ADV-002-2025
09 de mayo del 2025

Señora
Angela Mata Montero
Presidenta Ejecutiva
Instituto Nacional de Vivienda y Urbanismo

Estimada señora:

Reciba un cordial saludo.

En atención al cumplimiento del sistema de control interno y a lo dispuesto en el artículo 22 inciso d) de la Ley General de Control Interno (Ley N.º 8292), esta Auditoría Interna emite la presente advertencia en razón de la falta de un Marco de gestión de tecnologías de información, ausencia de políticas de Tecnología de información y obsolescencia del Plan Estratégico de TI (PETI), aunado a lo anterior, se advierte a la Presidencia Ejecutiva sobre los riesgos identificados en la gestión de Tecnologías de Información (TI).

La Ley General de Control Interno, Ley N.º 8292, faculta a esta Auditoría para alertar sobre las posibles consecuencias de acciones u omisiones institucionales en materia de control interno, disposiciones de acatamiento obligatorio. Asimismo, el artículo 36 del mismo cuerpo normativo, establece la obligatoriedad de atender las recomendaciones de Auditoría Interna en plazos perentorios, disponiendo que los responsables implementen las medidas correctivas en los plazos correspondientes. En observancia de estas disposiciones, se emite la presente advertencia, para instar la pronta corrección de las debilidades de control interno detectadas.

Hallazgos Críticos que se han comunicado y no han sido implementados:

1. **Hallazgo no. 1: Ausencia de un Marco de Gestión de Tecnologías de Información**: No se ha establecido ni aprobado un Marco de Gestión de Tecnologías de Información integral para la Unidad de TI, incumpliendo con las Normas de Control Interno aplicables y las Normas técnicas para la gestión y el control de las tecnologías de la información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT).

   El ítem 5.9 de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), modificado por resolución N.° **R-DC-17-2020** de la Contraloría General de la República, exige que cada entidad apruebe y ponga en práctica un marco de gestión de TI adecuado a su perfil. Incluso se dispuso, mediante el Transitorio I de dicha resolución, que todas las instituciones sujetas a fiscalización de la Contraloría General de la República debían declarar, aprobar y divulgar su marco de gestión de TIC a más tardar el **1° de enero de 2022**. A la fecha, el INVU no cuenta con ese marco formal. Esta falencia implica que la gestión de TI carece de una estructura de gobierno definida (procesos, roles, controles y métricas claramente establecidos), lo cual puede derivar en decisiones descoordinadas, duplicidad de esfuerzos, vulnerabilidades de seguridad y falta de rendición de cuentas en el ámbito tecnológico.

   De acuerdo con la ausencia de un Marco de Gestión de TI, el Encargado de la Unidad de Tecnología de Información, mediante oficio GG-TI-012-2025 de fecha 10 de abril de 2025, manifestó lo siguiente:

   > *"Con respecto a las normas técnicas del Micitt, debo indicar que el año anterior se realizó una contratación con el objetivo de lograr el Diseño del Marco de Gestión de Tecnología de Información el Instituto Nacional de Vivienda y Urbanismo (INVU), así como el establecimiento de la hoja de ruta de implementación, para el cierre de brechas y cumplimiento regulatorio. Se incluye referencia la documentación correspondiente con los entregables de dicha contratación*
   > *Aunque se trató de iniciar con un nuevo proceso de contratación, no se concretó y se incluyó en lista de proyectos para el 2025. Actualmente se está en revisión de alcance, para montar un pliego en SICOP que permita abarcar las tareas*

necesarias de implementación según hoja de ruta mencionada, puesto que está definida para varios años." (El subrayado no pertenece al original)

2. **Hallazgo no. 2: Ausencia de Políticas de Tecnología de Información (TI)**: Se evidenció la ausencia de aprobación formal en múltiples políticas institucionales de TI. En el oficio AI-078-2025 la Auditoría Interna detalló un listado de políticas cuyos registros carecen de firma de revisión y aprobación por la autoridad competente (ej: **la Junta Directiva**). Esta situación implica que dichas políticas no tienen validez jurídica ni operativa plena, dejando vacíos en la gobernanza de procesos críticos de TI. Además, contraviene los deberes legales institucionales establecidos en la normativa de control interno sobre documentar, actualizar y divulgar las políticas institucionales, lo que debilita el ambiente de control interno, tomando en consideración que estas políticas deben estar alineadas al Marco de Gestión de Tecnologías de Información, el cual como ya se indicó en hallazgo número 1 no se ha establecido ni aprobado.

   Sobre las Políticas de TI, el Encargado de la Unidad de Tecnología de Información, mediante oficio GG-TI-012-2025 de fecha 10 de abril de 2025, manifestó lo siguiente

   "(…) La documentación referenciada, pese a tener varios años de haberse creado, modificado y ajustado, por razones diversas no se ha remitido a Junta Directiva para su aprobación final. Actualmente, producto de labores de revisión y ajustes solicitados por la Comisión de Tecnología de Información, se encuentra cerca de concluir labores para realizar la remisión indicada."

3. **Hallazgo no. 3: Obsolescencia del Plan Estratégico de TI (PETI)**: El Plan Estratégico de Tecnologías de Información del INVU **2018-2022**[1], se encuentra desactualizado y ha cumplido su periodo de validez sin una renovación oportuna, adicionalmente, parte de sus iniciativas no fueron implementadas. Se constató que proyectos críticos contemplados en el PETI – por ejemplo, el plan de continuidad de TI – no se llevaron a cabo en los años 2020-2021, esto revela un rezago significativo, la institución ha estado operando sin una planificación estratégica de TI actualizada, lo que conlleva falta de alineación entre las inversiones tecnológicas y los objetivos institucionales, posibles redundancias o carencias en soluciones tecnológicas, y una visión poco clara para el desarrollo futuro en materia de TI.

Marco legal relacionado

Desde el punto de vista legal, normativo, los hallazgos anteriores constituyen **incumplimientos serios** de las obligaciones del INVU en materia de control interno y gestión de TI:

- **Ley General de Control Interno (LGCI), N° 8292:** Esta ley establece los pilares de la responsabilidad en control interno. En particular, dispone que **el jerarca y los titulares subordinados son responsables de establecer, mantener, perfeccionar y evaluar el sistema de control interno** en la institución. La ausencia de un Marco de Gestión, políticas de TI alineadas y aprobadas y un PETI vigente, contradice el deber de seguimiento (Artículo 17 de la citada Ley), la rendición de cuentas y el deber de mantener procedimientos y mecanismos de control actualizados. Además, el artículo 16 de la LGCI establece que los entes fiscalizados cuenten con sistemas de información que permitan cumplir sus objetivos y controlar su gestión, lo que implica una gestión tecnológica adecuada.

[1] Inicialmente el PETI estaba programado para iniciar en el 2018; no obstante, este fue aprobado por la Junta Directiva del INVU en el 2019 (Sesión Ordinaria No.6380, artículo 2, inciso I), celebrada el 09 de mayo de 2019.

- **Normas técnicas para la gestión y el control de las tecnologías de la información,** (elaboradas por el MICITT): Estas normas establecen lo siguiente:

"**ALCANCE**

Este Marco Normativo es de acatamiento obligatorio para las instituciones y órganos sujetos a la fiscalización de la Contraloría General de la República, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable. (El subrayado no pertenece al original)

RESPONSABILIDADES

La responsabilidad de las instancias institucionales en materia de Tecnologías de Información y comunicaciones como ente rector dentro de la organización, es velar por la implementación y seguimiento del Marco Normativo para la aplicación de sanas prácticas y adecuar su realidad basándose en este documento como referencia.

El máximo jerarca institucional, es responsable del establecimiento del Gobierno Corporativo que apoye y supervise la adecuada implementación de Marco Normativo y su gestión, por parte de la instancia competente en materia de TI.

PRINCIPIO DE CUMPLIMIENTO

El Marco Normativo de Gobierno y Gestión de las Tecnologías de Información orienta a la institución en la implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva los servicios brindados a través del uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo. Para el proceso de implementación es necesario tener conocimiento sobre la gestión institucional, naturaleza, tamaño y complejidad, volumen de operaciones y cómo esta se apoya en su operativa con el uso de los recursos tecnológicos y su nivel de dependencia. Este proceso puede ser progresivo, debidamente planificado, de acuerdo con las prioridades institucionales, criticidad de los procesos y riesgos asociados al uso de recursos tecnológicos y los servicios requeridos que se brindan a través de la gestión de TI." (El subrayado no pertenece al original).

(…)

PROCESOS DEL MARCO DE GESTIÓN DE TI

Para asegurar la disponibilidad del Marco de Gestión de Tecnología de Información Institucional, la institución debe establecer los procesos al nivel de Tecnologías de información, que permitan brindar servicios efectivos para mantener la operativa institucional, salvaguardar los datos que se capturan, procesan, organizan, distribuyen y resguardan.

I. GOBERNANZA DE TI

La institución debe disponer de un marco orientador que permita la definición de la acción institucional con un enfoque de valor público. Asimismo, debe considerar en la estrategia institucional la incorporación de iniciativas habilitadas por tecnologías de información.

La entidad pública debe tener un órgano rector que permita establecer las prioridades en cuanto al cumplimiento de estrategias propuestas por tecnologías de información; debidamente conformado por las autoridades institucionales administrativas competentes según corresponda a cada institución, participando a los titulares responsables de la Planificación Institucional y de las tecnologías de información y comunicaciones como un asesor en los modelos de habilitación de los objetivos, necesidades y oportunidades institucionales a través del uso de TI, así como elementos para la rendición de cuentas sobre el uso adecuado de las TI para responder a las necesidades, objetivos y oportunidades institucionales.

La conceptualización de este órgano rector debe ser una instancia de alto nivel que busca habilitar la gobernanza en torno a las Tecnologías de la Información y Comunicaciones (TIC), estableciendo un espacio

de diálogo y coordinación entre las gerencias de la institución y la unidad responsable de las Tecnologías de Información y Comunicaciones (DTIC), con el fin de asegurar el apoyo de las TIC a la gestión y el cumplimiento de la estrategia institucional. Al estar integrado por las máximas autoridades de gobierno y administración de la Institución, junto con la unidad de Tecnologías de la Información y Comunicaciones, y la Dirección de Planificación Institucional asume como cuerpo colegiado, la toma de decisiones sobre temas estratégicos asociados con las TIC que inciden en la prestación de los servicios a los usuarios. (…)"

- **Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE):** Estas normas, emitidas por la Contraloría General de la República (CGR), refieren a disposiciones específicas sobre información y tecnología. Las Normas vigentes establecen que se garantice la **confiabilidad, oportunidad, seguridad, acceso y protección de la información** institucional. Contar con políticas sin aprobar, desactualizadas o inexistentes y carecer de una planificación estratégica de TI atenta contra la confiabilidad y seguridad de la información, ya que no hay directrices claras para su manejo ni planes para su continuidad.

Cabe destacar que mediante la **Resolución R-DC-17-2020** (Despacho Contralor, marzo 2020), la CGR **derogó** expresamente las antiguas "Normas Técnicas para la Gestión y el Control de las TI" de 2007, e incorporó nuevas obligaciones en las Normas de Control Interno (N-2-2009) para reforzar la gobernanza de TI. En particular, **modificó los ítems 5.9 y 5.10**, estableciendo lo siguiente:

- **Ítem 5.9 – Tecnologías de Información:** El jerarca y sus subordinados *"deben propiciar el aprovechamiento de las tecnologías de información que apoyen la gestión institucional... En todo caso, deben instaurarse los mecanismos y procedimientos... que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información"*. Adicionalmente, *"se exige que el jerarca **apruebe el marco de gestión de tecnologías de información** de la institución y establezca un proceso para implementar gradualmente cada uno de sus componentes"*. Esto significa que cada ente público debe contar con un marco de gestión de TI integral y formal, acorde con su realidad (perfil tecnológico), que incluya políticas, procedimientos, estructuras organizativas, planes y controles para asegurar una adecuada administración de la tecnología. La resolución sugiere variables a considerar en dicho marco: un marco de procesos de gestión de TI, mapeo de procesos de negocio, organigrama, comité de TI, inventario de servicios y activos tecnológicos, proyectos de TI, plan de adquisiciones, análisis de riesgos de TI, entre otros. La **falta de este marco en el INVU** constituye un incumplimiento directo de esta norma actualizada. (El subrayado y resaltado no pertenece al original)

- **Ítem 5.10 – Sistemas de información en instituciones de menor tamaño:** Para entes públicos de pequeña envergadura, la norma permite un enfoque proporcional, disponiendo que *el jerarca debe establecer los procedimientos manuales o automatizados necesarios para obtener, procesar, almacenar y comunicar la información de la gestión institucional*, asegurando que dicha información esté accesible y ordenada conforme a las regulaciones archivísticas nacionales. Si bien el INVU no calificaría como institución de muy menor tamaño, esta disposición refuerza la idea de que **todas** las entidades públicas, sin excepción, deben contar al menos con procedimientos formales para gestionar su información y tecnología según su escala. En el caso del INVU, con una UTI establecida, la expectativa normativa recae en el desarrollo completo del marco de gestión de TI del punto 5.9.

  Importa resaltar que la **Resolución R-DC-17-2020** incluyó un **Transitorio I** que otorgó a todas las instituciones un plazo perentorio para adecuarse: a más tardar el **1° de enero de 2022** debían tener *"declarado, aprobado y divulgado"* su marco de gestión de tecnologías de información. Transcurrido ampliamente dicho plazo, la **ausencia de un marco de gestión de TI en el INVU** implica una contravención a una disposición expresa de la Contraloría General de la República.

  En síntesis, desde la perspectiva normativa, el INVU está obligado por ley y disposiciones técnicas a contar con un marco de gestión de TI robusto políticas de TI alineadas al citado Marco, formalmente aprobadas y divulgadas, a mantener actualizado su plan estratégico de informática. La situación actual de incumplimiento en esos tres aspectos contradice los mandatos de la LGCI y de las Normas de Control Interno, tanto en su versión

vigente (post R-DC-17-2020) como en los principios básicos preexistentes. Esto configura un escenario de **debilidad de control interno** en el área de TI y expone a la Institución a múltiples consecuencias adversas.

Buenas prácticas

Desde el punto de vista de las buenas prácticas, los hallazgos descritos en la presente advertencia permiten generar las oportunidades de mejora para mitigar los riesgos identificados. Por ejemplo:

- **Buenas Prácticas establecidas en la ISO/IEC 27001 y 27002 (Seguridad de la Información)**: El estándar ISO/IEC 27001 insta a las organizaciones establecer un **Sistema de Gestión de Seguridad de la Información (SGSI)**, que incluye políticas, procedimientos, evaluaciones de riesgo, controles y mejora continua. Uno de los controles fundamentales es contar con una **política de seguridad de la información** aprobadas, publicadas y comunicadas a todo el personal. El hecho de que las políticas de TI del INVU no estén aprobadas formalmente contradice este requisito internacionalmente aceptado. Asimismo, ISO 27001/27002 dedica un dominio completo a la **continuidad del negocio,** enfatizando que la organización debe **desarrollar, implementar y mantener planes de continuidad y recuperación ante desastres**, probándolos regularmente, para asegurar la disponibilidad de la información y los servicios en caso de incidente grave.

- **Buenas prácticas de gobierno de TI (COBIT 2019)**: COBIT es un marco de referencia para el gobierno y la gestión de TI en las organizaciones, que define procesos, prácticas y métricas para asegurar que la TI aporte valor al negocio y mitigue sus riesgos. Varias áreas de COBIT son relevantes a los hallazgos:

    - **Alineación estratégica** (**APO** – *Align, Plan, Organise*): El proceso *APO02 Gestionar la Estrategia* insta a desarrollar y mantener un plan estratégico de TI alineado con la estrategia institucional. No tener un PETI vigente se contrapone con esta buena práctica, arriesgando inversiones TI mal dirigidas o insuficientes.
    - **Gestión de la Seguridad (APO13 y DSS05)**: COBIT señala que debe establecerse una función de seguridad de la información con políticas y procedimientos. En particular, *APO13 Gestionar Seguridad* cubre la definición de una estrategia y políticas de seguridad coherentes con los objetivos de negocio, y *DSS05 Garantizar la Seguridad de los Servicios* abarca la operación segura de la infraestructura. La ausencia de políticas aprobadas refleja deficiencias en estos ámbitos. COBIT recomienda, por ejemplo, **gestionar la seguridad de la red y conexiones mediante controles y procedimientos adecuados en todo momento**, algo que difícilmente se logra sin evaluaciones técnicas como pentests.
    - **Gestión de Continuidad (DSS04)**: El proceso *DSS04 Gestionar la Continuidad* establece que se deben desarrollar y mantener planes de continuidad de negocio y recuperación de TI, alineados con prioridades del negocio, y probarlos regularmente. El INVU no cumple con esta práctica, careciendo de planes actualizados y pruebas (simulacros) de continuidad, lo que deja a la organización en una situación vulnerable ante interrupciones.
    - **Mejora continua y cumplimiento (MEA** – *Monitor, Evaluate, Assess*): COBIT enfatiza monitorear el cumplimiento de requisitos externos e internos. Tras la derogación de las Normas Técnicas específicas, el INVU debería analizar los estándares internacionales para llenar el vacío normativo. No hacerlo implicaría no aplicar el principio de mejora continua ni de evaluación de cumplimiento que COBIT sugiere.

Al respecto, la Contraloría General de la República se ha manifestado en diversos estudios relacionados con el índice de capacidad de gestión de las TI, haciendo énfasis en que las instituciones deben aprovechar las TI para generar valor en la satisfacción de las necesidades ciudadanas, a través de la generación de estrategias, gobernanza, seguridad de la información y la atención de los riesgos relacionados.

Además, las supervisiones a las que están sujetas las instituciones del sector público, exige contar con un perfil tecnológico definido y actualizado anualmente.

La CGR destaca que la capacidad de gestión de TI está directamente vinculada con la seguridad de la información, que es esencial para proteger la confidencialidad, integridad y disponibilidad de los datos sensibles, fundamentalmente para la toma de decisiones, el desarrollo económico y la seguridad ciudadana.

El no contar con un Marco de gestión de TI, la carencia en políticas de seguridad de la información aprobadas y el no tener una definición clara de sus servicios críticos, dificulta la toma de decisiones rápidas y efectivas, incrementando el riesgo de que funciones clave se vean comprometidas, afectando la continuidad del negocio.

Riesgos Institucionales, Legales y Operativos

La falta de atención a las áreas críticas descritas conlleva consecuencias institucionales significativas y diversos riesgos en el ámbito operativo, legal y reputacional:

- Consecuencias institucionales: Un entorno de TI mal gobernado impacta la capacidad del INVU, para cumplir su misión, sin políticas claras ni un plan estratégico vigente, las iniciativas tecnológicas pueden ser inconsistentes o desalineadas de los objetivos institucionales. Esto se traduce en pérdida de eficiencia, duplicidad de esfuerzos o retraso en proyectos clave de modernización (por ejemplo, sistemas para mejorar servicios habitacionales). Además, la inacción frente a recomendaciones de mejora debilita la cultura de control interno y puede generar señalamientos de los entes rectores, afectando la gobernabilidad interna.

  En línea con lo anterior las Normas técnicas para la gestión y el control de las tecnologías de la información establecen en el proceso "*GESTIÓN DE RIESGOS TECNOLÓGICOS*, lo siguiente:

  "La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el marco normativo que le resulte aplicable.

  La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución." (El subrayado no pertenece al original).

- **Riesgos Institucionales:** La falta de un Marco de Gestión, políticas aprobadas y de un PETI vigente crea un vacío en la dirección estratégica de la UTI. Sin un marco normativo claro, el personal puede operar con criterios disímiles o desactualizados, afectando la eficiencia y calidad de los servicios tecnológicos. Asimismo, un PETI obsoleto impide planificar adecuadamente proyectos prioritarios, exponiendo a la institución a rezagos tecnológicos, sobrecostos inesperados y dificultades para cumplir su misión en materia de vivienda y urbanismo apoyada por sistemas de información modernos.

- **Riesgos Legales:** La inobservancia de la Ley de Control Interno, las Normas de control interno y demás normativa de control interno, **debilitan el sistema de control interno o si omite las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo**. La falta de un marco de gestión de TI (exigido por la CGR) y la no actualización del PETI constituyen eventuales incumplimientos de las obligaciones de control y supervisión.

- **Riesgos Operativos:** Operativamente, las brechas señaladas incrementan la probabilidad de fallas e incidentes en TI. La ausencia de un marco de gestión de TI, políticas actualizadas en áreas como seguridad de la información, gestión de proyectos o continuidad del negocio deja a la institución sin lineamientos claros para prevenir y responder ante eventos adversos (por ejemplo, ciberataques o caídas de sistemas críticos). De igual forma, no contar con un plan estratégico vigente, limita la capacidad de reacción y adaptación tecnológica del INVU, pudiendo afectar la continuidad de los servicios a los usuarios internos y ciudadanos. En síntesis, la inacción **prolongada** ante estos hallazgos podría materializarse en interrupciones de operaciones, pérdida de información, uso ineficiente de recursos públicos **e incumplimiento de metas institucionales**.

Advertencia 002

Al respecto, de conformidad con lo que establece el artículo 22 inciso d) de la Ley General de Control Interno (Competencias de las Auditorías Internas), que, en lo que interesa indica: "(...) ***advertir a los órganos pasivos que fiscaliza sobre las posibles consecuencias de determinadas conductas o decisiones cuando sean de su conocimiento*** *(...)",* nos permitimos advertirle a la Presidenta Ejecutiva, que la ausencia de un Marco de Gestión de Tecnologías de Información que es de acatamiento obligatorio, genera incumplimientos normativos, debilita el sistema de control interno y por ende genera un nivel de riesgo muy alto, por lo que es de suma importancia que se tomen las acciones correctivas que correspondan, para mitigar los hallazgos indicados en el presente documento.

Recomendaciones a la Presidenta Ejecutiva

1. Instruir a la administración activa y brindar el seguimiento hasta su conclusión; para que se elabore y presente un plan remedial que establezca, implemente y apruebe formalmente un Marco de Gestión de Tecnologías de Información, el cual cumpla con los 14 procesos establecidos por las Normas técnicas para la gestión y el control de las tecnologías de la información, que se detallan de forma seguida:

1. Gobernanza de Ti,
2. Gestión de Ti,
3. Planificación Tecnológica Institucional,
4. Gestión de Riesgos Tecnológicos,
5. Arquitectura Empresarial,
6. Calidad de los Procesos Tecnológicos,
7. Recursos Humanos,
8. Contratación y Adquisiciones de Bienes y Servicios Tecnológicos,
9. Gestión de Proyectos que Implementan Recursos Tecnológicos,
10. Desarrollo, Implementación y Mantenimiento de Sistema de Información,
11. Seguridad Y Ciberseguridad,
12. Administración Infraestructura Tecnológica,
13. Continuidad Y Disponibilidad Operativa De Los Servicios Tecnológicos;
14. Aseguramiento.

En particular y para un mejor abordaje de lo antes indicado, se le sugiere la valoración, como mínimo, de los siguientes insumos:

- **Marco Normativo de Gestión de Tecnologías de Información**: Presentar una hoja de ruta para que se establezca y apruebe formalmente un Marco de Gestión de Tecnologías de Información, conforme lo establecido por las, las Normas de Control Interno, la resolución R-DC-17-2020 de la Contraloría y las Normas técnicas para la gestión y el control de las tecnologías de la información del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT). Este marco debe definir la estructura de gobierno de TI (los 14 procesos, políticas generales, roles y responsabilidades del personal de TI y usuarios clave). Una vez aprobado por la Junta Directiva, deberá ser **divulgado**. Ello cumplirá con el mandato de haber declarado y difundido dicho marco y proporcionará directrices claras para la administración de TI, reduciendo la incertidumbre actual.

- **Políticas de TI:** Una vez que se cuente con el citado Marco de Gestion de TI, elaborar las políticas de TI alineadas a este y someterlas a la respectiva **aprobación formal** de la Junta Directiva. Esto incluye asegurar que cada política institucional cuente con las firmas de aprobación respectivas y se encuentre debidamente divulgada dentro del INVU. La formalización de estas políticas dotará de respaldo normativo las actuaciones de la Unidad de TI y del personal en general, corrigiendo de inmediato el vacío de autoridad detectado.

- **Plan Estratégico de TI:** Presentar una hoja de ruta para la elaboración del **PETI**, alineado con el Plan Estratégico Institucional. Es importante que se evalúe el cumplimiento del PETI anterior (rendición de cuentas), identificar niveles de cumplimiento e incorporar las iniciativas pendientes que sigan siendo relevantes. Con base en ello, formular un nuevo Plan Estratégico de TI alineado con los objetivos institucionales, con metas claras, cronograma y recursos asignados para su ejecución. Este nuevo PETI debe ser aprobado por la Junta Directiva y divulgado a las unidades correspondientes, de manera que oriente eficazmente la inversión y desarrollo tecnológico en el corto y mediano plazo.

2. Se recomienda que se instruya a la alta administración, para que se establezca un **mecanismo formal** para el seguimiento y rendición de cuentas, (por ejemplo, informes periódicos a Junta Directiva, Comité de Gobernanza de TI, etc.), sobre el avance en la implementación de las medidas anteriores.

3. Presentar, en un plazo no mayor a 30 días hábiles contados a partir de la notificación de la presente advertencia, un informe que detalle las acciones emprendidas en cada uno de los puntos anteriores, adjuntando evidencia correspondiente.

Se adjuntan a esta advertencia los siguientes Anexos, para lo correspondiente:

1. ANEXO No.1 R-DC-17-2020 Derogatoria Normas TI**;**
2. ANEXO No.2 Oficio AI-078-2025-UTI-Estudio Carácter Especial-firmado;
3. ANEXO No.3 Oficio GG-TI-012-2025 Respuesta a AI-078-2025 Estudio Especial Auditoría Interna.

Atentamente,
HENRY ARLEY PEREZ (FIRMA)
Firmado digitalmente por HENRY ARLEY PEREZ (FIRMA)
Fecha: 2025.05.09 15:03:20 -06'00'
Henry Arley Pérez
Auditor Interno.

C: Consecutivo 2025 – Archivo