ATIC-246-2018
21-12-2018

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2018 del Área de Tecnologías de Información y Comunicaciones (TIC) de la Auditoría Interna, con el fin de evaluar la gestión de la Gerencia de Pensiones en el cumplimiento a las Normas Institucionales de Seguridad Informática.

Los resultados del estudio han permitido evidenciar oportunidades de mejora en la gestión de las medidas de seguridad informática por parte de la Gerencia de Pensiones en temas relacionados con el cumplimiento del modelo de datos institucional, actualización de las definiciones de Antivirus, administración de partes o repuestos y mecanismos de control de apoyo a la gestión del licenciamiento referente al software adquirido.

Por lo anterior, es importante considerar que el abordaje de los riesgos descritos en esa temática fortalecerá la integridad, confidencialidad y disponibilidad de la información gestionada asegurando la continuidad de los servicios.

En virtud de lo expuesto, este órgano de fiscalización ha solicitado a la Gerencia de Pensiones, adoptar acciones concretas para la atención de las recomendaciones insertas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

ATIC-246-2018
21-12-2018

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN DE CARÁCTER ESPECIAL REFERENTE A LA GESTIÓN DE LA GERENCIA DE PENSIONES EN EL CUMPLIMIENTO A LAS NORMAS DE SEGURIDAD INFORMÁTICA INSTITUCIONAL.

GERENCIA DE PENSIONES, U.E. 9108

ORIGEN DEL ESTUDIO

El estudio se efectuó en cumplimiento del Plan Anual Operativo de la Auditoría Interna 2018.

OBJETIVO GENERAL

Evaluar la gestión de la Gerencia de Pensiones en el cumplimiento a las Normas de Seguridad Informática Institucional.

OBJETIVOS ESPECÍFICOS

1. Determinar el cumplimiento de las directrices establecidas en torno al Modelo de Datos Institucionales en las aplicaciones utilizadas en la Gerencia.
2. Identificar el estado de actualización de las definiciones de Antivirus en los equipos de cómputo de la Gerencia.
3. Comprobar la gestión realizada en torno a la administración de partes y repuestos informáticos, así como de licenciamiento de software.

ALCANCE

El estudio comprende las acciones realizadas por la Gerencia de Pensiones en su gestión de cumplimiento a las Normas Institucionales de Seguridad Informática, durante el período comprendido entre enero del 2017 y octubre del 2018.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:

- Aplicación de Instrumento al Ing. Mario Villalobos Marín, Ing., Jose Manuel Solís Rodriguez y el Ing. Jose Pablo Rodriguez Guzman, funcionarios del Centro de Gestion Informática de la Gerencia de Pensiones.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

- Análisis de la información suministrada por la Administración Activa vía correo electrónico y en formato físico/digital, sobre las acciones desarrolladas para dar cumplimiento a actividades sustantivas al tema.

- Verificación de aplicaciones de la Gerencia de Pensiones incluidas en el Modelo de Datos Institucional.

MARCO NORMATIVO

- Ley General de Control Interno, 8292.
- Normas Técnicas para la Gestión de las Tecnologías de la Información (CGR), 2007.
- Normas Institucionales de TIC, 2012.
- Normas Institucionales de Seguridad Informática, 2008, CCSS.
- Modelo de Organización de los Centros de Gestión Informática, 2013.
- Lineamientos generales de inventario TIC, TIC–INV-0001, Versión 1.0.0., noviembre 2011
- Metodología para el modelo de datos institucionales (MDI), TIC-MDI-0001, 2010

ASPECTOS NORMATIVOS QUE CONSIDERAR

Esta Auditoria, informa y previene al Jerarca y a los titulares subordinados, acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

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

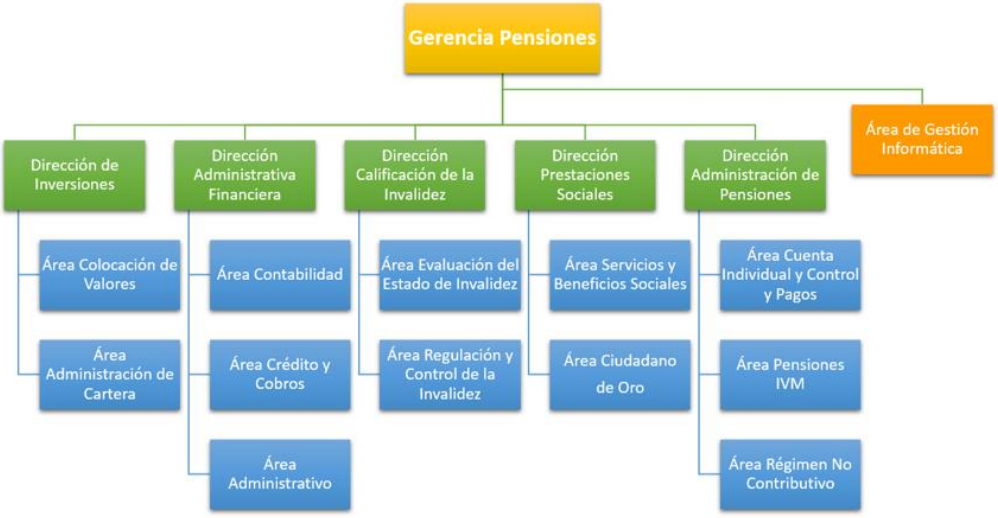
ANTECEDENTE

La Caja Costarricense de Seguro Social (CCSS) es la institución del sector salud que guía y facilita el cumplimiento de planes, políticas nacionales y estrategias en el campo de la salud y las pensiones, a través de la administración del Seguro de Enfermedad y Maternidad (SEM), el Seguro de Invalidez, Vejez y Muerte (IVM), así como del Régimen No Contributivo (RNC).

Parte de esa administración está a cargo de la Gerencia de Pensiones y sus unidades adscritas, de manera que están organizados de la siguiente forma:

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

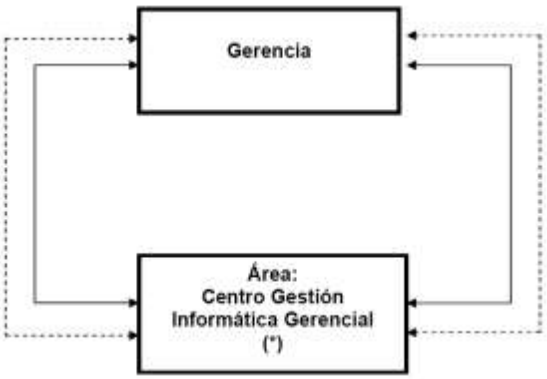
Figura 1
CCSS: Estructura Organizacional de la Gerencia de Pensiones, 2018



Fuente: *CCSS. http://intranet/Organizacion/GP/SitePages/Inicio.aspx, recopilado el 12 de noviembre del 2018.*

La estructura orgánica y funcional aplicable al Centro de Gestión Informática (en adelante CGI) de la Gerencia de Pensiones se encuentra establecida en el Modelo de Organización de los CGI (octubre 2013), mismo cuyas modificaciones fueron aprobadas por la Junta Directiva en el artículo No. 44 de la sesión No. 8555 del 26 de enero de 2012 y artículo No. 32 de la sesión No. 8658 del 29 de agosto de 2013. De acuerdo con dicho modelo de organización, el CGI objeto de evaluación debe considerarse como Tipo A, y su estructura orgánica se muestra en la Ilustración 1.

Figura 2
CCSS: Estructura Orgánica del CGI Tipo A



San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

De acuerdo con dicho modelo de organización, el nivel de responsabilidad de los establecimientos Tipo A (p.51-52) es el siguiente:

> *"…Es responsabilidad de mantener el óptimo funcionamiento las bases de datos, la administración de información y de proyectos estratégicos, de asesorar técnicamente a las diferentes unidades de trabajo en su ámbito de acción. Para cumplir con lo anterior, es fundamental que mantenga interrelaciones constantes con diferentes unidades de trabajo de nivel interno y externo a la Institución. Es responsable de la utilización efectiva del equipo de cómputo, de los materiales y suministros necesarios para ejercer sus labores, del cumplimiento eficaz de los procesos y subprocesos de trabajo que administra, de planificar, priorizar y de proponer alternativas de solución para los problemas o desafíos que se presentan en su ámbito de acción. El desarrollo de las acciones debe responder a criterios de eficiencia, eficacia y economía, con el objeto de que se traduzcan en una mejora sustancial de la gestión de los servicios en su ámbito de acción…"*

Específicamente en ese cuerpo normativo, se definen los factores a considerar relacionados a los Centros de Gestion Informática Gerenciales, entre los cuales se citan los siguientes:

> *"(…) Elaborar e implementar planes de seguridad y calidad informática, con fundamento en la normativa vigente, el aseguramiento de los recursos informáticos (hardware, software y de accesibilidad a los CGI) y de las comunicaciones, con el propósito de mantener un servicio que se caracterice por la integridad, confidencialidad y disponibilidad. (…)*
>
> *(…) Determinar las necesidades físicas, ambientales y de seguridad del área informática, de acuerdo con los requerimientos específicos y la normativa vigente, con la finalidad de proteger la inversión y lograr el óptimo funcionamiento de los recursos informáticos. (…)*
>
> *(…) Documentar e implementar la política de seguridad de la información, con base en la regulación y la normativa vigente, con el objeto de lograr confiabilidad: física y ambiental, en las operaciones y las comunicaciones, el control del acceso, la implementación, el mantenimiento de software e infraestructura tecnológica y la continuidad de los servicios, entre otros aspectos. (…)*
>
> *(…) Asesorar y capacitar a los funcionarios para que se cumplan las regulaciones relacionadas con la seguridad, confiabilidad y riesgos asociados en tecnologías de información y comunicaciones, de acuerdo con la normativa establecida, con el fin de reducir los riesgos de error humano, sustracción, fraude o uso inadecuado de los recursos tecnológicos. (…)*
>
> *(…) Implantar medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus, con base en la programación operativa y los antivirus disponibles (licencias), con el fin de garantizar la confiabilidad y seguridad de la información. (…)*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

(…) Asignar y controlar los derechos de acceso de los usuarios a los ambientes de desarrollo, mantenimiento y producción, de conformidad con los requerimientos de la organización y las políticas vigentes, con la finalidad de lograr mayor seguridad en la operación de los sistemas y un uso eficiente y eficaz de los recursos disponibles en tecnologías de información. (…)

(…) Desarrollar acciones de seguridad en la implementación y el mantenimiento de software e infraestructura tecnológica, de acuerdo con los lineamientos y procedimientos establecidos, con fin de evitar fallas operativas, daños o pérdida de información. (…)

(…) Establecer mecanismos de control de calidad, de oportunidad, de seguridad, entre otros, de servicios contratados a terceros, con base en la regulación y la normativa técnica, con la finalidad de lograr la efectividad de la gestión. (…)"

En cuanto a este nivel de responsabilidad de los Centros de Gestion Informática, es importante considerar el cumplimiento de las "Normas Institucionales de Seguridad Informática", TIC-ASC-SEG-0002, Versión 1.0 abril 2008, las cuales se describen tal como se cita a continuación:

"… Por lo anterior, además de detallar un conjunto de reglas o ajustes a las actividades relacionadas con el quehacer de los usuarios de las tecnologías de información, buscando la integridad, confidencialidad y disponibilidad de la información y recursos informáticos, se hace referencia a otros documentos como manuales o procedimientos, que sirven de guía en el cumplimiento de lo estipulado en el presente documento.

Los estándares técnicos o de configuración, también constituyen normas, las mismas son una descripción de cómo la política de seguridad de la información será implementada, así como los mecanismos de seguridad asociados…"

Adicionalmente, en ese mismo cuerpo normativo se define el siguiente alcance de aplicación:

"… Las normas (conjunto de reglas) aquí documentados deben ser de implementación obligatoria para todas aquellas Unidades Ejecutoras y funcionarios que estén involucrados directa o indirectamente con el uso de tecnologías de información y comunicaciones.
Cabe responsabilidad para aquel funcionario que incumpla las normas de Seguridad Informática establecidas en este documento, de conformidad con el régimen disciplinario vigente en la CCSS…"

Considerando lo anterior, se detallan a continuación los hallazgos evidenciados por esta Auditoría en torno al cumplimiento a las Normas de Seguridad Informática Institucional en la Gerencia de Pensiones.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

HALLAZGOS

1. SOBRE LA APROBACIÓN DEL MODELO DE DATOS DE LAS APLICACIONES DE LA GERENCIA DE PENSIONES BAJO EL ESTÁNDAR INSTITUCIONAL.

Esta Auditoría comprobó que aplicaciones como el Sistema Integrado de Pensiones (SIP), Sistema Control de Créditos (SICRE), Sistema de Concesión de Crédito(CCR), Sistema de Bienes Inmuebles(BI), Sistema de Vale de Transportes(SICOVE), Sistema Integrado de Prestaciones Sociales (SIPRESOC), Sistema de Control de Inversiones (SCI), Sistema de Trámites en Línea (WAPPIVM) y Gestión de Crédito (GECREDIT), las cuales son administradas por parte de la Gerencia de Pensiones; no disponen de la aprobación o validación del Modelo de Datos utilizado, lo anterior según se determinó en revisión del "Boletín Informativo MDI" Numero 178, emitido en octubre del 2018, en el cual se listan los sistemas avalados en este sentido.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información de la Contraloría General de la República, establecen en el artículo "2.2 Modelo de Arquitectura de Información" que:

> *"La organización debe optimizar la integración, uso y estandarización de sus sistemas de información de manera que se identifique, capture y comunique, en forma completa, exacta y oportuna, sólo la información que sus procesos requieren"*

Asimismo, el inciso "3.1 Consideraciones generales de la implementación de TI" de ese cuerpo normativo refiere que:

> *"La organización debe implementar y mantener las TI requeridas en concordancia con su marco estratégico, planificación, modelo de arquitectura de información e infraestructura tecnológica. (…)"*

Las Normas Institucionales en Tecnologías de Información y Comunicaciones, señalan en su artículo *"3.2 Implementación de Software"* que:

> *"Toda Área de trabajo debe implementar el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe: (…)*
>
> - *Aplicar lo establecido en la Metodología de Modelación de Datos Institucional. (…)"*

Por otro lado, las Normas Institucionales de Seguridad Informática, indican en el numeral *"6.5. Normas para la Política de Desarrollo, Mantenimiento y Actualización de Aplicaciones"* que:

> *"(…) 5. Todas las nuevas aplicaciones que se desarrollen deben contar con el modelo de datos debidamente aprobado, según lo establece la "Metodología para el Modelo de Datos", con el fin de asegurar su compatibilidad, interoperabilidad e integración con otros sistemas. (…)"*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

La *"Metodología para el Modelo de Datos Institucionales (MDI) TIC-MDI-0001"*, establece en su alcance que:

> *"Los estándares presentados en este documento son de acatamiento obligatorio a nivel institucional y en todas las áreas que involucren tecnologías de información e informática."*

En cuanto al tema, el Lic. Jorge Pablo Rodriguez Guzmán, funcionario CGI de la Gerencia de Pensiones mencionó:

> *"… no se dispone de Metodología para el Modelo de Datos específicamente para el desarrollo de nuevas aplicaciones, por ejemplo, en el caso más reciente de desarrollo (GCREDIT), no dispone de una aprobación de ese tipo, debido a que fue considerado como una migración y no como un desarrollo nuevo…"*

Por tanto, esta situación podría exponer a la administración a riesgos asociados al desarrollo de software sin la estandarización y el aval técnico requerido, conllevando esto a gestionar las tareas de forma aislada en detrimento de la compatibilidad de información e interoperabilidad entre los sistemas informáticos.

2. SOBRE LA ACTUALIZACIÓN DE LAS DEFINICIONES DE ANTIVIRUS.

Se comprobó por medio de revisión realizada a la consola centralizada del System Center Configuration Manager, que 270 equipos de cómputo de la Gerencia de Pensiones, se identifican como "clientes activos en riesgo", situación que corresponde a la falta de actualización en las definiciones del Antivirus en estos dispositivos.

Lo anterior, bajo el entendido que el antivirus utiliza periódicamente las definiciones para detectar las amenazas, con el objetivo de proteger al equipo de nuevas versiones de virus más recientes a los riesgos que eventualmente está preparado para identificar y minimizar.

Las Normas Institucionales de Seguridad Informática indican en el apartado 7.3. Normas para la Política Normas para la Política uso adecuado de estaciones de trabajo, que se debe de tener lo siguiente:

> *"(…) Actualización de los antivirus y parches necesarios para asegurar el buen funcionamiento del equipo. (…)"*

Además, en el Modelo de Organización de los Centros de Gestión Informática (2013), se establece al respecto de los CGI Tipo A o Gerenciales lo siguiente:

> *"(…) Implantar medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus, con base en la programación operativa y los antivirus disponibles (licencias), con el fin de garantizar la confiabilidad y seguridad de la información.*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Al respecto, el Lic. Jose Manuel Solís Rodriguez, funcionario CGI de la Gerencia de Pensiones, mencionó:

> *"todos los computadores tienen instalado el antivirus, esto se puede verificar a través del System Center Configuration Manager, no obstante, sin embargo, hemos tenido casos en los cuales los antivirus no se actualizan debido a problemas con la publicación de los paquetes de actualización por parte de los compañeros de la Dirección de Tecnologías de Información y Comunicaciones (DTIC), responsables de esa tarea y encargados de administrar el servicio de antivirus. Lo anterior, debido a que la DTIC hace algún tiempo ha puesto restricciones para realizar esta tarea. Para este caso no se documenta el acto de efectuar las revisiones al estado de los computadores de manera periódica o programada. "*

Por tanto, la desactualización de las definiciones de virus no garantiza el adecuado monitoreo del antivirus, exponiéndose a fallos o vulnerabilidades en la seguridad, lo anterior en detrimento del cumplimiento la normativa aplicable en esa materia, así como la salvaguarda de la información de los usuarios.

3. SOBRE LA ADMINISTRACIÓN DE PARTES O REPUESTOS.

Se comprobó que el Centro de Gestión Informática de la Gerencia de Pensiones no dispone de un inventario de repuestos o partes de equipo de cómputo, y por ende no se ha asignado formalmente un encargado de administrarlo.

Las Normas Institucionales de Seguridad Informática indican en el apartado 7.9. "Normas para la política de Administración de un stock de repuestos equipo de cómputo", lo siguiente:

> *"(…)1. Debe nombrarse formalmente mediante nota el responsable de la administración del stock de repuestos.*
> *2. El responsable de la administración del stock de repuestos deberá llevar actualizados los siguientes controles, ya que él o ella deberán responder por el correcto uso de estos.*
> *a. Inventario de todos los repuestos comprados, que incluya:*
> *i. las características técnicas de los mismos, considerando:*
> *• número de serie*
> *• modelo*
> *• otras señas técnicas relevantes según el tipo de repuesto*
> *ii. la fecha de adquisición*
> *iii. el monto que se pagó por cada repuesto,*
> *iv. en caso de ser utilizado, registrar el número de activo del computador donde se instaló, en caso de no contar con el número de placa utilizar el número de serie del equipo. (…)"*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Los Lineamientos Generales de Inventarios TIC (TIC–INV-0001), el Punto 4. Inventario de Reparaciones e Incidentes, inciso 4.1, indica lo siguiente:

> *"...4.1 Con el propósito de contar con componentes o partes para repuestos, los Centros de Gestión Informática deben contar con un Inventario de Partes TIC, los cuales son adquiridos u obtenidos de equipo en desecho, tal y como se señala en el Manual de Normas, Procedimientos Contables y Activos (Artículo 40, Retiro por Inservible u Obsolescencia) …"*

El Lic. Jose Manuel Solís Rodriguez, funcionario CGI de la Gerencia de Pensiones, indicó que:

> *"…No disponemos de controles específicos para repuestos o refacciones. Estos repuestos son obtenidos de equipo de cómputo que se han considerado para desecho, no obstante, se pueden utilizar parte de ellos para cubrir necesidades de hardware…"*
>
> *"José Solís: El encargado de activos del Área de Gestión Informática es el administrador del inventario de repuestos, sin embargo, no existe una nota de asignación al respecto."*

Sobre este particular, la falta de asignación formal de un titular para el manejo de inventario de partes, así como la ausencia de controles adecuados que permitan tener información sobre los repuestos disponibles en el Centro de Gestion Informática, podría restringir la utilización y aprovechamiento de estos en la Gerencia supra citada.

4. SOBRE MECANISMOS DE CONTROL DE APOYO A LA GESTIÓN DE LICENCIAMIENTO DE SOFTWARE

Se evidenció la ausencia de mecanismos de control de apoyo a la gestión de licenciamiento de software en la Gerencia de Pensiones.

Las Normas Institucionales en Tecnologías de Información y Comunicaciones, establecen en su apartado 4.2 "Administración y operación de la plataforma tecnológica", lo siguiente:

> *"4.2.1 Toda unidad de TIC debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
> *[…] Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas y soluciones.*
> *[…] Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas".*

Las Normas Institucionales de Seguridad Informática indican en el apartado 7.3. "Normas para la Política uso adecuado de estaciones de trabajo", se debe de disponer de lo siguiente:

> *"(…) Software autorizado por la Institución o bien licencias adquiridas por la Unidad. (…)"*

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

El Modelo de Centros de Gestión Informática Tipo A establece al respecto lo siguiente:

> *"…Custodiar las licencias de software, con base en la normativa vigente y verificaciones físicas periódicas, con el objeto de proteger la inversión institucional y atender en forma oportuna las solicitudes de los usuarios…"*

El Lic. Jose Manuel Solís Rodriguez, funcionario CGI de la Gerencia de Pensiones, citó:

> *"…Actualmente el Área dispone de las licencias del Software de Gestión Documental Vision 2020 y Aranda. No obstante, no se dispone de un control específico para identificar los equipos en los cuales se ha instalado la aplicación.*
> *En el caso de Vision 2020 es utilizado como complemento del Sistema Integrado de Pensiones para gestionar el Expediente Digital de Pensiones, en lo que respecta del ARANDA, éste se instala en todas las computadoras (Contrato por 440 equipos), así que se puede contabilizar por medio del mismo ARANDA…"*

Dicha situación podría afectar la administración del licenciamiento de software adquirido por la Gerencia de Pensiones en aprovechamiento de los recursos disponibles institucionalmente, así como en cumplimiento de la normativa establecida para tales efectos.

CONCLUSIONES

Actualmente las tecnologías de información y comunicaciones representan un instrumento que apoya los procesos sustantivos a nivel institucional, lo anterior aplicable asimismo en el cumplimiento de las normas de seguridad informática.

De ahí la importancia en relación con el tema, debido a la creciente complejidad de las relaciones con el entorno y la automatización de los procesos, situación que acelera la implantación de mecanismos de control en la gestión integral realizada por los Centros de Gestion Informática.

A partir de ello, resulta necesario que la toma de decisiones y la implementación de soluciones, sea orientada a fortalecer los servicios tecnológicos a partir de los hallazgos encontrados en el presente informe, relacionados con la estandarización de los modelos de datos en el desarrollo de software, la actualización de las definiciones del antivirus, la administración de partes o repuestos y los mecanismos de control en apoyo a la gestión de licenciamiento de software.

Por otra parte, se debe considerar las tecnologías de información junto con las normas de seguridad aplicables como un aliado que permite apoyar la gestión y alcanzar los objetivos planteados, esto dentro de un marco de control adecuado y oficializado en aras del cumplimiento a las Normas Institucionales de Seguridad Informática.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Finalmente, los procesos o actividades efectuadas en torno al desarrollo de las normas de seguridad son propias de cada unidad, por ello la situación evidenciada en el presente informe debe de ser considerado como una oportunidad de mejora con el propósito de que se realicen las acciones para corregir y minimizar los posibles riesgos a la infraestructura e información. En virtud de lo anterior, esta Auditoría propone una serie de recomendaciones a la administración activa, con el fin de solventar las oportunidades de mejora identificadas.

RECOMENDACIONES

AL LIC. JAIME BARRANTES ESPINOZA, EN SU CALIDAD DE GERENTE DE PENSIONES O QUIEN EN SU LUGAR OCUPE EL CARGO.

1. Según lo esbozado en el hallazgo uno del presente informe, en alineamiento con la normativa aplicable en materia de desarrollo de sistemas y con la finalidad de garantizar la integración e interoperabilidad de los sistemas desarrollados en esa Gerencia, se deberá analizar la viabilidad técnica y operativa para disponer del aval del área rectora en torno al cumplimiento de lineamientos asociados al Modelo de Datos Institucional (MDI), con el fin de establecer el criterio especializado respecto al tema.

   Una vez obtenidos los resultados del análisis, definir un plan de acción con plazos, responsables y actividades orientadas a subsanar y/o justificar ante las instancias institucionales correspondientes las oportunidades de mejora detectadas en torno al cumplimiento de las Normas Institucionales de Seguridad Informática.

   Esa Gerencia establecerá las medidas de control necesarias para garantizar el cumplimiento del plan mencionado.

   Para acreditar el cumplimiento de esta oportunidad de mejora, debe remitirse a esta Auditoría, en un plazo de 6 meses posteriores al recibo del presente informe, la documentación que respalde las acciones realizadas para evaluar la factibilidad en el cumplimiento de directrices relacionadas con el Modelo de Datos Institucional, así como en la definición del plan acción correspondiente.

2. En virtud de lo evidenciado en el hallazgo dos del presente estudio en torno a los riesgos en la actualización de las definiciones de antivirus en esa Gerencia, se recomienda en primera instancia solicitar criterio a la Dirección de Tecnologías de Información y Comunicaciones (DTIC) respecto a la situación detectada por esta Auditoría, con el objetivo de determinar las causas de la misma, y a la vez requerir sean ejecutadas desde esa instancia las correcciones que corresponda, lo anterior considerando que la administración de la herramienta es competencia de esa Dirección.

   Posteriormente, con base en el criterio emitido por la DTIC, y en caso de ser necesario, definir un plan con responsables, plazos y actividades por parte del Centro de Gestión Informática que permita solventar la problemática en su ámbito de competencia, respecto a la actualización de antivirus en los equipos de cómputo de esa Gerencia, así como establecer los mecanismos de control pertinentes para garantizar su atención.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Para acreditar el cumplimiento de la recomendación, debe enviarse a este Órgano de Fiscalización, en un plazo de seis meses posterior al recibo del presente informe, la documentación que respalde la solicitud de criterio a la DTIC, el plan de acción y los mecanismos de control establecidos por esa Gerencia para garantizar su ejecución.

3. Establecer un marco regulatorio a nivel gerencial que permita estandarizar, sistematizar, oficializar, divulgar y dar seguimiento al cumplimiento de las acciones mencionadas a continuación:

   a. Administración de partes y repuestos de equipo de cómputo.
   b. Designación formal del responsable de realizar la gestión requerida en el punto anterior.
   c. Mecanismos de control de apoyo a la gestión de licenciamiento de software.

   Para acreditar el cumplimiento de esta recomendación, debe remitirse a esta Auditoría, en un plazo de 6 meses posterior al recibo del presente estudio, el respaldo documental en torno a la definición del marco regulatorio solicitado.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, se procedió a comentar los resultados del informe el 14 de diciembre del 2018, con la Licda. Johanna Mora Ulate, Asesora de Gerencia y el Lic. Marco Vinicio González, funcionario del Centro de Gestión Informática de la Gerencia de Pensiones.

A continuación, se indican las observaciones realizadas en torno a los hallazgos y recomendaciones:

Sobre los hallazgos:

Hallazgo 1: No hay observaciones.

Hallazgo 2: El Lic. González indica que este procedimiento no depende directamente del Centro de Gestión Informática, debido a que la Administración de la Consola Centralizada del System Center Configuration Manager es competencia de la Direccion de Tecnologías de Información y Comunicaciones, además hemos gestionado con ellos para que nos resuelvan la problemática sin embargo las soluciones que nos han brindado no han sido eficientes.

Hallazgo 3: los representantes de la Administración Activa indican que, a pesar de lo mencionado al momento de aplicar el instrumento de cumplimiento, se dispone de documentación que evidencia la realización del diagnóstico anual de la plataforma tecnológica.

Hallazgo 4: No hay observaciones.

Hallazgo 5: No hay observaciones.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

Sobre las recomendaciones:

Recomendación 1: No hay observaciones

Recomendación 2: la Administración Activa solicita considerar la inclusión de la Direccion de Tecnologías de Información y Comunicaciones en la atención de la recomendación citada. En virtud de que se ha tratado de coordinar al respecto con esa Direccion, no obstante, no se ha resuelto la problemática.

Los representantes de la Administración Activa solicitan que se valore ampliar el plazo a 6 meses.

Recomendación 3: No hay observaciones

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Firmado digitalmente por OSCAR ENRIQUE MENA GRANADOS (FIRMA)
Fecha: 2018.12.21 10:27:55 -06'00'

Ing. Oscar Mena Granados
ASISTENTE DE AUDITORÍA

ESTEBAN ZAMORA CHAVES (FIRMA)
Firmado digitalmente por ESTEBAN ZAMORA CHAVES (FIRMA)
Fecha: 2018.12.21 10:04:37 -06'00'

Lic. Esteban Zamora Chaves
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2018.12.21 10:35:52 -06'00'

Lic. Rafael Ángel Herrera Mora
JEFE DE ÁREA

RAHM/EZCH/OMG/lba

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888