INFORME Nº 009-2017

INDICE

DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION Y COMUNICACION

RESUMEN EJECUTIVO
DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION Y COMUNICACION

En cumplimiento del Plan Anual de Trabajo del año 2017, se realizó una auditoría operativa, sobre el Departamento de Tecnologías de Información y Comunicación, cuyos objetivos fueron:

- Evaluar el cumplimiento de las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por la Contraloría General de la República y la Directriz con las regulaciones técnicas sobre la administración de los documentos producidos por medios automáticos emitida por la Junta Administrativa de la Dirección General del Archivo Nacional.

- Verificar la existencia del plan de acción para el cumplimiento de las Normas de T.I.

- Evaluar que se hayan adoptado las acciones para cumplir con el plan o con lo que disponen las normas.

- Evaluar la suficiencia y competencia del sistema de control interno.

- Verificar el cumplimiento de la normativa interna emitida.

El periodo del estudio comprendió de enero a diciembre del 2016, ampliándose en los casos que se consideró necesario. Para efectos del trabajo se verificó lo siguiente: **Controles de:** acceso, roles y niveles de privilegio, servicios de mantenimiento, desechos y reutilización de recursos de TI, ingreso y salida de equipos, , cumplimiento de que las copias de seguridad o Backups se realizan, **existencia de:** Comité Gerencial de Informática, publicación del Manual de Políticas y Estándares en Seguridad Informática, plan para el establecimiento de medidas de seguridad de la información, plan de contingencia ante desastres, políticas sobre justificación, autorización y documentación de solicitudes de mantenimiento de TI, procedimiento para la definición de los términos de referencia, procedimiento para la formalización de acuerdos de servicio de mantenimiento, procedimiento de la operación de la plataforma tecnológica, registro actualizado de los componentes de hardware y software, evaluaciones de efectividad y cumplimiento efectuadas por el jerarca a la gestión de TI, registro de las visitas autorizadas al Área de Servidores, solicitudes de equipos de protección contra incendios, inundaciones, etc, inventario de licencias, equipos físicos y programas instalados, estudio de factibilidad para adquisición de software y hardware, **inspecciones oculares de:** Ubicación física de los recursos de TI, protección y custodia de la información almacenada, funciones, responsabilidades y permisos del personal de TI.

Asimismo, se realizó una visita al Centro de Datos Alternos del MEIC, arrendado al Instituto Costarricense de Electricidad, ubicado en Guatuso del Guaco de Cartago, con la finalidad de efectuar una verificación acerca de las medidas de seguridad existentes, de acuerdo al contrato suscrito.

Seguidamente, se citan los resultados obtenidos de la revisión realizada:

- Debilidades de control en formularios “Boleta de Préstamo de equipo”.
- Ausencia de controles en servicios de mantenimiento.
- Ausencia de funciones, responsabilidades y permisos de acceso al personal a cargo de labores de implementación y mantenimiento de software.
- Ausencia de procedimiento para formalización de acuerdos de servicio.
- Ausencia de solicitudes de requerimiento de equipos de protección a la Dirección Administrativa.
- Ausencia de plan de contingencias.
- Ausencia de Comité Gerencial de Informática.
- Ausencia de control de backups o copias de respaldo y custodia inadecuada.
- Ausencia de planta eléctrica.
- Incumplimiento en envío de informes anuales.
- Ausencia de documentación de respaldo en Ciclo de Vida de Desarrollo de Sistemas.
- Ausencia de evaluaciones de efectividad y cumplimiento a la gestión de TI.
- Ausencia de contrato o convenio para el almacenamiento de base de datos de ASEMEIC en los servidores del MEIC.

De acuerdo con las verificaciones efectuadas al Departamento de Tecnologías de Información y Comunicación, se concluye, que en el periodo evaluado, se detectaron debilidades de control interno en relación con: control en formularios de "Boleta de Préstamo de Equipo", controles en servicios de mantenimiento, ausencia de funciones, responsabilidades y permisos de acceso al personal a cargo de labores de implementación y mantenimiento del software, ausencias de: procedimiento para formalización de acuerdos de servicio, solicitudes de requerimiento de equipos de protección a la Dirección

Administrativa, plan de contingencias, Comité Gerencial de Informática, control de backups o copias de respaldo y custodia inadecuada, documentación de respaldo en Ciclo de Vida de Desarrollo de Sistemas, evaluaciones de efectividad y cumplimiento a la gestión de TI, envío de informes anuales

No existe una planta eléctrica para abastecer los servidores ubicados en DTIC, ya que en la actualidad se corre el riesgo, de que, si se da una interrupción prolongada del fluido eléctrico, se puede perder información.

Asimismo, no existe un contrato o convenio para el almacenamiento de la base de datos de ASEMEIC, en los servidores del MEIC.

Por otra parte, la Jefatura de DTIC y la Dirección Administrativa Financiera, no están revisando ni supervisando en forma continua que los controles se estén ejerciendo.

Se obtuvieron resultados satisfactorios en relación a:

- Controles de acceso, roles y niveles de privilegio existentes.
- Publicación del Manual de Políticas y Estándares en Seguridad Informática.
- Existencia de un plan para el establecimiento de medidas de seguridad de la información y evaluación periódica del impacto de esas medidas.
- Manejo de los desechos y reutilización de recursos de TI.
- Políticas sobre justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
- Funciones por escrito asignadas por la jefatura, a todos los funcionarios de TI.

- Procedimiento para la definición de los términos de referencia que incluyan las especificaciones y requisitos o condiciones requeridas o aplicables, así como para la evaluación de ofertas (contratos con terceros en procesos de implementación o mantenimiento de software e infraestructura).

- Procedimiento para la administración y operación de la plataforma tecnológica.

- Registro actualizado de los componentes de hardware y software).

- Registro escrito de las visitas autorizadas al área de servidores.

- Inventario de licencias, equipos físicos y programas instalados.

- Estudio de factibilidad para adquirir hardware y software y para el desarrollo de nuevos sistemas de información computarizados.

Asimismo, en relación con la visita realizada al Centro de Datos Alternos del MEIC, arrendado al Instituto Costarricense de Electricidad, ubicado en Guatuso del Guarco de Cartago, en cuanto a las medidas de seguridad existentes, los resultados fueron satisfactorios.

Con el fin de subsanar las debilidades detectadas se giraron once recomendaciones a la Dirección Administrativa Financiera y una a la señora Ministra, las que deberán atenderse conforme a lo establecido en la Ley N° 8292 Ley General de Control Interno.

INFORME Nº 009-2017

DEPARTAMENTO DE TECNOLOGIAS DE INFORMACION Y COMUNICACION

1. INTRODUCCIÓN

1.1 Origen

El presente informe se origina en la ejecución de un estudio de auditoría operativa, sobre el Departamento de Tecnologías de Información y Comunicación, efectuado en cumplimiento del Plan Anual de Trabajo del año 2017.

1.2 Objetivos

- Evaluar el cumplimiento de las Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por la Contraloría General de la República y la Directriz con las regulaciones técnicas sobre la administración de los documentos producidos por medios automáticos emitida por la Junta Administrativa de la Dirección General del Archivo Nacional.
- Verificar la existencia del plan de acción para el cumplimiento de las Normas de T.I.
- Evaluar que se hayan adoptado las acciones para cumplir con el plan o con lo que disponen las normas.
- Evaluar la suficiencia y competencia del sistema de control interno.
- Verificar el cumplimiento de la normativa interna emitida.

1.3 Naturaleza y Alcance

El periodo del estudio comprendió de enero a diciembre del 2016, ampliándose en los casos que se consideró necesario. Para efectos del trabajo se verificó la siguiente información:

- **Controles de:** acceso, roles y niveles de privilegio, servicios de mantenimiento, desechos y reutilización de recursos de TI, ingreso y salida de equipos y cumplimiento de que las copias de seguridad o Backups se realizan.

- **Existencia de:** Comité Gerencial de Informática, publicación del Manual de Políticas y Estándares en Seguridad Informática, plan para el establecimiento de medidas de seguridad de la información, plan de contingencia ante desastres, políticas sobre justificación, autorización y documentación de solicitudes de mantenimiento de TI, procedimiento para la definición de los términos de referencia, procedimiento para la formalización de acuerdos de servicio de mantenimiento, procedimiento de la operación de la plataforma tecnológica, registro actualizado de los componentes de hardware y software, evaluaciones de efectividad y cumplimiento efectuadas por el jerarca a la gestión de TI, registro de las visitas autorizadas al Área de Servidores, solicitudes de equipos de protección contra incendios, inundaciones, etc, inventario de licencias, equipos físicos y programas instalados, estudio de factibilidad para adquisición de software y hardware, funciones, responsabilidades y permisos del personal de TI

- I**nspecciones oculares de:** Ubicación física de los recursos de TI, protección y custodia de la información almacenada.

- Se realizó una visita al Centro de Datos Alternos del MEIC, arrendado al Instituto Costarricense de Electricidad, ubicado en Guatuso del Guarco de Cartago, con la finalidad de efectuar una verificación acerca de las medidas de seguridad existentes, de acuerdo al de acuerdo al contrato suscrito.

El estudio se realizó de conformidad con el Manual de Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República y supletoriamente, con las Normas Internacionales de Auditoría Interna promulgadas por el IIA Global, así como el Reglamento de Organización y Funciones de la Auditoría Interna del Ministerio de Economía, Industria y Comercio.

1.4 Marco de referencia

- Ley General de Control Interno Nº 8292 y normativa conexa

- Normas de Control Interno para el Sector Público, Gaceta No 26 del 06 de febrero del 2009.

- Manual de Políticas y Estándares en Seguridad Informática.

- Procedimiento para el Uso de Equipo de Computo dentro del Ministerio de Economía, Industria y Comercio.

- Reglamento del Servicio del Comité Gerencial de Informática, Decreto 33628-MEIC.

- Reglamento para la Protección de los Programas de Computo en los Ministerios e Instituciones Adscritas al Gobierno Central., Decreto 37549-JP – Presidencia de la República.

- Normas técnicas para la gestión y el control de las Tecnologías de Información emitidas por la Contraloría General de la República.

1.5 Siglas

- **DTIC.** Departamento de Tecnologías de Información y Comunicación.
- **TIC.** Tecnologías de Información y Comunicación.
- **SCI.** Sistema de control interno.
- **MEIC.** Ministerio de economía, Industria y Comercio.
- **ASEMEIC.** Asociación Solidarista de Empleados del Ministerio de Economía, Industria y Comercio.
- **MTSS**. Ministerio de Trabajo y Seguridad Social.

2. RESULTADOS OBTENIDOS

2.1 Debilidades de control en formularios “Boleta de Préstamo de equipo”

En la revisión efectuada a los formularios “Boleta de Préstamos de Equipo”, utilizada para el control de ingreso y salida de equipos, se determinó que no tienen numeración consecutiva en el espacio asignado para llevar este control; asimismo, se presentan inconsistencias en relación a la información que debe consignarse en los espacios de la parte inferior de los formularios (**RECIBIDO CONFORME DE DTIC**), en algunos se llena toda la información, en otros parcialmente y otros están en blanco.

Esta situación obedece a que no se ha establecido un control consecutivo en los formularios; por otra parte, las personas que entregan y reciben los equipos, omiten llenar en todos los espacios del formulario la información que se requiere; asimismo, falta de supervisión por parte de la jefatura de DTIC.

Con respecto a esta situación, las Normas de Control Interno para el Sector Público, en la norma 4.4.2 “Formularios uniformes”, establece:

"El jerarca y los titulares subordinados, según sus competencias, deben disponer lo pertinente para la emisión, la administración, el uso y la custodia, por los medios atinentes, de formularios uniformes para la documentación, el procesamiento y el registro de las transacciones que se efectúen en la institución. Asimismo, deben prever las seguridades para garantizar razonablemente el uso correcto de tales formularios". (El destacado no es del original).

Por otra parte, la norma 4.5.1 "Supervisión constante", estipula:

"El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos". (El destacado no es del original).

Esta situación representan una deficiencia de control, en cuanto a que, no se le da el uso correcto a los formularios; asimismo, no se tiene un control establecido en relación a la numeración consecutiva.

2.2 Ausencia de controles en servicios de mantenimiento

Al realizar la verificación de los controles existentes en relación a los servicios de mantenimiento que brinda DTIC, la jefatura manifestó mediante correo electrónico, que no existen controles al respecto.

En relación a la ausencia de controles, el Jefe de DTIC manifestó *"… por otras ocupaciones de los técnicos no se brinda el mismo. Se brinda mantenimiento cuando algún funcionario lo solicita únicamente, o cuando los técnicos determinan que hay que hacerlo en alguna computadora, ya sea por lentitud, virus u otro asunto".* Asimismo, la Jefatura de DTIC, ha omitido establecer los controles respectivos.

Referente a esta situación, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en la norma 1.4.3 "Seguridad física y ambiental", dispone:

"*La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. // Como parte de esa protección debe considerar: … d. El debido control de los servicios de mantenimiento".* (El destacado no es del original).

Por otra parte, las Normas de Control Interno para el Sector Público, en la norma 4.1 "Actividades de control", se estipula:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI (…)". Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad. / El ámbito de aplicación de tales actividades de control debe estar referido a todos los niveles y funciones de la institución. En ese sentido, la gestión institucional y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior, debe hacer posible la prevención, la detección y la corrección ante debilidades del SCI y respecto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante". (El destacado no es del original).

La ausencia de controles en los servicios de mantenimiento que brinda la DTIC, representa una debilidad de control, en cuanto a que los recursos tecnológicos deben estar bajo medidas de control establecidas para su seguridad y protección; asimismo se da un incumplimiento a la normativa establecida.

2.3 Ausencia de funciones, responsabilidades y permisos de acceso al personal a cargo de labores de implementación y mantenimiento de software

Al solicitarle a la Jefatura DTIC las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software, se determinó que estas no se encuentran formalmente por escrito, la jefatura manifiesta mediante correo electrónico, que las labores se asignan por correos electrónicos, verbalmente o por medio de la cuenta de correo "Incidentes"; asimismo, esta Jefatura ha omitido establecer el control respectivo.

Con respecto a esta situación las Normas de Control Interno para el Sector Público, en la norma 2.5.1 "Delegación de Funciones", se estipula:

"El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que la delegación de funciones se realice de conformidad con el bloque de legalidad, y de que conlleve la exigencia de la responsabilidad correspondiente y la asignación de la autoridad necesaria para que los funcionarios respectivos puedan tomar las decisiones y emprender las acciones pertinentes." (El destacado no es del original).

Asimismo, en las Normas de Control Interno para el Sector Público, en la norma 4.1 "Actividades de control", se establece:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad…". (El destacado no es del original).

El personal a cargo de las labores de implementación y mantenimiento de software, al no tener por escrito las funciones y responsabilidades asignadas, representa una debilidad de control, ya que resulta difícil establecer responsabilidades ante eventuales situaciones que vayan en perjuicio de la Institución.

2.4 Ausencia de procedimiento para formalización de acuerdos de servicio

Al realizar la verificación de la existencia de un procedimiento para la formalización de acuerdos de servicio, la Jefatura DTIC mediante correo electrónico, manifestó que no existe ningún procedimiento para la formalización de acuerdos de servicio, lo cual obedece, a que la Jefatura ha omitido establecer el procedimiento respectivo.

En relación con esta situación, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en la norma 4.1 "Definición y administración de acuerdos de servicio", estipula:

"La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades. // El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben: … d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos". (El destacado no es del original). (El destacado no es del original).

Por otra parte, las Normas de Control Interno para el Sector Público, en la norma 4.1 "Actividades de control", se establece:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad…". (El destacado no es del original).

Esta situación representa una debilidad de control, dado que, al no existir un procedimiento para la formalización de los acuerdos de servicio, por lo que se da un incumplimiento a la normativa establecida.

2.5 Ausencia de solicitudes de requerimiento de equipos de protección a la Dirección Administrativa

Con respecto a la existencia de solicitudes de los equipos de protección, para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS, efectuadas por la jefatura DTI a la Dirección Administrativa Financiera, la Jefatura DTIC manifestó mediante correo electrónico, que:

"… No hay ninguna solicitud formal para tener equipos de protección para las instalaciones contra incendios, inundaciones…. Pues automáticamente la administración asigna extintores, también se adquieren las unidades de respaldo eléctrico pero basados en las necesidades de mantener 'arriba' toda la red informática".

Está situación obedece, a que la jefatura DTIC ha omitido realizar las solicitudes de requerimiento de equipos de protección, considerando únicamente los asignados por la administración, como por ejemplo los extintores.

Con respecto a las solicitudes, el Manual de Políticas y Estándares en Seguridad Informática del MEIC, en el numeral 4 "Administración de Operaciones en el Centro de Computo", punto 4.1.7, estipula:

"El Jefe de la DTIC deberá solicitar a la Dirección Administrativa y Oficialía Mayor los equipos de protección para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo, UPS". (El destacado no es del original).

Asimismo, las Normas de Control Interno para el Sector Público, en la norma 4.1 "Actividades de control", se establece:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad…". (El destacado no es del original).

La ausencia de solicitudes de requerimiento de equipos de protección, por parte de la Jefatura DTIC, representa una debilidad de control, en cuanto a que, este departamento es el responsable de realizar los requerimientos específicamente para la protección de los equipos y no descargar esta responsabilidad en la administración, lo cual, ante un eventual siniestro que vayan en perjuicio de la Institución, resulte difícil establecer responsabilidades.

2.6 Ausencia de plan de contingencias

En relación con la existencia de un plan de contingencias ante desastres para mitigar los riesgos de accidentes internos o externos, la Jefatura DTIC manifestó mediante correo electrónico, que se elaboró un Manual de Políticas de Contingencia y Otros, que en su momento se solicitó ser revisado por las autoridades, pero a la fecha no se ha realizado la respectiva revisión ni aprobación; no obstante, se denota falta de seguimiento y omisión de acciones por parte de la Jefatura DTIC, para que exista un plan de contingencias debidamente analizado, revisado y aprobado.

Con respecto al plan de contingencias, el Manual de Políticas y Estándares en Seguridad Informática del MEIC, en el numeral 4.11 “Planes de Contingencia ante Desastre”, punto 4.11.1, estipula:

“El plan de contingencia debe darse con fin de asegurar, recuperar restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total”. (El destacado no es del original).

Asimismo, el punto 4.11.2 de este Manual, establece:

“La DTIC debe tener en existencia la documentación de roles detallados y tareas para cada una de las personas involucradas en la ejecución del plan de recuperación ante desastre”. (El destacado no es del original).

Por otra parte, las Normas de Control Interno para el Sector Público, en la norma 4.1 “Actividades de control”, se establece:

“El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad…”. (El destacado no es del original).

La ausencia de un plan de contingencias, representa una debilidad de control, en cuanto a que, la Institución carece de un plan debidamente analizado, revisado, aprobado y probado por parte de la jefatura DTIC y la administración, para poder mitigar los riesgos ante eventuales desastres; asimismo, en el caso que ocurras un siniestros que vayan en perjuicio de la Institución, resulte difícil establecer responsabilidades.

2.7 Ausencia de Comité Gerencial de Informática

Con respecto a la existencia del Comité Gerencial de Informática del MEIC, el Despacho de la señora Ministra mediante memorando DM-MEM-062-17 del 28 de setiembre del 2017, manifestó lo siguiente:

"… la última minuta disponible referente a las reuniones del Comité Gerencial de Informática, minuta número 03-2009 del 23 de octubre del 2009… a partir de esa fecha no hay evidencia de que se haya reunido dicho Comité // De acuerdo a la normativa vigente, se entiende que ese Comité actualmente no está conformado ya que el decreto 33628-MEC establece en su artículo 6, que "Los nombramientos se realizarán por un periodo de dos años prorrogables por periodos iguales" // Dado lo anterior, se ha estado trabajando en el tema para el cual fue creado el Comité Gerencial de Informática y para facilitar el proceso, en principio se va a conformar de acuerdo con lo que establece el capítulo III De la Organización, Artículo 6 el decreto 33628-MEIC del Lunes 19 de marzo del 2007… // En los próximos días, ese Comité se estará conformando mediante resolución de la señora ministra e incluso se ha programado convocarlo a sesión para el 11 de octubre del año en curso" (El destacado no es del original).

En relación con esta situación, el Reglamento de Servicio del Comité Gerencial de Informática del Ministerio de Economía, Industria y Comercio, en el artículo 6 "Integración", dispone:

"El Comité Gerencial de Informática será designado por resolución del máximo jerarca del MEIC…" (El destacado no es del original).

Asimismo, el artículo 8 "De las sesiones", estipula:

"El Comité sesionará al menos una vez al mes en el lugar y hora que dicho órgano disponga…" (El destacado no es del original).

Por otra parte, las Normas de Control Interno para el Sector Público, en la norma 4.1 "Actividades de control", se establece:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad…". (El destacado no es del original).

La ausencia del Comité Gerencial de Informática del MEIC, representa una debilidad de control, ya que su función principal, es dar asesoramiento al jerarca en cuanto a la administración de los sistemas de información y de los recursos humanos, materiales y financieros que se destinan para su desarrollo, y en este momento no existe; asimismo, se está dando un incumplimiento a la normativa establecida.

Con respecto a esta situación no se gira ninguna recomendación, toda vez que en la resolución del Despacho de la Ministra DM-064-2017, del 27 de octubre del 2017, se dispone lo siguiente:

"SE PROCEDE A LA DESIGNACION DE LOS MIEMBROS DEL COMITÉ GERECIAL DE INFORMATICA DEL MINISTERIO DE ECONOMÍA, INDUSTRIA Y COMERCIO, DE CONFORMIDAD CON EL ARTÍCULO 6 DEL DECRETO EJECUTIVO No 33628-MEIC DEL 16 DE ENERO DE DOS MIL SIETE".

2.8 Ausencia de control de backups o copias de respaldo y custodia inadecuada

En relación con los backups o copias de respaldo que debe realizar cada funcionario, no se realiza el control por parte DTIC, en cuanto a la verificación que debe realizarse en forma periódica. Asimismo, al realizar una inspección ocular en algunas dependencias, se determinó disco duro externo ubicado en el mueble aéreo y otro encima del cubículo (ambos a la vista).

En cuanto al incumplimiento de verificar si los backups o copias de respaldo se realizan en forma periódica, se da, porque DTIC ha omitido realizar el control respectivo.

Con respecto a la custodia inadecuada de los discos duros, obedece a la falta de cuidado por parte de los funcionarios responsables de realizar esta función; asimismo, ausencia de procedimientos específicos para estos efectos.

Con respecto al cumplimiento del control de las copias de seguridad o Backups, el Manual de Políticas y Estándares en Seguridad Informática del MEIC, en el numeral 4.10. "Controles para la Generación y Restauración de Copias de Respaldo (Backups)", punto 4.10.4, dispone:

"Las copias de seguridad o Backups se deben realizar al menos una vez por quincena. Un funcionario de DTIC revisará el cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad". (El destacado no es del original).

Asimismo, las Normas de Control Interno para el Sector Público, en la norma 4.1 "Actividades de control", se establece:

"El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. Dichas actividades deben ser dinámicas, a fin de introducirles las mejoras que procedan en virtud de los requisitos que deben cumplir para garantizar razonablemente su efectividad…". (El destacado no es del original).

En relación con la custodia de los discos duros externos, las Normas de Control Interno para el Sector Público, en la norma 4.3.2 "Custodia de activos", se estipula:

"La custodia de los activos que cada funcionario utilice normalmente en el desarrollo de sus labores, debe asignársele formalmente. En el caso de activos especialmente sensibles y de aquellos que deban ser utilizados por múltiples funcionarios, la responsabilidad por su custodia y administración debe encomendarse específicamente, de modo que haya un funcionario responsable de controlar su acceso y uso". El destacado no es del original).

Estas situaciones representan una debilidad de control, en cuanto a que no se está supervisando que los backups o copias de seguridad, se estén realizando periódicamente; asimismo, en relación a la custodia, existe un alto riesgo de pérdida total de información, ante un eventual siniestro.

2.9 Ausencia de planta eléctrica

Al realizar la inspección ocular a los servidores ubicados en DTIC, se determinó que cuando se interrumpe el fluido eléctrico, quedan funcionando únicamente con la energía que les transmiten las UPS, no se tiene una planta eléctrica, en el caso que el tiempo de interrupción sea mayor al de la capacidad que tengan las UPS. Ante esta situación, la DTIC manifiesta que se han efectuado las acciones para que se incluya dentro del presupuesto la compra de una planta, pero aún no se ha comprado.

En relación con esta situación, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en la norma 1.4.3 "Seguridad física y ambiental", dispone:

"La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado, con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos. // *Como parte de esa protección debe considerar: … f. La continuidad, seguridad y control del suministro de energía eléctrica, del cableado de datos y de las comunicaciones inalámbricas".* (El destacado no es del original).

Asimismo, las Normas de Control Interno para el Sector Público, en la norma 4.3.3 "Regulaciones y dispositivos de seguridad", se establece:

"*Regulaciones y dispositivos de seguridad El jerarca y los titulares subordinados, según sus competencias, deben disponer y vigilar la aplicación de las regulaciones y los dispositivos de seguridad que se estimen pertinentes según la naturaleza de los activos y la relevancia de los riesgos asociados, para garantizar su rendimiento óptimo y su protección contra pérdida, deterioro o uso irregular, así como para prevenir cualquier daño a la integridad física de los funcionarios que deban utilizarlos".* (El destacado no es del original).

La ausencia de una planta eléctrica para abastecer los servidores ubicados en DTIC, representa una debilidad de control, ya que existe un riesgo alto de perder información, ante una eventual interrupción prolongada del fluido eléctrico y no se puedan establecer responsabilidades.

2.10 Incumplimiento en envío de informes anuales

Con respecto a los informes anuales que se deben presentar ante el Registro de Derechos de Autor y Derechos Conexos, la Jefatura DTIC manifestó mediante correo electrónico, que el último informe enviado fue en el año 2014 y que siempre fue solicitado por la Dirección Administrativa pero se dejó de generar, lo cual evidencia, que desde el año 2014 se ha omitido enviar la información correspondiente.

Referente a esta situación, el Reglamento para la Protección de los Programas de Computo en los Ministerios e Instituciones Adscritas a Gobierno Central, en artículo 2, dispone:

"Cada Ministerio e Instituciones adscritas al Gobierno Central, tendrán las siguientes obligaciones: //… c) El Ministro o Jerarca de la respectiva Institución, designará a una persona como responsable, entre otras cosas, de presentar el resultado de la auditoría y un informe anual ante el Registro Nacional de Derechos de Autor y Derechos Conexos". (El destacado no es del original).

Esta situación representa un incumplimiento al reglamento, con lo cual la Institución se puede ver expuesta a una sanción.

2.11 Ausencia de documentación de respaldo en Ciclo de Vida de Desarrollo de Sistemas

La Jefatura DTIC indica mediante correos electrónicos, que software en desarrollo hay tres programas: Gestión del Desempeño, Sistema de Gestión Vehicular e Inventario de Bienes; no obstante, manifiesta que no existe documentación de respaldo, con respecto a las cuatro etapas que conforman el Ciclo de Vida de Desarrollo de Sistemas. Esto obedece a que la Jefatura DTIC ha omitido ejercer el control respectivo.

Con respecto a esta situación, las Normas de Control Interno para el Sector Público, en la norma 4.4.1 "Documentación y registro de la gestión institucional", se estipula:

"El jerarca y los titulares subordinados, según sus competencias, deben establecer las medidas pertinentes para que los actos de la gestión institucional, sus resultados y otros eventos relevantes, se registren y documenten en el lapso adecuado y conveniente, y se garanticen razonablemente la confiabilidad y el acceso a la información pública, según corresponda". (El destacado no es del original).

Por otra parte, en esas mismas normas, en la norma 5.4 "Gestión documental", se establece:

"*El jerarca y los titulares subordinados, según sus competencias, deben asegurar razonablemente que los sistemas de información propicien una debida gestión documental institucional, mediante la que se ejerza control, se almacene y se recupere la información en la organización, de manera oportuna y eficiente, y de conformidad con las necesidades institucionales".* (El destacado no es del original).

La ausencia de documentación de respaldo en el desarrollo de los programas, representa una debilidad de control, en cuanto a que no se encuentra documentado el grado de avance de las diferentes etapas, que conforman el ciclo de vida del desarrollo de sistemas; asimismo, se da un incumpliendo de las medidas de control correspondientes.

2.12 Ausencia de evaluaciones de efectividad y cumplimiento a la gestión de TI

En relación con las evaluaciones de efectividad y cumplimiento que debe realizar el jerarca a la gestión de TI, el Despacho de la señora Ministra mediante oficio DM-705-17 del 20 de octubre del 2017, manifestó lo siguiente:

"… al igual que en todas las oficinas, las evaluaciones sobre efectividad y cumplimiento de la gestión que se realizan por parte de la Unidad de Planificación Institucional, se refieren al Plan Nacional de Desarrollo (PND), el Plan Anual Operativo (PAO corresponde al de presupuesto) y el Plan Estratégico Institucional (PEI)… // Es importante mencionar que una evaluación, con mayor nivel de detalle y específica sobre metas y gestión no se hace en TI ni en ninguna de las oficinas, debido a que la Unidad de Planificación Institucional no cuenta con el personal suficiente, incluso por un periodo significativo ha contado únicamente con una persona". (El destacado no es del original).

Con respecto a esta situación, las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República, en la norma 5.2 "Seguimiento y evaluación del control interno en TI", dispone:

"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" (El destacado no es del original).

Esta situación representa una debilidad de control, ya que no se está ejerciendo el control con respecto a la gestión de TI; asimismo se da un incumplimiento a la normativa establecida.

2.13 Ausencia de contrato o convenio para el almacenamiento de base de datos de ASEMEIC en los servidores del MEIC

De acuerdo a consultas realizadas a la Jefatura DTIC y a la Administradora de la Asociación Solidarista de Empleados del MEIC (ASEMEIC), se determinó que el almacenamiento de la base de datos de ASEMEIC, se realiza en los servidores del MEIC, sin que exista un contrato o convenio.

Esta situación obedece, según lo manifestado por la Administradora de ASEMEIC, a que se solicitó ayuda para almacenar la base de datos en los servidores del MEIC y se recibió la colaboración de DTIC, sin mediar un contrato o convenio alguno, donde se establecieran las condiciones y responsabilidades entre ambas partes.

Con respecto a la ausencia de un contrato o convenio, para que el MEIC almacene en sus servidores la base de datos utilizada por ASEMEIC, la directriz No 047-MTSS, de la Presidencia de la República y el Ministerio de Trabajo y Seguridad Social, en su considerando 3º, establece:

"Que la utilización de los recursos públicos para el fomento de las organizaciones sociales no menoscaban ni comprometen los recursos estables, siempre y cuando cumplan las disposiciones institucionales, relacionadas con el control y fiscalización del uso de los mismos". (El destacado no es del original).

Asimismo, la resolución, dispone:

"… Se emite la presente directriz para dotar de un espacio físico en beneficio de las organizaciones sociales, tales como Asociaciones Solidaristas, Cooperativas, Sindicatos, del sector público, dirigida a los Ministros de Estado, Presidentes Ejecutivos, Gerencias Generales, Directores Generales, y demás altos jerarcas de la Administración Pública, en los siguientes términos:

*… **II.** El espacio físico a utilizar será convenido entre el jerarca de la institución y los representantes de las Organizaciones Sociales del Sector Público, estableciéndose las condiciones que regirán la utilización del lugar pactado y cualquier recurso adicional convenido, conforme a la normativa jurídica vigente. // **III.** Las Organizaciones Sociales deberán cumplir con las exigencias que establece la Ley General de la Administración Pública. La Ley de Control Interno, y demás normativa que regule la utilización de los recursos públicos. // **IV.** Se firmará un convenio entre el jerarca de la Institución y el representante legal de la Organización Social, el cual será sometido al referendo interno por el órgano competente designado por la Institución, ante la Contraloría General de la República, para este trámite".*

Al no existir un convenio, que respalde este servicio brindado por el MEIC a la Asociación Solidarista de Empleados del MEIC, se da una debilidad de control interno, en cuanto a que, en el caso de ocurrir algún daño o pérdida de información, a causa de algún eventual desastre u otro factor, no se puedan delimitar responsabilidades entre las partes involucradas. Asimismo, esto puede causar alguna situación que vaya a perjudicar al MEIC.

2.14 Resultados satisfactorios

De acuerdo con las pruebas aplicadas, se obtuvieron resultados satisfactorios respecto a:

- Controles de acceso, roles y niveles de privilegio existentes.
- Publicación del Manual de Políticas y Estándares en Seguridad Informática.
- Existencia de un plan para el establecimiento de medidas de seguridad de la información y evaluación periódica del impacto de esas medidas.
- Manejo de los desechos y reutilización de recursos de TI.
- Políticas sobre justificación, autorización y documentación de solicitudes de implementación o mantenimiento de TI.
- Funciones por escrito asignadas por la jefatura, a todos los funcionarios de TI.

- Procedimiento para la definición de los términos de referencia que incluyan las especificaciones y requisitos o condiciones requeridas o aplicables, así como para

  la evaluación de ofertas (contratos con terceros en procesos de implementación o mantenimiento de software e infraestructura).

- Procedimiento para la administración y operación de la plataforma tecnológica.

- Registro actualizado de los componentes de hardware y software).

- Registro escrito de las visitas autorizadas al área de servidores.

- Inventario de licencias, equipos físicos y programas instalados.

- Estudio de factibilidad para adquirir hardware y software y para el desarrollo de nuevos sistemas de información computarizados.

Asimismo, en relación con la visita realizada al Centro de Datos Alternos del MEIC, arrendado al Instituto Costarricense de Electricidad, ubicado en Guatuso del Guarco de Cartago, en cuanto a las medidas de seguridad existentes, los resultados fueron satisfactorios.

3. CONCLUSIONES

1. De acuerdo con las verificaciones efectuadas al Departamento de Tecnologías de Información y Comunicación, se concluye, que en el periodo evaluado, se detectaron debilidades de control interno en relación con: control en formularios de “Boleta de Préstamo de Equipo”, controles en servicios de mantenimiento, ausencia de funciones, responsabilidades y permisos de acceso al personal a cargo de labores de implementación y mantenimiento del software, ausencias de: procedimiento para formalización de acuerdos de servicio, solicitudes de requerimiento de equipos de protección a la Dirección Administrativa, plan de contingencias, Comité Gerencial de Informática, control de backups o copias de respaldo y custodia inadecuada, documentación de respaldo en Ciclo de Vida de Desarrollo de Sistemas, evaluaciones de efectividad y cumplimiento a la gestión de TI, envío de informes anuales

2. No existe una planta eléctrica para abastecer los servidores ubicados en DTIC, ya que en la actualidad se corre el riesgo, de que, si se da una interrupción prolongada del fluido eléctrico, se puede perder información.

3. Asimismo, no existe un contrato o convenio para el almacenamiento de la base de datos de ASEMEIC, en los servidores del MEIC.

4. Por otra parte, la Jefatura de DTIC y la Dirección Administrativa Financiera, no están revisando ni supervisando en forma continua que los controles se estén ejerciendo.

4. RECOMENDACIONES

A la Dirección Administrativa Financiera

1. Establecer las medidas correctivas, para que a los formularios "Boleta de Préstamos de Equipo se les lleve un control consecutivo; asimismo, se consigne la información en todos los espacios que requiere el formulario. **(Resultado Nº 2.1)**

2. Establecer los controles pertinentes y ejercerlos, en relación con los servicios de mantenimiento que brinda DTIC. **(Resultado Nº 2.2)**

3. Asignar por escrito las funciones, responsabilidades y permisos de acceso al personal de DTI a cargo de las labores de implementación y mantenimiento de software. **(Resultado Nº 2.3)**

4. Elaborar un procedimiento que regule la formalización de acuerdos de servicio de DTIC. **(Resultado Nº 2.4)**

5. Establecer las medidas correctivas, para que el Departamento de Tecnologías de Información y Comunicación (DTIC), sea el que realice las solicitudes de los equipos de protección, para las instalaciones contra incendios, inundaciones, sistema eléctrico de respaldo y UPS, a la Dirección Administrativa. **(Resultado Nº 2.5)**

6. Ejercer las acciones respectivas, para que se establezca un plan de contingencias debidamente analizado, revisado y aprobado por las autoridades correspondientes. **(Resultado Nº 2.6)**

7. Establecer los controles y ejercerlos, para que el Departamento de Tecnologías de Información y Comunicación (DTIC), realice la verificación periódica, en relación con los backups o copias de respaldo que debe realizar cada funcionario. **(Resultado Nº 2.8)**

8. Tomar las medidas previsibles, para que cuando se traslade el MEIC al nuevo edificio, ante una eventual interrupción prolongada del fluido eléctrico, se tengan las fuentes de energía suficientes para no interrumpir el funcionamiento de los servidores ubicados en DTIC. **(Resultado Nº 2.9)**

9. Establecer las medidas correctivas, para que se envíen los informes anuales que se deben presentar ante el Registro de Derechos de Autor y Derechos Conexos; asimismo, ponerse al día con los que no se han enviado, correspondiente a periodos atrasados. **(Resultado Nº 2.10)**

10. Tomar las medidas correctivas para que se documenten, cada una de las etapas que conforman el Ciclo de Vida, de los sistemas que DTIC está desarrollando. **(Resultado Nº 2.11)**

11. Elaborar un contrato o convenio para el almacenamiento de la base de datos de la Asociación Solidarista (ASEMEIC) en los servidores del MEIC. **(Resultado Nº 2.13)**

A la Ministra

12. Ejercer las medidas correctivas, para que se realicen las evaluaciones de efectividad y cumplimiento a la gestión de TI. **(Resultado Nº 2.12)**

5. OBSERVACIONES

5.1 Discusión y remisión del Informe

Los resultados del informe se discutieron con la señora Geannina Dinarte Romero, Ministra y los señores Mario Álvarez Rosales, Director Administrativo Financiero y Luis Guillermo Rojas Solano, Jefe del Departamento de Tecnologías de Información y Comunicación, quienes manifestaron su aprobación y aceptación de las recomendaciones contenidas en él.

La remisión del informe se realiza mediante el oficio AI-OF-001-2018 del 09 de enero del 2018, fecha a partir de la cual se da por finalizado este estudio.

5.2 Plazo para ejecutar las recomendaciones

El plazo se establece de acuerdo con lo pactado con la Dirección Administrativa Financiera y el Despacho de la Ministra, en el Acta de Conferencia final, como a continuación se señala:

Nº Recomendación	Responsable del cumplimiento	Fecha de discusión	Fecha de cumplimiento
1	Mario Alvarez Rosales	20-12-2017	31-01-2018
2	Mario Alvarez Rosales	20-12-2017	31-03-2018
3	Mario Alvarez Rosales	20-12-2017	28-02-2018
4	Mario Alvarez Rosales	20-12-2017	31-03-2018
5	Mario Alvarez Rosales	20-12-2017	31-03-2018
6	Mario Alvarez Rosales	20-12-2017	31-01-2019
7	Mario Alvarez Rosales	20-12-2017	31-03-2018
8	Mario Alvarez Rosales	20-12-2017	31-05-2018
9	Mario Alvarez Rosales	20-12-2017	31-01-2018
10	Mario Alvarez Rosales	20-12-2017	30-04-2018
11	Mario Alvarez Rosales	20-12-2017	31-03-2018
12	Geannina Dinarte Romero	21-12-2017	31-08-2018

5.3 Algunos aspectos de la Ley General de Control Interno

En cumplimiento de una directriz de la Contraloría General de la República emitida el 17 de marzo del 2003, es de interés recordar que los artículos 36, 37, 38 y 39 de la Ley General de Control Interno Nº 8292, publicada en el Diario Oficial La Gaceta el día 04 de setiembre del 2002, disponen la forma de comunicación de los resultados de los informes de la Auditoría Interna y en ese sentido, también se previene al jerarca y a los titulares subordinados acerca de sus deberes en el trámite de dichos informes.

5.4 Responsable del estudio

El estudio fue realizado por el funcionario de esta Auditoría Interna, Milton Hernández Hernández, con la supervisión de Luis Orlando Araya Carranza, Auditor Interno.

Luis Orlando Araya Carranza, CPA
Auditor Interno

Cc. Geannina Dinarte Romero, Ministra
Cc Mario Alvarez Rosales
Cc Luis Guillermo Rojas Solano
Archivo