INVU
Instituto Nacional de Vivienda y Urbanismo

AUDITORÍA INTERNA

INFORME DE AUDITORÍA
NO. AI-011-2022

Evaluación del Grado de Cumplimiento del
Plan Estratégico de Tecnología de la Información (PETI)

Noviembre 2022

Estudio No. ATI-010-2022
Estudio No. ATI-016-2022

ÍNDICE DE CONTENIDO

I. RESUMEN EJECUTIVO 3

II. INTRODUCCIÓN 4

Origen del estudio 4
Objetivo general 4
Objetivos específicos 4
Alcance 4
Normativa 4
Implementación de recomendaciones (Ley General de Control Interno, artículo n.º 36). 5
Limitaciones 5
Comunicación preliminar de los resultados de la auditoría 5

III. RESULTADO 5

Oportunidad de mejora no. 1: Plan Estratégico de Tecnología de Información (PETI). 5
A) Porcentaje de Cumplimiento de las iniciativas del PETI 6
B) Estado de las iniciativas 7
C) Monitoreo y seguimiento con indicadores 12

IV. CONCLUSIONES 14

V. RECOMENDACIONES 15

VI. ANEXOS 16

Estudio No. ATI-010-2022
Estudio No. ATI-016-2022

I. RESUMEN EJECUTIVO

El presente estudio de Auditoría Interna tuvo como propósito analizar la labor de la Unidad de Tecnología de Información, durante el período comprendido entre junio a diciembre 2021; con respecto al cumplimiento del Plan Estratégico de Tecnología de la Información (PETI). El estudio se realizó con la finalidad de generar oportunidades de mejora que coadyuven al fortalecimiento de la Unidad como componente del sistema de control interno.

En este informe se expone, en detalle, el resultado del estudio llevado a cabo por la Auditoría Interna.

A continuación, se presentan los aspectos más relevantes que afectan el cumplimiento de los objetivos de control interno establecidos en el artículo no. 8 de la Ley General de Control Interno:

a. Garantizar eficiencia y eficacia de las operaciones.

i. A junio 2022, se ha observado un bajo avance en el cumplimiento de las iniciativas de la UTI, el cual podría ser similar al del I Semestre 2021 (58%).

ii. La Unidad de Tecnología de Información no considera en los Informes de Seguimiento las unidades de medida establecidas en el PETI.

b. Cumplir con el ordenamiento jurídico y técnico.

i. La institución no posee un Marco de Gestión de las Tecnologías de Información y Comunicación debidamente declarado, aprobado y divulgado, según lo dictado por la Contraloría General de la República.

Con base en lo anterior, y con el propósito de fortalecer la Unidad de Tecnología de Información, se les formulan las siguientes oportunidades de mejora a las personas funcionarias correspondientes; con el fin de establecer las acciones necesarias para solventar oportuna y eficazmente las situaciones descritas. Esto de acuerdo con lo establecido en la Ley General de Control Interno (ley no. 8292).

II. INTRODUCCIÓN

Origen del estudio

2.1. La Auditoría Interna realizó el presente estudio con el fin de Evaluar el grado de cumplimiento del Plan Estratégico de Tecnología de la Información (PETI), en la Unidad de Tecnología de Información, de acuerdo con el Plan Anual de Trabajo de la Auditoría Interna del año 2022, conocido por los miembros de la Junta Directiva en la Sesión Ordinaria No. 6522 articulo VII inciso del día 16 de diciembre de 2021.

Objetivo general

2.2. Evaluar el grado de cumplimiento del Plan Estratégico de Tecnología de la Información (PETI) y la atención de las recomendaciones emitidas a esta unidad.

Objetivos específicos

2.3. 1. Valorar el avance en el cumplimiento de los proyectos de TI contenidos en el Plan Estratégico de Tecnología de la Información (PETI).

2.4. 2. Brindar seguimiento a las recomendaciones de esta unidad que se encuentren en estado de sujeta a seguimiento.

Alcance

2.5. El alcance del estudio abarcó la revisión de aspectos de control interno y de los procedimientos internos y externos que observa la Unidad de Tecnología de Información, en el período comprendido entre los meses entre junio a diciembre 2021, el cual se amplió en aquellos casos en los que se consideró pertinente.

Normativa

La principal normativa observada en este estudio fue la siguiente:

- Constitución Política de Costa Rica.
- Ley Orgánica del Instituto Nacional de Vivienda y Urbanismo No. 1788.
- Ley General de la Administración Pública. No. 6227.
- Ley General de Control Interno, No. 8292.
- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- Normas Generales de Auditoría para el Sector Público.
- Normas para el Ejercicio de la Auditoría Interna en el Sector Público.
- Mejores prácticas, tales como: COBIT-5, ISACA y la Guía de Indicadores de MIDEPLAN.

Metodología

2.6. El presente estudio se realizó de acuerdo con las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, emitidas por la Contraloría General de la República y demás normativa atinente.

La metodología utilizada se enfocó en la aplicación de técnicas y prácticas de auditoría normalmente aceptadas, tales como: entrevistas, verificación de documentos y al análisis de la normativa legal y técnica aplicable.

Para el desarrollo de esta auditoría se utilizó la información suministrada por la Encargada de la Unidad de Tecnología de Información, así como los insumos de las entrevistas aplicadas.

Además, los resultados que se exponen en este informe se fundamentan en los procedimientos de auditoría dirigidos a la verificación del cumplimiento del INVU, en materia de Tecnología de Información.

Implementación de recomendaciones (Ley General de Control Interno, artículo n.º 36).

2.7. Se establece un plazo de 10 días hábiles para que se ordene la implementación de las recomendaciones. En caso de que se discrepe, en el transcurso de dicho plazo se debe elevar el informe a la Junta Directiva, con copia a la Auditoría Interna, y se deben exponer por escrito tanto las razones por las cuales no se está de acuerdo como las soluciones alternas que se propongan para los hallazgos.

Limitaciones

2.8. En el desarrollo del presente informe no se presentaron limitaciones.

Comunicación preliminar de los resultados de la auditoría

2.9. El viernes 28 de octubre 2022, la Auditoría Interna se reunió de forma virtual, a través de la plataforma Microsoft Teams, con la señora María Amalia Pessoa Araya, Encargada de la Unidad de Tecnología de Información, con la finalidad de comentar sobre las oportunidades de mejora y sus respectivas recomendaciones. Una vez comentados los temas, la señora María Amalia Pessoa Araya, manifestó estar de acuerdo con las oportunidades de mejora y la recomendación.

III. RESULTADO

3.1 El presente estudio permitió determinar una serie de hallazgos que cuentan con sus oportunidades de mejora, en cuanto al control interno de la Unidad de Tecnología de Información. A continuación, se detallan dichos hallazgos con sus respectivas oportunidades de mejora.

<u>Oportunidad de mejora no. 1: Plan Estratégico de Tecnología de Información (PETI).</u>

3.2 Las oportunidades de mejora relacionadas con el PETI, se describen en el presente hallazgo según la siguiente estructura:

A) Porcentaje de Cumplimiento de las iniciativas del PETI.

B) Estado de las iniciativas.

B.1) ITI-10 Diagnóstico de la gestión de las TI basado en Normas Técnicas y el plan de implementación de cierre de brechas e ITI-16 Actualización del marco normativo de seguridad informática (Normas Técnicas).

B.2) ITI-14 Establecer configuraciones de Seguridad en la plataforma crítica.

C) Monitoreo y Seguimiento de los indicadores.

A) Porcentaje de Cumplimiento de las iniciativas del PETI

3.3 En el Plan Estratégico de Tecnología de la Información (PETI), se establecen 19 iniciativas[1] (de la ITI-01 a la ITI-19), las cuales corresponden a las actividades, tareas o proyectos a ejecutar para el cumplimiento de los objetivos estratégicos de la Unidad de Tecnología de Información del año 2019 al 2023.

3.4 Se determinó que, al I Semestre de 2022, el PETI podría contar con un cumplimiento similar al presentado por esta Unidad a la Junta Directiva durante el I Semestre del 2021, el cual fue del 58%, lo anterior, tomando como parámetro que desde esa fecha a la actualidad (Junio 2021 a Junio 2022), el avance es del 0% ya que según manifestó la Encargada de la Unidad de TI, no hay iniciativas que se hayan cumplido durante el 2022, lo cual lo atribuye a temas de presupuesto, estructura y otros.

3.5 De forma seguida se detalla el estado de cumplimiento de las 19 iniciativas. Veamos:

- Once iniciativas tienen un cumplimiento del 100%; no obstante, siete[2] se encuentran pendientes de revisión por parte del Comité de TI, dado que actualmente este Comité se encuentra desintegrado por la renuncia del Subgerente General en febrero 2022.
- Una iniciativa se encuentra en un cumplimiento entre un 51% a 75%.
- Una iniciativa se encuentra en un cumplimiento entre un 26% a 50%.
- Seis iniciativas tienen un cumplimiento de 0%.

3.6 En relación con las 06 iniciativas que presentan un cumplimiento del 0%, se le consultó a la Encargada de la UTI, sobre la atención realizada a estas iniciativas. Al respecto indicó:

"ITI-01: no tienen avance por un tema presupuestario.
De momento no es viable la implementación de la ITI-05 ya que se desconoce la estructura del Core Bancario (ABANKS-FONT).
ITI-10 e ITI-11: no tienen avance por un tema presupuestario; no obstante, se incluyeron en el presupuesto 2023 para ser atendidas.
ITI-12: no tienen avance por un tema presupuestario; no obstante, se incluyó en el presupuesto 2023 para ser atendida.
ITI-13: se han realizado reuniones para atender la iniciativa; sin embargo, no se ha logrado puntualizar.
ITI-14: se está gestionando la contratación no. 2022CD-000020-0005800001 denominado "Contratación de Servicios para el Análisis de Vulnerabilidades del INVU", ya se realizó el estudio del exterior y se tienen un primer resultado con oportunidades de mejora.
ITI-16: se gestionó con un pasante; sin embargo, el documento entregado tiene pendiente ampliar unos temas. Se ha participado en reuniones con el MICITT para la implementación de las nuevas normas propuestas por el citado ministerio. Se estima necesario realizar una revisión por parte de un ente externo especialista en el tema, por lo que se incluyó en el presupuesto 2023.
ITI-18: se ha elaborado un cronograma con el detalle de las actividades para atender la iniciativa.

[1] Ver anexo 1 con el detalle de las iniciativas y su cumplimiento según el oficio GG-TI-050-2021.
[2] Las siete iniciativas pendientes de pendientes de revisión por parte del Comité de TI y de aprobación de la Junta Directiva, según lo indicado por la Encargada de la UTI, son: ITI-02 Definir una cartera de proyectos anual en conjunto con las áreas, departamentos, unidades y procesos que responda a las capacidades de la Unidad de TI, ITI-08 Implementar un programa de comunicación que propicie la mejora continua en el servicio al cliente interno, ITI-09 Desarrollar una metodología de proyectos de la Unidad de TI que permita gestionar los requerimientos institucionales, ITI-15 Implementar un modelo de gestión de parches y vulnerabilidades., ITI-16 Actualización del marco normativo de seguridad informática (Normas Técnicas), ITI-17 Definición de la metodología de desarrollo generalizada (pasos básicos para el desarrollo), ITI-19 Diseñar e implementar un plan de formación para mejorar la continuidad, eficiencia y productividad de las personas involucradas en la prestación de los servicios de la Unidad de TI.

En el 2022 se incluyó en el presupuesto las siguientes iniciativas: 16, 11, 09, 14 y 12; no obstante, no se le brindó contenido debido al equilibrio presupuestario."

3.7 Además, se le consultó a la Encargada de la Unidad de Tecnología de Información a qué obedece que en el Informe al I Semestre 2021 se presentan iniciativas con un avance del 100%, pero que se encuentran pendientes de revisión por parte del Comité de TI y de aprobación de la Junta Directiva. Al respecto, manifestó lo siguiente:

"Se encuentran a un 100% por parte de la gestión de UTI; no obstante, se encuentra pendiente de aprobación por parte de la Comisión de TI (la cual no se encuentra en funcionamiento) y posteriormente para aprobación de la Junta Directiva."

3.8 Por su parte, las Normas de Control Interno para el Sector Público, emitidas por el órgano contralor, establecen en el numeral 4.5.2, "Gestión de proyectos", que:

"El jerarca y los titulares subordinados, según sus competencias, deben establecer, vigilar el cumplimiento y perfeccionar las actividades de control necesarias para garantizar razonablemente la correcta planificación y gestión de los proyectos que la institución emprenda (...)"

(El subrayado no pertenece al texto original)

3.9 La atención de las iniciativas en los plazos establecidos permite el logro de los objetivos trazados mediante un uso eficaz de los recursos que son presupuestados, para ello se debe contar con una adecuada planificación, tal y como lo establece la Norma de Control Interno 4.5.2, denominada Gestión de proyectos.

3.10 En esta oportunidad de mejora no se elaboró recomendación dado que en el informe AI-015-2020, se comunicó la recomendación No. 2, la cual se encuentran proceso de atención y establece lo siguiente:

Número de recomendación	Detalle de la recomendación	Riesgo
2	*Realizar un documento integral de la Unidad de TI, que identifique como mínimo el mapeo de los procesos, objetivos, riesgos, asignación de responsables, transferencia de conocimientos entre el personal de la Unidad, servicios críticos y la cobertura del servicio, lo anterior con la finalidad de optimizar la gestión de esta Unidad, priorizar las actividades y necesidades institucionales; además, dejar esta gestión debidamente documentada.*	Alto

Fuente: Informe AI-015-2020.

B) Estado de las iniciativas

3.11 Las 19 iniciativas contenidas en el PETI tienen su grado de importancia ya que mediante su consecución se logran cumplir los objetivos, tanto institucionales como los de la UTI; no obstante, en este apartado se enfatiza el cumplimiento de las siguientes iniciativas considerando el seguimiento de las recomendaciones emitidas por la Auditoría Interna.

B.1) ITI-10 Diagnóstico de la gestión de las TI basado en Normas Técnicas y el plan de implementación de cierre de brechas e ITI-16 Actualización del marco normativo de seguridad informática (Normas Técnicas).

3.12 La Contraloría General de la República mediante la resolución R-DC-17-2020, del 27 de marzo de 2020, estableció en su artículo 1° la derogación de las *Normas Técnicas para la gestión y el control de las Tecnología de Información (N-2-2007-CO-DFOE)* a partir del 1° de enero del 2022. Además, en la citada resolución se señaló lo siguiente:

> *"Todas las instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República deberán haber declarado, aprobado y divulgado el marco de gestión de las Tecnología de información y comunicación requerido en la modificación incorporada en esta resolución a las Normas de Control Interno para el Sector Público (N-2-2009-CODFOE),* ***a más tardar el 1° de enero del 2022****."*
>
> (El subrayado y resaltado no pertenecen al texto original)

3.13 No obstante, la Unidad de Tecnología de Información, no cuenta con un *Marco de Gestión de las Tecnologías de Información y Comunicación* debidamente declarado, aprobado y divulgado, lo cual se ha venido señalando, por parte de esta Auditoría Interna, desde el 2020, inclusive mediante el informe AI-015-2020, se indicó lo siguiente:

> *"(…) es necesario que la Unidad de Tecnología de Información desarrolle un Marco de Gestión de las Tecnologías de Información y Comunicación que permita dar respuesta a la Iniciativa 16, a la resolución de la CGR, a las estrategias del PEI y al contexto de la UTI."*

3.14 Sobre el particular, se le consultó a la Encargada de la Unidad de Tecnología de Información sobre las gestiones realizadas para la declaración, aprobación y divulgación del *Marco de Gestión de las Tecnologías de Información y Comunicación*. Al respecto, manifestó lo siguiente:

> **Marco de Gestión de las Tecnologías de Información y Comunicación:**
>
> *"Se le hizo la propuesta al Comité de TI de adherirnos al marco COBIT-2019, pero (…) estamos a la espera de que se reanude el funcionamiento del Comité de TI, nótese, que la UTI realiza la propuesta, pero en este caso es la administración superior quien la aprueba (…)"*
>
> **ITI-10 e ITI-16**
>
> *"ITI-10 e ITI-11: no tienen avance por un tema presupuestario; no obstante, se incluyeron en el presupuesto 2023 para ser atendidas (…) ITI-16: se gestionó con un pasante; sin embargo, el documento entregado tiene pendiente ampliar unos temas. Se ha participado en reuniones con el MICITT para la implementación de las nuevas normas propuestas por el citado ministerio. Se estima necesario realizar una revisión por parte de un ente externo especialista en el tema, por lo que se incluyó en el presupuesto 2023."*

3.15 En esta oportunidad de mejora no se emitirá recomendación dado que en el citado Informe AI-015-2020, se comunicó la recomendación No. 5 la cual se encuentran pendiente de atención y establece lo siguiente:

Número de recomendación	Detalle de la recomendación	Riesgo
5	*Construir una ruta de trabajo para la elaboración del Marco de Gestión de TI, en vista de la derogación de las Normas técnicas para la gestión y el control de las Tecnología de Información emitidas por la CGR, dejando esa gestión debidamente documentada.*	Alto

Fuente: Informe AI-015-2020.

B.2) ITI-14 Establecer configuraciones de Seguridad en la plataforma crítica

3.16 La iniciativa *"ITI-14 Establecer configuraciones de Seguridad en la plataforma crítica"*, tiene como objetivo táctico el establecer los lineamientos fundamentales para la seguridad de la información y la seguridad informática en la Unidad de Tecnología de Información, que incluya la definición de las configuraciones de la plataforma crítica, la implementación de un modelo de gestión de parches y vulnerabilidades y el desarrollo de un marco normativo de seguridad informática.

3.17 De acuerdo a lo indicado en el párrafo anterior y a raíz de los ciberataques ocurridos a instituciones del Sector Público, la Auditoría Interna consultó el 21 de abril de 2022, a la Unidad de Tecnología de Información sobre la preparación del INVU, ante un eventual ciberataque, sobre el Plan de Contingencia para continuar con el servicio y sobre los riesgos que se han valorado en TI, de acuerdo a los eventos que se han presentado con otras instituciones y que planificación se ha realizado al respecto. En referencia a las consultas, la Encargada de la Unidad de Tecnología de Información manifestó:

"En el mismo orden las respuestas:
Se cuenta con las siguientes herramientas:

- *Por ordenanza del MICITT en reunión del pasado 22 de abril de los corrientes, se modificaron los DNS externos hacia el servicio umbrela.*
- *Posterior a ello se cuenta con un router cuyo sistema operativo posee características de seguridad propias del mismo.*
- *Detrás del router se encuentra un dispositivo IPS (Intrusion prevention system) por sus siglas en inglés, el cual analiza el tráfico y su comportamiento.*
- *Luego de esas capas se cuenta con un firewall de nueva generación que analiza el tráfico en cuanto a reglas de acceso, inteligencia de aprendizaje y reglas de aprendizaje heredada.*
- *El antivirus y las consolas de URL que se encuentra en línea que verifican el estado constante de equipos y consultas hacia internet de los usuarios en tiempo real.*
- *Parcheo de sistemas operativos y aplicaciones (office, java, adobe, etc.)*
- *Monitoreo y testeo diario de la red incluyendo análisis de vulnerabilidades*
- *Aplicación de alertas técnicas del MICITT (SCIRT).*

En caso de ataques depende del tipo de ataque:
Por ejemplo:

- *Un equipo usuario puntual que sea atacado debe ser desconectado y escaneado a profundidad y en su momento se define si debe ser reinstalado, parcheado o puesto en cuarentena.*

- *Un servidor físico debe de verse si es un servicio, aplicativo, puerto o usuario específico el que se ve afectado o bien una vulnerabilidad del sistema operativo y proceder a efectuar las correcciones del caso o restablecer los mismos desde un respaldo.*
- *Un servidor virtualizado, puede devolverse a su estado anterior y recuperarse desde un respaldo de sus datos o de la imagen de la máquina virtual como tal.*
- *En caso de servicios contratados en nube, la recuperación de los mismos depende del proveedor como tal.*

En todos estos casos se tiene el acompañamiento de los proveedores y casas matrices. A raíz de los riesgos valorados, contamos con una matriz de riesgos (adjunta) y se invierte anualmente en hardware, software de seguridad, software de respaldos y soporte técnico de terceros."

3.18 La Seguridad Informática, es un tema considerado de riesgo alto, es por ello que esta Auditoría Interna, mediante informe no. AI-009-2021, recomendó lo siguiente:

Número de recomendación	Detalle de la recomendación	Riesgo
2	*Realizar las gestiones que correspondan para contar con el contenido presupuestario, para llevar a cabo las pruebas de penetración Interna y externa de la infraestructura tecnológica del INVU y situación actual de los riesgos, con el objetivo de minimizar los riesgos y la vulnerabilidad de la infraestructura tecnológica.*	Alto

Fuente: Informe AI-009-2021.

3.19 Al respecto, en consulta efectuada en el Sistema Integrado de Compra Públicas (SICOP), se evidenció que el proceso de contratación se está efectuando mediante el número de procedimiento 2022CD-000020-0005800001 denominado *"Contratación de Servicios para el Análisis de Vulnerabilidades del INVU"*, el cual fue adjudicado y se giró la orden de inicio según oficio DAF-UAYC-144-2022.

3.20 Como complemento al párrafo anterior, es importante indicar que, la Encargada de la Unidad de Tecnología de Información, manifestó lo siguiente con respecto al avance de la iniciativa en mención:

"ITI-14: se está gestionando la contratación no. 2022CD-000020-0005800001 denominado "Contratación de Servicios para el Análisis de Vulnerabilidades del INVU", ya se realizó el estudio del exterior y se tienen un primer resultado con oportunidades de mejora."

3.21 Sobre el particular, las buenas prácticas de Gobierno de Tecnologías de Información incluidas en COBIT 5, indican lo siguiente sobre el tema de seguridad de la red:

"DSS05.02 Gestionar la seguridad de la red y las conexiones. Utilizar medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión. (...) 8. Realizar pruebas de intrusión periódicas para determinar la adecuación de la protección de la red. 9. Realizar pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema."

3.22 Aunado a lo anterior, las buenas prácticas también encomiendan la importancia de realizar periódicamente ejercicios[3] de intrusión/hacking ético sobre su plataforma tecnológica; a los sistemas más críticos y con especial atención en aquellos que sean directamente accesibles desde Internet.

3.23 Por su parte, las buenas prácticas desarrolladas por ISACA[4] hablan sobre la importancia de estar protegidos ante ciberataques o ser capaz de detectarlos es igualmente fundamental que la capacidad de reacción, tratamiento y respuesta ante los mismos. Por eso las organizaciones deben contar con adecuados procedimientos para gestionar incidentes, que incluyan al menos:

> *"**a. Su correcta identificación y clasificación:** una estimación de su posible impacto (financiero, regulatorio, reputacional).*
> ***b. Protocolos para su tratamiento**: comités de crisis, cascada de llamadas y análisis (investigaciones forenses, activación de la póliza de un ciberseguro o de fraude).*
> ***c. Notificación y escalado de los incidentes:** incluyendo posibles comunicaciones a clientes, medios de comunicación, organismos reguladores y alta dirección (Consejo de Administración y Comisión de Auditoría).*
> ***d. Mecanismos, medidas y procedimientos para su mitigación:** como activación de Planes de Continuidad de Negocio (PCN) y de Contingencia Tecnológica (PCT), o aislamiento parcial y/o total de los sistemas expuestos a Internet."*

3.24 El contar con los lineamientos para la seguridad de la información y la seguridad informática en la Unidad de Tecnología de Información, permiten que la institución mitigue los riesgos ante ciberataques, que sea capaz de detectarlos y tener capacidad de reacción, tratamiento y respuesta ante esta posible situación.

3.25 En esta oportunidad de mejora no se presentará recomendación dado que en el informe AI-009-2021 denominado *"Análisis de las gestiones de la Unidad de Tecnología de Información para el resguardo y Seguridad de la Información"* se comunicó la recomendación No. 2, a la cual se le estará brindando seguimiento en el Estudio de Auditoría denominado "Seguimiento de recomendaciones" (Ver párrafo 3.18).

3.26 Finalmente, es importante destacar que el Área de Fiscalización para el Desarrollo de las Capacidades de la División de Fiscalización Operativa y Evaluativa de la Contraloría General de la Republica solicitó un seguimiento de la gestión pública sobre la *"Aplicación de prácticas de seguridad de la información en las instituciones públicas"* mediante la aplicación del*"Instrumento Aplicación de prácticas de seguridad de la Información en las Instituciones Públicas"*, el cual fue suministrado por la Presidencia Ejecutiva del INVU, mediante oficio PE-259-09-2022 del 01 de setiembre de 2022, en donde se rescatan los siguientes aspectos de mejora:

- *"La implementación de lineamientos sobre los roles y responsabilidades de los encargados.*
- *La formalización de: Plan de contingencia, Planes de continuidad de negocio para los servicios críticos de la institución, Planes, procesos y procedimientos para el manejo de incidentes de seguridad*

[3] Estos ejercicios recrean un escenario similar a un ataque real, utilizando las técnicas, herramientas y conocimiento que un ciberdelincuente emplearía, por lo que resultan de gran utilidad para identificar vulnerabilidades de seguridad en la organización y facilitar su corrección y mitigación. Es recomendable que estos ejercicios se realicen desde el exterior y el interior de la organización (conexión a los sistemas como lo estaría un empleado)

[4] ISACA es el Information Systems Audit and Control Association encargado de desarrollar el marco COBIT.

y ciberseguridad, Planes de recuperación de incidentes y los Sitios alternos de procesamiento, de acuerdo al análisis de impacto del negocio.

- *Elaborar una matriz de riesgo de todos los activos relacionados con la información crítica o sensible.*
- *Establecer e implementar mecanismos para la identificación de desviaciones conforme a la tolerancia límite de riesgo definido como aceptable.*
- *Efectuar estudios de impacto sobre el funcionamiento de la entidad, en caso de materializarse riesgos relacionados con la pérdida de activos de información.*
- *Se debe efectuar un programa de concientización vigente hacia el personal sobre la seguridad de la información acorde con los procedimientos y/o políticas de seguridad de la información.*
- *Se debe encriptar la información almacenada clasificada como crítica o sensible; así como, cuando está en tránsito.*
- *Se debe definir e implementar un plan para la gestión de incidentes.*
- *Se debe realizar simulacros o pruebas de manejo de incidentes y contar con indicadores que midan el grado de seguridad alcanzado por la institución con las medidas ejecutadas a partir de los resultados de los simulacros o pruebas de incidentes.*
- *Se debe establecer un plan de capacitación institucional sobre temas de ciberseguridad, así como brindar capacitación sobre ciberseguridad periódica al personal."*

C) Monitoreo y seguimiento con indicadores

3.27 La Junta Directiva del INVU mediante el artículo II), inciso b) de la Sesión Ordinaria no. 6380, celebrada el 09 de mayo de 2019, acordó que la Unidad de Tecnología de Información, en conjunto con la Unidad de Planificación Institucional, construyeran una herramienta de monitoreo y seguimiento con indicadores objetivamente verificables para el cumplimiento del PETI.

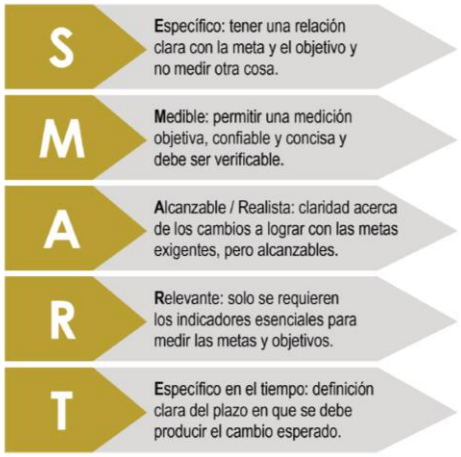
3.28 No obstante, se observó que, en el PETI, se cuenta con Unidades de Medida las cuales no se consideran en la gestión que realiza la Unidad de Tecnología de Información, debido a que su formulación es imprecisa; sin embargo, estas se pueden ajustar para contribuir con el seguimiento de las iniciativas plasmadas en el PETI.

3.29 Al respecto, se le consultó a la Encargada de la Unidad de Tecnología de la Información sobre el manejo de las unidades de medida contenidas en el PETI. Sobre el particular, manifestó lo siguiente:

> *"No se consideran en los Informes de Seguimiento debido a que como se encuentran las unidades de medida planteadas en el PETI presentan ambigüedad. El acuerdo de Junta Directiva de la Sesión Ordinaria no. 6380, articulo II, inciso 1), punto b), se pretende atender mediante la compra del software solicitado por Planificación Institucional, el cual se incluyó en el presupuesto 2022 no obstante no se le brindó contenido, y se planteó nuevamente para el 2023."*
>
> (El subrayado no pertenece al texto original)

3.30 Por su parte, la *"Guía de Indicadores"* del Ministerio de Planificación Nacional y Política Económica, establece que los indicadores deben cumplir con ciertos atributos o características basadas en el modelo SMART. A continuación, se detallan los atributos descritos en la citada guía:

Imagen no. 1
Características SMART de un indicador



Fuente: Mideplan con base en Jacoby (2008).

3.31 Adicionalmente, las buenas prácticas incluidas en COBIT, indican lo siguiente sobre Monitorear y evaluar el desempeño de TI:

> *"Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas."*

3.32 El tener indicadores y metas claramente definidas permiten dar un seguimiento adecuado al cumplimiento del PETI. Además, estas herramientas validan las acciones que se realizan para el cumplimiento de las estrategias y permiten tomar decisiones estratégicas sobre las oportunidades de mejora identificadas para cumplir con las metas trazadas.

IV. CONCLUSIONES

4.1 De conformidad con los resultados obtenidos, se formulan los siguientes comentarios:

4.2 El cumplimiento de los proyectos del PETI podría ser similar al del I Semestre 2021 (58%), debido a que durante el 2022 no se han concluido iniciativas según lo indicado por la Encargada de la UTI.

4.3 Además, se determinó que el INVU no cuenta con Marco de Gestión de las Tecnologías de Información y Comunicación debidamente declarado, aprobado y divulgado, según lo propuesto en el PETI y lo dictado por la Contraloría General de la República.

4.4 Por último, el primer seguimiento a las recomendaciones de la Unidad de Tecnología de Información se brindó mediante el Informe No. AI-006-2022, efectuado por esta Auditoría Interna en junio de 2022, y el segundo seguimiento se le brindará a las citadas recomendaciones, será durante el último bimestre de 2022.

V. RECOMENDACIONES

5.1 Para implementar las oportunidades de mejora planteadas en el presente informe, se proponen las siguientes recomendaciones, las cuales, de ser aplicadas de forma efectiva, agregarán un importante valor a la gestión y al robustecimiento de la Unidad de Tecnología de Información.

A la **Encargada de la Unidad de Tecnología de Información** o a quien, en su lugar, ocupe el cargo:

Número de recomendación	Detalle de la recomendación	Riesgo	Plazo de Implementación
1	Realizar el análisis y ajuste que corresponda, con la finalidad de que las Unidades de medida indicadas en el PETI contengan los atributos SMART y permitan evaluar el cumplimiento de las iniciativas de la Unidad de Tecnología de Información. ***Ver Oportunidad de Mejora No. 1: Párrafos del 3.27 al 3.32***	Medio	31 de marzo de 2023

El presente estudio estuvo a cargo del Lic. Rodrigo Quirós Torres, Profesional Especialista, asistido por la funcionaria María Fernanda Jiménez Espinoza y supervisado por el señor Henry Arley Pérez, Auditor Interno.

HENRY ARLEY PEREZ (FIRMA)

Firmado digitalmente por HENRY ARLEY PEREZ (FIRMA)
Fecha: 2022.11.07 09:39:18 -06'00'

VI. ANEXOS

Anexo No. 1
Resumen del porcentaje de cumplimiento de las iniciativas del PETI a julio 2021.

Porcentaje de cumplimiento	Planificación propuesta en el PETI					Iniciativas o Proyectos
	2019	2020	2021	2022	2023	
0%			■	■	■	ITI-01 Implementación de un marco de referencia para la gobernabilidad de TI.
	■					ITI-05 Diagramar las relaciones existentes (interfaces) entre los sistemas de información.
	■	■	■			ITI-10 Diagnóstico de la gestión de las TI basado en Normas Técnicas y el plan de implementación de cierre de brechas.
	■	■	■	■		ITI-11 Implementación de planes de acción para cerrar las brechas en la gestión de las TI.
			■			ITI-12 Constituir un marco de actuación apropiado para la Unidad de TI ante eventos que repercutan directamente el entorno operativo.
		■				ITI-14 Establecer configuraciones de seguridad en la plataforma crítica.
De 01% a 25%	-					No se presentan iniciativas en este rango.
De 26% a 50%				■		ITI-13 Estudio de centros de datos alternos.
De 51% a 75%		■				ITI-18 Definir un esquema de servicios tercerizados.
De 76% a 99%	-					No se presentan iniciativas en este rango.
100%		■	■	■	■	ITI-02 Definir una cartera de proyectos anual en conjunto con las áreas, departamentos, unidades y procesos que responda a las capacidades de la Unidad de TI.*
	■					ITI-03 Levantamiento de inventario de sistemas de información.
	■					ITI-04 Identificación de sistemas legado.
			■	■	■	ITI-06 Diseñar e implementar un modelo de servicios.
		■				ITI-07 Establecer la mesa de servicio.
	■					ITI-08 Implementar un programa de comunicación que propicie la mejora continua en el servicio al cliente interno.*
		■	■			ITI-09 Desarrollar una metodología de proyectos de la Unidad de TI que permita gestionar los requerimientos institucionales.*
		■				ITI-15 Implementar un modelo de gestión de parches y vulnerabilidades.*
	■	■				ITI-16 Actualización del marco normativo de seguridad informática (Normas Técnicas).*
				■	■	ITI-17 Definición de la metodología de desarrollo generalizada (pasos básicos para el desarrollo).*
	■					ITI-19 Diseñar e implementar un plan de formación para mejorar la continuidad, eficiencia y productividad de las personas involucradas en la prestación de los servicios de la Unidad de TI.*

Fuente: Oficio GG-TI-050-2021 del 23 de julio de 2021 e información suministrada en minuta de entrevista del 31 de agosto de 2022. *Iniciativas que se encuentran pendientes de pendientes de revisión por parte del Comité de TI y de aprobación de la Junta Directiva, según lo indicado por la Encargada de la Unidad de Tecnología de Información.