Fondo de Ahorro y Préstamo (FAP)
de los Empleados de la Caja Costarricense de Seguro Social

Carta a la Gerencia
Estructura de Control Interno para la Tecnología de Información
Visita Final al 31 de Diciembre de 2014

CARTA A LA GERENCIA VISITA FINAL
AL 31 DE DICIEMBRE DE 2014

FONDO DE AHORRO Y PRESTAMO DE LOS EMPLEADOS DE LA CAJA COSTARRICENSE DE SEGURO SOCIAL

Hemos organizado nuestra carta de gerencia de la siguiente forma:

MOORE STEPHENS
GUTIERREZ MARIN & ASOCIADOS
CONTADORES PUBLICOS AUTORIZADOS

Oficentro La Sabana
Edificio 6, Segundo Piso
San José, Costa Rica
Apartado 863 -1150

Tel: (506) 2232-31-85
Fax: (506) 2291-16-48
mercadeo@moorestephenscr.com
www.moorestephens-centroamerica.com

Febrero 26, 2015

Señores
Junta Administrativa
Atención: Sr. Víctor Fernandez, Director Ejecutivo
Fondo de Retiro de los Empleados de la Caja Costarricense de Seguro Social.

Estimados Señores:

Hemos finalizado nuestra visita al Fondo de Ahorro de los Empleados de la Caja Costarricense del Seguro Social (en adelante FAP). Dicha visita, corresponde a la auditoría financiera al 31 de diciembre de 2014 de dicho Fondo

a. Responsabilidad del auditor

Efectuamos nuestra auditoría de acuerdo con las Normas Internacionales de Auditoría y los requerimientos en contenidos en el cartel para la contratación de la auditoría. El Ítem 3 de dicho cartel menciona que como parte de la auditoría del periodo 2014 se debe evaluar la Normativa para la Gestión y Control de Tecnologías de Información de la Contraloría General de la República. Esas normas y requisitos requieren que planifiquemos y ejecutemos la auditoría para obtener seguridad razonable acerca de si los estados financieros se encuentran libres de errores significativos. En la planificación y ejecución de nuestra auditoría de los estados financieros, consideramos su estructura de control interno con el fin de determinar nuestros procedimientos de auditoría necesarios para expresar una opinión sobre esos estados financieros y no para proporcionar seguridad sobre la estructura de control interno.

b. Responsabilidad de la Administración

La Administración es responsable de establecer y mantener una estructura de control interno para administrar la Empresa. En el cumplimiento de esa responsabilidad, la administración debe hacer estimaciones y juicios para evaluar los beneficios esperados y los costos relativos a las políticas y procedimientos de dicha estructura de control interno. Los objetivos de la estructura de control interno son proporcionar certeza razonable, aunque no absoluta, de que los activos están salvaguardados contra pérdidas por usos o disposición no autorizados y que las transacciones se efectúan de acuerdo con autorización de la Administración y se registran apropiadamente de forma tal que permita la preparación adecuada de los estados financieros conforme Normas Internacionales de Información Financiera.

Debido a las limitaciones inherentes en cualquier estructura de control interno, errores o irregularidades pueden ocurrir y no ser detectados. Además la proyección de cualquier evaluación de la estructura a períodos futuros está sujeta al riesgo de que los procedimientos se puedan volver inadecuados por cambios en las condiciones o por deterioro en la efectividad del diseño y operación de las políticas y procedimientos.

c. Normativa que regula la estructura de control interno del FAP

La Contraloría General de la República publicó en La Gaceta 119 del 21 de junio de 2007 la resolución R-2-2007, "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (TI)". Esta normativa menciona que el artículo 3 de la Ley General de Control Interno, No.8292 del 31 de julio de 2002, refuerza las facultades de la Contraloría para emitir la normativa técnica de control interno necesaria para el funcionamiento efectivo del sistema de control interno de los entes y órganos sujetos de dicha Ley.

d. Descripción del trabajo realizado

Como parte de la auditoría externa al 31 de diciembre del 2014 nuestro trabajo consistió en evaluar el cumplimiento integral de la normativa mencionada en el párrafo anterior.

e. Definición de deficiencia significativa

Nuestra consideración de la estructura de control interno no revelaría necesariamente todos los asuntos de la estructura de control interno que pudieran considerarse como deficiencias significativas conforme a las normas profesionales. Una deficiencia significativa es una condición en la que el diseño o funcionamiento de elementos específicos de la estructura de control interno no reducen a un nivel relativamente bajo, el riesgo de que errores o irregularidades, en montos que podrían ser importantes en relación con los estados financieros auditados, puedan ocurrir y no ser detectados oportunamente por los funcionarios en el cumplimiento normal de sus funciones.

f. Conclusión

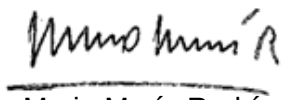
Observamos ciertos asuntos relacionados con la estructura del procesamiento electrónico de datos y su funcionamiento que consideramos constituyen condiciones que deben ser reportadas según las normas establecidas por las Normas Internacionales de Auditoría. Las condiciones a reportar comprenden aquellos asuntos que llegaron a nuestra atención en relación con deficiencias significativas en el diseño o funcionamiento de la estructura del procesamiento electrónico de datos que, a nuestro juicio, podrían afectar en forma adversa la capacidad de la entidad para registrar, procesar, resumir y presentar información financiera en forma consistente con las aseveraciones de la administración

A continuación las debilidades significativas observadas en nuestras visitas, el detalle de seguimiento a dichas observaciones se presenta en el Anexo B:

1. Falta disponer de normativa propia de Tecnología de Información.
2. Las aplicaciones o módulos del Sistema de Información utilizados por el FAP no se encuentran integrados, adicionalmente ante su antigüedad, se presentan limitantes que desfavorecen el control interno.
3. Falta disponer de un plan estratégico, en donde se pueda definir con claridad, los planes relacionados a tecnologías de información y donde se puedan identificar objetivos, requerimientos, términos de calidad, tiempo de ejecución.
4. Falta contar con un módulo o sistema, que facilite al usuario de manera eficiente y eficaz, la inclusión de requerimientos y su adecuada atención con respecto a las necesidades de TI.
5. No se cuenta con un registro de los incidentes presentados en TI, en donde se especifiquen las acciones y seguimientos realizados al mismo para sus adecuadas correcciones.
6. Participación proactiva de la Auditoria Interna en la Gestión de TI del FAP.

Quedamos a sus órdenes para cualquier ampliación de las recomendaciones incluidas en esta carta a la gerencia.

Atentamente,



Lic. Mario Marín Rodríguez
Contador Público Autorizado No.2005

Póliza de fidelidad 0116-FIG 8 vigente hasta el 30 de setiembre 2015

Exento del Timbre de Ley 6663 por disposición de su artículo 8

ANEXO A

Fondo de Ahorro de Empleados de la
Caja Costarricense de Seguro Social (FAP).

Resultados y Aspectos evaluados de Tecnología Informática

Auditoría al 31 de diciembre de 2014

Asunto a Evaluar	Análisis a efectuar	Observación	Recomendación
Normas de aplicación general			
Gestión de seguridad de Información	Verificar que la organización garantice, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales. Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa en relación con los siguientes aspectos: - La implementación de un marco de seguridad de la información. - El compromiso del personal con la seguridad de la información. - La seguridad física y ambiental. - La seguridad en las operaciones y comunicaciones. - El control de acceso. - La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica. - La continuidad de los servicios de TI. Además debe establecer las medidas de seguridad relacionadas con: - El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.	• La entidad cumple parcialmente con el punto evaluado. Se relaciona con hallazgo 3 del seguimiento de la carta de gerencia.	• Elaborar y comunicar a los funcionarios del FAP, la existencia de normativa institucional en Tecnología de información (T.I.)

	- El manejo de la documentación. - La terminación normal de contratos, su rescisión o resolución. - La salud y seguridad del personal. Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.		
Gestión de proyectos	Verificar que la organización administre sus proyectos de TI de manera que logre sus objetivos, satisfaga los requerimientos y cumpla con los términos de calidad, tiempo y presupuesto óptimos preestablecidos.	• La entidad no cumple con el punto evaluado. Se relaciona con el punto 1 del seguimiento a la carta de gerencia.	• Disponer de un módulo de atención de objetivos o requerimientos por parte de los usuarios en T.I.
Planificación y Organización			
Modelo de arquitectura de información	Verificar que la organización optimice 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.	• La entidad no cumple con el punto evaluado. Se relaciona con el punto 4 del seguimiento a la carta de gerencia	• Por la antigüedad de la herramienta y las limitaciones en cuanto a su actualización, considerar adquirir una nueva herramienta que disponga de una adecuada arquitectura de información.
Infraestructura tecnológica	Verificar que la organización cuenta con una perspectiva clara de su dirección y condiciones en materia tecnológica, así como de la tendencia de las TI para que conforme a ello, optimice el uso de su infraestructura tecnológica, manteniendo el equilibrio que debe existir entre sus requerimientos y la dinámica y evolución de las TI.	• La entidad no cumple con el aspecto evaluado. Se relaciona con el punto 4 del seguimiento a la carta de gerencia	• Por la antigüedad de la herramienta y las limitaciones en cuanto a su actualización, considerar adquirir una nueva herramienta que disponga de una adecuada arquitectura de información.
Independencia y	Verificar que el jerarca aseguré la	• La entidad no	• Disponer el FAP de

recurso humano de la Función de TI	independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas. Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.	cumple con el aspecto evaluado. Se relaciona con el punto 4 del seguimiento a la carta de gerencia	los recursos en T.I. que permita disponer de una herramienta informática funcional y apta a las necesidades actuales del fondo.
Implementación de Tecnologías de Información			
Implementación del software	Verificar que la organización implemente el software que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe: a. Observar lo que resulte aplicable de la norma "consideraciones generales de la aplicación del TI" 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 pos implantación de la satisfacción de los requerimientos. 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	• La entidad no cumple con el aspecto evaluado.	• Disponer el FAP de los recursos en T.I. que permita disponer de una herramienta informática funcional y apta a las necesidades actuales del fondo.

	migración. 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. f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento.		
Prestaciones de Servicios y Mantenimiento			
Definición y administración de acuerdos de servicio	Verificar que la organización posea 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 y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben: a. Tener una comprensión común sobre: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad. b. Contar con una determinación clara y completa de los servicios y sus atributos, y analizar su costo y beneficio. c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas. d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos. e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos. f. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros	• La entidad cumple parcialmente con el punto evaluado.	• Desarrollar una matriz de trabajo que identifique las necesidades actuales, sus plazos de atención, porcentaje de atención, responsables y seguimiento

Administración de datos	Verificar que la organización asegure que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.	• La entidad no cumple con el punto evaluado.	• Disponer de una herramienta que genere validaciones internas o reportes de control sobre el adecuado y segura inclusión de los datos.
Atención a requerimientos de los usuarios de TI	Verificar que 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	• La entidad no cumple con el punto evaluado.	• Disponer de un módulo de atención de objetivos o requerimientos por parte de los usuarios en T.I.
Manejo de incidentes	Verificar que 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.	• La entidad no cumple con el aspecto evaluado.	• Disponer de un módulo de atención de objetivos o requerimientos por parte de los usuarios en T.I.

ANEXO B

Fondo de Ahorro de Empleados de la Caja Costarricense de Seguro Social (FAP).

Seguimiento a Carta de Gerencia

Observaciones	Recomendaciones	Situación Actual
1. Disponibilidad de Plan Estratégico en T.I. Existe un PETI con un horizonte terminado en el 2012, el mismo fue aprobado por la gerencia financiera.	Elaborar un PETI que considere las expectativas del FAP a mayor plazo.	• Pendiente de atención
2. Identificación y seguimiento de los Riesgos en T.I. No se cuenta con riesgos de TI, pero se tiene una matriz de riesgos definida para el plan de continuidad, el mismo es evaluado de forma anual	Adicional a la matriz utilizada, analizar la existencia de otros riesgos en TI que puedan afectar el negocio.	• Pendiente de atención

Seguimiento a Carta de Gerencia de Auditorias anteriores

Observaciones	Recomendaciones	Situación Actual
NORMAS DE APLICACIÓN GENERAL		
3. Falta disponer de la normativa propia de Tecnología de Información. No logramos disponer de las políticas y procedimientos en T.I. que atendieran los aspectos mencionados en la normativa en TI aplicables al FAP.	Elaborar un plan de trabajo que considere: • En coordinación con la Dirección de Tecnología de Información de la CCSS definir un plan estratégico en TI que considere las necesidades o proyectos futuros del FAP. • Disponer de la normativa institucional existente relacionada con TI, que atiendan los aspectos requeridos en las Normas de TI establecida por la Contraloría General de la República. • Identificar y comunicar a los funcionarios del FAP, la normativa institucional en TI aplicable al FAP.	• En proceso

	• Para aquellas políticas y procedimientos en TI que estén pendientes o en proceso de elaboración, coordinar con la Dirección de Tecnología de Información de la CCSS, los plazos que se estima se logrará disponer de la normativa, así como dar seguimiento al cumplimiento de dichos plazos. • Para los casos de políticas y procedimientos que se consideren importantes para el FAP pero no considerados a desarrollar por la Dirección de Tecnología de Información de la CCSS, coordinar con dicha dirección su elaboración o delegación de manera que el FAP logre cumplir con los aspectos requeridos por la normativa.	
PLANIFICACIÓN Y ORGANIZACIÓN		
4. Las aplicaciones o módulos del Sistema de Información utilizado por el FAP no se encuentran integrados, adicionalmente ante su antigüedad, se presentan limitantes que desfavorecen el control interno. El programa informático que dispone el FAP, es un programa desarrollado en lenguaje COBOL, dicho lenguaje de programación se encuentra obsoleto, por su antigüedad la herramienta carece de integridad con procesos como contabilidad, préstamos, ahorros e inversiones. Adicionalmente, la herramienta es limitada en proveer herramientas o consultas que favorezcan los controles internos de la entidad.	Considerar la necesidad de adquirir un nuevo sistema o implementar medidas del caso, que permita disponer de un sistema integrado, que esté soportado en una robusta base de datos a través de la cual se garantice: • Independencia de los datos • Facilidad para el soporte y actualización • Eficiencia y eficacia en el procesamiento • La consistencia de la información • Agilización en la ejecución de los cambios • Aplicación de esquemas de seguridad desde los datos • Disponer de pistas de auditoría • Verificación de integridad de la información almacenada • Recurso Humano necesario para el mantenimiento y funcionamiento del sistema (programadores, analistas, administrador de base de datos)	• Pendiente de atención

SEGUIMIENTO		
5. Participación proactiva de la Auditoría Interna en la Gestión de TI A la fecha el Fondo de ahorro y préstamo de los empleados de la CCSS no dispone de una revisión formal de la auditoría interna institucional sobre la gestión de TI.	Se recomienda que tanto la administración activa como la auditoría interna participen, dentro de su competencia, de forma activa en el proceso de implementación del Manual de Normas Técnicas, colaborando con el seguimiento y monitoreo de la gestión de la TI.	• Pendiente de atención.