DIRECCIÓN DE AUDITORÍAS CENTRALIZADAS Y DESCENTRALIZADAS (DACD)

AUDITORÍA ESPECIAL SOBRE GOBERNANZA DE TECNOLOGÍA DE LA INFORMACIÓN (TI) PRACTICADA A LA EMPRESA NACIONAL DE ENERGÍA ELÉCTRICA ENEE

INFORME
Nº 003-2014-DACD-ENEE-A

POR EL PERÍODO COMPRENDIDO
DEL 01 DE ENERO AL 30 DE JUNIO DE 2014

EMPRESA NACIONAL DE ENERGÍA ELÉCTRICA
(ENEE)

AUDITORÍA ESPECIAL SOBRE GOBERNANZA DE TECNOLOGÍA DE LA INFORMACIÓN (TI)

INFORME
Nº 003-2014-DACD-ENEE-A

PERÍODO
DEL 01 DE ENERO DE 2014
AL 30 DE JUNIO DE 2014

DIRECCIÓN DE AUDITORÍAS
CENTRALIZADAS Y DESCENTRALIZADAS
DACD

CONTENIDO

INFORMACIÓN GENERAL

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

CAPÍTULO II

CAPÍTULO III

CAPÍTULO IV

Tegucigalpa, MDC 05 de junio de 2015

Oficio No. MMAME/TSC-521-2015

Ingeniero
Roberto Ordoñez
Secretario de Estado
Despacho de Infraestructura Productiva
Gerente General Interino
Empresa Nacional de Energía Eléctrica ENEE
Su Oficina.

Adjunto encontrarán el Informe Nº 003-2014-DACD-ENEE-A de la Auditoría Especial Sobre Gobernanza de Tecnología de la Información (TI) practicada a la Empresa Nacional de Energía Eléctrica ENEE, por el período comprendido del 01 de enero al 30 de junio de 2014. El examen se efectuó en ejercicio de las atribuciones contenidas en el Artículo 222 reformado de la Constitución de la República y los Artículos 3, 4, 5 numeral 4; 37, 45 numeral 7; y 46 de la Ley Orgánica del Tribunal Superior de Cuentas y conforme a las Normas del Marco Rector del Control Externo Gubernamental.

Las recomendaciones formuladas en este informe fueron analizadas oportunamente con los funcionarios encargados de su implementación y aplicación, mismas que contribuirán a mejorar la gestión de la institución a su cargo. Conforme al Artículo 79 de la Ley Orgánica del Tribunal Superior de Cuentas, el cumplimiento de las recomendaciones formuladas es obligatorio.

Para cumplir con lo anterior y dando seguimiento al cumplimiento de las recomendaciones, de manera respetuosa le solicito presentar dentro de un plazo de 15 días calendario a partir de la fecha de recepción de esta nota: (1) un Plan de Acción con un período fijo para ejecutar cada recomendación del informe; y (2) las acciones tomadas para ejecutar cada recomendación según el plan.

Atentamente,

Miguel Angel Mejia Espinoza
Magistrado Presidente por Ley

EMPRESA NACIONAL DE ENERGÍA ELÉCTRICA
ENEE

RESUMEN EJECUTIVO

A) NATURALEZA Y OBJETIVOS DE LA REVISIÓN

La presente auditoría se realizó en ejercicio de las atribuciones conferidas en el Artículo 222 reformado de la Constitución de la República y los Artículos 3, 4, 5 numeral 4; 37, 45 numeral 7; y 46 de la Ley Orgánica del Tribunal Superior de Cuentas, y en cumplimiento a la Orden de Trabajo No. 003-2014-DACD del 29 de septiembre de 2014.

Los principales objetivos de la revisión fueron los siguientes:

1. Obtener un suficiente entendimiento de los procesos y procedimientos del área de Tecnología relativo a la Gobernanza de Tecnología de la Información, evaluar el riesgo de control para planificar la auditoría, e identificar deficiencias significativas incluyendo debilidades importantes de control interno.

2. Verificar que la entidad haya definido e implementado adecuadamente en el ámbito de la Institución los mecanismos y estructuras de Gobernanza de Tecnología de la Información.

3. Verificar que la institución cuente con procesos de planificación de Tecnología de la Información.

4. Verificar que la institución cuente con procesos orientados hacia la adquisición de soluciones de Tecnología de la Información.

5. Verificar que la institución ponga en práctica la gestión de la Seguridad de la Información.

6. Determinar los hallazgos de control y comunicar las recomendaciones a los funcionarios de la institución para su implementación.

B) ALCANCE Y METODOLOGÍA:

La auditoría comprendió la revisión de la documentación de respaldo presentada por los funcionarios y empleados de la Empresa Nacional de Energía Eléctrica ENEE cubriendo el período del 01 de enero al 30 de junio de 2014, con énfasis en la revisión de las áreas siguientes:

1. Estructura de Gobernanza de Tecnología de la Información,
2. Proceso de Planificación de Tecnología de la Información
3. Adquisición de Soluciones de Tecnología de la Información.
4. Gestión de la Seguridad de la Información.

En el desarrollo de la auditoría especial sobre Gobernanza de Tecnología de la Información se aplicó las normas del Marco Rector de Control Interno de los Recursos públicos y se consideraron las fases de Planeación, Ejecución e Informe, entre otros aspectos de orden técnico.

En la fase de Planeamiento, se realizó una visita previa con el Jefe de la División de Informática, para darle a conocer el objetivo de la Auditoría, seguidamente procedimos a la evaluación del control interno para el suficiente conocimiento de los procesos y procedimientos manejados en la División de Informática, en relación a la Estructura de Gobernanza de Tecnología de la Información (TI), Proceso de Planificación de TI, Adquisición de Soluciones de TI y Gestión de la Seguridad de la Información, para obtener una comprensión de las áreas a auditar, seguidamente determinamos y programamos la naturaleza, oportunidad, alcance y procedimiento de auditoría a emplear.

La ejecución de la auditoría estuvo dirigida a obtener evidencia a través del programa aplicado que permitió concretar opinión sobre la información objeto de la auditoría con base en los resultados logrados utilizamos las técnicas de auditoría específicas y realizamos los siguientes procedimientos:

a) Entrevistas con el Jefe de la División de Informativa de la Empresa Nacional de Energía Eléctrica ENEE;

b) Examinamos la efectividad y confiabilidad de los procedimientos administrativos y controles internos de la División de Informática de la Institución, con el fin de determinar la calidad de los mismos, la eficacia y eficiencia en el cumplimiento de sus objetivos, utilizando el método de cuestionario de control interno y entrevistas.

c) La documentación para realizar la auditoría se solicitó mediante oficio.

d) Revisión analítica de la documentación soporte del período sujeto a revisión para obtener una seguridad razonable respecto a la existencia, legalidad, autenticidad y legitimidad de la misma;

e) Verificamos el cumplimiento de las disposiciones legales.

Después de haber desarrollado las etapas anteriores, y como resultado de la auditoría efectuada, se elaboró el correspondiente informe que contiene los hallazgos de control interno originadas de la misma.

Nuestra auditoría se efectuó de acuerdo con la Ley Orgánica del Tribunal Superior de Cuentas y su Reglamento, el Marco Rector de Control Interno de los Recursos Públicos aplicables a la Empresa Nacional de Energía Eléctrica (ENEE).

Como resultado de la auditoría se elaboró el correspondiente informe que contiene los hallazgos de control interno, originados de la misma.

C) ASUNTOS IMPORTANTES QUE REQUIEREN ATENCIÓN DE LA AUTORIDAD SUPERIOR

En el curso de nuestra Auditoría encontramos algunas deficiencias que merecen atención por parte de las autoridades superiores de la Empresa Nacional de Energía Eléctrica (ENEE), como ser:

1. No existen políticas de gobernanza en tecnología de la información definida, aprobadas e implementadas por la alta administración.

2. No existe un comité de tecnología de la información que coordine y supervise las diferentes actividades informáticas de la institución.

3. No existe un proceso de planificación de tecnología de la información.

4. No existe una norma interna donde se defina el proceso de planeamiento de tecnología de información.

5. No existe un plan estratégico institucional

6. No existe un plan estratégico de tecnología de información.

7. No existe un plan director de tecnología de información y/o planes tácticos de TI.

8. No existe un plan de compras y/o gastos de tecnología de la información

9. No existe una norma interna sobre el proceso de contrataciones de tecnología de la información.

10. No existe un plan de continuidad de negocio debidamente aprobado y publicado.

11. No existe un proceso para inventariar activos de información debidamente aprobado y publicado.

12. No existe un proceso para la clasificación de la información de la institución, debidamente aprobado y publicado.

13. No existe un proceso para la gestión de riesgos de la seguridad de la información y comunicaciones debidamente aprobado y publicado.

14. No existe un proceso para la gestión y manejo de incidentes, debidamente aprobado y publicado.

15. No está designado las personas o unidades para gestionar la seguridad de la información

16. No existe un comité de seguridad de la información y comunicaciones.

17. No existe una política de seguridad de la información y comunicaciones, debidamente aprobada y publicada.

18. No existe una política de control de accesos, debidamente aprobada y publicada.

19. No existe un proceso de gestión de continuidad de los servicios de tecnología de información debidamente aprobado y publicado.

Tegucigalpa MDC., 05 de junio de 2015.

Lic. Carlos Roberto Silva
Director de Tecnología
de Información

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

A. MOTIVOS DE LA AUDITORÍA

La presente auditoría se realizó en ejercicio de las atribuciones conferidas en el Artículo 222 reformado de la Constitución de la República y los Artículos 3, 4, 5 numeral 4; 37, 45 numeral 7; y 46 de la Ley Orgánica del Tribunal Superior de Cuentas, y en cumplimiento a la Orden de Trabajo No. 003-2014-DACD del 29 de septiembre de 2014.

B. OBJETIVOS DE LA AUDITORÍA

Los objetivos principales de esta auditoría fueron los siguientes:

Objetivos Generales:

1. Vigilar y verificar que los recursos públicos se inviertan correctamente en el cumplimiento oportuno de las políticas, programas, proyectos y la prestación de servicios y adquisición de bienes del sector público;

2. Contar oportunamente con la información objetiva y veraz, que asegure la confiabilidad de los informes y estados financieros;

3. Lograr que todo servidor público, sin distinción de jerarquía, asuma plena responsabilidad por sus actuaciones, en su gestión oficial;

4. Desarrollar y fortalecer la capacidad administrativa para prevenir, investigar, comprobar y sancionar el manejo incorrecto de los recursos del Estado;

5. Promover el desarrollo de una cultura de probidad y de ética públicas;

6. Fortalecer los mecanismos necesarios para prevenir, detectar, sancionar y combatir los actos de corrupción en cualquiera de sus formas; y,

7. Supervisar el registro, custodia, administración, posesión y uso de los bienes del Estado.

Objetivos Específicos:

1. Obtener un suficiente entendimiento de los procesos y procedimientos del área de Tecnología relativo a la Gobernanza de Tecnología de la Información, evaluar el riesgo de control para planificar la auditoría, e identificar deficiencias significativas incluyendo debilidades importantes de control interno.

2. Verificar que la entidad haya definido e implementado adecuadamente en el ámbito de la Institución los mecanismos y estructuras de Gobernanza de Tecnología de la Información.

3. Verificar que la institución cuente con procesos de planificación de Tecnología de la Información.

4. Verificar que la institución cuente con procesos orientados hacia la adquisición de soluciones de Tecnología de la Información.

5. Verificar que la institución ponga en práctica la gestión de la Seguridad de la Información.

6. Determinar los hallazgos de control y comunicar las recomendaciones a los funcionarios de la institución para su implementación.

C. ALCANCE DE LA AUDITORÍA

La auditoría comprendió la revisión de la documentación de respaldo presentada por los funcionarios y empleados de la Empresa Nacional de Energía Eléctrica ENEE cubriendo el período del 01 de enero al 30 de junio de 2014, con énfasis en la revisión de las áreas siguientes:

1. Estructura de Gobernanza de Tecnología de la Información,
2. Proceso de Planificación de Tecnología de la Información
3. Adquisición de Soluciones de Tecnología de la Información.
4. Gestión de la Seguridad de la Información.

Los procedimientos de auditoría más importantes aplicados durante nuestra revisión fueron los siguientes:

a. Entrevistas con el Jefe de la División de Informática de la Empresa Nacional de Energía Eléctrica (ENEE);

b. Examinamos la efectividad y confiabilidad de los procedimientos administrativos y controles internos de la División de Informática de la Institución, con el fin de determinar la calidad de los mismos, la eficacia y

eficiencia en el cumplimiento de sus objetivos, utilizando el método de cuestionario de control interno y entrevistas.

c. La documentación para realizar la auditoría se solicitó mediante oficio

d. Revisión analítica de la documentación soporte del período sujeto a revisión para obtener una seguridad razonable respecto a la existencia, legalidad, autenticidad y legitimidad de la misma;

e. Verificamos el cumplimiento de las disposiciones legales.

CAPÍTULO II

ANTECEDENTES

Durante los días del 21 al 25 de julio de 2014, el Tribunal de Cuentas de la Unión de la ciudad de Brasilia, Brasil, realizó el taller y reunión para la Planificación de la Auditoría Coordinada sobre Gobernanza de Tecnología de la Información, organizada por la Organización Latinoamericana y del Caribe de Entidades Fiscalizadores Superiores OLACEFS, con la finalidad de evaluar a nivel de Latinoamérica el gobierno de Tecnología de la Información, a raíz de lo anterior se procedió a definir las instituciones a ser auditadas, para lo cual la Dirección de Auditorías Centralizadas y Descentralizadas, emitió la Orden de Trabajo Nº 003-2014-DACD de fecha 29 de septiembre de 2014, para realizar auditoría especial sobre Gobernanza de Tecnología de la Información a la Empresa Nacional de Energía Eléctrica (ENEE), por el período comprendido del 01 de enero al 30 de junio de 2014.

Es importante mencionar que la gobernanza de TI, se define como un sistema a través del cual el uso actual y futuro de la TI, es dirigido y controlado, significa evaluar y direccionar el uso de la TI para dar soporte a la institución y monitorear su uso para realizar los planes, incluyendo la estrategia y las políticas de uso de la TI dentro de la Institución; por otra parte los controles de TI, son políticas, procedimientos, prácticas y estructuras organizacionales creadas para proveer una razonable garantía de que los objetivos del negocio están alcanzados y que los eventos indeseables serán evitados o detectados y corregidos.

Durante la ejecución de la auditoría, se procedió a evaluar los controles generales de TI implementados por la División de Informática de la Empresa Nacional de Energía (ENEE) y como producto de la revisión y análisis de la documentación presentada se determinaron algunas deficiencias de control interno que se consideran importantes para merecer la atención de aquellos a cargo de la máxima autoridad, mismas que son reportadas en el capítulo III de este informe.

CAPÍTULO III

DEFICIENCIAS ENCONTRADAS Y RECOMENDACIONES

1. NO EXISTEN POLÍTICAS DE GOBERNANZA DE TECNOLOGÍA DE LA INFORMACIÓN DEFINIDAS, APROBADAS E IMPLEMENTADAS POR LA ALTA ADMINISTRACIÓN.

Al evaluar la estructura de gobernanza de Tecnología de la Información de la institución, se comprobó que no existen políticas de gobernanza de TI definidas, aprobadas e implementadas por la alta administración, que permitan dirigir y controlar las Tecnologías de la Información a fin de alcanzar los objetivos institucionales, cabe mencionar que existen algunas políticas en la División de Informática como ser el Manual de Buenas prácticas del uso de internet institucional y las Políticas de TI, Gestión y Normativas aplicables a la Institución sin embargo las mismas no han sido aprobadas por la alta administración.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional del Recursos Público, TSC-NOGECI II-03 responsabilidad por el control interno y TSC-NOGECI III-08 adhesión a las políticas.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…1. Existen unas políticas que tienden a establecer un marco de gobernanza de tecnología de Información y de gestión y de uso corporativo de TI, sin embargo a la fecha no están aprobadas por la alta administración…"

Lo anterior no permite administrar eficientemente los recursos informativos de la institución.

RECOMEDACIÓN No. 1
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Diseñar, aprobar, socializar e implementar un manual que contenga las políticas de gobernanzas en Tecnología de la Información, el cual deberá contener los procesos para dirigir y controlar las Tecnologías de la Información a fin de alcanzar los objetivos institucionales, una vez implementadas crear un mecanismo para que dichas políticas sean fácilmente accesibles para todos los miembros de la institución.

b) Verificar el cumplimiento de esta recomendación

2. NO EXISTE UN COMITÉ DE TECNOLOGÍA DE LA INFORMACIÓN QUE COORDINE Y SUPERVISE LAS DIFERENTES ACTIVIDADES INFORMÁTICAS DE LA INSTITUCIÓN.

Al evaluar los procesos y controles generales de TI, de la División de Informática, se nos manifestó que la Institución no cuenta con un Comité de Tecnología de la Información que coordine y supervise las actividades informáticas de la Institución, además que sea responsable de orientar las acciones e inversiones en Tecnología de Información y Comunicación TIC, en cumplimiento con las respectivas planificaciones estratégicas de TI.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recurso Públicos, TSC-PRECI-04: Eficiencia y TSC -NOGECI V-03 Análisis de Costo/Beneficio.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…2. No ha sido conformado un comité de tecnología de información…"

La falta de formalización de un comité de Tecnología de la Información impide determinar efectivamente las prioridades de inversión y asignación de recursos en los diversos proyectos y acciones de TI, así como optimizar los recursos disponibles.

RECOMEDACIÓN No. 2
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Crear un Comité de Tecnología de la Información, que se responsabilice por la alineación de las inversiones de Tecnología de la Información con los objetivos institucionales, y para apoyar la priorización de proyectos a ser desarrollados, el cual determinará los objetivos, funciones y responsabilidad que este mantendrá en relación con el apoyo y asesoría en las diferentes actividades informáticas, además se deberá establecer la periocidad de las reuniones, dejando actas de dichas reuniones.

b) Asimismo, las actuaciones de este comité deberán ser supervisadas por la alta administración dejando también actas de las reuniones donde contemple las decisiones del Comité de TI.

c) El comité de Tecnología de la Información deberá estar integrado de la siguiente forma:

- Fiscal General de la República o su representante, quien lo coordinará

- Jefe del Departamento de Sistemas de Información o su representante, quien actuará como secretario del mismo.
- Sub-Gerente de Recursos Humanos o su representante
- Gerente de Servicio Legal o su representante
- Gerente Administrativo Financiero o su representante
- Auditoría Interna o su representante.

d) Entre las responsabilidades del comité, se sugieren:

- Evaluar las principales estrategias de Tecnologías de Información.
- Evaluar y priorizar los requerimientos de Tecnología de la Información de las áreas de la entidad.
- Decidir sobre las principales contrataciones en Tecnología de Información.
- Evaluar los riesgos y controles internos relativos a Tecnología de Información.
- Evaluar los indicadores claves de Tecnologías de Información y su relación con los indicadores claves de la Entidad.
- Aprobar y supervisar la ejecución del Plan estratégico de Tecnologías de Información.
- Elaborar y aprobar el Manual de políticas de tecnologías de información.
- Elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad en informática.
- Darle seguimiento al Plan Estratégico de Tecnologías de Información.
- Coordinar el análisis de riesgos, planes de contingencia y prevención de desastres.
- Efectuar la evaluación y revisión de la situación de la ENEE en cuanto a seguridad informática, incluyendo el análisis de incidentes ocurridos.
- Velar por el fiel cumplimiento de las políticas informáticas.

e) Verificar el cumplimiento de estas recomendaciones.

3. NO EXISTE UN PROCESO DE PLANIFICACIÓN DE TECNOLOGÍA DE LA INFORMACIÓN.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática de la Institución, no cuenta con un proceso de planificación de la tecnología de la Información, que contenga procedimientos debidamente aprobados e implementados para realizar el plan estratégico de TI, (PETI) y el plan director de TI (PDTI), sin embargo existe un proceso para elaborar el plan operativo de TI (POTI), se comprobó

la existencia del Plan Operativo anual de la División de Informativa elaborado el 02 de enero de 2014.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional del Recursos Público, TSC-PRECI-01: Planeación, TSC-PRECI-04: Eficiencia y TSC-NOGECI IV-02 Planificación.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4…Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

La falta de un proceso de planeamiento de Tecnología de información impide demostrar el cumplimiento de la eficiencia en la ejecución de las operaciones y en el logro de los objetivos institucionales.

RECOMEDACIÓN No. 3
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, socializar e implementar un proceso de planificación de Tecnologías de la Información que contenga los elementos esenciales del proceso de planificación estratégica de TI, tales como:

   - La participación de las partes interesadas (áreas de TI, y de la entidad).
   - El desglose del plan estratégico de TI, (PETI) y del plan Director de TI (PDTI) (establecimiento de planes de acción de corto y medio plazo de TI) por las unidades ejecutoras y correspondiente alineación con las iniciativas estratégicas de la Institución.
   - La existencia de evaluación y/o monitoreo del Plan Director de TI (PDTI).

b) Verificar el cumplimiento de esta recomendación.

4. NO EXISTE UNA NORMA INTERNA DONDE SE DEFINA EL PROCESO DE PLANEAMIENTO DE TECNOLOGÍA DE INFORMACIÓN.

Al evaluar los procesos y controles generales de TI, de la División de Informática de la Institución se comprobó que no existe una norma interna donde se defina el proceso de planeamiento de Tecnología de información.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recurso Públicos, TSC - NOGECI V-01 Prácticas y Medidas de Control.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4…Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite a entidad contar con un proceso de planeamiento de tecnología de Información como norma interna establecida dentro de sanos criterios de efectividad, economía y eficiencia.

RECOMEDACIÓN No. 4
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Diseñar, aprobar, socializar e implementar una norma interna que contenga el proceso de planeamiento de Tecnología de Información, donde se defina el proceso para elaborar el plan estratégico de TI, (PETI) y el plan director de TI (PDTI), y el plan operativo de TI (POTI).

b) Verificar el cumplimiento de esta recomendación.

5. NO EXISTE UN PLAN ESTRATÉGICO INSTITUCIONAL

Al evaluar los procesos y controles generales de TI, el Jefe de la División de Informática nos manifestó que existe un plan estratégico institucional, sin embargo no nos proporcionó evidencia.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recursos Públicos
TSC-PRECI-01: Planeación.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4…Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Al no existir un Plan Estratégico Institucional no se podrán reflejar las estrategias a seguir por la institución a medio plazo (entre 1 y 5 años), ni marcar las directrices y el comportamiento para que la institución alcance las aspiraciones plasmadas en el Plan Director

RECOMEDACIÓN No. 5
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar y socializar un plan estratégico institucional que contenga la estrategia global de la institución, estableciendo metas y objetivos a largo plazo, con el propósito de alcanzar un determinado resultado, de este modo el plan estratégico institucional debe constar al menos de los siguientes elementos: la institución (que hacemos), la visión del futuro, la misión institucional, el análisis de los ambientes internos y externos, la estrategia y el desglose y la forma de evaluación del plan.

b) Verificar el cumplimiento de esta recomendación.

6. NO EXISTE UN PLAN ESTRATÉGICO DE TECNOLOGÍA DE INFORMACIÓN.

Al evaluar los procesos y controles generales de TI, se comprobó que el la División de Informática no cuenta con un plan estratégico de Tecnología de Información para gestionar todos los recursos de TI, en alineación con las prioridades y estrategias de la planificación estratégica institucional y los requisitos de gobernanza.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recursos Públicos TSC-PRECI-01: Planeación, TSC-NOGECI IV-02 Planificación y TSC-NOGECI IV-05 Revisión de los objetivos.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4…Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos

sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Al no existir un plan estratégico de tecnología de Información no permite a la entidad gestionar el uso de la tecnología de información.

RECOMEDACIÓN No. 6
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Involucrar a todos los actores relevantes de la institución, como ser los Directores y Jefes de Departamento para que de manera conjunta con la División de Informática se elabore un plan estratégico de Tecnología de la Información alineado con el plan estratégico institucional a largo plazo o sea con horizonte de tres a cinco años, en el cual se describan como los recursos de TI contribuirán con los objetivos estratégicos de la institución, este plan deberá:
   - Declarar los objetivos y las iniciativas estratégicas del área de TI
   - Definir como los objetivos estratégicos de TI serán alcanzados y medidos, o sea, definir los indicadores de desempeño en conformidad con los objetivos estratégicos de TI.
   - Contemplar el presupuesto operacional y de inversiones, las estrategias de suministro y de adquisición (contratación de servicios y adquisición de equipo) y los requisitos legales y regulados.
   - Ser suficientemente detallado para posibilitar la definición de los planes tácticos de TI.
   - Ser formalmente liberado (aprobado y publicado) para que sea ejecutado por las partes interesadas.

b) Verificar el cumplimiento de esta recomendación.

7. NO EXISTE UN PLAN DIRECTOR DE TECNOLOGÍA DE INFORMACIÓN Y/O PLANES TÁCTICOS DE TI.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con un plan director de Tecnología de Información y/o planes tácticos de TI, derivado del plan estratégico de TI, que sirva de instrumento de diagnóstico, planificación y gestión de recursos y procesos de TI.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recursos Públicos TSC-PRECI-01: Planeación, TSC-NOGECI IV-02 Planificación y TSC-NOGECI IV-05 Revisión de los objetivos.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4…Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite atender las necesidades tecnológicas y de información de la entidad para un determinado período.

RECOMEDACIÓN No. 7
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Crear un portafolio de planes tácticos de Tecnología de Información derivados del plan estratégico de TI, estos planes tácticos deben describir cuales son las iniciativas de TI requeridas, cuales son los recursos necesarios y como el uso de los recursos y los beneficios alcanzados serán monitoreados y administrados, por lo tanto deben:

   - Contener las necesidades de información alineadas con la estrategia de la institución.
   - Contemplar programa de inversiones, propuesta presupuestaria, las estrategias de suministro y de adquisición (contratación de servicios y adquisición de equipo), la gestión de riesgo de TI, cuantitativo y capacitación del personal de TI y requisitos legales y reglamentarios.
   - Contener indicadores de desempeño en conformidad con los objetivos estratégicos de TI.
   - Ser suficientemente detallado para posibilitar la definición de los planes de acción o planes operacionales de TI.
   - Ser formalmente liberado (aprobado y publicado) para que sea ejecutado por las partes interesadas.

b) Verificar el cumplimiento de esta recomendación.

8. NO EXISTE UN PLAN DE COMPRAS Y/O GASTOS DE TECNOLOGÍA DE LA INFORMACIÓN

Al evaluar los procesos y controles generales de TI, de la División de Informática, se nos manifestó que no existe un plan de compras y/o gastos de tecnología de la Información donde se identifiquen los proyectos de TI de la institución tales como: proyecto para el desarrollo de software, proyectos de mejora en software existentes, proyectos para selección de soluciones de software, de hardware o de ambos, proyectos de integración de sistemas, proyectos de consultoría en TI.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recursos Públicos TSC-PRECI-01: Planeación, TSC-NOGECI IV-02 Planificación y TSC-NOGECI IV-05

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…3. Toda adquisición, contratación y planeamiento fueron desarrollados a través de las normativas del banco mundial y la División de Informática actuó como desarrollador de especificaciones técnicas de equipos y sistemas únicamente. Por lo anterior es que no existen dentro u originados de la División de informática planes de tecnología, documentos que contengan información sobre el progreso de las acciones de TI, normas de contrataciones, presupuesto de TI, plan de compra etc. Si existiesen documentos aprobados por la alta administración deberán estar en poder de la Unidad Ejecutora de proyectos de Promef.

La falta de un plan de compras y/ o gastos de Tecnología de la Información no permite conocer los proyectos de soluciones y adquisiciones de Tecnología de Información previstos por el Departamento de Sistemas de Información.

RECOMEDACIÓN No. 8
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Diseñar, aprobar, e implementar un plan de compras y/gastos de Tecnología de la Información donde se incluyan los proyectos de adquisidores y soluciones de TI de la institución con la estimación del costo de las contrataciones previstas.

b) Verificar el cumplimiento de esta recomendación.

9. NO EXISTE UNA NORMA INTERNA SOBRE EL PROCESO DE CONTRATACIONES DE TECNOLOGÍA DE LA INFORMACIÓN.

Al evaluar los procesos y controles generales de TI, de la División de Informática, se nos manifestó que en la Institución no existe una norma interna sobre el proceso de contrataciones de Tecnología de la Información, donde se defina, el proceso de evaluación y priorización de los requerimientos de TI, el proceso para el planeamiento de contrataciones de TI y el proceso de gestión de contratos de TI; sin embargo se nos informó que todas las contrataciones se realizan en cumplimiento a lo establecido en la Ley de Contratación del Estado.

Incumpliendo lo establecido en:
Marco Rector de Control Interno Institucional de los Recurso Públicos, TSC - NOGECI V-01 Prácticas y Medidas de Control.

Sobre el particular mediante oficio No. DI-096-II-2015 de fecha 25 de febrero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…3.Toda adquisición, contratación y planeamiento fueron desarrollados a través de las normativas del banco mundial y la División de Informática actuó como desarrollador de especificaciones técnicas de equipos y sistemas únicamente. Por lo anterior es que no existen dentro u originados de la División de informática planes de tecnología, documentos que contengan información sobre el progreso de las acciones de TI, normas de contrataciones, presupuesto de TI, plan de compra etc. Si existiesen documentos aprobados por la alta administración deberán estar en poder de la Unidad Ejecutora de proyectos de Promef.

La falta de una norma interna sobre el proceso de contrataciones de TI no permite conocer si las contrataciones de TI están alineadas con la planificación estratégica institucional, además no permite a la institución contar con un guía que le permita, evaluar, priorizar y gestionar de forma adecuada, eficiente y eficaz las contrataciones.

RECOMEDACIÓN No. 9
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Diseñar, aprobar, socializar e implementar una norma interna que contenga el proceso de contrataciones de Tecnología de la Información, donde se defina el proceso de evaluación y priorización de los requerimientos de TI, el proceso para el planeamiento de contrataciones de TI y el proceso de gestión de contratos de TI, con el fin de que las contrataciones de TI estén en armonía con el plan estratégico de TI, y alineadas con la planificación estratégica institucional, asimismo los

procesos de planeamiento de contrataciones de TI y el proceso de gestión de contratos deberán ser monitoreados periódicamente.

b) Verificar el cumplimiento de esta recomendación.

10. NO EXISTE UN PLAN DE CONTINUIDAD DE NEGOCIO DEBIDAMENTE APROBADO Y PUBLICADO.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con un plan de continuidad de negocio que permita a la institución continuar ofreciendo los servicios críticos en caso de que ocurra una interrupción de las actividades del negocio, y para proteger los procesos críticos contra efectos de fallas o desastres significativos como ser: falla humana, falla en componente de TI, Hurto o robo, incendio, eléctrica, desastres naturales, terrorismo interrupción de energía, virus, acceso indebido, ataque cibernético, sabotaje, vandalismo disturbio civil (huelga) entre otros.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4. En referencia a los puntos que se refieren a seguridad informática, existe en base a los sistemas actuales, los cuales están en proceso de ser sustituidos, procedimientos de respaldo de la información, personas designadas para tales efectos, procesos para la gestión de incidentes, sin embargo estos no están aprobados por la alta administración. Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Al no contar con un plan de continuidad del negocios, no están identificadas las operaciones críticas que son necesarias para la supervivencia de la institución, los recursos humanos y materiales que las soportan y un plan de restauración para normalizar las operaciones en caso que suceda un incidente o desastre.

RECOMEDACIÓN No. 10
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Analizar y evaluar los riesgos a los cuales está expuesta la organización, e identificar los eventos que puedan causar interrupciones en los procesos del negocio en aspectos relativos a la seguridad de la información y comunicaciones; luego elaborar, aprobar, socializar e implementar un Plan de Continuidad del Negocio para garantizar el funcionamiento de los servicios informáticos de la institución, en caso de suceder un incidente o desastre, el cual debe incluir de forma clara los procedimientos de respaldo y recuperación de la información, así como las pruebas y actualización de los planes. El plan de continuidad del negocio deberá comprender tres componentes o subplanes. Cada plan deberá establecer las contramedidas necesarias a llevar a cabo en caso de la materialización de cualquier amenaza:

   - El plan de respaldo: Deberá contemplar las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar la materialización de una amenaza.
   - El plan de emergencia: Deberá contemplar las contramedidas necesarias durante la materialización de una amenaza. Su finalidad es paliar los efectos adversos de la amenaza.
   - El plan de recuperación: Deberá contemplar las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.

b) Verificar el cumplimiento de esta recomendación.

11. NO EXISTE UN PROCESO PARA INVENTARIAR ACTIVOS DE INFORMACIÓN DEBIDAMENTE APROBADO Y PUBLICADO.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no con cuenta con un proceso para inventariar activos de información (datos, hardware, software e instalaciones) debidamente aprobado y publicado, sin embargo la División de Informática cuenta con un inventario del Equipo Informático.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI V-15 Inventarios Periódicos

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…Si bien es cierto dentro de la División de Informática existen mecanismos y políticas de control, seguridad, planeación de los sistemas informáticos y de la infraestructura tecnológica, estos no exponen la aprobación de la alta administración de la Empresa Nacional de Energía Eléctrica, ni se publican y/o divulgan a lo interno de la Empresa, sin embargo mucho agradeceremos el apoyo que el Tribunal Superior de Cuentas pueda otorgarnos para formalizar y oficializar todas las acciones que se refieran a las tecnologías de la información y comunicaciones de la Empresa Nacional de Energía Eléctrica…"

Al no contar con un proceso para inventariar activos de información no permite contar con un inventario detallado y así poder clasificarlos y determinar el nivel de protección a proveer a cada uno de ellos no permite identificar al propietario responsable del activo informático, ni la responsabilidad por el mantenimiento apropiado de los mismos.

RECOMEDACIÓN No. 11
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, e implementar con un proceso para inventariar activos de información con el objetivo que la institución identifique los activos y documente su importancia incluyendo todas las informaciones necesarias que permitan la recuperación del activo informático en caso de un desastre, esas informaciones incluyen tipo de activo, formato, ubicación, informaciones acerca de copias de seguridad, informaciones acerca de permisos y la importancia del activo para el negocio.

b) Verificar el cumplimiento de esta recomendación

12. NO EXISTE UN PROCESO PARA LA CLASIFICACIÓN DE LA INFORMACIÓN DE LA INSTITUCIÓN, DEBIDAMENTE APROBADO Y PUBLICADO.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con un proceso para la clasificación de la información de la institución debidamente aprobado y publicado, que cuente con los requerimientos legales, regulatorios, contractuales para mantener la privacidad y la confidencialidad de la información de la institución, con el fin de asegurar que la información reciba el nivel de protección adecuado.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control.

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…Si bien es cierto dentro de la División de Informática existen mecanismos y políticas de control, seguridad, planeación de los sistemas informáticos y de la infraestructura tecnológica, estos no exponen la aprobación de la alta administración de la Empresa Nacional de Energía Eléctrica, ni se publican y/o divulgan a lo interno de la Empresa, sin embargo mucho agradeceremos el apoyo que el Tribunal Superior de Cuentas pueda otorgarnos para formalizar y oficializar todas las acciones que se refieran a las tecnologías de la información y comunicaciones de la Empresa Nacional de Energía Eléctrica…"

Lo anterior no permite conocer quién es el propietario de la información, el proceso de otorgar acceso, la persona responsable de aprobar los derechos de acceso y los niveles de acceso, el grado y profundidad de los controles de seguridad, así como la importancia del activo de información, asimismo se corre el riesgo de divulgación indebida de información confidencial.

RECOMEDACIÓN No. 12
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, socializar e implementar un proceso de clasificación de la información de la institución en términos de su valor, requisitos legales, sensibilidad y criticidad para la institución, este proceso permitirá adoptar un esquema de clasificación y asignar la información a un nivel de sensibilidad permitiendo un tratamiento uniforme de los datos, aplicando políticas y procedimientos a nivel especifico y a la vez que los usuarios de la institución, reciban instrucciones de cómo tratar cada pieza de información.

b) Verificar el cumplimiento de esta recomendación

13. NO EXISTE UN PROCESO PARA LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES DEBIDAMENTE APROBADO Y PUBLICADO.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con un proceso para la gestión de riesgos de la seguridad de la información y comunicaciones debidamente aprobado

y publicado que ayude a identificar las vulnerabilidades y las amenazas para los recursos de información utilizados en la institución.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC -NOGECI IV-06 Gestión de Riesgos Institucionales

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4. En referencia a los puntos que se refieren a seguridad informática, existe en base a los sistemas actuales, los cuales están en proceso de ser sustituidos, procedimientos de respaldo de la información, personas designadas para tales efectos, procesos para la gestión de incidentes, sin embargo estos no están aprobados por la alta administración. Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite identificar los activos o recursos de información que son vulnerables a amenazas y los cuales necesitan protección.

RECOMEDACIÓN No. 13
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, socializar e implementar un proceso de gestión de riesgos, de la seguridad de la información y comunicaciones (Grsic), a fin de garantizar que la institución gestiona sus riesgos de forma coherente y adecuada, dicho proceso deberá contener los siguientes elementos:
   - La descripción del rol de los profesionales involucrados (alta administración y el gestor de seguridad de la información y comunicaciones)
   - Las actividades previstas
   - Los artefactos previstos (plan de riesgos y el plan de tratamiento de riesgos).

   El plan de riesgos con:
   - Listado de riesgos
   - Evaluación de los riesgos identificados por medio de probabilidad e impacto asociado
   - Relación de riesgos que requieren tratamiento en orden de prioridad.

   El Plan de tratamiento de riesgos con:
   - Formas de tratamiento de riesgos (aceptar, mitigar, transferir o

aceptar)
- Acciones que deben desarrollar para tratamiento de los riesgos.

b) Se debe designar una persona o equipo responsable de desarrollar e implementar el proceso de gestión de riesgos, de la seguridad de la información y comunicaciones (Grsic).

c) Verificar el cumplimiento de estas recomendaciones.

14. NO EXISTE UN PROCESO PARA LA GESTIÓN Y MANEJO DE INCIDENTES, DEBIDAMENTE APROBADO Y PUBLICADO.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con un proceso para la gestión y manejo de incidentes, debidamente aprobado y publicado, que permita realizar una gestión dinámica, proactiva y bien documentada, en caso de darse cualquier evento indeseable que no sea parte de la operación de un servicio y que pueda causar un daño, interrupción, o una reducción en la calidad del servicio o en las redes computacionales, sin embargo se nos manifestó que existe formalmente la designación del equipo de tratamiento y respuesta a incidentes, pero no se nos proporcionó la evidencia de su existencia.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control, TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4. En referencia a los puntos que se refieren a seguridad informática, existe en base a los sistemas actuales, los cuales están en proceso de ser sustituidos, procedimientos de respaldo de la información, personas designadas para tales efectos, procesos para la gestión de incidentes, sin embargo estos no están aprobados por la alta administración. Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite documentar, clasificar, y revisar los incidentes menores, mayores y de crisis hasta que se corrijan o resuelvan.

RECOMEDACIÓN No. 14
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, socializar e implementar un proceso para la gestión y manejo de incidentes, donde se realice una clasificación o categorización de los tipos de incidentes como ser: urgente, grave, significante etc, con el fin de restaurar lo más rápido posible los servicios de los cuales dependen los usuarios finales o responder a las requisiciones de los servicios dicho proceso deberá contener los siguientes elementos:

- Los papeles de los profesionales involucrados (descripción de los papeles del usuario y del gerente de Incidentes o encargado)
- Las actividades previstas,
- Los artefactos previstos en cuanto a esto es obligatorio que haya documentos que contengan las lista de incidentes registrados conteniendo: clasificación de los incidentes por escala de gravedad (ejemplo de clasificación Urgente, grave, significante etc…), fechas de apertura y cierre de incidente, histórico de accidentes ejecutadas en virtud del accidente.

b) Se debe designar una persona o equipo de tratamiento y respuestas a incidentes, a la cual se le deben notificar todos los incidentes relevantes tan pronto como sea posible; luego deben ejecutar el plan de recuperación y tomar las acciones apropiadas cuando ocurran incidentes de seguridad.

c) Verificar el cumplimiento de estas recomendaciones.

15. NO ESTÁ DESIGNADO LAS PERSONAS O UNIDADES PARA GESTIONAR LA SEGURIDAD DE LA INFORMACIÓN

Al evaluar los procesos y controles generales de TI, se comprobó que la institución no ha designado a las personas o unidades para gestionar la seguridad de la información, responsables por las acciones de seguridad de la información y comunicaciones de la institución.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4. En referencia a los puntos que se refieren a seguridad informática, existe en base a los sistemas actuales, los cuales están en proceso de ser sustituidos, procedimientos de respaldo de la información, personas designadas para tales efectos, procesos para la gestión de incidentes, sin embargo estos no están aprobados por la alta administración. Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite la optimización de las acciones de seguridad de la información.

RECOMEDACIÓN No. 15
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Se debe designar a las personas o unidades responsables de gestionar la seguridad de la información de la entidad con las siguientes responsabilidades:

- Promover una cultura de seguridad de la información y comunicaciones;
- acompañar las investigaciones y las evaluaciones de los daños derivados de quiebras de seguridad.
- Proponer recursos necesarios o acciones de seguridad de información y comunicaciones
- Coordinar el Comité de seguridad de la Información y Comunicaciones y el equipo de tratamientos y respuestas a incidentes.
- Realizar y acompañar estudios de nuevas tecnologías, en cuanto a posibles impactos en la seguridad de la información y comunicaciones.
- Proponer normas y procedimientos relativos a la seguridad de la información y comunicaciones en el ámbito de la entidad.

b) Verificar el cumplimiento de esta recomendación.

16. NO EXISTE UN COMITÉ DE SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES.

Al evaluar los procesos y controles generales de TI, se comprobó que la institución no cuenta con un comité de seguridad de la información y comunicaciones, para lograr un gobierno efectivo de la seguridad de la información, donde se establezca y se mantenga un marco para guiar el desarrollo y la gestión de un programa completo de seguridad de la información que apoye los objetivos estratégicos de la institución.

Incumpliendo lo establecido en:
Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4. En referencia a los puntos que se refieren a seguridad informática, existe en base a los sistemas actuales, los cuales están en proceso de ser sustituidos, procedimientos de respaldo de la información, personas designadas para tales efectos, procesos para la gestión de incidentes, sin embargo estos no están aprobados por la alta administración. Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite que se tenga una estrategia completa de seguridad de la información, mediante la cual se garantice que el riesgo de la seguridad de la información sea gestionado de manera apropiada y que los recursos de información de la institución se usen con responsabilidad.

RECOMEDACIÓN No. 16
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Conformar un comité de seguridad de la información y comunicaciones que desarrolle e implemente un marco de gobierno de la seguridad de la información que provea la garantía de que a los activos de información se le proporcione un nivel de protección acorde con su importancia o con el riesgo que representa para la institución si los mismos se ven comprometidos.

b) Verificar el cumplimiento de esta recomendación.

17. NO EXISTE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y COMUNICACIONES, DEBIDAMENTE APROBADA Y PUBLICADA.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática cuenta con un Manual de Políticas de seguridad de la información, sin embargo el mismo no se encuentra debidamente aprobado y publicado.

Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…4. En referencia a los puntos que se refieren a seguridad informática, existe en base a los sistemas actuales, los cuales están en proceso de ser sustituidos, procedimientos de respaldo de la información, personas designadas para tales efectos, procesos para la gestión de incidentes, sin embargo estos no están aprobados por la alta administración. Deberán desarrollarse nuevas políticas, planeamiento, normas internas, plan estratégico etc., en base a los nuevos sistemas informáticos que han sido adquiridos a través de un financiamiento del Banco mundial y que en la actualidad están regidos y coordinados por el proyecto promef…"

Lo anterior no permite que la ENEE cuente con una Infraestructura de seguridad adecuada a su necesidad institucional.

RECOMEDACIÓN No. 17
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Revisar la política de seguridad de la información para que por lo menos contenga: concepto y definición de la seguridad, sus objetivos y alcances, su importancia, una declaración de intención de la alta gerencia de apoyar las metas y principios de la seguridad de la información en línea con la estrategia y los objetivos institucionales de la institución, un marco de controles, evaluación y gestión de riesgos, cumplimiento de leyes, normas, procedimientos, requerimientos de formación y concientización, gestión de continuidad del negocio, consecuencias de violación de las políticas de seguridad, responsabilidades y competencias de la gerencia de la seguridad, revisión de la Posic etc., una vez analizada deberá ser aprobada socializada e implementada.

b) La política de seguridad de la información debe revisarse con intervalos planificados o cuando ocurrieran cambios significativos, para asegurar que siga siendo pertinente, adecuada, y eficaz.

c) Verificar el cumplimiento de estas recomendaciones.

18. NO EXISTE UNA POLÍTICA DE CONTROL DE ACCESOS, DEBIDAMENTE APROBADA Y PUBLICADA.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con una política de control de accesos debidamente aprobada y publicada donde se establezca las directrices para controles de acceso lógico (controles de acceso de activos de información), y directrices para controles de acceso físico (controles de acceso de áreas e instalaciones físicas, usuarios y activos de información.

Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…Si bien es cierto dentro de la División de Informática existen mecanismos y políticas de control, seguridad, planeación de los sistemas informáticos y de la infraestructura tecnológica, estos no exponen la aprobación de la alta administración de la Empresa Nacional de Energía Eléctrica, ni se publican y/o divulgan a lo interno de la Empresa, sin embargo mucho agradeceremos el apoyo que el Tribunal Superior de Cuentas pueda otorgarnos para formalizar y oficializar todas las acciones que se refieran a las tecnologías de la información y comunicaciones de la Empresa Nacional de Energía Eléctrica…"

Al no contar con una política que establezca el proceso adecuado para control de acceso, no permite contar con una identificación y autenticación de las personas que acceden a los recursos informáticos de la institución; y establecer criterios para definir permisos y otorgar privilegios de seguridad.

RECOMEDACIÓN No. 18
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, socializar e implementar una política de control de acceso con el objetivo de establecer criterios básicos para asignar el acceso técnico a los datos, programas, dispositivos y recursos específicos, incluyendo quien tendrá acceso y el nivel de permiso

permitido, la política de control de acceso deberá incluirse la separación de funciones para el control de accesos y los requisitos para autorización formal de solicitudes de acceso.

b) Verificar el cumplimiento de esta recomendación

19. NO EXISTE UN PROCESO DE GESTIÓN DE CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍA DE INFORMACIÓN DEBIDAMENTE APROBADO Y PUBLICADO.

Al evaluar los procesos y controles generales de TI, se comprobó que la División de Informática no cuenta con un proceso de gestión de continuidad de los servicios de tecnología de información debidamente aprobado y publicado, en este caso la gestión de servicios de TI, son los procesos de gestión de configuración, y gestión de cambios).

Marco Rector de Control interno Institucional de los Recursos Públicos TSC-NOGECI V-01 Prácticas y Medidas de Control. TSC-NOGECI- VI-04 Controles Sobre Sistemas de Información

Sobre el particular mediante oficio No. 044-I-2015 de fecha 26 de enero de 2015 el Ingeniero José Francisco Calix Jefe de la División de Informática manifestó lo siguiente: "…Si bien es cierto dentro de la División de Informática existen mecanismos y políticas de control, seguridad, planeación de los sistemas informáticos y de la infraestructura tecnológica, estos no exponen la aprobación de la alta administración de la Empresa Nacional de Energía Eléctrica, ni se publican y/o divulgan a lo interno de la Empresa, sin embargo mucho agradeceremos el apoyo que el Tribunal Superior de Cuentas pueda otorgarnos para formalizar y oficializar todas las acciones que se refieran a las tecnologías de la información y comunicaciones de la Empresa Nacional de Energía Eléctrica…"

Al no contar con un proceso de gestión de continuidad de los servicios de Tecnología de Información no permite aportar un servicio de calidad alineado a las necesidades del negocio de la institución.

RECOMEDACIÓN No. 19
AL COORDINADOR DEL GABINETE DE INFRAESTRUCTURA PRODUCTIVA Y GERENTE GENERAL INTERINO DE LA EMPRESA NACIONAL DE ENERGIA ELECTRICA (ENEE)

a) Elaborar, aprobar, socializar e implementar un proceso de gestión de continuidad de los servicios de Tecnología de Información (procesos de gestión de configuración, gestión de cambios).
La gestión de configuración tiene por objetivo identificar y controlar los activos de TI y los Items de configuración existentes en la institución

estableciendo las relaciones entre los ítems y los servicios de TI prestados, dicho proceso deberá tener los siguientes elementos:

- Los papeles de los profesionales involucrados.
- Las actividades previstas
- Los artefactos previstos (la base de datos administración de configuración del ambiente computacional y la herramienta de gestión de configuración implantada)

La gestión de cambios tiene como objetivo minimizar el impacto del cambio requerido para resolución del incidente o problema, manteniendo la calidad de los servicios, así como mejorar la operacionalización de la infraestructura, asimismo asegurar que todos los cambios sean aprobados, implementados y revisados de manera controlada dicho proceso deberá tener los siguientes elementos:

- Los papeles de los profesionales involucrados.
- Las actividades previstas
- Los artefactos previstos (clasificación de los cambios ejemplo de clasificación: de infraestructura , en aplicación, en servicios etc, priorización de los cambios, evaluación de impacto de los cambios y autorización de los cambios).

b) Verificar el cumplimiento de esta recomendación

CAPÍTULO IV

CONCLUSIONES

Como producto de nuestra auditoría especial sobre Gobernanza de Tecnología de la Información practicada a la Empresa Nacional de Energía Eléctrica (ENEE), se concluye que la institución no cuenta con mecanismos y estructuras de gobernanza de tecnologías de información, definidas e implementadas adecuadamente en la entidad, con el objetivo de dirigir y controlar la TI, lo que no permite evaluar la efectividad de la estructura de gobierno de TI para determinar si las decisiones, las direcciones, y el desempeño de TI respaldan las estrategias y los objetivos de la Empresa Nacional de Energía Eléctrica (ENEE), una estructura de gobernanza incluye las políticas de buena gobernanza de Tecnología que permitan administrar eficientemente los recursos informáticos de la institución, los procesos de planificación de Tecnología de Información, los procesos orientados hacia la adquisición de soluciones de tecnología de la Información, así como la puesta en práctica de la gestión de la seguridad de la información.

Tegucigalpa, M.D.C. 05 de junio de 2015.

Lic. Karla Janeth Escobar
Supervisora de Auditoría DACD

Lic. Everth Raúl Gutierrez
Técnico en Fiscalización

Lic. Carlos Roberto Silva
Director de Tecnología
de Información

Lic. Jonabelly Vanessa Alvarado
Directora de Auditorías
Centralizadas y Descentralizadas