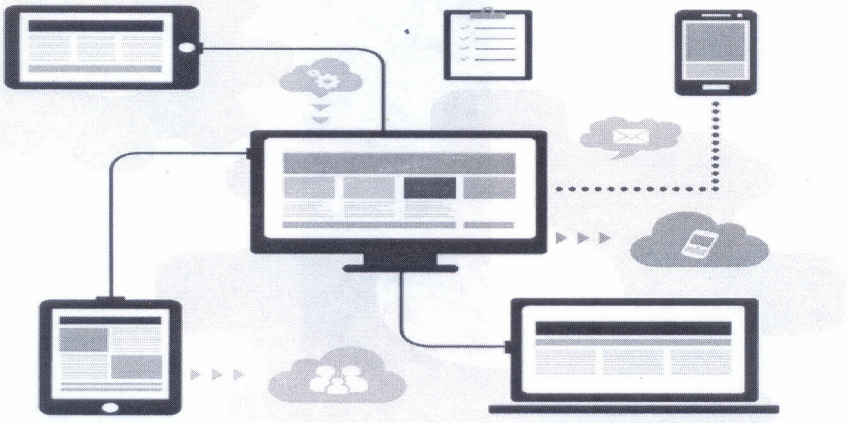
C-3-A 16/16

JAPDEVA

AUDITORÍA GENERAL

INFORME No. AG-AR-008-18

(28-02-2019)



ANÁLISIS SOBRE EL PROCESO DE MODIFICACIÓN Y MANTENIMIENTO DE PROGRAMAS INFORMÁTICOS

FEBRERO, 2019

166

AUDITORÍA GENERAL

ANÁLISIS SOBRE EL PROCESO DE MODIFICACIÓN Y MANTENIMIENTO DE PROGRAMAS INFORMÁTICOS

ÍNDICE

Limón, 28 de febrero del 2019
AG-AR-008-18

RESUMEN EJECUTIVO DEL INFORME DE AUDITORÍA "ANÁLISIS SOBRE EL PROCESO DE MODIFICACIÓN Y MANTENIMIENTO DE PROGRAMAS INFORMÁTICOS"

¿Qué examinamos?

La auditoría abarcó las acciones realizadas desde el 01 de enero del 2017 al 15 de febrero del 2019, ampliándose en aquellos casos en que se consideró necesario.

¿Por qué es importante?

El proceso de modificación y mantenimiento de programas informáticos, así como el desarrollo de nuevos módulos o sistemas de información, debe realizarse de conformidad con la normativa técnica, legal y reglamentaria correspondiente, de acuerdo con políticas y procedimientos formalmente establecidos para mantener la integridad de dichos procesos y evitar el acceso no autorizado, daño o pérdida de información.

¿Qué encontramos?

1. El Departamento de Cómputo carece de una política formalmente establecida sobre la justificación, autorización y documentación de solicitudes de modificación o mantenimiento de programas informáticos, lo que podría afectar la integridad de dichos procesos.

2. El Departamento de Informática carece de un Plan Anual de Trabajo, lo que no permite asignar y controlar el trabajo de sus colaboradores en forma adecuada.

3. En el Departamento de Informática no se han realizado estudios de valoración de riesgo institucional, lo que causa que no estén debidamente identificados y documentados los posibles riesgos y no se pueda responder en forma adecuada a las amenazas que puedan afectar las Tecnologías de Información (en adelante TI).

4. No se han establecido parámetros básicos de medición de la gestión del Departamento de Informática, lo que causa que no pueda evaluarse ni controlarse en forma adecuada la función sustantiva y vital de dicha

dependencia en procesos básicos como planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento de las TI.

5. En el Departamento de Informática no se han realizado autoevaluaciones de control interno, lo que causa una debilidad manifiesta en dicho control, ya que no se evalúa su efectividad y cumplimiento, no se mantiene un registro de las excepciones que se presenten ni de las medidas correctivas que se puedan implementar.

6. El Departamento de Informática carece de un procedimiento formalmente establecido para el mantenimiento o modificación de programas, lo que podría propiciar el acceso no autorizado, daño o pérdida de información.

7. En el Departamento de Informática no existe un control de solicitudes de modificación o mantenimiento de programas informáticos, lo que impide manejar en forma ordenada y debidamente documentada dichas solicitudes ni permite establecer prioridades en la atención de las mismas.

8. El Departamento de Informática no exige a las dependencias usuarias el uso de los formularios definidos para atender sus requerimientos, lo que les permite enviar las solicitudes por diferentes vías como notas, oficios, mensajes de correo electrónico, minutas de reuniones e inclusive en forma verbal y telefónica.

9. La Sección de Análisis y Programación carece de mecanismos de control para la asignación de trabajos a los analistas-programadores, lo que impide controlar la ejecución de sus labores mediante una adecuada programación, supervisión y registro de sus labores.

10. Los analistas-programadores utilizan un "super usuario" en el ambiente de Desarrollo y poseen acceso al ambiente de Producción, lo que podría causar la modificación no autorizada de programas, daño y pérdida de información.

11. El Departamento de Informática no lleva una bitácora formal de novedades o eventos de los servidores y sistemas de información, lo que impide determinar en forma fehaciente las razones por las cuales dichos servidores o sistemas dejaron de operar y el tiempo de interrupción de los servicios.

12. El Departamento de Informática no ha definido formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, lo que dificulta la atención de incidentes y levantar los sistemas y servidores en caso de emergencias calificadas.

¿Qué sigue?

1. Se recomienda a la Dirección Administrativa Financiera instruir a la División Financiera Contable y Departamento de Informática para que en un plazo perentorio elaboren y presenten ante esa Dirección las políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI y los procedimientos para el mantenimiento y puesta en producción del software e infraestructura tecnológica, tal como se solicitó en los Informes de Auditoría No. Au-Inf-002-15, AG-EE-04-16 y AG-AR-002-18.

2. Se insta a la División Financiera Contable a solicitar al Departamento de Informática la elaboración y presentación ante esa División del Plan Anual de Trabajo, correspondiente al año 2019, alineado a los objetivos estratégicos de la Institución.

3. Se recomienda a la División Financiera Contable instruir al Departamento de Informática para que coordine con la Unidad de Control Interno la realización del estudio de identificación y valoración de riesgos en dicha dependencia, de forma tal que sean considerados en un futuro cercano, para responder en forma adecuada a las amenazas que puedan afectar las TI.

4. Se insta a la Dirección Administrativa Financiera a instruir a la División Financiera Contable para que establezca parámetros básicos de medición de la gestión del Departamento de Informática, con el objetivo de evaluar y controlar el logro de los objetivos de esa dependencia y asegurar que dichos objetivos estén debidamente alineados con los planes estratégicos de la Institución.

5. Se recomienda a la División Financiera Contable instruir al Departamento de Informática para que realice autoevaluaciones anuales de control interno, con el fin de valorar la efectividad en el cumplimiento de sus funciones e implementar las medidas correctivas necesarias para atender las excepciones o atrasos en la ejecución de su Plan Anual de Trabajo.

6. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que establezca una lista o control formal de las solicitudes de modificación o mantenimiento de programas informáticos y de las solicitudes de nuevos desarrollos, con el objetivo de manejar en forma ordenada y debidamente documentada dichas solicitudes, estableciendo prioridades en la atención de las mismas.

7. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que adapte los formularios "Reporte de Incidencias" y "Solicitud de Nuevos Requerimientos" a las condiciones actuales y luego los envíe mediante oficio o circular a todo el personal de la Institución, indicando que su uso será obligatorio para solicitar la modificación o mantenimiento de

recursos informáticos, así como para solicitar el desarrollo de nuevos programas, módulos o sistemas de información.

7.1 Cada vez que la jefatura del Departamento de Informática reciba uno de los formularios arriba indicados, deberá otorgarle un número consecutivo y entregar la Hoja de Asignación formal al funcionario encargado de atenderlo.

7.2 Una vez que el funcionario del Departamento de Informática reciba la Hoja de Asignación correspondiente y se reúna con los usuarios de la dependencia solicitante, deben elaborarse todas las minutas no solamente de los acuerdos logrados y compromisos adquiridos por ambas partes, sino de la ejecución y aceptación satisfactoria de las pruebas, así como la aceptación de los cambios o nuevos desarrollos en el ambiente de Producción.

8. Se recomienda a la División Financiera Contable instruir al Departamento de Informática para que suspenda o bloquee en forma inmediata el acceso de los funcionarios de la Sección de Análisis y Programación en el ambiente de Producción y bloquee el super usuario denominado "ADVANCE" en el ambiente de Desarrollo.

9. Se recomienda a la División Financiera Contable solicitar al Departamento de Informática la confección de una bitácora formal de novedades o eventos de los servidores y/o sistemas de información, donde se registre claramente el evento o incidente presentado, así como las horas de inicio y fin del mismo.

10. Se insta a la División Financiera Contable a instruir al Departamento de Informática para que defina formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, considerando la prioridad que debe asignársele a los sistemas vitales para la operatividad de la Institución.

INFORME DE AUDITORÍA No. AG-AR-008-18

ANÁLISIS SOBRE EL PROCESO DE MODIFICACIÓN Y MANTENIMIENTO DE PROGRAMAS INFORMÁTICOS

1. INTRODUCCIÓN.

1.1 ORIGEN DEL ESTUDIO.

El presente análisis sobre el proceso de modificación y mantenimiento de programas informáticos, forma parte del Plan Anual de Trabajo de la Auditoría General para el año 2018.

1.2 OBJETIVOS DEL ESTUDIO.

1.2.1 OBJETIVO GENERAL.

Analizar si la modificación y mantenimiento de los programas informáticos se realiza de conformidad con la normativa técnica legal y reglamentaria correspondiente.

1.2.2 OBJETIVOS ESPECÍFICOS.

- Determinar si las actividades de control existentes aseguran que todas las tareas de modificación y mantenimiento de los programas informáticos cuentan con las debidas justificaciones y autorizaciones previas que las validen.

- Examinar si el proceso de modificación a los programas cuenta con un procedimiento definido por escrito, y si el mismo contempla actividades de control adecuadas que impidan la utilización de los cambios efectuados para fines distintos a los autorizados.

- Establecer las recomendaciones sobre posibles mejoras al proceso.

1.3 EQUIPO DE TRABAJO.

- Lic. Marvin Jiménez León, Auditor General.
- Lic. Mainor Segura Bejarano, Sub-Auditor General.
- Lic. Mainor Loría Núñez, Auditor Designado.

1.4 ALCANCE DEL ESTUDIO Y PERÍODO REVISADO.

El estudio abarcó políticas, procedimientos, actividades y documentación sobre la modificación y mantenimiento de programas informáticos, existente en el Departamento de Informática y Sección de Análisis y Programación, mediante el análisis de la información relacionada, según se detalla:

- Reporte de Incidencias, utilizado por las dependencias usuarias para solicitar la modificación y mantenimiento de programas en los sistemas de información.
- Formulario de Nuevos Requerimientos, utilizado por las dependencias usuarias para solicitar el desarrollo de nuevos programas, módulos o sistemas de información.
- Políticas y procedimientos para la modificación y mantenimiento de programas informáticos.
- Expediente de cada sistema de información, existente en la Sección de Análisis y Programación.

Adicionalmente se efectuaron entrevistas a los siguientes funcionarios, relacionados todos con la materia.

- MSc. René Palacios Castañeda, Jefe Departamento de Informática.
- Bach. Alexis Cubillo Solano, Jefe Sección Análisis y Programación.
- Bach. Walter Lamsick Alguera, Analista-programador.
- Bach. John Gordon South, Analista-programador.

Para la ejecución del trabajo se observaron las políticas definidas en el Manual de Normas Generales de Auditoría para el Sector Público (R-DC-064-2014), Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), Directrices Generales sobre Principios y Enunciados Éticos a observar por parte de los jerarcas, titulares subordinados, funcionarios de la CGR, auditorías internas y servidores públicos en general (D-2-2004-CO). Asimismo, se observó lo estipulado en la siguiente normativa:

- Ley General de Control Interno No. 8292, publicada en La Gaceta No. 169 del 04 de setiembre del 2002.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE), publicadas en La Gaceta No. 119 del 21 de junio del 2007.
- Reglamento para la utilización de recursos informáticos, publicado en La Gaceta No. 6 del 09 de enero del 2006.

El período que abarca el estudio está comprendido entre el 01 de enero del 2017 y el 15 de febrero del 2019, ampliándose en aquellos casos en que se consideró necesario.

1.5 LIMITACIONES.

No se presentaron limitaciones que afectaran la ejecución de la presente revisión.

2. RESULTADOS.

De la revisión efectuada se obtuvieron los siguientes resultados:

2.1 El Departamento de Cómputo carece de una política sobre la justificación, autorización y documentación de solicitudes de modificación o mantenimiento de programas informáticos.

De acuerdo con la documentación revisada en el Departamento de Informática, se determinó que dicha dependencia no posee una política formalmente establecida sobre la justificación, autorización y documentación de solicitudes de modificación o mantenimiento de programas informáticos, autorizada por las jefaturas.

En su Informe No. AG-EE-04-16, del 16 de mayo del 2016, esta Auditoría recomendó al Departamento de Cómputo "*elaborar y someter a la aprobación de la jefatura de División Financiera Contable una política sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI*".

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo III (Implementación de tecnologías de información), artículo 3.1 (Consideraciones generales de la implementación de TI), determinan lo siguiente:

> "*La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:*
>
> *a. Adoptar políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI*".
>
> (...)

Por su parte la Ley General de Control Interno No. 8292, en su capítulo III (La Administración Activa), sección I (Deberes del jerarca y los titulares subordinados), artículo 15 (Actividades de control), establece lo siguiente:

> *"Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
>
> *a) 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.*
>
> *b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
>
> (...)
>
> *v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación".*

En su oficio DCI-118-2017, del 22 de junio del 2017, la ex-jefatura del Departamento de Informática comunicó a esta Auditoría que dicha labor no se había iniciado, pero que se incluyó en la calendarización del Plan de Remediación del informe arriba indicado y sería concluida 31 de octubre del 2017, hecho que no sucedió.

Dado que la jefatura del Departamento de Informática renunció en forma inesperada y los seguimientos a los informes de auditoría los realizaba personalmente, sin conservar documentación que lo evidenciara y sin comunicarle a las jefaturas jerárquicas sobre lo realmente ejecutado y no se nombró oficialmente en un tiempo prudencial a su sustituto, nuevamente esta Auditoría recomendó en su Informe No. AG-AR-002-18 del 02 de julio del 2018, pero ahora a la División Financiera Contable, "*instruir al Departamento de Informática para que elabore y presente a esa División las políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI, solicitadas en informes anteriores de esta Auditoría*", sin que a la fecha de presentación del presente informe se haya realizado dicha labor.

La actual jefatura del Departamento de Informática, quien en ese entonces se desempeñaba como jefe de la Sección de Análisis y Programación y fue uno de los funcionarios designados para integrar el equipo de trabajo, argumentó el 26 de noviembre del 2018 que desconocía el oficio arriba mencionado y que nunca

recibió, verbalmente o por escrito, instrucciones de su jefatura para que elaborara junto a otros dos funcionarios las políticas mencionadas.

El hecho de que el Departamento de Informática no haya definido ni implementado formalmente una política sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI podría afectar no solamente la integridad de los procesos de implementación y mantenimiento de programas informáticos, sino que impide determinar si todas las solicitudes han sido debidamente justificadas, autorizadas y documentadas.

2.2 El Departamento de Informática carece de un Plan Anual de Trabajo.

El Departamento de Informática no ha definido un Plan Anual de Trabajo, mediante el cual se programen las actividades de modificación y mantenimiento de programas informáticos en la Sección de Análisis y Programación, indicando responsables, fechas de inicio y finalización de dichas actividades.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo II (Planificación y organización), artículo 2.1 (Planificación de las tecnologías de información), determinan lo siguiente:

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

Esas mismas Normas, en su capítulo III (Implementación de tecnologías de información), artículo 3.1 (Consideraciones generales de la implementación de TI), establecen lo siguiente:

> "*La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. Para esa implementación y mantenimiento debe:*
>
> (...)
>
> *h. Formular y ejecutar estrategias de implementación que incluyan todas las medidas para minimizar el riesgo de que los proyectos no logren sus objetivos, no satisfagan los requerimientos o no cumplan con los términos de tiempo y costo preestablecidos*".
>
> (...)

El actual jefe del Departamento de Informática no recibió de su antecesor, dada su renuncia inesperada, un Plan Anual de Trabajo y el 28 de noviembre del 2018 comunicó a esta Auditoría que buscaría en la documentación recibida dicho plan, pero a la fecha de presentación del presente informe no ha logrado localizarlo.

El hecho de que el ex-jefe del Departamento de Informática no elaborara ni presentara ante su jefatura y subalternos un Plan Anual de Trabajo no solo impide asignar y controlar el trabajo de sus colaboradores en forma adecuada, a pesar de estar distribuidos en tres secciones con su correspondiente jefatura, sino que no se brinda el apoyo racional y necesario a la Administración para que se logre el balance óptimo entre los requerimientos de los usuarios, su capacidad presupuestaria y las oportunidades que brindan las tecnologías nuevas y existentes.

2.3 En el Departamento de Informática no se han realizado estudios de valoración de riesgo institucional.

De acuerdo con información suministrada a esta Auditoría por la Unidad de Control Interno, se determinó que en el Departamento de Informática no se han realizado estudios de valoración de riesgo institucional en los últimos años.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.3 (Gestión de riesgos), establecen lo siguiente:

> "*La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable*".

Por su parte la Ley General de Control Interno No. 8292, en su capítulo III (La Administración Activa), sección II (Sistema Específico de Valoración de Riesgo), artículo 18, determina lo siguiente:

> "*Todo ente u órgano deberá contar con un sistema específico de valoración del riesgo institucional por áreas, sectores, actividades o tarea que, de conformidad con sus particularidades, permita identificar el nivel de riesgo institucional y adoptar los métodos de uso continuo y sistemático, a fin de analizar y administrar el nivel de dicho riesgo.*
>
> *La Contraloría General de la República establecerá los criterios y las directrices generales que servirán de base para el establecimiento y funcionamiento del sistema en los entes y órganos seleccionados, criterios y directrices que serán obligatorios y prevalecerán sobre los que se les*

opongan, sin menoscabo de la obligación del jerarca y titulares subordinados referida en el artículo 14 de esta Ley".

Según información suministrada el 23 de noviembre del 2018 por la jefatura de la Unidad de Control Interno, en el Departamento de Informática no se han realizado estudios de riesgos por las siguientes razones:

- El 13 de diciembre del 2017 indicó que "*el Sistema Específico de Valoración de Riesgo Institucional (en adelante SEVRI) se realizó en el año 2010 y que este año se intentó actualizarlo, mediante coordinación con las jefaturas de División Financiera Contable y Departamento de Informática, pero no fue posible debido a justificaciones o excusas esgrimidas por dichas áreas, consideradas pobres e irrelevantes, aparte de que han quedado en suspenso debido a una posible reestructuración de JAPDEVA*".

- El 22 de mayo del 2018 informó que "*la situación se mantiene igual o peor, ya que el jefe del Departamento de Informática está enfocado en atender demandas laborales y conflictos internos*".

- El 18 de julio del 2018 comunicó que "*lo descrito por mí el 13 de diciembre del 2017 ha empeorado, pues el jefe de informática renunció y el nuevo, que es el Sr. René Palacios Castañeda, apenas se está acomodando también, para hacerle el SEVRI habría que prácticamente pedirle permiso a la Sra. Karla Ávila, quien es su superior inmediato y esto para ella no es prioritario en este momento*".

- El 23 de noviembre del 2018 indicó que "*por instrucciones de la Gerencia General el único SEVRI que se pudo realizar este año es el relacionado con los objetivos estratégicos del Plan Operativo Institucional (POI) para el año 2019 del Departamento de informática".*

Dado lo anterior, esta Auditoría consultó el 07 de diciembre del 2018 a las jefaturas de División Financiera Contable y Departamento de Informática las razones por las cuales no ha sido posible la ejecución de dichos estudios, pero a la fecha de presentación del presente informe no se ha recibido su respuesta.

El hecho de que el Departamento de Informática no realice una gestión continua de riesgos, integrada al SEVRI y en conjunto con la Unidad de Control Interno, ocasiona que no estén debidamente identificados y documentados los posibles riesgos y por ello no se pueda responder en forma adecuada a las amenazas que puedan afectar las TI, como ya se han presentado en el pasado con el computador central y los servidores, limitando o impidiendo la operatividad de la Institución en caso de que la ocurrencia de dichos riesgos se materialice, pues no se cuenta con medidas preventivas o paliativas que minimicen sus efectos.

2.4 No se han establecido parámetros básicos de medición de la gestión del Departamento de Informática.

La División Financiera Contable no ha establecido parámetros básicos de medición de la gestión del Departamento de Informática ni ha realizado una evaluación regular de todos los procesos de TI a medida que transcurre el tiempo, para determinar su calidad y el cumplimiento de los requerimientos de control, por lo que no se tienen resultados tangibles ni objetivos de dicha evaluación.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo introductorio, establecen lo siguiente:

> *"El uso de las TI ha implicado, al menos, tres situaciones relevantes: la dedicación de porciones importantes del presupuesto de las organizaciones, con el costo de oportunidad que ello conlleva, principalmente en organizaciones con recursos limitados y actividades sustantivas esenciales para la sociedad; un marco jurídico cambiante tendente a buscar su paralelismo con las nuevas relaciones que se dan a raíz del uso de esas TI; y una presión importante de proveedores y consumidores por la implementación de más y mejores servicios apoyados en estas tecnologías.*
>
> *Dado el impacto de dichas situaciones, las TI deben gestionarse dentro de un marco de control que procure el logro de los objetivos que se pretende con ellas y que dichos objetivos estén debidamente alineados con la estrategia de la organización".*

Esas mismas Normas en su capítulo II (Planificación y organización), artículo 2.5 (Administración de recursos financieros), determinan lo siguiente:

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

Las Normas arriba indicadas, en su Glosario, definen **Gestión de las TI** como:

> *"El conjunto de acciones fundamentadas en políticas institucionales que, de una manera global, intentan dirigir la gestión de las TI hacia el logro de los objetivos de la organización. Para ello se procura, en principio, la alineación entre los objetivos de TI y los de la organización, el balance óptimo entre las necesidades de TI de la organización y las oportunidades que sobre ello existen, la maximización de los beneficios y el uso*

responsable de los recursos, la administración adecuada de los riesgos y el valor agregado en la implementación de dichas TI.

Tales acciones se relacionan con los procesos (planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento), recursos tecnológicos (personas, sistemas, tecnologías, instalaciones y datos), y con el logro de los criterios de fidelidad, calidad y seguridad de la información. También se entiende como Gobernabilidad de TI".

En ese mismo Glosario, las Normas arriba citadas definen **Seguimiento de las TI** como:

"La evaluación regular de todos los procesos de TI a medida que transcurre el tiempo para determinar su calidad y el cumplimiento de los requerimientos de control. Es parte de la vigilancia ejercida por la función gerencial sobre los procesos de control de la organización y la garantía independiente provista por la auditoría interna y externa u obtenida de fuentes alternativas".

Esta Auditoría consultó mediante correo electrónico el 08 de diciembre del 2017 a la ex-jefatura de División Financiera Contable y el 20 de noviembre del 2018 a la actual jefatura si se han establecido parámetros básicos de medición de la gestión de Informática, pero a la fecha de presentación del presente informe no se ha recibido su respuesta.

El hecho de que la División Contable Financiera no haya establecido parámetros básicos de medición de la gestión de Departamento de Informática causa que no pueda evaluarse ni controlarse en forma adecuada la función sustantiva y vital de dicha dependencia en procesos básicos como planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento de las TI, impidiendo que se evalúe el posible cumplimiento de objetivos que se pretende con ellas y que dichos objetivos estén debidamente alineados con la estrategia de la organización, utilizando en forma racional y responsable los recursos financieros invertidos en su gestión.

2.5 En el Departamento de Informática no se han realizado autoevaluaciones de control interno.

Esta Auditoría determinó que en el Departamento de Informática no se han realizado autoevaluaciones de control interno, las cuales conducirían a dicha dependencia al perfeccionamiento del sistema de control interno, que es de su entera responsabilidad.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo V (Seguimiento), artículo 5.2 (Seguimiento y evaluación del control interno en TI), determinan lo siguiente:

> "*El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas*".

Por su parte la Ley General de Control Interno No. 8292, en su capítulo III (La Administración Activa), sección I (Deberes del jerarca y los titulares subordinados), artículo 17 (Seguimiento del sistema de control interno), establece los siguiente:

> "*Entiéndese por sèguimiento del sistema de control interno las actividades que se realizan para valorar la calidad del funcionamiento del sistema de control interno, a lo largo del tiempo; asimismo, para asegurar que los hallazgos de la auditoría y los resultados de otras revisiones se atiendan con prontitud.*
>
> *En cuanto al seguimiento del sistema de control interno, serán deberes del jerarca y los titulares subordinados, los siguientes:*
>
> (...)
>
> *c) Que la administración activa realice, por lo menos una vez al año, las autoevaluaciones que conduzcan al perfeccionamiento del sistema de control interno del cual es responsable. Asimismo, que pueda detectar cualquier desvío que aleje a la organización del cumplimiento de sus objetivos*"
> (...)

Es necesario destacar que la anterior jefatura del Departamento de Informática comunicó a esta Auditoría el 11 de diciembre del 2017 y el 22 de mayo del 2018 que no se realizan autoevaluaciones de control interno, por lo que se consultó nuevamente el 20 de noviembre del 2018 al jefe actual, pero a la fecha de presentación del presente informe no se ha recibido respuesta.

El hecho de que el Departamento de Informática no realice autoevaluaciones de control interno causa una debilidad manifiesta en dicho control, ya que no se evalúa su efectividad y cumplimiento, no se mantiene un registro de las excepciones que se presenten ni de las medidas correctivas que se puedan implementar, aparte de que no es posible asegurar que los hallazgos de la auditoría y los resultados de otras revisiones se atiendan con prontitud, como ha ocurrido en los últimos años.

2.6 Ausencia de un procedimiento formalmente establecido para el mantenimiento o modificación de programas.

Según documentación revisada en el Departamento de Informática, se determinó que dicha dependencia no posee un procedimiento formalmente establecido para el mantenimiento y puesta en producción del software e infraestructura tecnológica, debidamente autorizado por las jefaturas.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.4.6 (Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica), determinan lo siguiente:

> *"La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.*
> *Para ello debe:*
>
> (...)
>
> *b) Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.*
>
> (...)

Por su parte la Ley General de Control Interno No. 8292, en su capítulo III (La Administración Activa), sección I (Deberes del jerarca y los titulares subordinados), artículo 15 (Actividades de control), establecen lo siguiente:

> *"Respecto de las actividades de control, serán deberes del jerarca y de los titulares subordinados, entre otros, los siguientes:*
>
> *a) 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.*
>
> *b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
>
> (...)

v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación".

En su Informe No. Au-Inf-002-15, del 14 de agosto del 2015, esta Auditoría recomendó al Departamento de Cómputo "*elaborar y someter a la aprobación de la jefatura de División Financiera Contable un procedimiento para el mantenimiento y puesta en producción del software e infraestructura tecnológica, así como los formularios para el Reporte de Incidencias y Solicitud de Nuevos Requerimientos*".

En su oficio DCI-118-2017, del 22 de junio del 2017, la ex-jefatura del Departamento de Informática comunicó a esta Auditoría que dicha labor no se había iniciado, pero que se incluyó en la calendarización del Plan de Remediación del informe arriba indicado y sería concluida 31 de octubre del 2017, hecho que no sucedió.

Dado que la jefatura del Departamento de Informática renunció en forma inesperada, los seguimientos a los informes de auditoría los realizaba personalmente, sin conservar documentación que lo evidenciara y sin comunicarle a las jefaturas jerárquicas sobre lo realmente ejecutado y no se nombró oficialmente en un tiempo prudencial a su sustituto, nuevamente esta Auditoría recomendó en su Informe No. AG-AR-002-18 del 02 de julio del 2018, pero ahora a la División Financiera Contable, "*instruir al Departamento de Informática para que elabore y presente a esa División el procedimiento para el mantenimiento y puesta en producción del software e infraestructura tecnológica*", sin que a la fecha de presentación del presente informe se haya realizado dicha labor.

El actual jefe del Departamento de Informática, quien fue uno de los funcionarios designados para integrar el equipo de trabajo, argumentó el 26 de noviembre del 2018 que desconocía el oficio arriba mencionado y que nunca recibió, verbalmente o por escrito, instrucciones de su jefatura para que elaborara junto a otros dos funcionarios los procedimientos de marras.

El hecho de que el Departamento de Informática carezca de un procedimiento formalmente establecido para el mantenimiento o modificación de programas, podría propiciar no solamente el acceso no autorizado, daño o pérdida de información, sino que impide establecer un punto de retorno a la situación actual, en caso de que las modificaciones no funcionen en forma adecuada.

2.7 En el Departamento de Informática no existe un control de solicitudes de modificación o mantenimiento de programas informáticos.

Esta Auditoría detectó que no existe un control formalmente establecido sobre las solicitudes que realizan las dependencias usuarias para las modificaciones y mantenimiento de programas informáticos.

Además de lo anterior, las reuniones donde los analistas-programadores analizan con los funcionarios de las dependencias usuarias los requerimientos formulados, pruebas efectuadas y verificación de cambios en el ambiente de Producción, entre otras cosas, carecen de minutas, pues según su opinión generalmente la atención brindada a dichas solicitudes se comunica mediante llamadas telefónicas o personalmente.

El Reglamento para la utilización de recursos informáticos, publicado en el año 2006, en su capítulo I (Del Departamento de Informática), artículo 1°, establece lo siguiente:

> *"El Departamento de Informática es el responsable de la administración de todo el equipo de cómputo, sus accesorios y la red en cuanto al mantenimiento preventivo y correctivo del equipo, instalación y mantenimiento de software, aplicaciones desarrolladas, configuración de equipo y ubicación"* (el subrayado no es del original).

Según lo informado a esta Auditoría el 21 de noviembre del 2018 por la jefatura del Departamento de Informática, no existe un control formalmente establecido sobre las solicitudes de mantenimiento o modificación de programas informáticos y el 03 de diciembre del año en curso los 4 funcionarios entrevistados reconocieron en las entrevistas efectuadas la inexistencia de minutas de reuniones con las dependencias usuarias.

Al no llevar formalmente el Departamento de Informática el control arriba indicado, no solamente incumple con su responsabilidad en la instalación y mantenimiento de software y aplicaciones desarrolladas, sino que impide manejar en forma ordenada y debidamente documentada dichas solicitudes ni se establecen prioridades en la atención de las mismas, tomando en consideración los escasos recursos disponibles y las necesidades estratégicas u operativas de la Institución.

Al carecerse de minutas de reuniones, resulta imposible verificar los asuntos tratados, los acuerdos logrados y compromisos acordados entre las partes, por lo que no se tiene la certeza, por ejemplo, si las pruebas se realizaron de conformidad, si los requerimientos fueron atendidos en forma satisfactoria y si se realizaron todas las validaciones en el ambiente de Producción por parte de las dependencias usuarias.

2.8 El Departamento de Informática no exige a las dependencias usuarias el uso de formularios para atender sus requerimientos.

Esta Auditoría determinó que el Departamento de Informática no exige a las dependencias usuarias el uso de los formularios denominados "Reporte de Incidencias" y "Solicitud de Nuevos Requerimientos", por lo que las solicitudes para modificación y mantenimiento de programas, así como las de nuevos desarrollos, se reciben por diferentes vías como notas, oficios, mensajes de correo electrónico, minutas de reuniones e inclusive en forma verbal y telefónica, según necesidades catalogadas como "urgentes" por las dependencias arriba indicadas.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.2 (Gestión de la calidad), determinan lo siguiente:

> "*La organización debe generar los productos y servicios de TI de conformidad con los requerimientos de sus usuarios con base en un enfoque de eficiencia y mejoramiento continuo*".

En el artículo 1.6 (Decisiones sobre asuntos estratégicos de TI) de ese mismo capítulo, las citadas Normas establecen lo siguiente:

> "*El jerarca debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización*".

Esas mismas Normas, en su capítulo 3 (Implementación de tecnologías de información), artículo 3.2 (Implementación de software), determinan lo siguiente:

> "*La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:*
> (...)
>
> *b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación post-implantación de la satisfacción de los requerimientos*".

(...)

Finalmente, las Normas arriba indicadas en su capítulo IV (Prestación de servicios y mantenimiento), artículo 4.4 (Atención de requerimientos de los usuarios de TI), establecen lo siguiente:

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

El 05 de diciembre del 2018 la jefatura de Sección de Análisis y Programación confirmó lo comunicado el 28 de noviembre del año en curso por uno de los analistas-programadores, respecto a la existencia de los formularios arriba indicados, los cuales no siempre se utilizan por las dependencias usuarias para tramitar sus solicitudes de cambios en los sistemas y nuevos desarrollos.

El hecho de que no se exija a los funcionarios de las dependencias usuarias el uso de los formularios denominados "Reporte de Incidencias" y "Solicitud de Nuevos Requerimientos", les permite enviar sus requerimientos por diferentes vías como notas, oficios, mensajes de correo electrónico, minutas de reuniones e inclusive en forma verbal y telefónica, causando que el Departamento de Informática no pueda controlar en forma adecuada y ordenada dichos requerimientos, pues resulta difícil asignar recursos y priorizar la atención de los mismos de manera eficaz, eficiente y oportuna.

2.9 Ausencia de mecanismos de control adecuados para la asignación de trabajos a los analistas-programadores.

Esta Auditoría determinó que en la Sección de Análisis y Programación no se cuenta con un control formalmente establecido para la asignación de trabajos a los analistas-programadores de las solicitudes de modificación o mantenimiento a los sistemas de información, pues generalmente se les entrega el oficio, Reporte de Incidencias, nota, mensaje de correo electrónico o se les indica verbalmente sobre la atención de un determinado requerimiento.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo IV (Prestación de servicios y mantenimiento), artículo 4.2 (Administración y operación de la plataforma tecnológica), determinan lo siguiente:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*

(...)

e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro".

(...)

Por su parte el Reglamento para la utilización de recursos informáticos, publicado en el año 2006, en su capítulo I (Del Departamento de Informática), artículo 1°, establece lo siguiente:

> *"El Departamento de Informática es el responsable de la administración de todo el equipo de cómputo, sus accesorios y la red en cuanto al mantenimiento preventivo y correctivo del equipo, instalación y mantenimiento de software, aplicaciones desarrolladas, configuración de equipo y ubicación"* (el subrayado no es del original).

El 23 de noviembre del 2018 los analistas-programadores entrevistados comunicaron a esta Auditoría que "este año *no se les entregó un Plan Anual de Trabajo para el mantenimiento o desarrollo de sistemas de información y que lo más cercano a ello es el Cuadro de Asignaciones que maneja la jefatura de la Sección arriba indicada, pero a pesar de que se les envió por correo electrónico, no se ha discutido por el atraso de la huelga y la acumulación de proyectos pendientes; están a la espera para programar dicha reunión*".

Al no llevar formalmente la Sección de Análisis y Programación el control arriba indicado, no solamente incumple con su responsabilidad en la asignación de trabajos para la instalación y mantenimiento de software, sino que impide controlar la ejecución de los trabajos de cada analista-programador mediante una adecuada programación, supervisión y registro de sus labores.

2.10 El Departamento de Informática no lleva una bitácora formal de novedades o eventos de los servidores y sistemas de información.

En el Departamento de Informática no existe una bitácora formal con novedades o eventos de los sistemas de información o servidores a su cargo, donde se indiquen claramente los problemas, errores o incidentes significativos y las horas en que los equipos y/o servicios se mantuvieron fuera de operación.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo IV (Prestación de servicios y mantenimiento), artículo 4.5 (Manejo de incidentes), determinan lo siguiente:

> "*La organización debe identificar, analizar y resolver de manera oportuna los problemas, errores e incidentes significativos que se susciten con las TI. Además, debe darles el seguimiento pertinente, minimizar el riesgo de recurrencia y procurar* el aprendizaje necesario".

Es necesario destacar que el 21 de noviembre del 2018 el jefe del Departamento de Informática comunicó a esta Auditoría que la bitácora de novedades o eventos se lleva informalmente.

El hecho de que no se lleve una bitácora de novedades o incidentes en forma adecuada impide determinar en forma fehaciente las razones por las cuales los servidores o sistemas de información dejaron de operar, el tiempo de interrupción de los servicios y tomar las medidas correctivas necesarias para subsanar los problemas, errores e incidentes reportados, estableciendo las responsabilidades del caso, si las hay.

2.11 Control inadecuado en los ambientes de Desarrollo y Producción.

A pesar de que se mantienen separados los ambientes de Desarrollo y Producción, el control sobre los mismos no es el adecuado, ya que en el primero de ellos se permite a los analistas-programadores el uso de un "super usuario" denominado "ADVANCE" (a pesar de que cada uno de ellos posee su propio código de acceso), el cual según la jefatura del Departamento de Informática fue creado por la empresa que diseñó, desarrolló e implementó el Sistema Integrado de Administración Financiera de JAPDEVA (conocido como SIAFJ) y en el caso del ambiente de Producción, todos los funcionarios de la Sección de Análisis y Programación poseen acceso con sus usuarios y contraseñas, aparte de que existe igualmente el "super usuario" arriba indicado.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo I (Normas de aplicación general), artículo 1.4.6), establecen lo siguiente:

> "*La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.*
>
> *Para ello debe:*
>
> (...)
>
> *c) Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.*

d) Controlar el acceso a los programas fuente y a los datos de prueba".

Esas mismas Normas, en su capítulo III (Implementación de tecnologías de información), artículo 3.2 (Implementación de software), determinan lo siguiente:

"*La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:*

(...)

c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.

d) Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.

(...)

f) Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento".

Finalmente, las Normas arriba indicadas, en su capítulo IV (Prestación de servicios y mantenimiento), artículo 4.2 (Administración y operación de la plataforma tecnológica), establecen lo siguiente:

"*La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*

(...)

f) Mantener separados y controlados los ambientes de desarrollo y producción".

(...)

De acuerdo con lo indicado el 21 de noviembre del 2018 por la jefatura del Departamento de Informática, se controla el acceso de los analistas-programadores en el ambiente de Producción y en el pase de programas del ambiente de Desarrollo al de Producción, pero "*no de la forma recomendada*".

Por su parte el jefe de la Sección de Análisis y Programación expresó el 28 de noviembre del año en curso que "*tal vez en forma errada se ha confiado en la buena fe y profesionalismo del personal a su cargo, pero lo cierto del caso es que a la fecha no se han detectado, presentado o denunciado cambios no autorizados por las jefaturas en los sistemas de información*".

Según criterio de esta Auditoría, la debilidad en el control interno se debe a la carencia de políticas y procedimientos formalmente establecidos para regular el proceso de mantenimiento y modificación de programas informáticos, estableciendo mediante los mismos un mecanismo formal para el pase (conversión y migración de programas) del ambiente de Desarrollo al de Producción y a que no se han definido con claridad las funciones, responsabilidades y permisos de acceso al personal del departamento arriba citado.

El hecho de que los analistas-programadores posean acceso en el ambiente de Producción podría causar la modificación no autorizada de programas, daño y pérdida de información, lo que dificulta mantener la integridad de los procesos de implementación y mantenimiento de programas informáticos.

2.12 El Departamento de Informática no ha definido formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos.

En el Departamento de Informática no se han definido formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007-CO-DFOE) en su capítulo III (Implementación de tecnologías de información), artículo 3.2 (Implementación de software), determinan lo siguiente:

> "*La organización debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:*
>
> (...)
> *e) Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos*"

(...)

Es necesario indicar que el 28 de noviembre del 2018 el jefe de la Sección de Análisis y Programación comunicó a esta Auditoría que no se han definido formalmente los criterios arriba indicados.

Al no definirse formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, se dificulta no solamente la atención de incidentes y levantar los sistemas y servidores en caso de emergencias calificadas, sino que interrumpe el trabajo normal de los programadores en las tareas asignadas con antelación, pues deben atender requerimientos catalogados como "urgentes" por las dependencias usuarias (según sus propios intereses), sin que el Departamento de Informática logre determinar "a priori" si dicha atención se debe a situaciones de verdadera emergencia institucional.

2.13 Análisis de riesgos y mapa térmico.

En el Anexo No. 1 se presentan los riesgos más relevantes, analizados en el presente estudio, considerando su probabilidad de ocurrencia, calificación (según su impacto para la Administración activa y Auditoría), nivel del riesgo y controles asociados, establecidos por dicha administración.

3. CONCLUSIONES.

De conformidad con los resultados del presente estudio, esta Auditoría arribó a las siguientes conclusiones:

3.1 El Departamento de Cómputo carece de una política formalmente establecida sobre la justificación, autorización y documentación de solicitudes de modificación o mantenimiento de programas informáticos, lo que podría afectar la integridad de dichos procesos.

3.2 El Departamento de Informática carece de un Plan Anual de Trabajo, lo que no permite asignar y controlar el trabajo de sus colaboradores en forma adecuada.

3.3 En el Departamento de Informática no se han realizado estudios de valoración de riesgo institucional, lo que causa que no estén debidamente identificados y documentados los posibles riesgos y no se pueda responder en forma adecuada a las amenazas que puedan afectar las Tecnologías de Información.

3.4 No se han establecido parámetros básicos de medición de la gestión del Departamento de Informática, lo que causa que no pueda evaluarse ni controlarse en forma adecuada la función sustantiva y vital de dicha dependencia en procesos básicos como planificación, organización, implementación, mantenimiento, entrega, soporte y seguimiento de las TI.

3.5 En el Departamento de Informática no se han realizado autoevaluaciones de control interno, lo que causa una debilidad manifiesta en dicho control, ya que no se evalúa su efectividad y cumplimiento, no se mantiene un registro de las excepciones que se presenten ni de las medidas correctivas que se puedan implementar.

3.6 El Departamento de Informática carece de un procedimiento formalmente establecido para el mantenimiento o modificación de programas, lo que podría propiciar el acceso no autorizado, daño o pérdida de información.

3.7 En el Departamento de Informática no existe un control de solicitudes de modificación o mantenimiento de programas informáticos, lo que impide manejar en forma ordenada y debidamente documentada dichas solicitudes ni se establecen prioridades en la atención de las mismas.

3.8 El Departamento de Informática no exige a las dependencias usuarias el uso de los formularios definidos para atender sus requerimientos, lo que les permite enviar las solicitudes por diferentes vías como notas, oficios, mensajes de correo electrónico, minutas de reuniones e inclusive en forma verbal y telefónica.

3.9 La Sección de Análisis y Programación carece de mecanismos de control para la asignación de trabajos a los analistas-programadores, lo que impide controlar la ejecución de sus labores mediante una adecuada programación, supervisión y registro de sus labores.

3.10 Los analistas-programadores utilizan un "super usuario" en el ambiente de Desarrollo y poseen acceso al ambiente de Producción, lo que podría causar la modificación no autorizada de programas, daño y pérdida de información.

3.11 El Departamento de Informática no lleva una bitácora formal de novedades o eventos de los servidores y sistemas de información, lo que impide determinar en forma fehaciente las razones por las cuales dichos servidores o sistemas dejaron de operar y el tiempo de interrupción de los servicios.

3.12 El Departamento de Informática no ha definido formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, lo que dificulta la atención de incidentes y levantar los sistemas y

servidores en caso de emergencias calificadas.

4. RECOMENDACIONES.

De conformidad con los hechos señalados y las conclusiones a las que arribó, esta Auditoría se permite efectuar las siguientes recomendaciones:

Para la Dirección Administrativa Financiera:

4.1 Instruir a la División Financiera Contable y Departamento de Informática para que en un plazo perentorio elaboren y presenten ante esa Dirección las políticas sobre la justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI y los procedimientos para el mantenimiento y puesta en producción del software e infraestructura tecnológica, tal como se solicitó en los Informes de Auditoría No. Au-Inf-002-15, AG-EE-04-16 y AG-AR-002-18.

4.2 Instruir a la División Financiera Contable para que establezca parámetros básicos de medición de la gestión del Departamento de Informática, con el objetivo de evaluar y controlar el logro de los objetivos de esa dependencia y asegurar que dichos objetivos estén debidamente alineados con los planes estratégicos de la Institución.

Para la División Financiera Contable:

4.3 Solicitar al Departamento de Informática la elaboración y presentación ante esa División del Plan Anual de Trabajo, correspondiente al año 2019, alineado a los objetivos estratégicos de la Institución.

4.4 Instruir al Departamento de Informática para que coordine con la Unidad de Control Interno la realización del estudio de identificación y valoración de riesgos en dicha dependencia, de forma tal que sean considerados en un futuro cercano, para responder en forma adecuada a las amenazas que puedan afectar las TI.

4.5 Instruir al Departamento de Informática para que realice autoevaluaciones anuales de control interno, con el fin de valorar la efectividad en el cumplimiento de sus funciones e implementar las medidas correctivas necesarias para atender las excepciones o atrasos en la ejecución de su Plan Anual de Trabajo.

4.6 Instruir al Departamento de Informática para que establezca una lista o control formal de las solicitudes de modificación o mantenimiento de programas informáticos y de las solicitudes de nuevos desarrollos, con el objetivo de

manejar en forma ordenada y debidamente documentada dichas solicitudes, estableciendo prioridades en la atención de las mismas.

4.7 Instruir al Departamento de Informática para que adapte los formularios "Reporte de Incidencias" y "Solicitud de Nuevos Requerimientos" a las condiciones actuales y luego los envíe mediante oficio o circular a todo el personal de la Institución, indicando que su uso será obligatorio para solicitar la modificación o mantenimiento de recursos informáticos, así como para solicitar el desarrollo de nuevos programas, módulos o sistemas de información.

4.7.1 Cada vez que la jefatura del Departamento de Informática reciba uno de los formularios arriba indicados, deberá otorgarle un número consecutivo y entregar la Hoja de Asignación formal al funcionario encargado de atenderlo.

4.7.2 Una vez que el funcionario del Departamento de Informática reciba la Hoja de Asignación correspondiente y se reúna con los usuarios de la dependencia solicitante, deben elaborarse todas las minutas no solamente de los acuerdos logrados y compromisos adquiridos por ambas partes, sino de la ejecución y aceptación satisfactoria de las pruebas, así como la aceptación de los cambios o nuevos desarrollos en el ambiente de Producción.

4.8 Instruir al Departamento de Informática para que suspenda o bloquee en forma inmediata el acceso de los funcionarios de la Sección de Análisis y Programación en el ambiente de Producción y bloquee el super usuario denominado "ADVANCE" en el ambiente de Desarrollo.

4.9 Solicitar al Departamento de Informática la confección de una bitácora formal de novedades o eventos de los servidores y/o sistemas de información, donde se registre claramente el evento o incidente presentado, así como las horas de inicio y fin del mismo.

4.10 Instruir al Departamento de Informática para que defina formalmente los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, considerando la prioridad que debe asignársele a los sistemas vitales para la operatividad de la Institución.

Lic. Mainor Loría Núñez
Auditor Designado

Lic. Mainor Segura Bejarano
Sub-Auditor General

Lic. Marvin Jiménez León
Auditor General

AUDITORÍA GENERAL

ANEXO No. 1: Análisis de riesgos y mapa térmico

A. Posibles Riesgos o eventos	Calificación (Según su impacto para la Auditoría Interna)	Calificación (Según su impacto para la Administración activa)	Nivel de riesgo (B*C)	Ref. P. de T.
En el Departamento de Informática no hay un control establecido que enliste las solicitudes de modificación y/o mantenimiento de programas informáticos tramitados por las distintas dependencias usuarias, ni la priorización de cada una de ellas, lo que podría dificultar la asignación de recursos necesarios para atenderlas con oportunidad	5	4	Muy alto	E-1-A
No ha sido posible establecer el uso obligatorio por parte de las dependencias usuarias del Reporte de Incidencias y el Formulario de Nuevos Requerimientos, lo que ocasiona que se reciban solicitudes, incidencias y nuevos requerimientos por múltiples vías como por ejemplo oficios, mensajes de correo electrónico, minutas de reuniones, llamadas telefónicas o instrucciones verbales, limitando al Departamento de Informática para que valore, atienda y documente en forma adecuada todas las solicitudes recibidas	4.3	4	Muy alto	E-1-B
No siempre se documentan las minutas de las reuniones que se realizan entre los analistas-programadores y los funcionarios de las dependencias usuarias, manejándose información incompleta sobre los asuntos tratados, acuerdos logrados o compromisos acordados, por lo que no se tiene la certeza, por ejemplo, si las pruebas se realizaron de conformidad, si los requerimientos fueron atendidos en forma satisfactoria y si se realizaron todas las validaciones en el ambiente de Producción por parte de las dependencias usuaria	4.3	3.8	Muy alto	E-1-D
Al no haberse exigido a las dependencias usuarias el uso del Reporte de Incidencias y el Formulario de Nuevos Requerimientos existe el riesgo de que las jefaturas por la vía telefónica o verbalmente ordenen la atención inmediata de solicitudes no contemplados inicialmente por la jefatura de la Sección de Análisis y Programación a la hora de asignar los recursos correspondientes, lo que contribuye a la informalidad con que se atienden las solicitudes recibidas y ocasiona el cambio de prioridades en la ejecución de tareas programadas	4.3	4.3	Muy alto	E-1-F

Área de mapa Térmico

Muy alto	4
Alto	0
Medio	0
Bajo	0
Muy bajo	0