vigente de “Las normas de control interno para los sistemas de información computarizados” y entes reguladores entre otros.

.

BIBLIOGRAFÍA

1. *Palomo Asch Rafael, Material del Curso Proceso de Auditoría, UCR 2005*
2. *EDP Audit Committee, International Organization of Supreme Audit Institutions, Guide to Developing IT Strategies in Supreme Audit Institutions, October 1995.*
3. *Echenique García José Antonio, Auditoría en Informática, Editorial McGraw-Hill, Segunda Edición, México, 2001.*
4. *Muñoz Razo, Carlos. Auditoría en Sistemas Computacionales. Editorial Prentice Hall, Primera Edición, México, 2002.*
5. *Consultas al personal de las unidades GAUS y Remunerados de la Contraloría General de la República, Costa Rica. ..*
6. Contraloría General de la República*. Manual de normas generales de control interno para la Contraloría General de la República y las entidades y órganos sujetos a su fiscalización, M-1-2002-CO-DDI*. CGR: San José, Costa Rica. 2002.
7. IT Governance Institute. *Control Objectives for Information and related Technology (COBIT).* Tercera edición. ISACF:Chicago. 2000.
8. IT Governance Institute. COBIT Management Guidelines. Tercera edición. ISACF:Chicago. 2000.
9. United States General Accounting Office (GAO). GAO/AIMD-00-21.3.1, *Standards for Internal Control in the Federal Government*. GAO:Washington D.C. 1999.
10. Jenkins, George. *Information Systems Policies and Procedures Manual*. Segunda edición en inglés. Prentice Hall, USA. 1997.
11. David, Fred R. *Conceptos de Administración Estratégica*. Quinta edición. Pearson Education: México. 1997.
12. Andreu Rafael et al. *Estrategia y Sistemas de Información*. Segunda edición. Mc Graw Hill: México. 1996.

13. Rosales Posas, Ramón. Formulación y Evaluación de Proyectos. ICAP: Costa Rica. 1999.

14. United States General Accounting Office (GAO). GAO/AIMD-10.1.13, *Assesing Risks and Returns: A Guide for Evaluating Federal Agencies´IT Investment Decision-making*. GAO:Washington D.C. 1997.

15. Government of Western Australia. *Guidelines for Managing Risk in the Western Australian Public Sector.* 1999.

ANEXOS

Glosario

Condición: Se refiere a la situación o problema observado.

Criterio: Es la norma, práctica o la técnica de control con la que se evalúa la condición observada.

Causa: Es la razón de las desviaciones observadas entre el criterio y la condición o problema presente.

CNFL: Acrónimo de “Compañía Nacional de Fuerza y Luz, S.A.”.

Conclusión: Es la opinión del auditor sobre la situación observada con relación en el objetivo de auditoría que se ha trazado.

Confiabilidad (disponibilidad): conjunto de elementos de control tanto automatizados como manuales, que permiten garantizar razonablemente la disponibilidad del producto.

Confidencialidad: Conjunto de elementos los cuales permiten garantizar razonablemente que la información magnética o documentos fuentes sean accesados o procesados por personal debidamente autorizado.

Consistencia: Relacionado con la integridad de los datos, específicamente que estos no pierdan su forma inicial y la relación coherente con otros datos, campos o tablas a través del tiempo.

Dato: Unidad mínima de información.

Efecto: Es el impacto real o potencial de las desviaciones observadas sobre las operaciones y resultados que espera la obtener de la entidad.

Información: Elemento fundamental conformado por un conjunto de datos coherentes entre sí con sentido común, que permite tomar una decisión en torno a él.

Informática: Ciencia de la ingeniería que estudia el comportamiento de los sistemas de información.

Integridad: Concepto asociado a la información magnética, mediante controles apropiados, consiste en que se mantenga en forma modular sin perder su coherencia ni su consistencia.

Recomendación: Es la acción correctiva que permitirá eliminar la causa de la desviación de lo observado respecto del criterio evaluado.

Resguardo: Acciones manuales o automatizadas, para la custodia de la información magnética.

Soporte: Es un concepto vinculado a las acciones o procesos que se encargan de mantener la integridad y la consistencia de una determinada información.

Servidor: Genéricamente, dispositivo de un sistema computacional que resuelve peticiones de otros elementos del sistema denominados CLIENTES.

Sistema: Conjunto de elementos con un objetivo común, cuyas partes están relacionadas entre sí. Conjunto de “hardware” y “software”.

Sistema Abierto: Se le denomina a sistemas computacionales cuya característica es la compatibilidad técnica con otras plataformas distintas a él.

Software: Concepto computacional que se relaciona con aplicaciones, programas, sistemas operativos y, en general, lógica programas.

Soporte: Es un concepto vinculado con las acciones o procesos que se encargan de mantener la integridad y la consistencia de una determinada información.

TIC: Tecnologías de información y comunicaciones.