INSTITUTO NACIONAL DE APRENDIZAJE
AUDITORÍA INTERNA

INFORME DE CONTROL INTERNO

AI-ICI-01-2026

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS DE TI

13 de febrero del 2026

AI-ICI-01-2026

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS DE TI

RESUMEN EJECUTIVO 3

1. INTRODUCCIÓN 4
   1.1 Origen 4
   1.2 Objetivos 4
   1.3 Alcance 4
   1.4 Terminología y siglas utilizadas en el informe 5

2. RESULTADOS 6
   2.1 Desarticulación entre el Plan de Continuidad de Tecnologías de la Información y Comunicaciones (PCTIC) y el Plan de Continuidad del Negocio (PCN) 6
   2.2 Inconsistencias en el análisis de riesgos, tratamientos y planes de acción dentro del PCTIC 11
   2.3 Debilidades en la capacitación, documentación y comunicación del Plan de Continuidad de Tecnologías de Información (PCTIC) 14

3. CONCLUSIONES 17

4. RECOMENDACIONES 18

5. OBSERVACIONES 20
   5.1 Comunicación de resultados, observaciones de la administración y remisión del informe 20
   5.2 Plazo para el avance y ejecución de las recomendaciones 21
   5.3 Responsable del informe 21

Anexo 1 22

RESUMEN EJECUTIVO
GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
GESTIÓN DE LA CONTINUIDAD DE LOS SERVICIOS DE TI

En cumplimiento del Plan Anual de Trabajo de la Auditoría Interna, se realizó un estudio de carácter especial en la Gestión de Continuidad de los Servicios de Tecnologías de la Información, cuyo objetivo fue verificar mediante procedimientos de auditoría, los planes y acciones implementados para establecer y mantener la continuidad de los servicios de tecnología de la información (I&T) en cumplimiento de los niveles de disponibilidad institucional pactados, la normativa vigente y las mejores prácticas.

Para tales efectos se revisó la normativa interna establecida para la gestión de la continuidad, tales como: el Plan de Continuidad del INA, Plan de Continuidad de TI, el Marco Normativo, las Normas Técnicas, entre otros. A los efectos, se verificó el grado de implementación y alineación con las mejores prácticas internacionales.

De acuerdo con el análisis y revisión efectuada, se citan los resultados obtenidos:

- Desarticulación entre el Plan de Continuidad de Tecnologías de la Información y Comunicaciones (PCTIC) y el Plan de Continuidad del Negocio (PCN).
- Inconsistencias en el análisis de riesgos, tratamientos y planes de acción dentro del PCTIC.
- Debilidades en la capacitación, documentación y comunicación del Plan de Continuidad de Tecnologías de Información (PCTIC).

Los resultados evidencian debilidades que afectan la gestión integral de la continuidad institucional, particularmente en la articulación entre el Plan de Continuidad de Tecnologías de la Información y Comunicación (PCTIC) y el Plan de Continuidad del Negocio (PCN). Se identificaron inconsistencias en la definición, documentación y actualización de procesos, así como en la trazabilidad entre los servicios tecnológicos y las actividades clave institucionales.

Asimismo, se detectaron incongruencias en el análisis y tratamiento de riesgos, ausencia de mecanismos efectivos de supervisión y validación por parte de la Alta Gerencia, y limitaciones en la preparación del personal y en la disponibilidad de documentación actualizada para la continuidad de servicios críticos. Estas situaciones reflejan una gobernanza debilitada, falta de estandarización y descoordinación entre áreas, lo que impacta negativamente en la capacidad institucional para responder y recuperarse eficazmente ante eventos disruptivos, comprometiendo la continuidad y la resiliencia organizacional.

Para subsanar las debilidades detectadas se giraron 4 recomendaciones: **una** a la Gerencia, y **tres** a la Gestión de Tecnologías de la Información y Comunicación.

1. INTRODUCCIÓN

1.1 Origen

El presente informe se origina en la ejecución de un estudio de auditoría efectuado en cumplimiento del Plan Anual de Trabajo del año 2025.

1.2 Objetivos

Evaluar mediante procedimientos de auditoría los planes y acciones implementados para establecer y mantener la continuidad de los servicios de tecnología de la información (I&T) en cumplimiento de los niveles de disponibilidad institucional pactados, la normativa vigente y las mejores prácticas.

1.3 Alcance

Se efectuó una auditoría de carácter especial en la Gestión de Tecnologías de la Información y Comunicación (GTIC) en relación con los planes y acciones implementados para establecer y mantener la continuidad de los servicios de tecnología de la información (I&T). El período del estudio abarcó desde enero 2023 hasta diciembre 2024, ampliándose en los casos que se consideró pertinente para una evaluación exhaustiva.

Para tales efectos, se revisó la normativa interna establecida para la gestión de la continuidad, tales como: el Plan de Continuidad del INA, Plan de Continuidad de TI, el Marco Normativo, las Normas Técnicas, entre otros. A los efectos, se verificó el grado de implementación y alineación con las mejores prácticas internacionales.

El estudio fue realizado de acuerdo con las Normas para el Ejercicio de la Auditoría Interna en el Sector Público (NEAISP) y de conformidad con las Normas Generales de Auditoría para el Sector Público (NGAISP), emitidas por la Contraloría General de la República (CGR). Lo anterior, sin perjuicio de la normativa supletoria que aplique según el caso acorde con el ordenamiento jurídico y de otros criterios relevantes como los estándares de aceptación general en la materia que se trate, así como las mejores prácticas reconocidas en los ámbitos técnicos particulares.

Además, en el **anexo 1** se cita la normativa utilizada como base para las revisiones específicas.

1.4 Terminología y siglas utilizadas en el informe

- **BIA (Análisis de impacto en el negocio)**: Proceso para identificar y evaluar los efectos de una interrupción en los procesos críticos de la organización. Del inglés *Business Impact Analysis*.

- **CGI**: Comisión Gerencial Informática

- **GTIC:** Gestión de Tecnologías de la Información y Comunicación.

- **INA:** Instituto Nacional de Aprendizaje.

- **INTE/ISO 22301:2020**: Estándar para Sistemas de Gestión de Continuidad del Negocio, que especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar y mejorar la gestión de continuidad de negocio en una organización. Este estándar ayuda a asegurar que las organizaciones puedan responder eficazmente a interrupciones y mantener operaciones críticas.

- **INTE/ISO/IEC 27031:2017:** Directrices para la Preparación para la Continuidad de los Servicios de Tecnologías de la Información y Comunicación (TIC). Proporciona un marco para mejorar la preparación de TI ante interrupciones, estableciendo pautas para planificar y ejecutar la recuperación de servicios y asegurar la disponibilidad y resiliencia de las tecnologías críticas.

- **MNTTIINA**: Manual de Normas Técnicas de Tecnologías de la Información del Instituto Nacional de Aprendizaje

- **Plan de continuidad de negocio (PCN)**

- **Plan de continuidad de tecnologías de información y comunicación (PCTIC)**

- **RPO:** Punto objetivo de Recuperación. Del inglés, *Recovery Point Objective.*

- **RTO:** Tiempo objetivo de recuperación. Del inglés, *Recovery Time Objective.*

- **Service Desk**: Es un punto de contacto centralizado que gestiona las solicitudes y problemas de tecnología de la información (TI), actuando como interfaz entre los usuarios y el área de TI.

- **Servicio crítico:** Servicio cuya interrupción puede afectar significativamente la operación, reputación o cumplimiento legal de la institución.

- **SLA:** Acuerdo de nivel de servicio. Del inglés, *Service Level Agreement*.

2. RESULTADOS

2.1 Desarticulación entre el Plan de Continuidad de Tecnologías de la Información y Comunicaciones (PCTIC) y el Plan de Continuidad del Negocio (PCN)

La efectividad de la continuidad operativa institucional depende de la alineación estratégica y operativa entre el Plan de Continuidad del Negocio (PCN) y el Plan de Continuidad de Tecnologías de la Información y Comunicaciones (PCTIC). No obstante, se identificó una desarticulación significativa entre ambos instrumentos, evidenciada en los siguientes aspectos:

1. Inconsistencias en la identificación de los procesos institucionales

El análisis comparativo entre el Plan de Continuidad del Negocio (PCN) y el Plan de Continuidad de Tecnologías de Información y Comunicaciones (PCTIC) reveló inconsistencias en el listado de procesos institucionales utilizados como base. Se constató que los procesos descritos en el PCTIC no se alinean con los procesos críticos establecidos en el PCN, y además presentan discrepancias con los procesos formalizados en el Manual Organizacional, la Valoración de Riesgos (SICOI), el Sistema de Gestión de Calidad y la facilitada por la GTIC mediante oficio GTIC-340-2024, al consultarle sobre el flujograma de los procesos de dicha Gestión.

La siguiente tabla evidencia las principales situaciones detectadas:

Cuadro 1. Contraste de identificación de procesos GTIC en instrumentos institucionales

Unidad	Proceso identificado	Manual Organizacional	SICOI	PCN INA	PCTIC	Sistema de Gestión de Calidad (SGC)	Oficio GTIC-340-2024	Observación
Unidad de Servicios de Informática y Telemática	Operación de Servicios	✔	✔	✔	✔	✘	✘	Único proceso con trazabilidad completa entre los instrumentos de continuidad, mas no se ubica en el SGC ni fue confirmado por la GTIC.
Unidad de Servicios de Informática y Telemática	Acciones para mantener la continuidad de los servicios TIC	✘	✔	✔	✔	✘	✘	No se encuentra en el Manual Organizacional.
Unidad de Soporte a Servicios Tecnológicos	Atención de solicitudes del Service Desk	✘	✔	✔	✘	✘	✘	Se encuentra en el SICOI y el PCN, pero no figura en el PCTIC.
Unidad de Servicios Virtuales	Atención de solicitudes de soporte para las plataformas tecnológicas educativas	✘	✔	✔	✔	✘	✘	En el PCTIC el nombre cambia y se limita únicamente a las plataformas educativas.
Unidad de Servicios Virtuales	Centro Virtual de Formación	✘	✘	✘	✔	✘	✘	Identificado solo en el PCTIC como proceso crítico.

Fuente: Elaboración propia con base en el Manual Organizacional, SICOI, PCN INA, PCTIC, Sistema de Gestión de Calidad institucional y oficio GTIC-340-2024.

2. Desfase temporal en las actualizaciones y falta de aprobación formal:

La elaboración del PCTIC se ha basado en versiones desactualizadas del PCN. La versión 5.0 del PCTIC (2021) se construyó utilizando el PCN de 2013, que era la versión vigente al momento de su formulación (8 años de desfase). Por su parte, la versión 6.0 (2024) se desarrolló a partir del PCN de 2022 (2 años de desfase). Cabe indicar, además, que ambas versiones del PCTIC (2021 y 2024) carecen de firmas de aprobación.

3. Ausencia de supervisión y validación gerencial:

Según consta en el historial de revisión del Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC) en su versión 6.0 (2024), la última validación formal por parte de la Comisión Gerencial de Informática (CGI) corresponde a junio del 2014. Las seis actualizaciones posteriores (2016-2024) han sido gestionadas exclusivamente por la Gestión de Tecnologías de Información (GTIC), sin evidencia de revisión, aprobación ni respaldo por parte de la CGI u otra instancia superior. Esta situación fue previamente señalada por auditorías externas realizadas por la empresa Trango en el 2018 y la realizada por Moore-AGC en el año 2025.

4. Deficiencias en la definición y establecimiento de los servicios tecnológicos críticos:

La base para identificar y establecer los servicios de tecnología críticos presenta deficiencias conceptuales y metodológicas.

- El PCTIC utiliza una nomenclatura propia ("identificador de servicio") que no se alinea con el PCN y presenta registros duplicados.

- El Catálogo de Servicios de la GTIC figura entre los principales insumos utilizados para el análisis de continuidad; sin embargo, la definición de los servicios de este catálogo no responde a una conceptualización institucional, pues describe requerimientos e incidencias de los usuarios finales a través del "Service Desk", en lugar de capacidades tecnológicas que sostienen la operación de procesos institucionales. Un ejemplo de esta situación es el correo electrónico (Correo Electrónico-USIT-03), presentado como un conjunto de gestiones de soporte operativo de criticidad baja, sin incorporar una definición del servicio como capacidad tecnológica, con su propósito, alcance y su rol esencial en la comunicación institucional.

- El PCTIC, de la definición del RPO (Objetivo de Punto de Recuperación) para los servicios indicados, un parámetro crítico para la continuidad.

En la Ley General de Control Interno 8292, en su Artículo 15, inciso a), indica como deberes del jerarca y de los titulares subordinados:

> *"Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones".*

En las Normas de Control Interno para el Sector Público, en su Capítulo IV, apartado 4.2.e Documentación, se regula:

> *"Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación".*

Adicionalmente, en el Capítulo V, apartado 5.6 Calidad de la información, se dispone:

> *"El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información contemplen los procesos requeridos para recopilar, procesar y generar información que responda a las necesidades de los distintos usuarios. Dichos procesos deben estar basados en un enfoque de efectividad y de mejoramiento continuo. Los atributos fundamentales de la calidad de la información están referidos a la confiabilidad, oportunidad y utilidad.*
>
> *5.6.1 Confiabilidad: La información debe poseer las cualidades necesarias que la acrediten como confiable, de modo que se encuentre libre de errores, defectos, omisiones y modificaciones no autorizadas, y sea emitida por la instancia competente.*
>
> *5.6.2 Oportunidad: 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.*
>
> *5.6.3 Utilidad: La información debe 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".*

Al respecto, la norma INTE/ISO 22301:2020. Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio – Requisitos, se dispone:

> ***"5.1 Liderazgo y compromiso***
> *La alta dirección debe demostrar liderazgo y compromiso con respecto al SGCN al:*
> *(…)*
> *b) asegurar la integración de los requisitos del SGCN en los procesos de negocio de la organización; (…) //*
>
> ***8.1 Planificación y control operacional***
> *La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos y para implementar las acciones determinadas en el apartado 6.1:*

a) estableciendo criterios para los procesos;
b) implementando el control de los procesos de acuerdo con los criterios;
c) manteniendo la información documentada en la medida necesaria para tener la confianza de que los procesos se han llevado a cabo según lo planeado".

Por otra parte, en su sección 8.2.2 Análisis de Impacto del Negocio (BIA), indica:

"La organización debe implementar y mantener un proceso para analizar el impacto del negocio que: a) define los tipos y criterios de impacto para medir el impacto; b) identifica actividades que apoyan la provisión de productos y servicios; c) analiza los impactos a lo largo del tiempo resultantes de la interrupción de estas actividades; d) identifica el tiempo dentro del cual los impactos de no reanudar las actividades serían inaceptables a la organización; e) establece plazos prioritarios dentro del tiempo identificado en d) anterior para reanudar las actividades interrumpidas a una capacidad mínima aceptable especificada; f) utiliza los impactos comerciales para identificar actividades priorizadas; g) determina qué recursos se necesitan para apoyar las actividades priorizadas; h) determina las dependencias e interdependencias de las actividades priorizadas".

En las normas de INTECO (INTE/ISO/IEC 27031:2 017), Técnicas de seguridad. Directrices para la tecnología y comunicación de preparación para la continuidad del negocio, indica:

"7.2.5 Procesos
Los procesos de la PTCN deberían documentarse claramente y con suficiente detalle para permitir ejecutarlos al personal competente (…) //".

Además, la norma INTE/ISO TS 22317:2016, Seguridad de la sociedad. Sistema de gestión de continuidad del negocio. Directrices para el análisis de impacto al negocio (BIA), enfatiza en:

"5.2.2 Consideraciones iniciales del BIA
Una organización que ejecuta un BIA por primera vez, debe planificar tiempo adicional para:

(…) documentar el flujo de trabajo a nivel de procesos y actividades, y (..)".

La misma norma, en su sección 5.1 Rol del PTCN, indica:

"La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión holístico que identifica los impactos potenciales que amenazan la continuidad de las actividades de negocio de una organización y proporciona un marco de referencia para construir la resiliencia y la capacidad para dar una respuesta efectiva que salvaguarde de interrupciones los intereses de la organización. Como parte del proceso de BCM, la PTCN se refiere a un sistema de gestión que complementa y apoya la BCM de una organización y/o el programa SGSI, para mejorar la preparación de la organización para: a) responder al entorno de riesgo en constante cambio; b) asegurar la continuidad de las operaciones críticas de negocio con el apoyo de los servicios de las TIC relacionados".

Adicionalmente, en el punto 5.4 Resultados y beneficios, inciso g), se menciona:

> *"Proporcionar una confianza adicional en la estrategia de continuidad de negocio a través de la vinculación de la inversión en soluciones de TI a las necesidades de negocio y asegurar que los servicios de las TIC están protegidos en un nivel apropiado, dada su importancia para la organización".*

Adicionalmente, en el punto 6.3.1 Generalidades, indica:

> *"Como parte de su programa de BCM, la organización tendrá categorizadas sus actividades de acuerdo a su prioridad para la continuidad (como se determina por un análisis del impacto al negocio) y definido el nivel mínimo en que cada actividad crítica necesita ser ejecutadas tras la reanudación. La alta dirección debería estar de acuerdo con los requisitos de continuidad de negocio de la organización y estos requisitos darán lugar al tiempo objetivo de recuperación (RTO) y el Punto objetivo de Recuperación (RPO) para el mínimo objetivo de Continuidad de Negocio (MBCO) por producto, servicio o actividad".*

Adicionalmente, en el punto 6.3.2 Comprensión de los servicios críticos de las TIC, se establece:

> *"Puede haber un número de servicios de las TIC que se consideran críticos y necesarios para que la recuperación tenga lugar. Cada uno de estos servicios críticos de las TIC deberían tener documentado su propio tiempo objetivo de recuperación (RTO) y el Punto objetivo de Recuperación (RPO) para el objetivo mínimo de Continuidad de Negocio (MBCO) del servicio de las TIC. (Estos pueden incluir aspectos de la entrega de servicios de las TIC, como la mesa de ayuda). El RTO de los servicios críticos de las TIC será invariablemente menor que el RTO la continuidad del negocio".*

En el punto 6.3.3 Identificación de brechas, se dispone:

> *"Para cada servicio crítico de las TIC los acuerdos actuales de preparación para las TIC - como la prevención, el seguimiento, la detección, respuesta y recuperación - deberían compararse con los requisitos de continuidad de negocio y las brechas deberían ser documentadas. La alta dirección debería ser informada de cualquier brecha entre los requisitos críticos de capacidad de la PTCN y la continuidad de negocio".*

En el punto 7.2.5 Procesos, indica:

> *"Los procesos de la PTCN deberían documentarse claramente y con suficiente detalle para permitir ejecutarlos al personal competente".*

Finalmente, en el punto 7.4.2 Contenido de los documentos del Plan, se establece:

> *"Los planes de respuesta y recuperación de las TIC deberían ser concisos y accesibles a las personas con responsabilidades definidas en los planes. Los planes deberían contener los siguientes elementos: a) Propósito y alcance: El propósito y el alcance de cada plan específico deberían ser definidos, acordados por la alta dirección, y comprendidos por los que invocará el plan. Cualquier relación con otros planes o documentos dentro de la organización, en particular a los planes pertinentes de continuidad del negocio, deberían estar claramente referenciados y el método de obtención y acceso a estos planes descritos".*

En la norma INTE/ISO TS 22317:2016, en su sección 5.2.2 Consideraciones iniciales del BIA, indica:

> *"Una organización que ejecuta un BIA por primera vez, debe planificar tiempo adicional para: (…) documentar el flujo de trabajo a nivel de procesos y actividades".*

La desarticulación entre el PCN y el PCTIC se origina en la ausencia de un inventario único y oficial de procesos que sirve como base común y obligatoria para el PCN, el PCTIC y los demás sistemas de gestión (Calidad y Valoración de Riesgos), así como, la falta de alineación conceptual entre ambos planes y la ausencia de revisión y aprobación por parte de la Alta Administración. Por otra parte, en el PCN se consignaron valores asociados al 'Tiempo máximo sin sistemas o servicios de TI', los cuales fueron interpretados por la administración como el RPO del PCTIC; de ahí se debe que el PCTIC carezca de la definición explícita del RPO para los servicios establecidos en este plan.

Estas situaciones debilitan la integración efectiva entre los planes y por ende la efectividad del esquema institucional de continuidad, al generar inconsistencias entre los procesos críticos, los servicios tecnológicos y los tiempos de recuperación definidos. Asimismo, limitan la capacidad de respuesta ante eventos disruptivos, comprometen la cobertura de procesos esenciales, incrementan el riesgo operativo y debilitan la continuidad institucional. Adicionalmente, la ausencia del RPO genera una debilidad documental. El PCTIC debe ser un documento autocontenido y operativamente claro. Al depender de la interpretación de una métrica definida en otro documento (el PCN), el PCTIC pierde integridad conceptual y no ofrece, por sí mismo, el panorama completo necesario para la ejecución y gestión de la recuperación.

2.2 Inconsistencias en el análisis de riesgos, tratamientos y planes de acción dentro del PCTIC

La revisión del Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC), evidenció las siguientes inconsistencias:

a) **Amenazas y causas iguales:** No se diferencia entre causas y amenazas, ya que los mismos elementos que se presentan como causas en la sección 4.1.1 (páginas 25 y 26), se repiten en la sección 4.1.2 como amenazas (páginas 27 a 32).

b) **Incongruencias entre causas del riesgo:** En la sección 4.1.2 se establece una causa principal para un riesgo que no se encuentra alineada con las causas previamente identificadas y listadas en la sección 4.1.1.

c) **Omisión de opciones de tratamiento:** Para el riesgo "Interrupción de servicios", específicamente en el punto "1.7 Fallos en equipos y enlaces de comunicación", se calculó un Nivel de Riesgo Inherente con prioridad "Media" y condición de "Tratamiento", sin que se documentara la opción de tratamiento correspondiente.

d) **Inconsistencias en los nombres de eventos y riesgos:** Se observaron cambios en el nombre de riesgos y eventos sin justificación a lo largo del documento. Por ejemplo, el evento "Falla o saturación de equipos del Centro de Datos" aparece con un nombre distinto en secciones distintas.

e) **Clasificación incorrecta del tratamiento:** Se detectaron inconsistencias en la clasificación del tipo de tratamiento. Por ejemplo, una acción que implica activar contratos con terceros se clasifica como "Aceptar", cuando representa una forma de "Transferir" el riesgo.

f) **Desalineación entre secciones del documento:** Las opciones y tipos de tratamiento definidos en la sección 4.1.3 no se mantienen en la sección 5.1 (Planes de acción). Algunos tratamientos fueron omitidos y otros presentan una clasificación distinta en cuanto al tipo (por ejemplo, pasar de "Mitigar/Transferir" a "Aceptar/Mitigar").

g) **Enfoque reactivo insuficiente:** Los Planes de acción para administración de riesgos establecidos en el capítulo V se enfocan principalmente en acciones preventivas, sin incluir medidas claras, específicas y operativas para la atención de incidentes una vez que los riesgos se materializan.

h) **Ausencia de referencias a planes y/o protocolos:** Se constató la ausencia de referencias a Plan de Crisis y Contingencia, así como Protocolos de Atención vigentes que resultan esenciales para una respuesta coordinada y efectiva ante eventos que afecten la continuidad.

Al respecto, en las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), se dispone:

> *"4.2 Requisitos de las actividades de control*
> *(…)*
>
> *b. Respuesta a riesgos. Las actividades de control deben ser congruentes con los riesgos que se pretende administrar, lo que conlleva su dinamismo de acuerdo con el comportamiento de esos riesgos".*

Según lo establecido en la norma INTE/ISO/IEC 27031:2017 Tecnología de la información. Técnicas de seguridad. Directrices para la tecnología y comunicación de preparación para la continuidad del negocio, se establece lo siguiente:

> *"7.4.3 La documentación del Plan de Respuesta y Recuperación de las TIC*
>
> *La documentación del Plan de Respuesta y Recuperación de las TIC debería:*
> *a) ser flexible, viable y pertinente;*

b) ser fácil de leer y entender; y
(…)
e) Procedimientos de recuperación de tecnología: descripción de los procedimientos a seguir para recuperar el servicio de las TIC, incluyendo las siguientes:

i) una lista de actividades, por ejemplo, soporte de escritorio y restaurar la información de contacto;
ii) una lista de actividades para la recuperación de red, sistemas, aplicaciones, bases de datos, entre otros, a un nivel acordado en un lugar alterno, teniendo en cuenta los cambios del entorno (por ejemplo, esto podría afectar la capacidad de la línea, la comunicación de sistema a sistema, entre otros);
iii) una lista de actividades para restaurar la funcionalidad básica, como la seguridad, enrutamiento y acceso;
iv) coordinación dentro de la aplicación, o entre aplicaciones, sincronización de datos y procedimientos automatizados potenciales para el manejo de un remanente de información;
v) el proceso necesario para restaurar los servicios de las TIC y entregarlos a sus usuarios para operar en modo de recuperación;
vi) procedimiento de respaldo; y
vii) dónde y cómo las personas pueden obtener más información, instrucciones, entre otros, por ejemplo, números de línea directa; y los pasos a seguir para retornar a la normalidad.

En las Norma INTE/ISO 31000:2018 Gestión del riesgo – Directrices, se estipula:

"4 PRINCIPIOS
(…)

b) Estructurada y exhaustiva

Un enfoque estructurado y exhaustivo hacia la gestión del riesgo contribuye a resultados coherentes y comparables.

(…)

6.5.3 Preparación e implementación de los planes de tratamiento del riesgo
El propósito de los planes de tratamiento del riesgo es especificar la manera en la que se implementarán las opciones elegidas para el tratamiento, de manera tal que los involucrados comprendan las disposiciones, y que pueda realizarse el seguimiento del avance respecto de lo planificado. El plan de tratamiento debería identificar claramente el orden en el cual el tratamiento del riesgo se debería implementar.
Los planes de tratamiento deberían integrarse en los planes y procesos de la gestión de la organización, en consulta con las partes interesadas apropiadas.

Las inconsistencias identificadas se originan en errores humanos durante la elaboración del documento y en la falta de una revisión exhaustiva por parte de las personas responsables de su verificación y aprobación, que puedan garantizar un plan confiable y operativamente sólido.

Estas inconsistencias debilitan la calidad técnica del plan de continuidad, afectan la interpretación de los riesgos y las acciones asociadas, generando un alto riesgo de que se ejecuten medidas inadecuadas o tardías ante una interrupción real, lo que prolongaría la recuperación de servicios críticos. Asimismo, la falta de coherencia interna y la omisión de medidas reactivas específicas impiden evaluar con precisión el riesgo residual, dejando a la institución sin una comprensión clara de su exposición real ante contingencias y dificultando la toma de decisiones informadas para fortalecer sus controles.

2.3 Debilidades en la capacitación, documentación y comunicación del Plan de Continuidad de Tecnologías de Información (PCTIC)

De acuerdo con la información recopilada con la Jefatura de la USIT, se evidenció que:

1. No se ha considerado necesario realizar procesos de capacitación en relación con el Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC).

2. La documentación tipo manual de usuario que permite el restablecimiento de la continuidad de los servicios institucionales, cubre únicamente las operaciones del Data Center para apagado y encendido de la SAN, sin abarcar la totalidad de los servicios críticos definidos por la institución.

3. No cuentan con un proceso formal de divulgación y comunicación del PCTIC a las áreas responsables de su ejecución.

Al respecto, en las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), se dispone:

> *"5.7.1 Canales y medios de comunicación*
> *Deben establecerse y funcionar adecuados canales y medios de comunicación, que permitan trasladar la información de manera transparente, ágil, segura, correcta y oportuna, a los destinatarios idóneos dentro y fuera de la institución.*
>
> *5.7.2 Destinatarios*
> *La información debe comunicarse a las instancias competentes, dentro y fuera de la institución, para actuar con base en ella en el logro de los objetivos institucionales.*
>
> *5.7.3 Oportunidad*
> *La información debe comunicarse al destinatario con la prontitud adecuada y en el momento en que se requiere, para el cumplimiento de sus responsabilidades.*
>
> *5.7.4 Seguridad*
> *Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran".*

La norma INTE/ISO 22301:2020, Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio – Requisitos, estipula.

> *"8.5 Programa de ejercicios*
> *La organización debe implementar y mantener un programa de ejercicios y pruebas para validar la efectividad de sus estrategias y soluciones de continuidad del negocio.*
>
> *La organización debe realizar ejercicios y pruebas que:*
> *a) son consistentes con sus objetivos de continuidad del negocio;*
> *b) se basan en escenarios apropiados que están bien planificados con metas y objetivos claramente definidos;*
> *c) desarrollen el trabajo en equipo, la competencia, confianza y el conocimiento para aquellos que tienen roles que desempeñar en relación con las disrupciones;*
> *d) en conjunto, a lo largo del tiempo, validen sus estrategias y soluciones de continuidad del negocio;*
> *e) produzcan informes formales posteriores al ejercicio que contengan resultados, recomendaciones y acciones para implementar mejoras;*
> *f) se revisen en el contexto de la promoción de la mejora continua;*
> *g) se realicen a intervalos planificados y cuando hay cambios significativos dentro de la organización o el contexto en el que opera".*

En el Plan de Continuidad de Tecnologías de Información y Comunicación del Instituto Nacional de Aprendizaje, se establece:

> *"1.4 Introducción (…)*
> *Los aspectos principales que deben considerarse dentro del plan son:*
>
> *(…)*
> *✓ Estrategias específicas de acción en los diferentes casos (procedimientos a seguir para la continuidad de servicios).*
> *(…) //*
> *✓ Capacitación, entrenamiento y pruebas del PCTIC.*
> *✓ Divulgación del PCTIC a lo interno de la GTIC.*
> *✓ Divulgación a la comunidad institucional del PCTIC a nivel macro.*
>
> *La importancia de este plan radica en que permite a la GTIC contar con una guía para afrontar posibles eventos que impliquen un desastre o interrupción significativa de la continuidad de los SCFP;*
> *(…)*
>
> *2.1. Planeación de la continuidad de TIC*
> *(…)*
> *Los equipos de trabajo se definen como:*
> *✓ Equipo de Lineamientos.*
> *✓ Equipo de Monitoreo.*
> *✓ Equipo de Restablecimiento de la Plataforma Tecnológica.*

> *Estos equipos se encargarán de revisar, modificar o crear acciones, manuales, guías específicas y planes de acción, así como de ponerlos en práctica según el momento apropiado en que se deban ejecutar.*
>
> *Un detalle importante es la capacitación al personal que va a intervenir en caso de que se produzca un evento. De igual manera, debe preverse la estrategia de recuperación de los servicios que conforman la plataforma tecnológica, con el fin de minimizar el tiempo de reanudación de las operaciones".*

La Jefatura de la USIT no priorizó la capacitación del personal relacionado con la ejecución del plan, bajo la perspectiva de que la estrategia de recuperación no ha cambiado respecto a las versiones anteriores del PCTIC, además considera que con la documentación existentes son suficientes para reestablecer la operatividad de las plataformas, y no cuenta con procedimientos formales para su divulgación y comunicación a las áreas responsables.

La ausencia de capacitación, documentación integral y procedimientos formales de divulgación limita la capacidad del personal para ejecutar el PCTIC de manera uniforme y oportuna ante una contingencia. Esto incrementa el riesgo de errores, retrasos en la recuperación de los servicios críticos y dependencia de conocimiento tácito, lo que podría ocasionar interrupciones prolongadas en la continuidad operativa institucional y afectar la prestación de servicios a los usuarios internos y externos.

3. CONCLUSIONES

De acuerdo con los resultados del estudio se evidenciaron áreas donde se requieren mejoras importantes respecto a: la gestión del Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC), en aspectos clave para la preparación y respuesta ante eventos que puedan afectar la disponibilidad de los servicios críticos de TIC.

Se evidenció una desarticulación entre el PCTIC y el Plan de Continuidad del Negocio (PCN), lo que impide una integración efectiva de las estrategias tecnológicas con las necesidades operativas institucionales, y debilita el enfoque integral requerido para la gestión de la continuidad.

Se evidenció que la falta de estandarización en los procesos limita la capacidad de respuesta ante incidentes, afecta la eficiencia en el uso de recursos y pone en riesgo la continuidad de los servicios institucionales.

En relación con la preparación del personal, se constató la ausencia de entrenamientos y documentación actualizada y de fácil acceso, situación que compromete la efectividad del PCTIC ante escenarios disruptivos y disminuye la capacidad de recuperación operativa.

Asimismo, se identificaron inconsistencias en el análisis de riesgos y en los planes de acción asociados, lo cual debilita la coherencia del PCTIC y limita su utilidad como herramienta para la gestión oportuna de situaciones críticas.

4. RECOMENDACIONES

A la señora Paula Valenciano Campos, en su calidad de Gerente General

1. Establecer un inventario único y oficial de procesos institucionales que sirva como fuente para todos los sistemas de gestión Calidad, Valoración de Riesgos y planes institucionales de continuidad (PCN, PCTIC), mediante un plan de acción que incluya la definición, unificación y estandarización formal de los procesos de la institución, con un enfoque basado en procesos y no en estructuras organizativas.

   Se dará por cumplida esta recomendación, mediante una certificación por parte de la Gerencia General que acredite la construcción del "Inventario Único de Procesos Institucionales" formalmente aprobado y las instrucciones a los diferentes Sistemas de Gestión para su implementación. Como parte del avance deberá presentar un cronograma del plan de acción. **Fecha de cumplimiento:** 31/12/2026 y **fecha de los avances:** 30/06/2026. **(Resultado 2.1)**

Al señor Gustavo Ramírez de la Peña, en su calidad de Gestor de la Gestión de Tecnologías de la Información

2. Ajustar el Catálogo de Servicios Tecnológicos alineándolo con el inventario único de procesos, que sirva como base confiable para el PCTIC, mediante un plan de acción que contemple:

   a) La identificación, caracterización y priorización de todas las capacidades tecnológicas que soportan los procesos críticos, es decir, los servicios tecnológicos estratégicos que difieren de los servicios operativos del *Service Desk*. Para cada uno se debe establecer su propósito, alcance, componentes y su vínculo directo con los procesos institucionales del inventario único y, de manera fundamental, su nivel de criticidad, el cual se derivará del impacto que su interrupción cause en el proceso de negocio al que sirve.

   b) La definición y documentación de los parámetros de continuidad (RTO y RPO) para cada servicio tecnológico crítico identificado.

   c) La formalización y socialización del catálogo con la Alta Gerencia y las áreas usuarias.

   Se dará por cumplida esta recomendación con una certificación emitida por la Jefatura de la Gestión donde se evidencie las acciones implementadas. **Fecha de cumplimiento:** 31/12/2026 y **fecha de los avances:** 30/06/2026. **(Resultado 2.1)**

3. Implementar un plan de acción para corregir las inconsistencias identificadas en el Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC). Este plan de acción debe contemplar como mínimo:

a) Asignación de responsables claramente definidos para cada actividad.

b) Plazos y actividades establecidos para la ejecución, seguimiento y cierre.

c) Revisión cruzada entre el PCTIC y el PCN que aseguren la alineación, coherencia y completitud.

d) Ajuste del análisis de riesgos, los tratamientos asociados y los planes de acción del PCTIC.

Se dará por cumplida esta recomendación con la actualización del PCTIC en la que se evidencie la atención de los aspectos señalados, así como, la revisión y aprobación formal por parte de la Comisión Gerencial de Informática (CGI). Como parte del seguimiento se deberá presentar el cronograma del plan de acción una vez elaborado. **Fecha de cumplimiento:** 30/06/2027 y **fecha de los avances:** 30/03/2027. **(Resultado 2.1, Resultado 2.2)**

4. Implementar un plan de acción para fortalecer la efectividad del Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC). Este plan deberá contemplar, de manera conjunta, los siguientes aspectos:

a) La capacitación y entrenamiento continuo del personal con roles asignados en la ejecución del PCTIC, incluyendo simulacros, talleres y/o sesiones informativas para fortalecer sus competencias en la respuesta ante eventos disruptivos.

b) La elaboración, revisión y mantenimiento actualizado de manuales y/o guías específicas para cada servicio crítico, con instrucciones claras y estandarizadas que apoyen la ejecución del PCTIC.

c) La definición y formalización de un mecanismo seguro, controlado y oportuno de divulgación y acceso al PCTIC y su documentación asociada, garantizando su disponibilidad ante la activación del plan.

La recomendación se dará por cumplida, con una certificación por parte del Gestor, sobre la implementación del plan de acción. **Fecha de cumplimiento:** 30/09/2027 y **fecha de los avances:** 30/03/2027. **(Resultado 2.3)**

5. OBSERVACIONES

5.1 Comunicación de resultados, observaciones de la administración y remisión del informe

5.1.1 Los resultados del informe fueron comunicados a la señora Paula Valenciano Campos, Gerente General y al señor Gustavo Ramírez de la Peña, Gestor de la Gestión de Tecnologías de la Información y Comunicación, quienes manifestaron su aprobación y aceptación de las recomendaciones contenidas en él.

5.1.2 Se toma nota de la observación realizada por la GTIC en la reunión de comunicación de resultados realizada el 19 de enero del 2026:

Recomendación Nº 4			
Observación de GTIC	Incluir el siguiente punto adicional en la recomendación: a) Establecer un procedimiento para asegurar que el PCTIC sea conocido, aprobado y actualizado.		
¿Se acoge?	Sí (X)	No ( )	Parcialmente ( )
Argumentos Auditoría Interna:	Se acoge lo solicitado, se modifica la numeración de las viñetas de la redacción original, quedando de la siguiente forma: 4. Implementar un plan de acción para fortalecer la efectividad del Plan de Continuidad de Tecnologías de Información y Comunicación (PCTIC). Este plan deberá contemplar, de manera conjunta, los siguientes aspectos: a) Establecer un procedimiento para asegurar que el PCTIC sea conocido, aprobado y actualizado. b) La capacitación y entrenamiento continuo del personal con roles asignados en la ejecución del PCTIC, incluyendo simulacros, talleres y/o sesiones informativas para fortalecer sus competencias en la respuesta ante eventos disruptivos. c) La elaboración, revisión y mantenimiento actualizado de manuales y/o guías específicas para cada servicio crítico, con instrucciones claras y estandarizadas que apoyen la ejecución del PCTIC. d) La definición y formalización de un mecanismo seguro, controlado y oportuno de divulgación y acceso al PCTIC y su documentación asociada, garantizando su disponibilidad ante la activación del plan.		

5.1.3 La remisión del informe se realiza mediante el oficio AI-0037-2026 del 13 de febrero del 2026 fecha a partir de la cual se da por finalizado este estudio.

5.2 Plazo para el avance y ejecución de las recomendaciones

De acuerdo con el artículo 36 de la Ley General de Control Interno 8292, se dispone un plazo de diez días hábiles a partir de la fecha de recibido el informe, para ordenar la implementación de las recomendaciones y comunicarlo a este órgano de fiscalización y control; de lo contrario, se recuerda los artículos 36, 37, 38 y 39 de la citada ley, que al efecto disponen la forma de comunicación de los resultados de los informes de la Auditoría Interna y se previene al jerarca y a los titulares subordinados acerca de sus deberes en el trámite.

El plazo se establece de acuerdo con lo pactado con la jefatura de la unidad correspondiente en el *acta de conferencia final*, como a continuación se señala:

Recomendación	Responsable del cumplimiento	Fecha de comunicación	Fecha de los avances	Fecha de cumplimiento
1	Gerencia General	23-01-2026	30/06/2026	31/12/2026
2	Gestión de Tecnologías de la Información y Comunicación	19-01-2026	30/06/2026	31/12/2026
3	Gestión de Tecnologías de la Información y Comunicación	19-01-2026	30/03/2027	30/06/2027
4	Gestión de Tecnologías de la Información y Comunicación	19-01-2026	30/03/2027	30/09/2027

5.3 Responsable del informe

El estudio fue realizado por las personas funcionarios de esta Auditoría: Silvia Carranza Marín y Albertina Cruz Casco bajo la supervisión Didier Chavarría Chaves, Encargado del Proceso de Fiscalización de Tecnologías de la Información y Comunicación.

Firmado digitalmente
Silvia Elena Carranza Marín
Auditora encargada del estudio

Firmado digitalmente
Albertina Cruz Casco
Auditora colaboradora del estudio

Firmado digitalmente
Didier Chavarría Chaves
Encargado de Proceso

Firmado digitalmente
Alfredo Hasbum Camacho
Auditor General

Anexo 1

Normativa utilizada como base para la revisión efectuada

- Ley General de Control Interno 8292.
- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE).
- Marco Normativo Manual de Normas y Estándares de Seguridad de la Información, diciembre, 2020.
- Marco de Referencia COBIT 2019: Objetivos de gobierno y gestión.
- Manual de Normas Técnicas de Tecnologías de la Información del Instituto Nacional de Aprendizaje.
- Manual Organizacional INA, edición 1, aprobado por MIDEPLAN en 2020.
- Reglamento de Recursos Informáticos.
- Plan de Continuidad de Negocio, INA, noviembre 2022.
- Plan de Continuidad de Tecnologías de Información y Comunicación, setiembre 2019.
- Plan de Continuidad de Tecnologías de Información y Comunicación, mayo 2024.
- Política de Seguridad de la Información, diciembre 2020, edición 4.
- Procedimiento de Gestión de Vulnerabilidades, P USIT POS 05, EDICIÓN 1, marzo 2023.
- Procedimiento de revisión de seguridad física y ambiental de equipos de comunicación, cuartos de comunicación y gabinetes, P USIT POS 02, edición 1, marzo 2023.
- Procedimiento de monitoreo y gestión de incidentes relacionados a los servicios de TIC, P USIT POS 1, agosto 2016.
- COBIT 2019 "Objetivos de gobierno y gestión". Marco de Referencia COBIT® 2019.

- ISO/IEC 22301:2019, Seguridad y resiliencia, Sistemas de gestión de la continuidad del negocio.

- Norma INTE/ISO 22301:2020. Seguridad y resiliencia - Sistemas de gestión de continuidad del negocio – Requisitos.

- INTE/ISO TS 22317:2016, "*Seguridad de la sociedad. Sistema de gestión de continuidad del negocio. Directrices para el análisis de impacto al negocio (BIA)".*

- INTE/ISO/IEC 27031:2017, *"Directrices para la Preparación para la Continuidad de los Servicios TIC".*

- Norma INTE/ISO/IEC 27031:2017 Tecnología de la información. Técnicas de seguridad. Directrices para la tecnología y comunicación de preparación para la continuidad del negocio.

- Norma INTE/ISO 31000:2018 Gestión del riesgo – Directrices.

- Catálogo de servicios de la GTIC, edición 2, febrero 2024.