INFORME AU-006-2020 INF

INFORME DE LOS RESULTADOS DE LA AUDITORÍA DE CARÁCTER ESPECIAL SOBRE LA EVALUACIÓN DEL CUMPLIMIENTO DE NORMAS TÉCNICAS, SISTEMAS DE TECNOLOGÍA, CONTROL DE CALIDAD Y SEGURIDAD DE LA INFORMACIÓN

Octubre, 2020

Resumen ejecutivo

¿Qué examinamos?

Se procedió a examinar y evaluar el cumplimiento de los sistemas de control interno, de tal forma que nos permitiera determinar si las actividades desarrolladas y ejecutadas por la Unidad de Tecnologías de la Información de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE) se realizan en cumplimiento de las Normas, estándares, procedimientos y demás regulaciones internas o externas que rigen las Tecnologías de la Información dentro del sector público costarricense.

¿Por qué es importante?

Las Normas de Control Interno para el Sector Público en su apartado 1.6: Responsabilidad de la Auditoría Interna sobre el Sistema de Control Interno (SCI), indica que la auditoría interna, en cumplimiento de sus funciones, debe brindar servicios de auditoría interna orientados a fortalecer el SCI, de conformidad con su competencia institucional y la normativa jurídica y técnica aplicable.

La misma norma en el punto 5.9 sobre Tecnologías de información, indica que el jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance. Para ello deben observar la normativa relacionada con las tecnologías de información, emitida por la Contraloría General de la República (CGR). En todo caso, deben instaurarse los mecanismos, procedimientos y manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información.

Las Normas técnicas para la gestión y control de las Tecnologías de Información apartado1.6: Decisiones sobre asuntos estratégicos de TI, indican que el jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.

La norma 2.1 sobre la planificación de las tecnologías de información señala que la organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

El estudio se realiza en atención al apartado 12 del Plan de Trabajo Anual del 2020 de la Auditoría Interna de la Comisión Nacional de Atención de Emergencias y Previsión de Riesgo, dicho apartado busca verificar el sistema de control interno, la calidad y la seguridad de la información confidencial, según las tecnologías de información para la toma de decisiones de procesos sustantivos de la Alta Gerencia de la CNE.

¿Qué encontramos?

Como resultado del estudio realizado, se encontraron deficiencias asociadas a la implementación y formalización de control interno dentro de la Unidad de Tecnologías de la Información de la

CNE, dichas deficiencias se relacionan principalmente con la carencia de Manuales de Procedimientos debidamente formalizados y promulgados, así como por la no aplicación de políticas internas que se relacionan con las actividades que debe desarrollar dicha Unidad.

La revisión efectuada permite determinar oportunidades de mejora en la gestión de la UTI derivadas de los periodos 2018 y 2019, algunos continúan en el periodo 2020, relacionados con los siguientes procesos o actividades:

- Estado del control interno en el Departamento TI de la CNE
- Cumplimiento de las regulaciones internas y externas relacionadas a TI
- Control sobre los proyectos ejecutados por la UTI
- Control sobre los requerimientos de mejoras a los sistemas
- Metodologías para el desarrollo de software
- Segregación de funciones dentro de la UTI
- Control y seguridades físicas en el área de tecnología
- Ambiente de control de la información gestionada y almacenada de los sistemas informáticos
- Planes de Contingencia o continuidad del servicio ante eventualidades
- Ambiente de control de los procesos y activos de cómputo
- Control de la red y accesos a la nube
- Capacidad de los sistemas y bases de datos
- Informes de rendimiento de los equipos en producción
- Gestión de labores de capacitación
- Esquemas de seguridad
- Control de salidas e ingresos de información de la CNE
- Uso e implementación de nuevas tendencias en seguridad informática
- Ciberseguridad
- Requerimientos compras
- Control del presupuesto de la UTI
- Planificación estratégica relacionada con Tecnologías de la información
- Estado de los servicios de TI con los que cuenta la CNE.

¿Qué sigue?

La CNE y la UTI principalmente, deben tener presente y tomar acciones prontas con relación a la Resolución R-DC-17-2020, que emite la Contraloría General de la República el 17 de marzo de 2020, derogando la Normas Técnicas para la Gestión y el Control de las Tecnologías de Información emitidas en el 2007, con el fin de que cada entidad emita su propia regulación a nivel de la gestión de TI, a partir del 01 de enero de 2022. Así como que la implementación de controles e identificación de los riesgos asociados a los objetivos estratégicos y operativos deben estar debidamente establecidos y administrados en búsqueda del logro de los objetivos institucionales y de los artículos 8 y 10 de la Ley General de Control Interno.

El estudio presenta una serie de recomendaciones en atención y mejora del control interno de la UTI; en cumplimiento de las recomendaciones (1-24) debe implementarse en el plazo de 15 días un cronograma o plan de acción formalizado (nombre del hallazgo, recomendación, acción (es), fecha de cumplimiento, responsable, observaciones, etc.), a la Auditoría Interna y a la Dirección Ejecutiva de la CNE.

1. Introducción

1.1 Origen del estudio:

El estudio se realiza en atención al apartado 12 del Plan de Trabajo Anual del 2020 de la Auditoría Interna de la Comisión Nacional de Atención de Emergencias y Previsión de Riesgo, dicho apartado busca verificar el sistema de control interno, la calidad y la seguridad de la información confidencial, según las tecnologías de información para la toma de decisiones de procesos sustantivos de la Alta Gerencia de la CNE.

1.2 Objetivo del estudio

- Evaluar el cumplimiento de los sistemas de control interno para determinar si las actividades relacionadas con el departamento de tecnologías de información se realizan cumpliendo las normas, estándares, procedimientos y cualquier otra regulación interna o externa emitida para el manejo de las tecnologías de información.

1.3. Objetivos específicos

1. Analizar y evaluar la aplicación de regulaciones emitidas por la Contraloría General de la República que son de carácter obligatorio, así como la aplicación de circulares, comunicados y procedimientos emitidos a nivel institucional.
2. Analizar y evaluar si existe un control adecuado de los proyectos presentados por las diferentes unidades de la CNE.
3. Analizar y evaluar el control sobre los requerimientos presentados para las mejoras a los sistemas por las diferentes unidades de la CNE.
4. Analizar si se diseña, desarrolla, o compra software de acuerdo con las necesidades de las diferentes unidades de la CNE y de acuerdo con la metodología aprobada a nivel institucional.
5. Analizar y evaluar si se cumple con una adecuada segregación de funciones en los procesos manuales y automatizados para que no se concentren en una sola persona.
6. Analizar y evaluar el control y seguridades físicas en el área de tecnología.
7. Analizar el ambiente de control de la información que es gestionada y almacenada dentro y fuera de los sistemas informáticos con el objetivo de identificar enumerar y evaluar los controles que se tengan implementados para garantizar la confidencialidad, integridad y disponibilidad de la información.
8. Analizar y evaluar si se cuenta con un plan de contingencia o continuidad del servicio en caso de presentarse una eventualidad.
9. Analizar el ambiente de control de los procesos y activos de cómputo central, computo personal, telecomunicaciones, accesos locales y remotos, servicios en la nube, entre otros., para identificar riesgo de negocio y ofrecer recomendaciones factibles, que solventen o mitiguen estos riesgos.
10. Analizar y evaluar si se administra adecuadamente la red que soporta tanto el área de comunicación entre las diferentes oficinas de la dependencia, así como las oficinas remotas ubicadas en otras localizaciones, y los accesos a la nube.
11. Evaluar si se realizan análisis de la capacidad de los sistemas y bases de datos.
12. Analizar si se realizan informes de rendimiento de los equipos en producción.
13. Analizar y evaluar si se coordina y realizan labores de capacitación y concientización en materia de seguridad de acuerdo con los lineamientos institucionales y con los objetivos estratégicos de TI.

14. Analizar si se cuenta con una plataforma tecnológica Institucional con esquemas de seguridad como Firewalls entre otros que garanticen la integridad y confidencialidad de los datos.
15. Verificar que los servicios de TI se encuentran al nivel que la organización requiere para habilitar, potenciar y soportar de manera efectiva y eficiente sus funciones.
16. Analizar y evaluar si se efectúan evaluaciones a la plataforma tecnológica Institucional sobre aspectos de esquemas de seguridad (Firewalls, entre otros) que garanticen la integridad y confidencialidad de los datos.
17. Evaluar si se cuenta con un Esquema de Seguridad, que controle tanto la salida como el ingreso de información hacia y desde la red interna de la Institución
18. Evaluar si la unidad de tecnología realiza investigaciones de las nuevas tendencias en seguridad informática
19. Evaluar si se planifica, coordina y realiza las labores de capacitación y concientización en materia de seguridad de acuerdo con los lineamientos institucionales y con los objetivos estratégicos de TI, generando la evidencia respectiva Informes de Capacitación y cierre del proceso
20. Analizar si se efectúa una planificación Estratégica tomando en cuenta el análisis de la capacidad de las necesidades de los diferentes departamentos de la CNE, así como verificar las acciones plasmadas en el cumplimiento de dichos Planes Estratégicos.
21. Analizar y evaluar si se lleva un adecuado seguimiento de los Proyectos del Negocio que estén relacionados con Tecnologías de Información
22. Evaluar si los requerimientos anuales de compras se realizan considerando lo establecido en el Plan Estratégico de la Institución y el Plan Estratégico de TI.
23. Evaluar si existe control sobre el presupuesto de gastos e inversiones asignado a la Unidad de tecnología.

1.4 Naturaleza, alcance y periodo del estudio

La naturaleza del estudio es de carácter especial. El alcance del servicio de auditoría se enfoca en el estudio del proceso de Tecnologías de Información de la Comisión Nacional de Prevención de Riesgos y Atención de Emergencias de Costa Rica, el plazo del estudio corresponde a los años 2018 y 2019, esto sin limitar la ampliación de este en caso de ser necesario.

1.5 Limitaciones al alcance

El estudio presenta como principal limitación la situación de emergencia vivida a nivel nacional durante el periodo 2020 a raíz de la pandemia del Covid -19, situación que afecto la agilidad con la que fue suministrada la información, de igual forma imposibilitó la ejecución de trabajo de campo 100% en el sitio, esto debido a las restricciones y medidas sanitarias dictadas por el Gobierno de la República y tomadas por la institución para frenar la propagación del virus.

1.6 Criterios utilizados por la Auditoría Interna

Los criterios de auditoría utilizados para desarrollar el estudio fueron los siguientes:

- Normas para el ejercicio de la Auditoría Interna en el Sector Público, R-DC-119-2009, publicado en La Gaceta N° 28, miércoles 10 de febrero, 2010.
- Normas Generales de Auditoría para el Sector Público, (R-DC-064-2014), publicado en La Gaceta No. 184 del 25 de setiembre de 2014.

1.7 Criterios de control interno utilizados

Los criterios utilizados a nivel de control interno para desarrollar el estudio fueron los siguientes:

- Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), Publicada en La Gaceta Nro.119 del 21 de junio, 2007.
- Las Normas de control interno para el Sector Público, (N-2-2009-CO-DFOE). Publicado en La Gaceta N.º 26 del 6 de febrero, 2009.
- Ley General de Control Interno, N°8292. Publicada en La Gaceta oficial 169, 4/set./2002.
- Matriz de COSO[1].

1.8 Declaración de Cumplimiento de Normas

De conformidad con lo establecido en la Norma 1.3.3 de las Normas para el Ejercicio de la Auditoría Interna en el Sector Público[2], se declara que las actividades del presente estudio se realizaron de conformidad con lo establecido en las Normas Generales de Auditoría para el Sector Público[3], entre otra normativa legal y técnica atinente a la materia.

1.9 Siglas/Nomenclaturas utilizadas

LGCI: Ley General de Control Interno

CGR: Contraloría General de la República

CNE: Comisión Nacional de Emergencias

UTI: Unidad de Tecnologías de Información

TI: Tecnología de Información

CI: Control Interno

PEI: Plan Estratégico Institucional

PETI: Plan Estratégico de Tecnología de Información

TIC: Tecnologías de Información y Comunicación

GLPI: Administrador de equipos informáticos gratuito (Siglas originales en francés Gestionnaire Libre de Parc Informatique)

PIC: Plan Institucional de Capacitación

[1] COSO (Committee of Sponsoring Organizations of the Treadway) es una Comisión voluntaria constituida por representantes de cinco organizaciones del sector privado en EE. UU., para proporcionar liderazgo intelectual frente a tres temas interrelacionados: la gestión del riesgo empresarial (ERM), el control interno, y la disuasión del fraude.
[2] R-DC-119-2009, publicadas en La Gaceta N°28 de 10 de febrero de 2010.
[3] R-DC-064-2014, publicado en La Gaceta N°184 del 25 de setiembre de 2014.

1.10 Disposiciones legales sobre recomendaciones

Los artículos del 36 al 38 de la Ley General de Control Interno Nº8292 (LGCI), establecen los plazos para la implementación de las recomendaciones a partir de la fecha de recibido del informe de Auditoría Interna por parte de los titulares subordinados o el Jerarca.

Al respecto, se estima conveniente transcribir a continuación, en lo de interés, lo que disponen los artículos N°36, 37 y 38:

> ***"Artículo 36. —Informes dirigidos a los titulares subordinados****. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera: / El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados. /b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes. /c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."*
>
> ***"Artículo 37. —Informes dirigidos al jerarca. Cuando el informe de auditoría esté dirigido*** *al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente."*
>
> ***"Artículo 38. —Planteamientos de conflictos ante la Contraloría General de la República****. Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas. / La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, Nº7428, de 7 de setiembre de 1994."*

1.11 Antecedentes

La Comisión Nacional de Prevención de Riesgos y Atención de Emergencias (CNE) es la institución pública rectora en lo referente a la coordinación de las labores preventivas de situaciones de riesgo inminente, de mitigación y de respuesta a situaciones de emergencia. Es un órgano de desconcentración máxima adscrito a la Presidencia de la República, con personería jurídica instrumental para el manejo y la administración de su presupuesto y para la inversión de sus recursos, con patrimonio y presupuesto propio. Su domicilio estará en la capital de la República, donde tendrá su sede principal.

El país cuenta con la Ley Nacional de Emergencias y Prevención del Riesgo N° 8488 (2006) que supera una serie de vacíos de legislaciones anteriores que limitaban el accionar de la institución. Introduce, además el concepto de prevención de riesgo y da un giro en el accionar institucional:

regula la actividad extraordinaria del Estado frente a un estado de emergencia, así como poner en práctica las acciones de prevención en todo el territorio nacional.

La Ley 8488 faculta a la CNE a coordinar el Sistema Nacional de Prevención y Atención de Emergencias, en donde cada institución debe participar en los temas específicos de su competencia y colaborar con los comités locales de prevención de riesgo y atención de emergencias.

La presente auditoría ha sido elaborada con el propósito de evaluar la eficiencia, eficacia y economía de la gestión administrativa del Departamento TI de la CNE, teniendo en cuenta el Plan Estratégico de la Institución y el PETI, cumplimiento de objetivos y normas aplicables a la gestión y operación de este departamento.

La Auditoría al Departamento TI de la CNE; pretende establecer un control integral, a partir de la evaluación de las actividades administrativas y operativas, su proyección hacia el futuro y la evaluación de sus resultados históricos, para detectar variaciones y tendencias, con el propósito de determinar la eficiencia y eficacia de las operaciones, misma que está asociada al cumplimiento de Normas y al logro de los resultados, por eso es que no debe entenderse como un conjunto de actividades, sino de logros.

1.12 Comunicación verbal de los resultados

Los resultados de este estudio fueron expuestos y comentados en reunión celebrada el 02 de diciembre del 2020, por medio de la plataforma virtual Zoom, entre las 09:00 am – 11:15 am horas.

Por parte de la Administración estuvieron presentes los señores:

-Señora Yamilette Mata Dobles, Directora Ejecutiva y Coordinadora Comité TI
-Señora Mónica Jara González, Jefa de Planificación y Staff Comité de TI
-Señor Wilgen Saborío Córdoba, jefe de TI y Representante del Comité TI
-Señor Danilo Mora Hernández, Dirección de Gestión Administrativa y Representante Comité TI.

La Auditoría estuvo representada por la Lcda. Elizabeth Castillo Cerdas, Auditora Interna y la Licda. Rossy González Jiménez, Profesional 3.

En el caso particular del presente estudio, se contó con la participación de la firma de auditoría externa BCR Consultores S.A., que tuvo a cargo el desarrollo del estudio, la cual fue representada por el Lic. Arturo Baltodano, Socio Director, Lic. Guillermo Vado Lacayo, Director de Auditoría, Lic Arturo Ramírez Hegg, Líder del Proyecto y el señor Marco Vallejos Obando, Soporte Técnico.

Una vez realizada la comunicación del presente informe y en el plazo para recibir observaciones de los administrados, se recibió un único oficio con la referencia: CNE-DE-OF-543-2020 de 21 de diciembre, de 2020 y remitido vía correo electrónico el 23 de diciembre de 2020 en forma conjunta por la señora Yamileth Mata Dobles, Directora Ejecutiva y Wilgen Saborío Córdoba, Jefe, a.i., de la UTI., donde se presentan las observaciones a las recomendaciones solicitando ampliar el plazo propuesto en el borrador del Informe, conocido en la Conferencia, ampliación de plazo que es aceptado conforme lo requerido.

2. Resultados

De acuerdo con las pruebas desarrolladas en relación con los objetivos planteados en el estudio, se obtuvieron los siguientes resultados.

Hallazgo N°1: Estado del control interno en el Departamento TI de la CNE

La revisión efectuada en la evaluación del sistema de control interno dentro de la UTI, en la cual se aplica la Matriz de COSO para la evaluación del Control Interno y Riesgo (se aplica para el periodo 2020).

El modelo de madurez del sistema de control interno según COSO 2013 (Matriz evaluación control interno y riesgo), permite determinar el nivel de experiencia del sistema de control interno y monitorear su mejora continua. La herramienta comprende cinco secciones que se identifican con cada uno de los componentes funcionales del sistema de control interno de acuerdo con COSO 2013, a saber: ambiente de control, evaluación del riesgo, actividades de control, sistemas de información y seguimiento.

La Matriz de COSO busca determinar el grado de cumplimiento de los mecanismos de control interno establecidos por la institución, de tal forma que brinda como base los rangos que permiten determinar el nivel “Novato” indicado anteriormente. A continuación, se muestra la calificación utilizada según los porcentajes de cumplimiento obtenidos:

Porcentaje de cumplimiento	Nivel
<= 0%	Indeterminado
> 0% < 21%	Incipiente
>=21% < 41%	Novato
>=41% < 61%	Competente
>=61% < 81%	Diestro
>=81% <=100%	Experto

Una vez analizados los resultados obtenidos en dicha Matriz, se observa que el sistema de control interno dentro de la Unidad se considera como Novato, esto ya que se arroja un promedio de cumplimiento global de un 35%. Dicho porcentaje se obtiene del ponderado de cada uno de los componentes del Control Interno evaluados, tal y como se muestra a continuación:

Componente	% de cumplimiento
Ambiente de control	43%
Evaluación de riesgos	32%
Actividades de control	39%
Información y comunicación	28%
Monitoreo y seguimiento	31%
Global	**35%**

La ausencia de Políticas y Procedimientos formalmente establecidos, así como un bajo cumplimiento en el establecimiento de actividades de control que ayuden a disminuir los riesgos existentes en la UTI son la principal causa del nivel de cumplimiento presentado por dicha Unidad. De igual forma, no se cuenta con mecanismos que permitan medir los niveles de cumplimiento que tiene el sistema de control interno de la Unidad, esto ya que únicamente se realizan las evaluaciones de control interno que aplica la Unidad de Planificación, las cuales abarcan aspectos de control interno de forma general, dejando factores relevantes y propios de evaluar con relación a la gestión de TI y los servicios brindados a los diferentes departamentos.

Hallazgo N°2: Evaluación de las regulaciones internas y externas

Al revisar y analizar las regulaciones emitidas por la Contraloría General de la República, evidencia que existen Normas Técnicas de Gestión y Control de la Información que no están siendo aplicadas por la UTI de la CNE, algunas de estas Normas se exponen a lo largo del presente estudio.

Las regulaciones emitidas de forma interna que fueron facilitadas permiten evidenciar que la UTI no cuenta con Manuales de Procedimientos o Políticas que regulen las actividades desarrolladas por el personal de la Unidad, únicamente se obtuvo respaldo de la existencia de una Directriz sobre el buen uso de las tecnologías de la información dentro de la CNE. Cabe destacar que la UTI participó en un taller desarrollado por la Unidad de Planificación, en donde se realizaron ejercicios para determinar los procedimientos que se ejecutan en el Área de TI, sin embargo, a los mismos no se les brindó el seguimiento correspondiente por lo cual no fueron oficializados. Se adjunta información de la Unidad de Planificación:

Informe
Diagnóstico Situacic

La Contraloría General de la República emite el 17 de marzo de 2020, la Resolución R-DC-17-2020, derogando la Normas Técnicas para la Gestión y el Control de las Tecnologías de Información y con el fin de que cada entidad emita su propia regulación a nivel de la gestión de TI.

La gestión de la UTI actualmente y para los periodos en estudio, está regulada por las Normas Técnicas de Gestión y Control de TIC, y el capítulo V: Normas sobre Sistemas de Información[4] de las Normas de Control Interno para el Sector Público, ambos de la Contraloría General de la República; el Reglamento para la Protección de los Programa de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central y la Directriz sobre el buen uso de las tecnologías de la información dentro de la CNE.

La ausencia de normativa interna y el incumplimiento de algunas de las normativas externas, se debe al insuficiente seguimiento a la implementación de estas regulaciones. A esta causa se le debe de sumar la falta de recurso humano que tiene la UTI, situación que dificulta destinar recurso humano al establecimiento de políticas y procedimientos propios del Área de TI, sin abandonar las demás labores que se deben desarrollar como parte de las funciones del personal.

[4] Este Capítulo incorpora lo establecido en el artículo 16 de la LGCI.

Hallazgo N°3: Análisis y evaluación de la existencia de un control sobre los proyectos presentados por las diferentes unidades de la CNE

Las Unidades de la CNE no presentan proyectos que deban ser desarrollados por la UTI, tales como la implementación o desarrollo de un nuevo sistema, ya que la UTI, únicamente se encarga de dar soporte a usuarios sobre los sistemas y equipos de cómputo existentes.

Las Unidades de la CNE sí remiten a la UTI, otros proyectos relacionados con la adquisición de sistemas y equipo de cómputo, los cuales se encuentran incluidos en el PETI y son ejecutados por medio de contratación o licitación a través de la UTI.

Sin embargo, la Unidad de TI carece de una metodología para dar seguimiento a los proyectos establecidos en el PETI, solicitados por otras Unidades, esto debido a la existencia de algunas inconsistencias que impiden establecer una matriz para dar seguimiento a los objetivos establecidos en el PETI. De igual forma, se determina que existen algunos objetivos y tareas establecidas en el PETI que al 2019 debían haberse culminado o tener cierto grado de avance, sin embargo, se aduce por la UTI que por falta de presupuesto, no se ha avanzado satisfactoriamente y se presentan retrasos en los tiempos de ejecución.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, N-2-2007-CO-DFOE, en los puntos 1.5 Gestión de proyectos y 3.1 Consideraciones generales de la implementación de TI, indican sobre la gestión que debe desarrollar la UTI para llevar un control y seguimiento adecuado de los proyectos de TI. De igual forma, el Capítulo IV Prestación de servicios y mantenimiento en el punto 4.6 Administración de servicios prestados por terceros, se indica algunos aspectos a considerar en la administración de los servicios contratados relacionados con las TI.

La condición evidencia inconsistencias en los objetivos planteados en el PETI, los cuales imposibilitan establecer una matriz que permita medir el avance y cumplimiento de los objetivos establecidos. En cuanto al poco avance que se ha tenido en la ejecución de las tareas establecidas en el PETI en apariencia se debe a que la Unidad de TI, durante el periodo 2019, no contó con el presupuesto correspondiente para poder atender las necesidades y tareas establecidas en dicho plan, carencia que obedece principalmente, a que cuando se formuló el presupuesto para el periodo 2019, no existía el PETI (herramienta de planificación estratégica que no había sido aprobada en el periodo 2018).

Hallazgo N°4: Análisis y evaluación de control sobre los requerimientos de mejoras a los sistemas

El PETI 2019-2022 (julio 2019) indica que la UTI no cuenta con un sistema formal para la gestión de Servicios de TIC, tampoco existe un catálogo de servicios formalizado el cual permitiría, entre otras cosas, categorizar los servicios de TIC según la orientación y generación de valor al cliente o usuarios.

La UTI implementa en el periodo 2020, el sistema GLPI para la solución de los problemas que se presentan con los equipos o servicios que provee la Unidad de TI, así como los nuevos requerimientos que se generan diariamente en la CNE y que deben ser atendidos con celeridad y orden, de manera que estos puedan ser resueltos eficientemente sin afectar la labor que los funcionarios de la institución realizan.

La UTI está en constante cambio, tanto a nivel físico como virtual con relación a los almacenamientos y respaldos de la información según el "Informe de fin de gestión" presentado por la anterior Jefatura de TI en marzo, 2020, con alcance de mayo 2016 a febrero 2022.

El Capítulo IV[5] Prestación de servicios y mantenimiento en el inciso 4.4 Atención de requerimientos de los usuarios de TI, indica:

> *La organización debe hacerle fácil al usuario el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI. Asimismo, debe atender tales requerimientos de manera eficaz, eficiente y oportuna y dicha atención debe constituir un mecanismo de aprendizaje que permita minimizar los costos asociados y la recurrencia.*

Las TI de la CNE, han estado en constante cambio tanto a nivel físico como virtual; existe documentación informal de trabajo, tanto en el periodo 2018 como en el primer semestre 2019, en apariencia porque no se contaba con el PETI y aunque mediante el Acuerdo N°146 del 19 de julio 2019, en Sesión Junta Directiva de la CNE, se aprueba dicha planificación, no se le ha dado el seguimiento respectivo.

Hallazgo N°5: Metodología desarrollada en software

La práctica utilizada en la CNE para el diseño, desarrollo y compra de sistemas, determina que la UTI no dispone de una metodología para el ciclo de vida de desarrollo de Sistemas, según indica el oficio del 18 de agosto, 2020 el CNE-UTI-OF-074-2020 "no se encuentra evidencia al momento de su búsqueda e investigación".

Al revisar el Plan de Compras 2018 y 2019 se verifica la línea del Código UNSPSC 81111508 Servicios de implementación de aplicaciones, no obstante, no detalla la lista de las implementaciones de sistemas realizados, de igual manera el rubro del Código UNSPSC 81112299 Mantenimiento de software y soporte de sistemas de información, no detalla cuales softwares se incluyen en el mantenimiento.

Según se desprende del informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019 en el cuadro N. 2 identificado como debilidades Unidad de Tecnologías de Información, establece que la UTI carece de procedimientos y metodologías para la implementación de softwares nuevos adquiridos por medio de los diferentes proveedores. Ver "Cuadro N.º 2 Debilidades Unidad de Tecnologías de Información"[6].

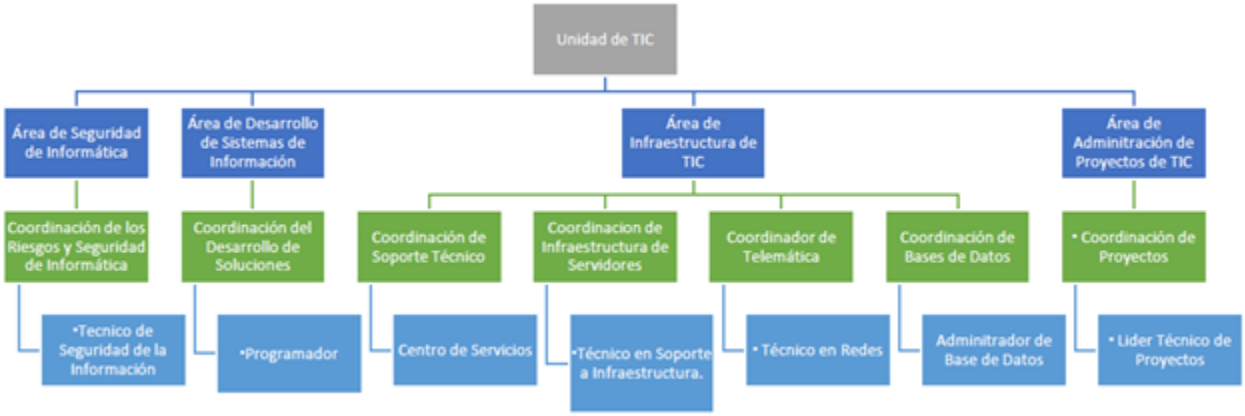
Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), indican en el punto 3.2 Implementación de software, lo siguiente:

> *Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post implantación de la satisfacción de los requerimientos.*

[5] Normas técnicas para la gestión y el control de las Tecnologías de Información, (N-2-2007-CO-DFOE).
[6] El informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019.

Hallazgo N°6: Evaluación de la segregación de funciones

La UTI cuenta con una distribución de funciones la cual se detalla en su Plan Estratégico 2019–2022. El Organigrama de la Unidad de TI, fue presentado al Comité de Tecnologías de la Información como parte del PETI, y fue aprobado por la Junta Directiva de la CNE por medio del Acuerdo No 146-07-07-19 en la sesión ordinaria del 13 de julio del 2019. Se adjunta el Organigrama de la Unidad:



Las entrevistas realizadas al personal determinan qué, la UTI no cuenta con documentos oficiales donde se les indique a sus colaboradores sus funciones, roles y responsabilidades que deben de cumplir dentro de la Unidad, únicamente uno de los funcionarios de TI indica contar con este tipo de documento respectivamente firmado.

La UTI utiliza como referencia el Manual de Clases Anchas de la Dirección General de Servicio Civil. De igual forma, es importante mencionar que dicho organigrama corresponde al presentado en el Plan Estratégico a partir del 2019, a la fecha la UTI ha sufrido algunos cambios de personal, siendo la más significativa la salida del Encargado de la Unidad en marzo de 2020, cargo que, a la fecha, se encuentra recargado en un profesional de la Unidad.

La UTI debe establecer una adecuada segregación de funciones en concordancia con lo establecido en las Normas de Control Interno para el Sector Público de la CGR (2.5.1 Delegación de funciones y 2.5.3 Separación de funciones incompatibles y del procesamiento de transacciones)[7] y el Manual de Clases Anchas de la Dirección General de Servicio Civil.

El incumplimiento a una adecuada segregación de funciones se debe a la ausencia de un procedimiento formalmente establecido y promulgado, donde se indique a cada uno de los funcionarios, cuáles son las labores por realizar de acuerdo con el puesto, así como las responsabilidades que conlleva cada puesto de trabajo dentro de la UTI.

[7] 2.5.1 El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que la delegación de funciones se realice de conformidad con el bloque de legalidad, y de que conlleve la exigencia de la responsabilidad correspondiente y la asignación de la autoridad necesaria para que los funcionarios respectivos puedan tomar las decisiones y emprender las acciones pertinentes.
2.5.3 El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de activos, estén distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores. Cuando por situaciones excepcionales, por disponibilidad de recursos, la separación y distribución de funciones no sea posible debe fundamentarse la causa del impedimento. En todo caso, deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables.

Hallazgo N°7: Análisis y evaluación del control y seguridades físicas en el área de tecnología

La CNE cuenta con un espacio físico para el resguardo de equipos de cómputo, conformado entre otros por los Routers, servidores, sistema de cableado interno e inalámbrico. Sin embargo, el edificio principal y el COE presentan condiciones que pueden ser un riesgo para los equipo de TI, tal y como lo son la entrada de terceros a los cuartos de servidores, prevista de agua en el cuarto del servidor central y acceso por parte de terceros al espacio donde se encuentran ubicadas las cajas de breakers que alimentan el fluido eléctrico del edificio COE, de igual forma se pudo observar que el personal de mantenimiento de la CNE, utiliza dicho espacio para almacenamiento de suministros eléctricos.

De igual forma, es importante destacar que el territorio donde se encuentran ubicadas las oficinas de la CNE presenta un riesgo de derrumbe que en caso de manifestarse afectaría de forma general a la institución.

Lo anterior deja en evidencia que, a la fecha del estudio, la CNE no cuenta, con un espacio físico adecuado que le permita a la UTI, tener un resguardo adecuado de sus activos, principalmente de su cuarto de servidores, ya que de materializarse algunos de los riesgos descritos, el equipo puede sufrir daños severos que afecten las operaciones y resguardo de información.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), en el inciso 1.4.3 Seguridad física, indica que:

La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.

Como parte de esa protección debe considerar:

a. *Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.*
b. *La ubicación física segura de los recursos de TI.*
c. *El ingreso y salida de equipos de la organización.*
d. *El debido control de los servicios de mantenimiento.*
e. *Los controles para el desecho y reutilización de recursos de TI.*
f. *La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas.*
g. *El acceso de terceros.*
h. *Los riesgos asociados con el ambiente.*

Hallazgo N°8: Análisis del ambiente de control de la información gestionada y almacenada dentro y fuera de los sistemas informáticos

La CNE cuenta con los siguientes documentos oficiales de referencia relacionados al ambiente de control de la información:

- Boleta de salida de equipos[8].

De igual forma, la institución cuenta con un documento denominado: "Lineamientos para uso, resguardo y custodia de los equipos de cómputo asignados a los Comités Municipales de Emergencias" sin embargo, no se obtuvo evidencia de que dicho documento se encuentre respectivamente oficializado. Así como tampoco se obtuvo evidencia de que la UTI acatara las advertencias realizadas por la Auditoria Interna con relación al cumplimiento del Reglamento para la Protección de los Programas de Cómputo en los Ministerios e Instituciones adscritas al Gobierno Central, N° 37549-JP.

Por otra parte, no se obtuvo evidencia de convenios o contratos de confidencialidad con respecto a la información gestionada y su almacenamiento.

En el documento "Fortalecimientos de la Unidad de TI" suministrado por la Unidad de Planificación, así como en el análisis realizado del Plan Estratégico de la Unidad de TI, se destaca la carencia de apoyo oportuno por parte de los diferentes Jerarcas, situación que ocasiona que los documentos no estén debidamente formalizados[9], no se han establecido documentos concretos relacionados al manejo de la información gestionada y almacenada dentro o fuera de los sistemas informáticos.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) y las Normas de Control Interno para el Sector Público, (N-2-2009-CO-DFOE), en el numeral 1.4.6: Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica[10] y la norma 4.3 Protección y conservación del patrimonio[11], respectivamente, indican que la organización debe proteger y mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de la información.

Hallazgo N°9: Planes de Contingencia o continuidad del servicio ante eventualidades

De acuerdo con lo indicado en el oficio del 18 de agosto, 2020 (CNE-UTI-OF-074-2020), la UTI no cuenta a la fecha de este informe, con un Plan de Contingencias formalizado, por consiguiente, no se cuenta a la fecha, con capacitaciones ni pruebas de contingencia.

El informe de fin de gestión presentado por la anterior Jefatura de TI en marzo 2020, con alcance de mayo 2016 a febrero 2020; menciona que según recomendación contenida en el informe

---

[8] Circular DGBACA-0053-2020, 13 de agosto del 2020, Ministerio de Hacienda.

[9] Informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019, elaborado por la Unidad de Planificación Institucional de la CNE

[10] 1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica. La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de prueba información. Para ello debe: a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura. b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura. c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción. d. Controlar el acceso a los programas fuente y a los datos de prueba.

[11] 4.3 Protección y conservación del patrimonio El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de tales activos y los riesgos relevantes a los cuales puedan verse expuestos, así como los requisitos indicados en la norma 4.2 (…).

CG-1-TI-2011 de la Auditoría Externa, la UTI "*debe contar con un Plan de Continuidad en el que estén definidas las acciones a seguir para minimizar el impacto en los sistemas informáticos que se encuentran en producción"*

A su vez, el informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019, elaborado por la Unidad de Planificación Institucional de la CNE, dirigido a la Unidad de TI, revela debilidades de control interno presentadas en la UTI, entre otras razones, por la falta de documentación y procedimientos.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), en el inciso 1.4.7 Continuidad de los servicios de TI indican que:

> *La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.*

Importante indicar, que, como parte de la respuesta dada a esta Auditoria por la UTI, en el oficio CNE-UTI-OF-074-2020, se indica que dichos planes se encuentran en proceso de elaboración.

Hallazgo N°10: Análisis del ambiente de control de los procesos y activos de cómputo

Las Directrices[12] para el buen uso de las tecnologías de información en la CNE[13], versión 1.0; elaboradas en junio, 2019 por la Unidad de Tecnologías de Información, indican que la UTI en coordinación con otras instancias internas implementarán los procedimientos o tecnología necesaria para validar la integridad de aquellos equipos que se conecten a las redes de datos institucionales, considerando, cuando el equipo lo permita, al menos la presencia de un antivirus debidamente actualizado.

La Matriz de Riesgos de la UTI, vigente a la fecha, no evidencia como parte de los riesgos identificados, ningún evento relacionado a los procesos y activos en mención, asimismo, durante las visitas de campo realizadas, se pudo observar que en la CNE no se aplica un procedimiento en la entrada y salida de personas con equipos de cómputo externo, que permita el resguardo de los activos internos (hardware, software, información).

Adicionalmente, la CNE como parte de las Directrices internas, carece de procedimientos para el control de los procesos relacionados con los activos de cómputo central, computo personal, telecomunicaciones, accesos locales y remotos, servicios en la nube, entre otros. De igual forma, no se logra identificar al momento de la verificación, la existencia de un procedimiento físico en resguardo de los activos internos.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE)*[14]*, en su norma 1.4 Gestión de la seguridad de la información y las Normas de control

[12] Dicho de una cosa: Que determina las condiciones de generación de algo. Ideas, líneas directrices. https://dirae.es/palabras/directriz.
[13] CNE-UTI-DIR-001-19, junio 2019.
[14] La norma 1.4 Gestión de la seguridad de la información, indica que organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales, entre otros aspectos; además las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.

Interno para el Sector Público[15], (N-2-2009-CO-DFOE), en su *norma 4.3 Protección y conservación del patrimonio, El jerarca y los titulares subordinados,* deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución.

Hallazgo N°11: Control de la red y accesos a la nube

El Oficio CNE-UTI-OF-074-2020 del 18 de agosto de 2020, en respuesta a la información requerida, indica respecto a las políticas y procedimientos de comunicaciones (control de la red y el acceso a la nube) que "no se encuentra evidencia al momento de su búsqueda e investigación".

Las Normas[16] en el inciso 1.4.4. Seguridad en las operaciones y Comunicaciones, citan:

> *La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.*
> *Para ello debe:*
>
> a. *Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.*
> b. *Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.*
> c. *Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus.*

La UTI cuenta con el documento CNE-UTI-DIR-001-19, "Directrices[17] para el buen uso de las tecnologías de información en la CNE, versión 1.0 ", no obstante, se logra verificar que carece de procedimientos formalmente establecidos que garanticen un manejo eficaz y eficiente, del control de la red y acceso a la nube por parte de los demás funcionarios de la institución.

Hallazgo N°12: Análisis de la capacidad de los sistemas y bases de datos

El oficio CNE-UTI-OF-074-2020 del 18 de agosto, 2020, indica con respecto al procedimiento para el análisis de las capacidades de los sistemas y base de datos que "no se encuentra evidencia al momento de su búsqueda e investigación".

Identificando esta Auditoría que tampoco se localizaron estudios de Reportes de capacidades de los sistemas y bases de datos del 2019, por lo tanto, la UTI carece de políticas y procedimientos en materia de evaluación de capacidad de su plataforma tecnológica, condición que es ratificada en el informe del "Taller de Fortalecimiento de la Unidad de TI" desarrollado por la Unidad de

---

[15] La norma 4.3 Protección y conservación del patrimonio, El jerarca y los titulares subordinados, según sus competencias, deben establecer, evaluar y perfeccionar las actividades de control pertinentes a fin de asegurar razonablemente la protección, custodia, inventario, correcto uso y control de los activos pertenecientes a la institución, incluyendo los derechos de propiedad intelectual. Lo anterior, tomando en cuenta, fundamentalmente, el bloque de legalidad, la naturaleza de tales activos y los riesgos relevantes a los cuales puedan verse expuestos.

[16] Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE). Publicada en La Gaceta Nro.119 del 21 de junio, 2007.

[17] Dicho de una cosa: Que determina las condiciones de generación de algo. Ideas, líneas directrices. https://dirae.es/palabras/directriz

Planificación. Ver cuadro "Cuadro N.º 2 Debilidades Unidad de Tecnologías de Información"[18] (ver apartado 3 Conclusiones del informe).

De acuerdo con lo anterior, la Norma N-2-2007-CO-DFOE, en el inciso 4.2 Administración y operación de la plataforma tecnológica[19], indica lo siguiente:

> *Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*

Hallazgo N°13: Análisis de existencia de informes de rendimiento de los equipos en producción

El oficio CNE-UTI-OF-074-2020 del 18 de agosto, 2020, indica que con relación a la existencia de informes de rendimiento de los equipos en producción "no se encuentra evidencia al momento de su búsqueda e investigación".

Identificando esta Auditoría que la UTI no cuenta con políticas y procedimientos en materia de evaluación de desempeño de la plataforma tecnológica, condición que también es señalada en el informe de la Unidad de Planificación sobre el Taller "Fortalecimiento de la Unidad de TI" Ver "Cuadro N.º 2 Debilidades Unidad de Tecnologías de Información" (ver apartado 3 Conclusiones del informe).

Las Normas N-2-2007-CO-DFOE[20] indican en el inciso 4.2 Administración y operación de la plataforma tecnológica:

> *La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.*

Hallazgo N°14: Análisis de la gestión de labores de capacitación

El informe de fin de gestión presentado por la anterior Jefatura de TI en marzo 2020, con alcance de mayo 2016 a febrero 2020, no registra evidencias de posibles coordinaciones para la capacitación y concientización en materia de seguridad; lo más cercano fue para el 2018, cuando se realizó una capacitación sobre la plataforma de la Gestión documental Share Point. No obstante, es importante señalar que de acuerdo con la respuesta del requerimiento del punto 18 del oficio CNE-UTI-OF-074-2020 del 18 de agosto, 2020, se indica: *en la Unidad de Tecnologías de Información no se cuenta con esta información, sin embargo, como parte de las competencias de la Unidad de Desarrollo Humano, se desarrolla un plan de capacitación a nivel institucional y su debido seguimiento, en el cual se consideran las necesidades de capacitación para TI.*

[18] El informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019.
[19] Normas técnicas para la gestión y el control de las Tecnologías de Información, (N-2-2007-CO-DFOE). Publicada en La Gaceta Nro.119 del 21 de junio, 2007.
[20] Normas técnicas para la gestión y el control de las Tecnologías de Información, (N-2-2007-CO-DFOE). Publicada en La Gaceta Nro.119 del 21 de junio, 2007.

A su vez, el citado informe (entre las páginas 11 a la 13), presenta situaciones de atención sobre la cultura organizacional en los periodos 2018 y 2019. Dicho documento menciona problemas de comunicación, rotación de personal, estilo de dirección, cambios en los procedimientos, y otros que afectan la eficiente gestión, entre ellos la oportuna e idónea capacitación en temas de seguridad de la información, lo que se considera relevante a tomar en cuenta por parte de la UTI y el Comité de Tecnología de Información, ya que lo indicado podría estar entorpeciendo la eficacia y eficiencia del servicio prestado en la CNE por dicha Unidad.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), indica en sus incisos 1.4.1 y 1.4.2 que la organización debe implementar un marco de seguridad de la información y el compromiso del personal con la seguridad de la información[21].

Hallazgo N°15: Análisis de existencia de una plataforma tecnológica institucional con esquemas de seguridad

La UTI brinda constante mantenimiento a la infraestructura de red y seguridad de los sistemas de información (Firewall Fortinet y antivirus Kaspersky).

La UTI cuenta con el documento “Lista de Manuales de Procedimientos Operativos Internos (Procesos General 004 Wilgen Saborío, que no se encuentra oficializado a la fecha), para la revisión continua de la unidad de informática de la CNE. Este documento indica que todo el software se actualiza a la última versión, se identifica y resuelven todas las anomalías en el rendimiento del sistema y se cumplen todos los requisitos de cumplimiento de seguridad. El monitoreo constante asegura que cualquier comportamiento irregular sea inmediatamente identificado e investigado.

El PETI 2019-2022 indica en el apartado “SERVICIOS, APLICACIONES E INFRAESTRUCTURA DE TIC”, pag.27, señala que existe una identificación informal de los servicios que brinda la UTI, estos servicios se listan de la siguiente forma:

•Soporte Técnico.
•Correo electrónico.
•Servicio de gestión de la plataforma tecnológica.
•Servicio de conectividad a la red.
•Servicio de administración de la plataforma Moodle.
•Servicio de administración de página web.
•Servicio de administración del ERP.
•Servicio de control de marcas y asistencia TAS.
•Servicio de gestión de la infraestructura.
•Comunicaciones unificadas.
•Servicio de Impresión.
•Gestión de la Intranet o plataforma de gestión documental.

[21] 1.4.1 Implementación de un marco de seguridad de la información. La organización debe implementar un marco de seguridad de la información, para lo cual debe: a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.
1.4.2 Compromiso del personal con la seguridad de la información. El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe:
a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.

•Gestión de almacenamiento en la nube.
•Gestión de servicios de red.
•Gestión de antivirus.
•Gestión de actualizaciones de software.

Logra identificar esta Auditoría que en relación con los servicios brindados por la UTI que se indican en el apartado "SERVICIOS, APLICACIONES E INFRAESTRUCTURA DE TIC", estos, no se ajustan a los procedimientos formalizados que identifica la normativa, de tal manera que describa la forma en la que se debe realizar la prestación de dichos servicios en función de cumplir con los objetivos de la Unidad

La Normas N-2-2007-CO-DFOE[22] indican en su inciso 4.2 Administración y operación de la plataforma tecnológica lo siguiente:

> *La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
>
> *a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
> *b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
> *c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.*
> *d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.*
> *e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.*
> *f. Mantener separados y controlados los ambientes de desarrollo y producción.*
> *g. Brindar el soporte requerido a los equipos principales y periféricos.*
> *h. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.*
> *i. Controlar los servicios e instalaciones externos.*

Hallazgo N°16: Estado de los servicios de TI

La Auditoría envío cuestionarios a diferentes unidades de la CNE con la intención de medir la satisfacción sobre los servicios de TI con los que cuenta la CNE, mediante encuesta de satisfacción de los servicios de la UTI el pasado 11 de setiembre de 2020. Se reciben 4 (36.36%) respuestas de un total de 11 funcionarios a los que se le hizo llegar la encuesta. Únicamente se recibió respuesta por parte de la Unidad de Proveeduría (2), Desarrollo Humano (1) y Recursos Financieros (1), no se obtuvo respuesta de las siguientes Unidades:

[22] Normas técnicas para la gestión y el control de las Tecnologías de Información, (N-2-2007-CO-DFOE). Publicada en La Gaceta Nro.119 del 21 de junio, 2007.

- Asesoría Legal
- Unidad de Planificación
- Gestión de Operaciones
- Gestión de Procesos de Reconstrucción
- Desarrollo estratégico de sistema nacional de gestión de riesgo
- Servicios Generales
- Presidencia

Los resultados obtenidos indican que los cuatro funcionarios de la CNE, que emitieron respuesta, consideran que los servicios de TI, son adecuados para poder cumplir con las funciones de esas Unidades, obteniendo como resultado un grado de satisfacción entre 3.5 y 4, de una nota total de 5, no obstante, como se indicó anteriormente, la consulta fue enviada a 11 funcionarios, pero; 7 de ellos no respondieron, lo que representa un 63.64%.

Los inconvenientes que tiene la CNE, con relación a los servicios de TI, se dan en función del sistema Wizdom, esto según los usuarios que dieron respuesta a las encuestas. Es importante destacar que en ocasiones los inconvenientes generados por dicho sistema deben ser solventados por el proveedor del sistema, de forma que se generan algunos problemas de oportunidad de respuesta por parte del proveedor, además, representan un costo económico adicional que debe ser asumido por la CNE.

Como ya se ha mencionado, durante el periodo 2020, la UTI puso a disposición de los usuarios el sistema GLPI (control de incidentes), para tener un mejor control sobre los problemas que se presentan con los equipos o servicios que brinda la Unidad de TI. Con relación a esto, a la fecha de finalización del presente estudio no se obtuvo evidencia de que se tenga un proceso de implementación y aplicación formal de esta herramienta.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE)[23], en sus incisos 4.1 Definición y administración de acuerdos de servicio, el 4.2 Administración y operación de la plataforma tecnológica, 4.4 Atención de requerimientos de los usuarios de TI, 4.5 Manejo de incidentes y 4.6 Administración de servicios prestados por terceros, indican que la organización debe establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos, además debe vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de eventuales fallas, debe facilitar al usuario, el proceso para solicitar la atención de los requerimientos que le surjan al utilizar las TI; además, identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI, así como asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente, entre otros aspectos importantes para el buen manejo y funcionamiento de las TI y el logro de los objetivos de la UTI y de la CNE en general.

De acuerdo con lo comprobado se identifica que la Unidad de TI mantiene una dependencia directa de los servicios de soporte que le brinda el proveedor del sistema Wizdom, de ahí que para la atención de algunos problemas generados por el sistema institucional, se debe esperar la atención por parte de la empresa que brinda soporte, situación que podría estar encareciendo el servicio que se brinda a los usuarios del sistema, por lo que, la UTI en coordinación con el Comité de TI, debe tomar medidas correctivas inmediatas para subsanar tal debilidad de control y así agilizar la labor que se realiza con eficiencia y eficacia.

[23] Capítulo IV Prestación de servicios y mantenimiento (4.1, 4.2, 4.4, 4.5, 4.6)

Hallazgo N°17: Evaluación a los esquemas de seguridad

Los informes de evaluaciones de la plataforma tecnológica, según el oficio CNE-UTI-OF-074-2020 del 18 de agosto de 2020, indican que "no se encuentra evidencia al momento de su búsqueda e investigación".

Identificando esta Auditoría que la Unidad de Planificación de la CNE, como parte del Informe denominado Taller "Fortalecimiento de la Unidad de TI" realizado en abril 2019, concluyó que, en la Unidad de TI, no se logró verificar la existencia de una metodología establecida que permita realizar evaluaciones de los esquemas de seguridad con los que cuenta la CNE. Situación que de acuerdo con nuestro análisis se continúa presentando. Ver "Cuadro N.º 2 Debilidades Unidad de Tecnologías de Información"[24] (ver apartado 3 Conclusiones del informe).

El informe de la Auditoría Externa *"CG TI-2019 CNE"* presentado el 28 febrero 2020, en el Hallazgo 08 ausencia de estudios de vulnerabilidad de la red institucional de la CNE indica lo siguiente:

> *Producto de la revisión efectuada, se determinó que la CNE no ha realizado estudios o pruebas de vulnerabilidad de la red institucional los cuales permitan identificar debilidades en la seguridad u oportunidades de mejora en esta. Se indicó que estos se encuentran pendientes de realizarse.*
>
> *Al no contar con estudios o pruebas de vulnerabilidad, existe el riesgo de que terceros puedan acceder a recursos sin contar con la debida autorización, comprometiendo la integridad, confidencialidad y disponibilidad de los datos. Además, se dificulta poder identificar deficiencias que posee la red, así como las mejoras que se podrían realizar a esta.*

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), en sus incisos 4.2 Administración y operación de la plataforma tecnológica, 5.2 Seguimiento y evaluación del control interno en TI y 1.4 Gestión de la seguridad de la información[25], indican que la Administración debe procurar una gestión tecnológica formal y segura, así como un seguimiento oportuno al control interno.

Hallazgo N°18: Control de salida e ingreso de información de la CNE

El oficio CNE-UTI-OF-074-2020 del 18 de agosto, 2020, con respecto al esquema de seguridad, correspondientes al requerimiento #21 del oficio-02-2020 del 06 de agosto, 2020, esta Auditoría recibió dos documentos, denominados:

1. Sistemas de Control de acceso
2. Arquitectura_Seguridad_Informática

---

[24] El informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019.

[25] 4.2 Administración y operación de la plataforma tecnológica. La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma. b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas. c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas. d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas. e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro. f. Mantener separados y controlados los ambientes de desarrollo y producción. g. Brindar el soporte requerido a los equipos principales y periféricos. h. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración. i. Controlar los servicios e instalaciones externos. 5.2 Seguimiento y evaluación del control interno en TI. El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas. 1.4 Gestión de la seguridad de la información. La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales (…).

Para el documento Sistemas de control de acceso, básicamente contiene:

a) Control de la puerta principal,
b) Puerta del Centro de Datos
c) Puerta Centro de Datos del Edificio COE

Los mecanismos de control no incluyen la salida ni el ingreso de información hacia y desde la red interna de la Institución.

Con el documento "Arquitectura_Seguridad_Informática", revisa el esquema de seguridad. En él se observa, que solo incluye los términos de Referencia para la contracción de la Arquitectura de seguridad informática, cuyo documento en Word es un extracto de la línea de contratación, pero no garantiza que en la práctica dichas especificaciones operen en la actualidad.

Las normas N-2-2007-CO-DFOE [26] indican en su inciso 1.4.5 Control de acceso[27]:

La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:

a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.
b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.
c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.
d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.
e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.
f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
i. *Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.*
j. *Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.*
k. *Manejar de manera restringida y controlada la información sobre la seguridad de las TI.*

No logrando esta Auditoría identificar que la UTI, cuente con políticas y procedimientos establecidos en materia relacionada con los esquemas de seguridad, lo que podría estarla exponiendo a la materialización del riesgo en el resguardo de la información, careciendo la CNE

[26] Normas técnicas para la gestión y el control de las Tecnologías de Información, N-2-2007-CO-DFOE.
27 El original del inciso 1.4.5. de la norma mencionada omite los ítems g y h dentro de su codificación

de confidencialidad y seguridad de la información, por lo que la UTI y el Comité de TI, deben realizar un análisis de tales debilidades y corregir en forma inmediata lo enunciado en este apartado.

Hallazgo N°19: Evaluación de la UTI en cuanto a nuevas tendencias en seguridad informática

El oficio CNE-UTI-OF-074-2020 del 18 de agosto, 2020, en consulta con los resultados de *Estudios de nuevas tendencias de seguridad,* indica “que no se encuentra evidencia al momento de su búsqueda e investigación”. Evidenciando, esta Auditoría, que no se permite evaluar las nuevas tendencias en seguridad informática, para mantener los niveles de seguridad requeridos en la CNE, conforme lo establecido en la normativa aplicable.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), indican en sus apartados 2.3 Infraestructura tecnológica y el inciso 1.4 Gestión de la seguridad de la información[28], sobre las perspectivas de dirección y condiciones en materia tecnológica, que la organización debe garantizar, de manera razonable la confidencialidad, integridad y disponibilidad de la información.

De acuerdo con lo anterior, esta Auditoría podría evidenciar que la UTI carece de políticas y procedimientos que permitan orientar formalmente, los estudios de tendencia tecnológica, ya que los mismos, no se lograron visualizar.

Hallazgo N°20: Evaluación de capacitación y concientización en ciberseguridad

La CNE establece los planes de capacitación, con base en la evaluación del desempeño que realiza la Jefatura de cada Unidad, así como otra información considerada por la Unidad de Desarrollo Humano y que es requerida por el Servicio Civil, dicha información es recolectada y consolidada por la Unidad de Desarrollo Humano, lo que le permite generar el Plan Institucional de Capacitación (PIC), que es ejecutado durante el transcurso del año. Para los efectos del presente estudio se evaluaron únicamente los planes de capacitación correspondientes a los periodos 2018 y 2019.

Los planes de capacitación no presentan necesariamente un enfoque que busque hacer conciencia sobre la seguridad de las tecnologías de información, ya que como se menciona, los planes de capacitación se basan en lo indicado por el jefe de la Unidad en las evaluaciones del desempeño, así como en requerimientos del Servicio Civil.

[28] 2.3 Infraestructura tecnológica. La organización debe tener una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI. Inciso 1.4 Gestión de la seguridad de la información, presente en el documento "La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos: -La implementación de un marco de seguridad de la información. -El compromiso del personal con la seguridad de la información. -La seguridad física y ambiental. -La seguridad en las operaciones y comunicaciones. -El control de acceso. -La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica. -La continuidad de los servicios de TI. -Además, debe establecer las medidas de seguridad relacionadas con: -El acceso a la información por parte de terceros y la contratación de servicios prestados por estos. -El manejo de la documentación. -La terminación normal de contratos, su rescisión o resolución. -La salud y seguridad del personal. -Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.

Los PIC´s analizados para los periodos en estudio, no muestran actividades de capacitación que estén enfocadas en temas de seguridad informática, así como en el buen uso de las tecnologías de la información.

La UTI no cuenta con un plan de capacitación formalizado y continuo, pero, en caso de existir en el mercado alguna capacitación que se considera de interés para la Unidad, se realiza la gestión correspondiente. Tampoco se obtuvo evidencia de que la UTI, ejecutara en los periodos 2018 y 2019, un plan de capacitación dirigido a funcionarios de la CNE, en temas de ciberseguridad y buen uso de las TI. No obstante, se identifica que en el periodo 2019, se brindó una capacitación sobre el uso de la herramienta SharePoint. Se adjunta lista de los participantes que asistieron a dicha actividad:

Anexo 5. Listados Curso Administrado

Se adjunta documentos de capacitaciones recibidas por los funcionarios de TI para los periodos 2018 y 2019 así como los Planes Institucionales de Capacitación:

Anexo 2. Cursos 2019.pdf

Anexo 1. Cursos 2018.pdf

Anexo 4. PIC 2019.pdf

Anexo 3. PIC 2018 aprobado.pdf

No visualizando esta Auditoría que la UTI cuente con un procedimiento o cronograma que garantice un proceso constante de capacitación en temas de seguridad informática, ya que como se indicó, las necesidades de capacitación son determinadas por el jefe de cada Unidad y la Unidad de Desarrollo Humano, por lo cual, estas no siempre se relacionan con las necesidades de capacitación determinadas en periodos anteriores y así como en los temas que se identifiquen con la seguridad de las tecnologías de información.

Para el periodo 2020, la UTI cuenta en con un proyecto que busca brindar capacitación sobre el buen uso de las Tecnologías de la Información, a las Unidades de la CNE, sin embargo, no se obtuvo evidencia de que dichas capacitaciones hayan sido impartidas a la fecha.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información en su norma 1.4.1 Implementación de un marco de seguridad de la información[29] y las Normas de Control Interno para el Sector Público en su norma 2.4 Idoneidad del personal, ambas de la CGR indican sobre la necesidad de una capacitación continua para el logro de la idoneidad del personal y el cumplimiento de los objetivos.

[29] 1.4.1 La organización debe implementar un marco de seguridad de la información, para lo cual debe: a. Establecer un marco metodológico que incluya la clasificación de los recursos de TI, según su criticidad, la identificación y evaluación de riesgos, la elaboración e implementación de un plan para el establecimiento de medidas de seguridad, la evaluación periódica del impacto de esas medidas y la ejecución de procesos de concienciación y capacitación del personal.

2.4 El personal debe reunir las competencias y valores requeridos, de conformidad con los manuales de puestos institucionales, para el desempeño de los puestos y la operación de las actividades de control respectivas. Con ese propósito, las políticas y actividades de planificación, reclutamiento, selección, motivación, promoción, evaluación del desempeño, capacitación y otras relacionadas con la gestión de recursos humanos, deben dirigirse técnica y profesionalmente con miras a la contratación, la retención y la actualización de personal idóneo en la cantidad que se estime suficiente para el logro de los objetivos institucionales.

Hallazgo N°21: Análisis sobre la Planificación Estratégica de TI

La CNE aprueba mediante el acuerdo N°146 del 19 de julio, 2019, el PETI 2019-2022, el cual se encuentra alineado al Plan Estratégico Institucional 2018-2022. En los periodos 2018 y I semestre 2019 la UTI no contaba con dicha herramienta de planificación estratégica.

La Auditoría Externa presenta el 28 de febrero, 2020 el informe "*CG TI-2019 CNE"* el cual indica la "*ausencia de un seguimiento al Plan Estratégico de Tecnologías de Información y debido a eso no se puede identificar el avance que se ha obtenido en cada uno de los productos definidos. Además, el no cumplimiento de los plazos podría conducir a que no se cumpla satisfactoriamente con los objetivos institucionales"*

A la fecha de este Informe, tampoco se obtuvo evidencia del seguimiento y avances al cumplimiento e implementación del PETI 2019-2022, según la información presentada por la UTI, esto dado por inconsistencias en los objetivos planteados que imposibilitan establecer una matriz de seguimiento que garantice el cumplimiento de dichos objetivos.

La implementación y el cumplimiento del PETI se ha visto afectado principalmente por la carencia de una Matriz que cuente con los parámetros necesarios para poder medir y llevar un control sobre los aspectos considerados dentro dicho plan. Esta situación podría darse debido a que existen algunos objetivos dentro del PETI, que no fueron planteados de forma que se pueda medir su avance. No obstante, aunque el PETI fue aprobado en el II semestre del año 2019, el mismo se tenía previsto terminarlo a finales del 2018 e implementarse a inicios del 2019, por lo que se logra visualizar, falta de planificación a la hora de preparar el presupuesto ordinario correspondiente al año 2019. De acuerdo con lo anterior no resulta justificable no contar con el presupuesto disponible para ejecutar las tareas del PETI, en el segundo semestre de 2019, cuando lo correcto sería que quedara un superávit.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), en sus normas 1.1 [30] y la 2.1 [31], establecen que el Jerarca mediante un proceso continuo debe promulgar y divulgar las estrategias y políticas organizacionales de manera comprensiva, coordinado con su contenido presupuestario y en armonía con la tecnología existente.

Hallazgo N°22: Análisis del control de los proyectos de TI

Esta Auditoría logra identificar la falta de proyectos que sean ejecutados por funcionarios de la Unidad de TI, las labores o proyectos relacionados a Tecnologías de la Información se manejan por medio de compras o licitaciones, por lo cual, las tareas se centran en dar seguimiento al cumplimiento de los objetivos establecidos en cada contratación. No contando con una metodología previamente establecida que le permita llevar un control sobre los proyectos o contrataciones relacionados con TI.

Como parte de la herramienta SharePoint, se dispone de un espacio donde se lleva un control de los documentos relacionados a cada una de las contrataciones, sin embargo; esto es algo

30 1.1 Marco estratégico de TI. El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido.

31 2.1 Planificación de las tecnologías de información. La organización debe lograr que las TI apoyen su misión, visión y objetivos estratégicos mediante procesos de planificación que logren el balance óptimo entre sus requerimientos, su capacidad presupuestaria y las oportunidades que brindan las tecnologías existentes y emergentes.

que se realiza por orden de la Jefatura, ya que como se indica, no se encuentra debidamente establecido y oficializado un procedimiento para este concepto, en la Unidad de TI.

El seguimiento de las contrataciones y ejecución de los objetivos se realiza verificando el cumplimiento de los alcances de cada licitación y dando seguimiento al cronograma presentado por el proveedor en cada contratación. De igual forma, el proceso descrito anteriormente no se encuentra establecido de manera formal.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, N-2-2007-CO-DFOE, en los puntos 1.5 Gestión de proyectos y 3.1 Consideraciones generales de la implementación de TI[32], indican sobre la gestión que debe desarrollar la UTI para llevar un control y seguimiento adecuado de los proyectos de TI. De igual forma, el Capítulo IV. Prestación de servicios y mantenimiento en el punto 4.6 Administración de servicios prestados por terceros, se indican algunos aspectos a considerar en la administración de los servicios contratados relacionados con las TI.

La condición evidenciada se presenta debido a que la UTI, no cuenta con una metodología o procedimiento formalmente establecido que le permita dictar una guía estándar sobre cómo se deben desarrollar los proyectos (contrataciones) que se relacionan con las Tecnologías de la Información. Tampoco se dispone de una adecuada planificación de temas presupuestarios que permitan la ejecución de los proyectos en forma oportuna, eficaz y eficiente.

Hallazgo N°23: Evaluar los requerimientos anuales de compras

La Proveeduría Institucional de la CNE publicó en la página[33] de dicha Comisión, en enero de cada año, los planes de compra de los periodos 2018 y 2019. En julio de 2019 se publica el Plan Estratégico de Tecnologías de Información, sin embargo; no se logra obtener evidencia que al menos las compras del periodo 2019 se hayan planificado y publicado en coordinación con dicha planificación estratégica, tampoco se cuenta con un control de seguimiento y cumplimiento de dichas compras, así como de la ejecución del presupuesto asociado.

Durante la sesión de entrevistas, esta auditoría consultó a funcionarios de la UTI de la CNE, sobre el seguimiento y cumplimiento de los objetivos estratégicos, así como en atención a los indicadores o riesgos identificados en el PETI. Al respecto, de acuerdo con la Minuta de Reunión y/o Supervisión N° 9, del 02 de setiembre, 2020, se indica:

[32] 1.5 Gestión de proyectos. La organización debe administrar sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.

3.1 Consideraciones generales de la implementación de TI. La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe: a. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI. b. Establecer el respaldo claro y explícito para los proyectos de TI tanto del jerarca como de las áreas usuarias. c. Garantizar la participación activa de las unidades o áreas usuarias, las cuales deben tener una asignación clara de responsabilidades y aprobar formalmente las implementaciones realizadas. d. Instaurar líderes de proyecto con una asignación clara, detallada y documentada de su autoridad y responsabilidad. e. Analizar alternativas de solución de acuerdo con criterios técnicos, económicos, operativos y jurídicos, y lineamientos previamente establecidos. f. Contar con una definición clara, completa y oportuna de los requerimientos, como parte de los cuales debe incorporar aspectos de control, seguridad y auditoría bajo un contexto de costo –beneficio. g. Tomar las previsiones correspondientes para garantizar la disponibilidad de los recursos económicos, técnicos y humanos requeridos. h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos.

i. Promover su independencia de proveedores de hardware, software, instalaciones y servicios.

[33] https://www.cne.go.cr/transparencia/compras_contrataciones/licitaciones/Plan_Compra_Presupuesto_2018.pdf
https://www.cne.go.cr/transparencia/compras_contrataciones/licitaciones/plan_compras_2019.pdf

1. *Como lleva el control la UTI de los proyectos presentados por las diferentes Unidades de la CNE*

El seguimiento se realiza por medio del PETI. Se debe realizar una matriz en conjunto con la Unidad de Planificación para dar seguimiento a los proyectos que están dentro del PETI. Aún no se ha realizado dicha matriz ya que la Unidad de Planificación determino algunas inconsistencias en ciertos objetivos del PETI que impiden dar el seguimiento correspondiente.

Como parte de la revisión practicada al PETI, en su apartado de Procesos Sustantivos/Operativos GO[34], respecto a las actividades relacionadas a la UTI y a las compras, señala:

Presupuesto operativo	• Elaboración de insumos para el Presupuesto Operativo y Plan de Compras
	• Modificaciones presupuestarias y al plan de compras
	• Seguimiento del Presupuesto Operativo
	• Informe de avance de ejecución presupuestaria

Como ya se indicó, la implementación y cumplimiento del PETI 2019-2022, formalizado en el II semestre del 2019 (julio), se ha visto afectado principalmente, por no contar con una debida planificación del contenido presupuestario requerido para hacer frente a los compromisos establecidos, así como, a la falta de seguimiento, ya que a la fecha, no se cuenta con una Matriz que contenga los parámetros y recursos debidamente asignados, entre otros factores, que han influido en la gestión de la CNE y el país en general en el periodo 2020.

Hallazgo N°24: Evaluar el control sobre el presupuesto de TI

La UTI cuenta con los formatos Plan de compras-presupuesto Tecnologías de Información para periodos 2018 y 2019, pero no están relacionados al PETI 2019-2022[35]. No se logró obtener evidencia del seguimiento al control del presupuesto de gastos e inversiones asignado a la Unidad de tecnología de información para esos periodos.

Además, se evidenció que la UTI carece de un control implementado y alineado al presupuesto asignado y al PETI, que permita el control de la ejecución presupuestaria en atención de los proyectos y necesidades establecidas a corto y mediano plazo, tal y como lo establece la normativa legal vigente, y en apego a los principios de eficiencia y eficacia necesarios para demostrar calidad y buen uso de los recursos dentro de la CNE.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, (N-2-2007-CO-DFOE), indica en su norma:

2.5 Administración de recursos financieros. La organización debe optimizar el uso de los recursos financieros invertidos en la gestión de TI procurando el logro de los objetivos de esa inversión, controlando en forma efectiva dichos recursos y observando el marco jurídico que al efecto le resulte aplicable.

[34] PLAN ESTRATÉGICO DE TIC 2019-2022, pag.109.
[35] Acuerdo aprobación N°146 del 19 de julio de 2019 Sesión Junta Directiva de la CNE.

3. Conclusiones

Después de identificar la posible falta de un adecuado Sistema de Control que le permita a la UTI, asegurar que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios, basados en un enfoque de efectividad y mejoramiento continuo, referidos a la confiabilidad, oportunidad y utilidad; por cuanto la información debe poseer las cualidades necesarias que la acredite como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente, así como, qué las actividades de recopilar, procesar y generar información deben realizarse y darse en tiempo a propósito y en el momento adecuado, de acuerdo con los fines institucionales, debiendo poseer características que la hagan útil para los distintos usuarios, en términos de pertinencia, relevancia, suficiencia y presentación adecuada, de conformidad con las necesidades específicas de cada destinatario.

Por lo antes expuesto, se enumera una serie de deficiencias encontradas a saber:

1. La UTI no cuenta con mecanismos adecuados para hacerle frente a los riesgos que se relacionan con las Tecnologías de la Información, así como a los servicios brindados a los diferentes departamentos, por lo cual existe una mayor probabilidad de que dichos riesgos sean materializados, afectando el cumplimiento de los objetivos de las Unidades e institucionales.

2. La UTI presenta un débil cumplimiento de las regulaciones contenidas en las Normas Técnicas de Gestión y Control de las TIC, las cuales indican que “El jerarca debe traducir sus aspiraciones en materia de TI en prácticas cotidianas de la organización, mediante un proceso continuo de promulgación y divulgación de un marco estratégico constituido por políticas organizacionales que el personal comprenda y con las que esté comprometido” esto, debido principalmente a que dicha Unidad carece de Políticas Internas oficializadas.

Las Políticas y Procedimientos son herramientas de control interno que nos ayudan a brindar cierto grado de seguridad sobre los procedimientos realizados dentro por la Unidad y a su vez, colaboran en el cumplimiento de los objetivos planteados.

La ausencia de este tipo de documentación puede generar que el colaborador de la Unidad no tenga claro su forma de actuar ante ciertos eventos. De igual forma, el no contar con Políticas y Procedimientos establecidos de manera formal imposibilita el establecimiento de sanciones por parte de la Administración de la CNE.

3. El no contar con una matriz de seguimiento de los objetivos y proyectos establecidos en el PETI, y anterior al PETI, genera que no exista un control sobre los proyectos que se tienen determinados en la Planificación Estratégica, lo que no permite comprobar si los mismos estas siendo ejecutados de manera correcta.

4. El no contar con un catálogo de servicios, facilita la pérdida de trazabilidad de los servicios que provee la UTI y no permite identificar si dichos servicios satisfacen las necesidades

de los usuarios y colaboran en el logro de la razón de ser de la CNE, además limita la evaluación de la calidad de los servicios brindados y del valor que aporta la tecnología de información y comunicación.

5. Las actividades de control relacionadas con el desarrollo de aplicaciones adquiridas a través proveedores no siguen un proceso estandarizado, por lo cual, la CNE, podría estar expuesta al debilitamiento del control interno respecto a la ejecución de cada uno de los proyectos desarrollados por terceros.

6. La actual segregación de funciones no permite que las labores que lleva a cabo UTI se den de forma completa. No haber delimitado de manera juiciosa las responsabilidades de cada funcionario dentro de la Unidad, podría generar un recargo laboral en algunos de colaboradores de la UTI, no determinando si la Unidad cuenta con el recurso humano necesario para operar de manera que le permita el cumplimiento de sus objetivos y los institucionales.

7. Las condiciones actuales de la ubicación del edificio principal y el COE permiten el acceso al cuarto de servidores al personal de mantenimiento y los técnicos de outsourcing, quienes en muchas ocasiones deben ingresar equipos eléctricos de mantenimiento para atender otras necesidades del edificio. Dicha situación puede favorecer la presencia de daños físicos en los equipos de cómputo del cuarto de servidores, o bien, que el equipo esté expuesto a la manipulación de personas que no forman parte de la UTI.

8. El no contar la UTI con un procedimiento debidamente formalizado con responsabilidades sobre pruebas técnicas, funcionamiento, mantenimiento “preventivo y proactivo” de hardware y software, manipulación del equipo, personal autorizado para realizar la instalación de software y o sistemas, respaldos y actualizaciones, puede afectar el proceso de TI y poner en riesgo el manejo adecuado de los equipos, pérdida y deterioro de información, así como del hardware**.**

9. La CNE cuenta con niveles de capacidad de reacción limitadas, así como con un nivel de resiliencia muy bajo, esto ante posibles eventos inesperados que puedan poner en riesgo la continuidad del servicio que brinda la UTI e interrumpir la función rectora de la CNE en materia de prevención de riesgo y atención de emergencias.

10. La CNE carece de procedimientos relacionados a las actividades de TI y en resguardo de los activos de cómputo central, los cuales se encuentran expuestos a posibles eventualidades que afecten el buen desarrollo y continuidad de los servicios y actividades de TI y de la CNE en general.

11. Las prácticas actuales y las medidas de seguridad de la UTI para la protección e integridad de la información en materia de acceso a la red y la nube no poseen controles o medidas detectivas, preventivas y correctivas para minimizar el riesgo de fallas.

12. La CNE no cuenta con un procedimiento formalizado para el análisis de las capacidades de los sistemas y base de datos, lo que no permite garantizar la adecuada disponibilidad, capacidad y desempeño de la plataforma tecnológica, ni minimizar los riesgos asociados.

13. La ausencia de informes de rendimiento del equipo de cómputo no permite garantizar la adecuada disponibilidad, capacidad y desempeño de los equipos en producción, ni los riesgos relacionados al rendimiento de esos equipos.

14. La ausencia del plan de capacitación y concientización en materia de ciberseguridad, limita la capacitad de respuesta de la UTI y de la institución ante posibles ataques de incidentes de seguridad, de acuerdo con los lineamientos institucionales y los objetivos estratégicos de TI.

15. El no contar la UTI actualmente con una política de seguridad de la información, formalizada y comunicada, genera que los funcionarios de la institución desconozcan las responsabilidades y riesgos asociados con la operación de la plataforma.

16. La dependencia generada sobre terceros para la atención de incidentes relacionados con el Sistema Wizdom, ocasiona que algunos inconvenientes no se atiendan de forma oportuna, lo que puede retrasar el cumplimiento de los planes de trabajo que tienen establecidos cada una de las Unidades de la CNE.

17. La efectividad del sistema de control interno en la UTI con relación a las actividades de evaluación de los esquemas de seguridad es reducida, condición que no permite tener una gestión oportuna y confiable de los accesos y genera vulnerabilidad de la información. La ausencia de estudios o pruebas de vulnerabilidad podría incrementar el riesgo de que terceros accedan a recursos sin contar con la debida autorización, comprometiendo la integridad, confidencialidad y disponibilidad de los datos. Además, dificulta identificar posibles deficiencias que posee la red, así como eventuales mejoras que se pueden realizar.

18. La ausencia de un control para el flujo de información sensible, entrante y saliente hacia y desde la red interna de la Institución, imposibilita proteger de manera adecuada el acceso de la información.

19. La ausencia de investigaciones de nuevas tendencias tecnológicas limita mantener la plataforma tecnológica en óptimas condiciones y puede incrementar el riesgo de fallas, ante posibles cambios en las tendencias tecnológicas y genera niveles de obsolescencia acelerados.

20. El no contar con un plan continuo de capacitación en materia de ciberseguridad y nuevas tendencias, podría generar que los funcionarios se encuentren desactualizados en algunos temas específicos como pueden ser aquellos que se relacionan con la seguridad de los sistemas que utiliza la CNE. De igual forma, el no contar con un plan de capacitación específico para la UTI, podría estar limitando el alcance de las capacidades reales que tienen los funcionarios de la Unidad y que serían muy útiles para la realización de sus funciones.

21. y 23. Al no contar la UTI con una planificación adecuada en materia compras y presupuesto vinculadas al PETI, la limitan a ejercer un seguimiento oportuno de su gestión estratégica, la expone a pérdida de oportunidades, asignación inadecuada de recursos, poca o ninguna eficiencia, incumplimiento de metas, incertidumbre y otras desventajas como instancia asignada al control, a la administración de los proyectos y activos relacionados con la tecnología de información y comunicación. En consecuencia, se podría estar afectando el cumplimiento de los objetivos institucionales.

22. La carencia de procedimientos oficializados e implementados de manera correcta genera incertidumbre con relación a la uniformidad sobre el desarrollo de los proyectos e impide

a la UTI, tener adecuado control de aspectos y condiciones que aseguren que los proyectos se están ejecutando de manera correcta y según los objetivos planteados por la UTI y la CNE en general.

23. El no contar la UTI con un procedimiento formalmente establecido, para llevar un adecuado control del presupuesto y del PETI, podría estar favoreciendo un uso inadecuado de los recursos económicos y humanos de esa Unidad, situación que incide directamente en el debilitamiento del valor agregado que deben generar las TIC.

Finalmente, y a manera de conclusión, se rescata la importancia de hacer uso y establecer las condiciones necesarias para implementar las recomendaciones contenidas en el informe CNE-PLAI-INF-003-19 Taller "Fortalecimiento de la Unidad de TI" de abril 2019, elaborado por la Unidad de Planificación Institucional de la CNE, en el cual se revelan una serie de debilidades de control interno que presenta la UTI, los cuales deben ser atendidas de manera oportuna, considerando entre otras, al menos las referidas a los siguientes aspectos:

CUADRO Nº 2 Debilidades Unidad de Tecnologías de Información

Cantidad	Debilidades	Porcentaje
4	Incumplimiento de Plazos	22%
2	Infraestructura Física	11%
1	Falta de Apoyo Administrativo	6%
2	Falta de Documentación	11%
3	Falta de Procedimientos	17%
2	Poco Personal	11%
2	Falta de Estructura Organizacional	11%
1	Falta de Comunicación	6%
1	Falta de Disponibilidad	6%
18		**100%**

Fuente: Personal Unidad TI

Las debilidades presentadas en la UTI afectan el cumplimiento del Artículo 16 de la Ley General de Control Interno, el cual señala:

> *Sistemas de información. Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, entendiendo esta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar de modo adecuado la información producida o recibida en la organización, en el desarrollo de sus actividades, con el fin de prevenir cualquier desvío en los objetivos trazados.* ***Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada***[36]*.*

[36] Ley General de Control Interno, N°8292. Publicado en La Gaceta oficial 169, 4/set./2002.

4. Recomendaciones

A la señora Yamileth Mata Dobles, Directora Ejecutiva o a quien ocupe el cargo:

Aceptar y aprobar el Informe de Sobre los *"Resultados de la Auditoría de Carácter Especial sobre la Evaluación del Cumplimiento de Normas Técnicas, Sistema de Tecnología, Control de Calidad y Seguridad de la Información"*, a su vez, brindar, en la forma y condiciones que corresponda conforme a su competencia, el apoyo necesario a las acciones que proponga el Comité de Tecnologías de Información y la UTI para el cumplimiento de las recomendaciones contenidas en este servicio de auditoría, con el fin de potenciar las oportunidades de mejora en la gestión administrativa y de tecnologías de información, a efecto de contar con la atención e información de calidad para la toma de decisiones, la transparencia en la gestión institucional y la posterior rendición de cuentas. **(Plazo: 1 semana)**

Al Comité de Tecnologías de la Información y a la Unidad de Tecnologías de Información

1. Identificar y establecer a través de una matriz los riesgos que puedan afectar el cumplimiento de los objetivos de la Unidad. Una vez identificados los riesgos, establecer los mecanismos de control interno necesarios y pertinentes para lograr mitigar dichos riesgos a un nivel de riesgo aceptable, a fin de que en caso de que alguno de los riesgos se materialice, no se afecte de forma significativa las operaciones de la institución. Dichas acciones deben fortalecer los sistemas de control interno con los que cuenta la UTI **(Plazo: seis meses).**

2. Establecer la normativa interna necesaria, adaptada al 100% de la operatividad de la institución, así como establecer las Políticas que sean necesarias y que se enfoquen en el cumplimiento de los objetivos de la Unidad para lo cual la UTI debe dar continuidad a la identificación y formalización de los procesos desarrollados en el Taller impartido por la Unidad de Planificación de la CNE. Es de suma importancia que, una vez desarrollados los Manuales de Procedimientos y Políticas correspondientes, sean aprobados por la Dirección Ejecutiva y oficializados por parte de la Presidencia para que formen parte de los procesos internos de la institución y se ordene su implementación a aplicación **(Plazo: seis meses).**

3. Establecer un procedimiento formal que le permita a la UTI, mantener un control permanente de los proyectos que deba llevar a cabo en materia de adquisición de sistemas y equipo de cómputo para el uso institucional, para lo cual debe de considerar la posible adquisición del sistema Microsoft Project. El procedimiento que se establezca para este fin debe ser aprobado por el Comité de TI y la Dirección Ejecutiva quien, a su vez, deberá ordenar su implementación y aplicación en todos los proyectos que se ejecuten **(Plazo: seis meses).**

4. Ordenar y establecer el procedimiento que corresponda para dar seguimiento a la implementación del PETI 2019-2020, dando énfasis a la revisión y ejecución de los de los requerimientos no ejecutados en los periodos 2018-2019 y de ser necesario, someter a aprobación las modificaciones que correspondan. Una vez que dicho procedimiento cuente con la aprobación de la Dirección Ejecutiva, quien ordenará su aplicación, corresponderá al Comité de TI, vigilar su aplicación, mantener el control del avance y cumplimiento de los objetivos contenidos en dicha herramienta. (**Plazo: tres meses).**

5. Establecer una metodología que guíe los procesos de implementación de software y que considere entre otros aspectos: la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post implantación de la satisfacción de los requerimientos, considerando que algunas de estas actividades son realizadas por terceros para lo cual es necesario mantener evidencia de la aplicación de dicha metodología en cada ocasión a fin de garantizar su efectividad **(Plazo: ocho meses).**

6. Producto de la situación descrita en el Hallazgo No 6: Evaluación de la segregación de funciones, se derivan las siguientes recomendaciones:

6.1 Actualizar la información contenida en el Organigrama de la UTI que fue presentado en conjunto con el PETI, ya que se han dado movimientos en la dicha Unidad, luego de la presentación y aprobación por parte de la Junta Directiva de la CNE. Una vez actualizado, debe ser presentado nuevamente tanto al Comité de TI como a la Junta Directiva de la institución para realizar la formalización respectiva y distribuir dentro de los funcionarios de la CNE **(Plazo: seis meses).**

6.2 Establecer, las funciones y responsabilidad de cada uno de los puestos de trabajo de los funcionarios de la UTI, con base en la distribución realizada en el Organigrama y los Manuales de Puestos. Dichos Manuales deben ser comunicados a cada uno de los funcionarios de la Unidad, quienes firmarán el recibido de la comunicación para que no puedan alegar desconocimiento de las funciones y responsabilidad de cada puesto **(Plazo: tres meses).**

7. Realizar las acciones que correspondan para eliminar la prevista de agua que se encuentra en el cuarto principal de servidores y Routers, así como, mejorar la calidad de cielo raso del espacio físico actual para evitar que el aire frio, se filtre hacia el exterior. Establecer e implementar controles para el acceso de personas y materiales que ingresan al cuarto de redes ubicado en el edificio COE, ya que en ese espacio se encuentra la caja de breakers que suministra de fluido eléctrico a este edificio. De igual forma, se debe considerar y vigilar el riesgo de derrumbe que presenta el edificio. **(Plazo: tres meses)**

8. Revisar el documento borrador denominado “Lineamientos para uso, resguardo y custodia de los equipos de cómputo asignados a los Comités Municipales de Emergencias” con el fin de realizar las modificaciones necesarias y formalizar dicho documento. Contemplar además, lo relativo al Teletrabajo respecto a la entrada y salida de equipos de cómputo, y solicitar el apoyo del jerarca para su respectiva formalización **(Plazo: seis meses).**

9. Desarrollar y formalizar procedimientos para que la organización mantenga una continuidad razonable de sus procesos y que su interrupción no afecte significativamente a los usuarios, para lo cual se puede tomar como referencia el apartado 1.4.7 de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) considerando los nuevos lineamientos que se debe establecer la CNE. Como parte de ese esfuerzo, documentar y poner en práctica en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de los recursos de TI, según su criticidad**. (Plazo: ocho meses).**

10. Implementar, en coordinación con las instancias internas correspondientes, los procedimientos e identificar los riesgos relacionados a los procesos y activos de TI, en cumplimiento de las normas técnicas aplicables a la fecha y con sustento en la gestión actual y futura. Dichos procedimientos deben ser aprobados, oficializados y aplicados para mitigar los riesgos correspondientes al ambiente de control **(Plazo: ocho meses).**

11. Desarrollar y formalizar normativa interna que permita a la UTI, asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información, considerando, además, mecanismos de control que serán revisados permanentemente, conforme sea requerido. Para este propósito se puede tomar como referencia lo dispuesto en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), inciso 1.4.4, Seguridad en las operaciones y Comunicaciones. **(Plazo: ocho meses).**

12. Implementar mediante un procedimiento formal lo dispuesto en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, inciso 4.2, Administración y operación de la plataforma tecnológica, para garantizar y asegurar la correcta operación y mantener pistas de auditoria de eventuales fallas, presentes y futuras, lo cual debe ser documentado de manera razonable **(Plazo: seis meses).**

13. Implementar mediante un procedimiento formal lo dispuesto en las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) inciso 4.2, Administración y operación de la plataforma tecnológica, con el fin de asegurar la correcta operación del equipo en producción **(Plazo: seis meses).**

14. Planificar, coordinar y ejecutar un plan de capacitación y concientización permanente en materia de seguridad de la información para los funcionarios de la CNE, **(Plazo: seis meses).**

15. Revisar el documento en borrador “Lista Manuales de Procedimientos Operativos Internos” (Procesos General 004 Wilgen Saborío), para verificar que este cumpla con el inciso 4.2 Administración y operación de la plataforma tecnológica de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE). Una vez, revisado y actualizado solicitar apoyo de la Dirección Ejecutiva para su aprobación, oficialización y aplicación permanente en la CNE. **(Plazo: dos meses).**

16. Producto de la situación descrita en el Hallazgo No 16: Estado de los servicios de TI, se derivan las siguientes recomendaciones:

16.1 Establecer un Plan de capacitación continuo para el personal de la UTI, que les permita ampliar y actualizar sus conocimientos en temas como el uso y manejo de las herramientas y sistemas con los que cuenta la CNE y atender de manera oportuna y eficiente, los incidentes e inconvenientes que reportan los usuarios de las diferentes Unidades y no tener que depender del proveedor. Dicho Plan debe abarcar los aspectos indicados y contar con el presupuesto requerido para lo cual, la Jefatura de TI y el Comité de TI deben justificar dicho plan y contar con la aprobación de la Dirección Ejecutiva. **(Plazo: dos meses).**

16.2 Formalizar la implementación del sistema de incidencias GLPi, este software de código abierto está editado en PHP (lenguaje de programación) y distribuido bajo una licencia GPL. El uso de este sistema inició en el mes de agosto 2020, la

formalización va a permitir a la UTI y la Dirección Ejecutiva tener un mejor control sobre la atención de los inconvenientes surgidos con relación a TI. **(Plazo: dos meses).**

17. Desarrollar los procedimientos internos y las responsabilidades asociados con la operación de la plataforma tecnológica, tomando como referencia lo indicado en los incisos: 4.2 y 5.2 de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE). Asimismo, es pertinente realizar evaluaciones a dicha plataforma e implementar las medidas correctivas resultantes de dichos procesos. **(Plazo: seis meses).**

18. Implementar formalmente los procedimientos y políticas internas que sean necesarias y que permitan contar con esquema de seguridad que ayude a filtrar y controlar la información entrante o saliente hacia y desde la red interna de la Institución, para esto se puede tomar como referencia lo indicado en el inciso 1.4.5 Control de acceso, de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE). **(Plazo: seis meses).**

19. Formalizar los planes de renovación en materia de seguridad y actualización tecnológica. Es importante validar la tendencias tecnológicas y nuevas fallas de seguridad que la CNE necesite implementar **(Plazo: seis meses).**

20. Producto de la situación descrita en el Hallazgo No 20: Evaluación de capacitación y concientización en ciberseguridad, se derivan las siguientes recomendaciones:

20.1 Establecer un plan de capacitación propio de la UTI donde se contemplen capacitaciones constantes en temas de seguridad informática, esto con el fin de dar continuidad y mantener a los funcionarios actualizados en temas de ciberseguridad. **(Plazo: dos meses).**

20.2 Continuar con los planes de capacitación al personal de la CNE en temas del buen uso de las tecnologías de la información, así como en temas de ciberseguridad, manejo de la información y concientización sobre el uso de las TI. Mantener evidencia de dichas capacitaciones y de la satisfacción por parte de la UTI del alcance de estas. El citado plan de capacitación debe de ser considerado como parte del plan solicitado en la Recomendación N°16, de manera que sea elaborado por el Encargado de la TI, cuente con el Visto bueno del Comité de TI y sea aprobado por la Dirección Ejecutiva **(Plazo: dos meses).**

21. y 23. Revisar y valorar los objetivos establecidos en el PETI y, evaluar las situaciones que han limitado el cumplimiento y seguimiento del PETI y que no ha permitido contar con un instrumento idóneo para su validación, a su vez se debe valorar si las actividades y plazos acordados se mantienen o deben ajustarse. Una vez que el PETI, esté actualizado y se cuente con un instrumento desarrollado para darle seguimiento, debe mantenerse actualizado procurando que la gestión de los proyectos y demás necesidades tecnológicas y de comunicación de la CNE, sean atendidas conforme lo establecido en el PETI **(Plazo: tres meses).**

22. Establecer un procedimiento formal y uniforme para el control de los proyectos, haciendo uso de la herramienta Microsoft Project que se planea adquirir durante el periodo 2020. El procedimiento que se establezca debe ser aprobado por el Comité de TI con el fin de que sea implementado dentro de la Unidad de TI **(Plazo: tres meses).**

24. Implementar un control (formal) para asegurar que las inversiones que se realicen, por medio de la UTI, permitan el logro de los objetivos y se garantice que los recursos asignados fueron utilizados para el logro del fin propuesto, aplicando el marco regulatorio que al efecto le resulte aplicable y a su vez permita dar el seguimiento requerido. **(Plazo: tres meses).**

La CNE y principalmente la UTI, debe tener presente y tomar acciones prontas para poner en aplicación la Resolución R-DC-17-2020 emitida por la Contraloría General de la República, e pasado 17 de marzo de 2020. Dicha resolución deroga las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE) y, dispone que cada entidad debe emitir su propia regulación para la gestión de TI, y aplicarla a partir del 01 de enero de 2022. Asimismo, debe implementar los controles e identificar los riesgos asociados a los objetivos estratégicos y operativos, los cuales deben estar debidamente administrados en búsqueda del logro de los objetivos institucionales y en cumplimiento del artículo 8 y 10 de la Ley General de Control Interno[37].

La UTI en cumplimiento de las recomendaciones anteriores (1-24) debe implementar en el plazo de **15 días,** un cronograma o plan de acción formalizado y aprobado por la Dirección Ejecutiva, donde conste el nombre del hallazgo, la recomendación, acción (es) a implementar, fecha de cumplimiento, responsable y observaciones. Este cronograma debe ser remitido de manera formal a la Auditoría Interna, para la fiscalización que resulte pertinente.

Las conclusiones y recomendaciones expresadas en los últimos apartados del presente informe se relacionan directamente con el número de cada uno de los hallazgos expuestos en el apartado ***2 Resultados***.

PAMELA CASTRO QUIROS (FIRMA)

Firmado digitalmente por PAMELA CASTRO QUIROS (FIRMA)
Fecha: 2021.02.01 15:28:08 -06'00'

Aval al Informe Externo de TI
Pamela Castro Quirós
Auditora Interna, ai
CNE

[37] Ley General de Control Interno, N°8292. Publicado en La Gaceta oficial 169, 4/set./2002. Artículo 8º-Concepto de sistema de control interno. Para efectos de esta Ley, se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos:
a) Proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal, b) Exigir confiabilidad y oportunidad de la información, c) Garantizar eficiencia y eficacia de las operaciones, d) Cumplir con el ordenamiento jurídico y técnico.
Artículo 10.-Responsabilidad por el sistema de control interno. Serán responsabilidad del jerarca y del titular subordinado establecer, mantener, perfeccionar y evaluar el sistema de control interno institucional. Asimismo, será responsabilidad de la administración activa realizar las acciones necesarias para garantizar su efectivo funcionamiento.