INSTITUTO MIXTO DE AYUDA SOCIAL | GOBIERNO DE COSTA RICA

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

AUD 003-2025

INFORME SOBRE LOS RESULTADOS OBTENIDOS EN LA EVALUACION DEL PROCESO DE CONTINUIDAD DE NEGOCIO Y LAS TECNOLOGÍAS DE INFORMACIÓN DEL IMAS

TABLA DE CONTENIDO

INSTITUTO MIXTO DE AYUDA SOCIAL | GOBIERNO DE COSTA RICA

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

RESUMEN EJECUTIVO

¿Qué examinamos?

Se examinó si el proceso de la Continuidad del Negocio y las TIC's permiten garantizar la pronta recuperación de los servicios críticos tras un incidente o contingencia, así como la elaboración, implementación y el seguimiento de las estrategias definidas para brindar el cumplimiento del fin público.

¿Por qué es importante?

Para garantizar la pronta recuperación de los servicios críticos tras un incidente o contingencia, así como la elaboración, implementación y el seguimiento de las estrategias definidas para brindar el cumplimiento del fin público.

¿Qué encontramos?

Entre los resultados más relevantes se detectaron los siguientes:

- Con respecto a los planes de recuperación si bien, el área de Tecnologías de Información, ha llevado a cabo pruebas de recuperación y/o restauración, estas no evidencian la ejecución de otros escenarios de pruebas que contemplen componentes y/o sistemas de información que forman parte de la Infraestructura Tecnológica del IMAS y que se encuentran tipificados como críticos dentro del documento del "*Plan de Recuperación antes Desastres (PRD) IMAS*", donde se incluyen: aplicaciones, equipo de telecomunicaciones e Infraestructura y Bases de Datos, así como la preparación de la Institución ante la materialización de algún riesgo identificado y plasmado dentro del documento "*Plan de Continuidad de TI*".

- Se determinó que si bien el proceso de sensibilización y concientización que ha llevado a cabo el área de Tecnologías de Información ha tocado distintos puntos referentes a la seguridad de la información, este no ha abarcado otro factor importante en lo que a Ciberseguridad se refiere como lo es la responsabilidad y conciencia que las personas funcionarias deben de tener al utilizar y/o hacer uso de dispositivos móviles personales (celulares inteligentes o "*smartphones*", tabletas, entre otros) para el acceso a herramientas laborales como correo electrónico, Teams, OneDrive, entre otros; y sus potenciales riesgos.

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

- Se observó que los documentos consultados como parte de este estudio: "*Plan de Continuidad de TI (v3 - dic2020)*" y "*Plan de Recuperación Ante Desastres PRD (v1_1 - nov2021)*" fueron aprobados en el año 2020 y 2021 respectivamente, aspecto que representa un desfase se aproximadamente dos años con relación al actual 2023. Misma condición se logró visualizar con otras políticas y procedimientos que fueron consultadas como parte de este estudio como lo son "*POL-EDI-14-Política Plan de Continuidad de los servicios de TI*" con fecha aprobación noviembre 2009 y "*POL-TI-06 Política de Respaldo y Recuperación de la Información (emisión 02)*" actualizada en el año 2021, "*P-TI-06 Procedimiento plan de recuperación de desastres",* con fecha de 2010, entre otras

¿Qué sigue?

Dadas las situaciones encontradas, esta Auditoría recomendó al jefe del Área de Tecnologías de Información para el primer aspecto fortalecer el proceso de ejecución de los planes de pruebas que se aplican sobre el Plan de Continuidad y Plan de Recuperación de Desastres de manera que este proceso contemplen procesos críticos tipificados y riesgos identificados y mencionados en dichos planes de manera que permita evaluar el estado de preparación de la Institución ante una eventualidad y de esta manera certificar la debida ejecución del plan.

Sobre el proceso de sensibilización y concientización en temas de Ciberseguridad y seguridad de la información incluir dentro de futuras actividades de sensibilización un apartado que abarque o hable acerca del uso y/o utilización de dispositivos móviles personales para el acceso a la información Institucional y sus eventuales riesgos.

En relación con el proceso de actualización sobre normativa Institucional relacionada con Continuidad de Negocio esta Auditoría recomienda analizar la conveniencia para que cuando la normativa que dispone Tecnologías de Información sea revisada o actualizada como parte de sus procesos de diagnóstico, su resultado quede debidamente evidenciado como se establece en la normativa y específicamente en el apartado "Revisión y Actualización" de manera que se visualice y pueda dar trazabilidad si esta ha sido cambiada y/o actualizada desde su fecha de aprobación

INSTITUTO MIXTO
DE AYUDA SOCIAL

GOBIERNO
DE COSTA RICA

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

AUD 003-2025

INFORME SOBRE LOS RESULTADOS OBTENIDOS EN LA EVALUACION DEL PROCESO DE CONTINUIDAD DE NEGOCIO Y LAS TECNOLOGÍAS DE INFORMACIÓN DEL IMAS

1. INTRODUCCIÓN

1.1.Origen

Esta auditoría se realizó de conformidad con lo establecido en el Plan Anual de Trabajo de la Auditoría Interna para el año 2024.

1.2. Objetivo General

Evaluar si el proceso de la Continuidad del Negocio y las TIC's permiten garantizar la pronta recuperación de los servicios críticos tras un incidente o contingencia, así como la elaboración, implementación y el seguimiento de las estrategias definidas para brindar el cumplimiento del fin público.

1.3. Alcance

El estudio abarcó la evaluación del proceso de Continuidad del Negocio y las Tecnologías de Información y Comunicación (en adelante TIC’s) permiten garantizar la pronta recuperación de los servicios críticos tras un incidente o contingencia, así como la elaboración, implementación y el seguimiento de las estrategias definidas para brindar el cumplimiento del fin público; así como el cumplimiento de la normativa técnica y legal aplicable al proceso en cuestión.

El periodo del estudio comprende del 01 de enero del 2023 hasta el 30 de setiembre del 2023, extendiéndose en los casos que se consideró necesario.

El estudio se efectuó de conformidad con la Ley General de Control Interno, las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, las Normas Generales de Auditoría para el Sector Público, el Manual de Procedimientos de Auditoría Interna del IMAS, así como la demás normativa de auditoría interna de aplicación y aceptación general.

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

1.4. Comunicación de resultados

En reunión celebrada el día 21 de marzo del 2025, se comunicaron los resultados del presente informe, en la cual se efectuaron observaciones que, en lo pertinente, una vez valoradas por esta Auditoría Interna, fueron incorporadas en el acápite de recomendaciones del presente informe.

2. RESULTADOS

2.1. Proceso de pruebas sobre el Plan de Continuidad y Plan de Recuperación de Desastres

El IMAS a través del área del Tecnologías de Información en materia de Continuidad de Negocio ha elaborado, aprobado y publicado dos documentos al respecto: "*Plan de Continuidad de TI (v3 - dic2020)*", el cual tiene por objetivo prevenir emergencias y minimizar el efecto que pueda provocar un posible desastre en los recursos informáticos y por ende en las operaciones normales Instituto Mixto de Ayuda Social (IMAS) y "*Plan de Recuperación Ante Desastres PRD (v1_1-nov2021)*", cuyo fin es brindar continuidad a los servicios informáticos del IMAS en caso de presentarse una situación de contingencia mayor o catastrófica.

Al respecto, y sobre los planes antes mencionados, en ellos se indica que los mismos deben de someterse a procedimientos periódicos de pruebas que permitan certificar que las actividades que ahí se mencionan permitan mantener de manera razonable la continuidad de las operaciones que presta la Institución y validar el estado de preparación del IMAS ante un evento, incidente o catástrofe. Al respecto, esta Auditoría solicitó la documentación soporte de las pruebas ejecutadas por parte del área de Tecnologías de Información, y las cuales fueron remitidos vía correo electrónico el día 25 de octubre de 2023, los escenarios de pruebas que se realizaron para los años 2021, 2022 y 2023; escenarios que se describen a continuación:

Periodo de la Prueba	Escenario de Prueba
Periodo 2021	Restauración y respaldo por cambio de Switch y cambio en módulos F.O, pisos 4 y 2.
Periodo 2022	Restauración y respaldo por cambio de Switch y cambio en módulos F.O, pisos 1 y 3.
Periodo 2023	Infraestructura total del ambiente de SAP Desarrollo

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

Con respecto a lo anterior, si bien, el área de Tecnologías de Información, ha llevado a cabo pruebas de recuperación y/o restauración como se mencionan en el cuadro anterior, estas no evidencian la ejecución de otros escenarios de pruebas que contemplen componentes y/o sistemas de información que forman parte de la Infraestructura Tecnológica del IMAS y que se encuentran tipificados como críticos dentro del documento del "*Plan de Recuperación antes Desastres (PRD) IMAS*", donde se incluyen: aplicaciones, equipo de telecomunicaciones e Infraestructura y Bases de Datos, así como la preparación de la Institución ante la materialización de algún riesgo identificado y plasmado dentro del documento "*Plan de Continuidad de TI*", lo anterior en aras de garantizar de manera la razonable la funcionalidad de dichos planes y por ende la prestación de los servicios Institucionales a las personas funcionarias así como a las personas ciudadanas en caso de contingencia y/o incidencia o catástrofe.

Sobre el tema expuesto en el párrafo anterior, en la sección denominada "***Plan de Pruebas del PRD***", del documento "***Plan de Recuperación Ante Desastres PRD (v1_1 - nov2021)***" que estipula textualmente lo siguiente:

> *"…El plan de prueba del PRD deberá de realizar las siguientes actividades:*
> - *Validar que las tareas, acciones, y estrategias de recuperación sean suficientes para que se puedan restablecer los Servicios de Cómputo y telecomunicaciones de la institución y así lograr la continuidad de las operaciones ante un evento informático…"*

Asimismo, en el documento "***Plan de Continuidad de TI***" en la sección **4.0. Implementación, actualización y divulgación del plan** en el punto 6 indica lo siguiente:

> *"El Área de Tecnologías de Información deberá planificar periódicamente y de acuerdo con las circunstancias de conveniencia Institucional en donde no se afecten los servicios operacionales, las pruebas para evaluar la operación de este plan y el estado de preparación de la Institución ante una eventualidad o riesgo identificado en este mismo documento. Se recomiendan los simulacros de escritorio o las pruebas parciales o totales del plan bajo la supervisión total del coordinador del área y evitando afectar la operacionalidad institucional y de los servicios que se prestan".*
> (lo subrayado no forma parte del texto original)

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

Consecuentemente con lo anterior, la política "***Política plan de continuidad de los servicios de TI***" en la sección **5 Responsabilidades**, en lo de interés señala lo siguiente:

> *El Área de Desarrollo Informático: mantener actualizado el Plan de Continuidad de los servicios de TI, así como, definir el calendario y guiones para las pruebas periódicas que* ***certifiquen la debida ejecución del plan*****.** (lo subrayado y negrita no forma parte del texto original)

Sobre el particular, mediante una reunión llevada a cabo el día 24 de octubre de 2023 con el Sr. Luis Adolfo González Alguera, Jefe del Área de Tecnologías de Información indicó a esta Auditoría al respecto de lo anteriormente indicado, lo transcrito a continuación:

> *"...a la luz de los esos planes si se hacen pruebas anuales, donde una vez al año se escoge un sistema para hacerle una recuperación completa o se realiza un simulacro como que pasara algo; y también a aprovechamos, cuando hay que hacer alguna migración y se aprovecha para hacer una restauración cuando se pasa un sistema de un lugar a otro, de tal manera que se aprovecha esos momentos para hacer esos simulacros..."*

La situación antes comentada, conlleva a un riesgo potencial que los escenarios de pruebas, no permitan de manera razonable garantizar la debida ejecución del plan y por ende la debida restauración de la Infraestructura tecnológica, sistemas, bases de datos de la Institución ante una contingencia, incidente, evento de seguridad o catástrofe que afecte la prestación de servicios por parte del IMAS a las personas funcionarias como a las personas ciudadanas y por ende no se haya constatado que los lineamientos y actividades del plan minimizan el tiempo en el restablecimiento de los servicios de la Institución o mitigar los riesgos identificados.

2.2. Proceso de sensibilización y concientización sobre el uso de dispositivos móviles personales y normativa relacionada.

El área de Tecnologías de Información como parte del proceso de sensibilización y en pro de fortalecer, crear conciencia y promover cultura a la comunidad Institucional en la adopción y aplicación de buenas prácticas a nivel de Ciberseguridad y protección de la información, no solo se ha dado a la tarea de divulgar una serie de cápsulas informativas, avisos o comunicados referentes a: medios oficiales de comunicación Institucional, repositorios oficiales para el resguardo y manejo de información, uso de aplicaciones gratuitas para el

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

envío, recepción y recolección de información de la Institución, suscripción a estas aplicaciones, entre otros; sino que además se ha planteado el objetivo de complementar lo anterior, con la ejecución de capacitaciones para toda la comunidad Institucional referentes a la Ciberseguridad, seguridad y protección de la información; como por ejemplo la capacitación que se llevó a cabo el día miércoles 27 de setiembre de 2023 denominada "*Seguridad de la Información en el Entorno Laboral (Ciberseguridad Laboral)*", donde se expuso acerca de las diferentes medidas y herramientas de seguridad y protección que dispone la Institución así como el papel y la responsabilidad que como personas usuarias de equipo tecnológico debemos de emprender dado los diferentes incidentes de Ciberseguridad que diario se presentan.

Sin embargo; y en relación con lo antes expuesto, esta Auditoría determinó que dicho proceso si bien ha tocado distintos puntos referentes a la seguridad de la información, este no ha abarcado otro factor importante en lo que a Ciberseguridad se refiere como lo es la responsabilidad y conciencia que las personas funcionarias deben de tener al utilizar y/o hacer uso de dispositivos móviles personales (celulares inteligentes o "*smartphones*", tabletas, entre otros) para el acceso a herramientas laborales como correo electrónico, Teams, OneDrive, entre otros; y sus potenciales riesgos que se derivan del acceso no solo a la Información Institucional ya sea de acceso irrestricto, restringido, sensible y/o confidencial o bien, conversaciones con temas estratégicos, a las cuales se puede tener acceso con solo tener una licencia de "*Microsoft Office 365*" y proceder con la descarga e instalación en estos dispositivos móviles personales.

Aunado al tema mencionado en el párrafo anterior, esta Auditoría determinó que el IMAS a través del área de Tecnologías de Información en relación con la seguridad de la Información dispone de una serie de políticas y procedimientos cuyo objetivo radica en contar lineamientos aprobados, publicados y de acatamiento obligatorio para todas las personas funcionarias sobre el uso correcto y razonable de los sistemas de Información, Infraestructura y equipo tecnológico. Entre dicha documentación se pueden mencionar normativa como: "*POL-TI-08 Política Seguridad información (em03) ACD-339-11-2021*", "*P-TI-29 Procedimiento para la administración de seguridad de los sistemas*", "*MGTIC - Perfil Marco Gestión TIC IMAS (v1 dic2021)*", "*Reglamento para el Uso y Control de las Tecnologías de Información IMAS (RUCTI) (1)"*, entre otras; no obstante, no se identificó u observó que contengan lineamientos relacionados sobre la utilización o riesgos en el uso de dispositivos móviles personales dentro del entorno laboral Institucional.

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

Sobre el tema en cuestión, la política POL-TI-08 "Política de Seguridad de la Información" en la sección "Disposiciones Generales de la Política, en el párrafo 4 se indica lo siguiente:

> *"El Área de Tecnologías de Información* ***debe identificar y recomendar a la Gerencia General, las necesidades de concienciación y capacitación*** *del personal del IMAS en temas de Seguridad de la Información…"*

Por otra parte, en lo relacionado al tema de la normativa, el Reglamento para el uso y control de las Tecnologías de Información del IMAS, en el capítulo II "*Competencias del Área de Tecnologías de Información*", artículo 3 "*Competencias generales en la administración de las TI institucionales*", en su punto e indica lo siguiente:

> "***Proponer ante la Dirección Superior la normativa contemplada en políticas, directrices, procedimientos y regulaciones en materia de tecnología de información que regirán la Institución…***". (Lo subrayado no forma parte del texto original).

Sobre el particular, mediante una reunión llevada a cabo con el Sr. Luis Adolfo González Alguera el día 24 de octubre de 2023, Jefe del Área de Tecnologías de Información indicó a esta Auditoría lo transcrito a continuación sobre el uso de dispositivos móviles, normativa y capacitación sobre este tema:

> "*… el área de Tecnologías de Información no se ha recibido por parte de la Institución un requerimiento de parte de la institución en sobre ese punto, así como tampoco han visto como materializado ni visto algún riesgo sobre esto*".

La situación antes indicada, conlleva a un riesgo potencial de no contar con un proceso de capacitación que permita crear conciencia y sensibilizar sobre posibles implicaciones y eventuales riesgos a las que una persona funcionaria puede exponerse al tener instalado herramientas y/o aplicaciones que le faculten el acceso a la información Institucional ya sea sensitiva, irrestricta o restringida desde su dispositivo móvil personal, así como medidas de seguridad mínimas que deberíamos poner en práctica al utilizarlos.

2.3. Proceso de actualización sobre normativa Institucional relacionada con Continuidad de Negocio.

Como aspecto complementario a lo ya mencionado en los apartados anteriores, esta Auditoría observó que los planes mencionados en el apartado 2.1 de esta sección; "*Plan de Continuidad*

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

de TI (v3 - dic2020)" y "*Plan de Recuperación Ante Desastres PRD (v1_1 - nov2021)*" fueron aprobados en el año 2020 y 2021 respectivamente, aspecto que representa un desfase se aproximadamente dos años con relación al actual 2023. Misma condición se logró visualizar con otras políticas y procedimientos que fueron consultadas como parte de este estudio como lo son "*POL-EDI-14-Política Plan de Continuidad de los servicios de TI*" con fecha aprobación noviembre 2009 y "*POL-TI-06 Política de Respaldo y Recuperación de la Información (emisión 02)*" actualizada en el año 2021, "*P-TI-06 Procedimiento plan de recuperación de desastres",* con fecha de 2010, entre otras.

Sobre el particular, se consultó al Jefe del Área del Tecnologías de Información durante la reunión llevada a cabo el 24 de octubre de 2023, en relación con el tema de actualización de políticas y procedimientos, e indicó lo siguiente:

> *"…lo hacemos más de acuerdo con la dinámica que se va presentando, digamos con los cambios que se van haciendo en la institución, de repente hay una política que no hay o que hay que cambiarla cuando realmente esa operación se viene manteniendo en el tiempo, entonces no vamos a cambiarla solo por cambiar, digamos algo que realmente no da valor y solo como para cumplir con indicar que algo se cambió no…"*

Asimismo, sobre este mismo tema, vía correo electrónico enviado el 25 de octubre de 2023 el área de Tecnologías de Información detalla la situación en relación con la actualización de las políticas y/o procedimientos consultados y que esta Auditoría utilizó como referencia, donde se mencionaron lo siguiente:

> *"POL-EDI-14-Política Plan de Continuidad de los servicios de TI: es de noviembre 2009 y no se ha actualizado. Sin embargo, durante el diagnóstico 2017-2018 se validó que no requerían un ajuste mayor.*
> *POL-TI-06 Política de Respaldo y Recuperación de la Información (emisión 02), actualizada noviembre 2021.*
> *PR-TI-22 Procedimiento administración respaldos y restauraciones de datos (emisión 04), actualizada noviembre 2021.*
> *P-TI-06 Procedimiento plan de recuperación de desastres, es de marzo 2010 y no se ha actualizado. Sin embargo, durante el diagnóstico 2017-2018 se validó que no requerían un ajuste mayor."*

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

Al respecto del tema en cuestión, la "*POL-EDI-14 Política plan de continuidad de los servicios de TI*", indica en su apartado **6. Revisión y actualización** en el punto 12 indica:

> *"12 Los documentos serán revisados al menos una vez cada dos años, con el fin de identificar la necesidad de cambios y/o actualizaciones. Sin embargo, dichas actualizaciones pueden realizarse cuando sea necesario…"*

El documento "Plan de Continuidad de TI" en su apartado sección **4.0. Implementación, actualización y divulgación del plan**, en su párrafo 4, desprende lo siguiente:

> *"La actualización de este plan se llevará a cabo con una revisión **cada vez que se genere un nuevo Plan Estratégico Institucional**, con el objetivo de validar si por los cambios o necesidades del nuevo PEI, se requiere algún ajuste al Plan de Continuidad. En caso de ser requerido, el Equipo de Continuidad de TI realizará la revisión y propuesta de actualización a la jefatura de TI para que este lo eleve a la Gerencia General para su aprobación y posterior divulgación"* (Lo subrayado no forma parte del texto original)

Si bien el área de Tecnologías de Información como parte de sus actividades y responsabilidades que le competen, realizan diagnósticos donde someten a revisión y validación normativa de Tecnologías de Información como la mencionada en el apartado 2.1 y este apartado, para de esta forma determinar si requieren o no actualización, el resultado de esta actividad no se refleja o visualiza en el documento ya que si se consulta dicha normativa, solo se visualiza su fecha de aprobación y/o publicación, aspecto que sugiere que no se revisan o no se actualizan y por consiguiente no permite evidenciar concordancia y cumplimiento con lo indicado en el apartado "**Revisión y actualización**". Aunando a lo anterior, y como se indicó no todos los documentos consultados han sido actualizados, o al menos revisados, situación que conlleva a un riesgo potencial de no garantizar de manera razonable si los lineamientos y/o actividades que ahí se mencionan se ajustan o están alineados al funcionamiento actual de las Tecnologías de Información.

3. CONCLUSIONES

De conformidad con los resultados obtenidos en el presente estudio, se concluye lo siguiente:

3.1 Se detectaron oportunidades de mejora en la ejecución de las pruebas que se realizan para validar lo indicado en los Planes "*Plan de Continuidad de TI (v3 - dic2020)*" y "*Plan de Recuperación Ante Desastres PRD (v1_1 - nov2021)*", otros procesos tipificados como

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

críticos en dichos documentos como lo son: aplicaciones, equipo de telecomunicaciones e Infraestructura y Bases de Datos, así como la preparación de la Institución ante la materialización de algún riesgo identificado y plasmado dentro del documento "*Plan de Continuidad de TI*". Por el contrario, para dichos años se evidenciaron pruebas ejecutadas por cambios de switch e Infraestructura total del ambiente de SAP Desarrollo.

3.2 Con respecto al proceso de sensibilización a la comunidad Institucional sobre temas como Ciberseguridad, seguridad y protección de la información, si bien el área de Tecnologías de Información ha utilizado distintos mecanismos tales como comunicados, cápsulas informativas, entre otras, así como capacitaciones para todas las personas funcionarias, dicho proceso no abarca y tampoco se tiene previsto incluir otro factor importante en lo que a Ciberseguridad se refiere como lo es la utilización y uso de dispositivos móviles personales para el acceso a herramientas laborales (correo electrónico, Teams, OneDrive, entre otros) y sus potenciales riesgos que se derivan del acceso no solo a la Información Institucional ya sea de acceso irrestricto, restringido, sensible y/o confidencial a través de dispositivos móviles personales.

3.3 Se detectaron oportunidades de mejora en el proceso de actualización de normativa, políticas y procedimientos de Tecnologías de Información, los cuales pese a que algunas han sido sujetas a revisión como parte de los procesos de diagnóstico que está área realiza, su resultado no se ve reflejado en el documento, aspecto que sugiere que dicha normativa, política y/o procedimientos no son revisadas desde su fecha de aprobación en concordancia y cumplimiento con el apartado "**Revisión y actualización**" que se mencionan en estos documentos. Por otra parte, se identificó normativa que desde su fecha de aprobación y publicación no han sido debidamente actualizados.

En virtud de lo anterior es necesario que la Administración implemente medidas preventivas y correctivas que solventen las debilidades presentadas en el estudio y con tal propósito en el capítulo siguiente se formulan las recomendaciones que se consideran pertinentes en las circunstancias determinadas.

4. RECOMENDACIONES

Esta Auditoría Interna respetuosamente se permite recordar que de conformidad con lo preceptuado por el artículo 36 de la Ley N.º 8292 "Ley General de Control Interno", disponen de diez días hábiles, contados a partir de la fecha de recibido de este informe, para ordenar la implantación de las recomendaciones que les correspondan.

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

Al respecto, se estima conveniente transcribir a continuación, en lo de interés, lo que disponen los artículos 12, 36, 38 y 39 de la Ley N.º 8292:

> **Artículo 12. -Deberes del jerarca y de los titulares subordinados en el sistema de control interno**. En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes: …/c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan…
>
> **Artículo 36. -Informes dirigidos a los titulares subordinados.** Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera: /a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados. /b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes. /c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.
>
> **Artículo 38.-Planteamientos de conflictos ante la Contraloría General de la República.** Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas. /La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N.º 7428, de 7 de setiembre de 1994.

Artículo 39. _ Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios […]

AL JEFE DEL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN

4.1 Emprender las acciones administrativas en coordinación con las instancias correspondientes para fortalecer el proceso de ejecución de los planes de pruebas que se aplican sobre el Plan de Continuidad y Plan de Recuperación de Desastres de manera que este proceso contemplen procesos críticos tipificados y riesgos identificados y mencionados en dichos planes de manera que permita evaluar el estado de preparación de la Institución, ante una eventualidad y de esta manera certificar la debida ejecución del plan, como se establece en la normativa relacionada a Continuidad de Negocio que dispone la Institución. (Véase punto 2.1 del acápite de resultados del informe)

4.2 Analizar la conveniencia para incluir dentro de futuras actividades de sensibilización un apartado que abarque o hable acerca del uso y/o utilización de dispositivos móviles personales para el acceso a la información Institucional y sus eventuales riesgos, lo anterior como parte del fortalecimiento del proceso de sensibilización y concientización para la comunidad Institucional sobre temas de ciberseguridad, seguridad y protección de la información. (Véase punto 2.2 del acápite de resultados del presente informe)

4.3 Analizar la conveniencia para que cuando la normativa que dispone Tecnologías de Información sea revisada o actualizada como parte de sus procesos de diagnóstico, su resultado quede debidamente evidenciado como se establece en la normativa y específicamente en el apartado “Revisión y Actualización” de manera que se visualice y

Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000
auditoria@imas.go.cr

pueda dar trazabilidad si esta ha sido cambiada y/o actualizada desde su fecha de aprobación. (Véase punto 2.3 del acápite de resultados del presente informe)

PLAZOS DE RECOMENDACIONES

Para la implementación de las recomendaciones del informe, fueron acordados con la Administración (titulares subordinados correspondientes) los siguientes plazos y fechas de cumplimiento:

N° Recomendación	Fecha de Cumplimiento acordada
4.1	31/07/2025
4.2	30/05/2025
4.3	30/06/2025

JUAN CARLOS GARCIA CRUZ (FIRMA)
Firmado digitalmente por JUAN CARLOS GARCIA CRUZ (FIRMA)
Fecha: 2025.03.26 12:43:52 -06'00'

Realizado por
Juan Carlos García Cruz
PROFESIONAL EN AUDITORÍA GESTIÓN DE TECNOLOGÍA

WADY BERNY SOLANO SILES (FIRMA)
Firmado digitalmente por WADY BERNY SOLANO SILES (FIRMA)
Fecha: 2025.03.26 12:59:20 -06'00'

Revisado y aprobado
Wady Solano Siles
COORDINADOR DE LA UNIDAD DE AUDITORIA GESTIÓN DE TECNOLOGIA

MARIANELA NAVARRO ROMERO (FIRMA)
Firmado digitalmente por MARIANELA NAVARRO ROMERO (FIRMA)
Fecha: 2025.03.26 13:32:04 -06'00'

Marianela Navarro Romero
AUDITORA GENERAL

AUDITORIA INTERNA
Marzo, 2025