Al contestar refiérase a: **ID-95625**

AS-ATIC-0073-2023
1 de agosto de 2023

Máster
Víctor Fernandez Badilla, director
DIRECCIÓN FONDO DE RETIRO, AHORRO Y PRÉSTAMO – 1182

Ingeniero
Danilo Hernández Monge, subgerente a.i.
DIRECCIÓN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES-1150

Estimados señores:

ASUNTO:	**Oficio de Asesoría sobre la formalización del "Marco de Gestión en TIC del Fondo de Retiro Empleados (FRE) de la Caja Costarricense de Seguro Social",**

La Auditoría Interna en cumplimiento de las labores preventivas consignadas en el Plan Anual Operativo para el período 2023, y con fundamento en los artículos 21 y 22 de la Ley General de Control Interno, informa sobre aspectos a considerar tras haberse oficializado el "Marco de Gestión en TIC del Fondo de Retiro Empleados (FRE) de la Caja Costarricense de Seguro Social", a fin de que sea valorado para la toma de decisiones que competen a esa Administración.

1- ANTECEDENTES

La Caja Costarricense del Seguro Social (CCSS) tiene el Fondo de Retiro de Empleados (FRE) que se encuentra bajo la supervisión y regulación de la Superintendencia de Pensiones (SUPEN).

Es decir, está sujeto a la normativa y reglamentos establecidos por esa Institución, incluido el "Reglamento General de Gestión de la Tecnología de Información" del Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), el cual se aplica a determinadas entidades financieras.

En ese sentido, desde el año 2017 cuando el CONASSIF emitió el reglamento supra citado se dio a conocer el objetivo del marco normativo, citando:

> "*establecer los requerimientos mínimos para la gestión de la tecnología de información que deben acatar las entidades supervisadas y reguladas del sistema financiero costarricense*"

Para tales efectos, las entidades reguladas por la SUPEN, entre ellas la CCSS particularmente el FRE, debía cumplir con las disposiciones del Reglamento en cuestión en un plazo máximo de cinco años desde su publicación. Durante este período, se esperaba llevar a cabo una implementación gradual de los procesos establecidos en el marco de gestión que refiere a las Tecnologías de Información y Comunicaciones (TIC).

Durante ese período, fue necesario cumplir con diversas consideraciones normativas estipuladas en el "Reglamento General de Gestión de la Tecnología de Información". Un ejemplo de ello es el "Artículo 8. Gestión de TI", el cual se encuentra directamente relacionado con el tema tratado en esta misiva.

> *"Las entidades supervisadas son responsables de planificar, implementar, controlar y mantener un marco de gestión de TI, conforme a los procesos descritos en los Lineamientos Generales y considerando los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el órgano de dirección de cada una de las entidades.*
>
> *El marco de gestión de TI debe formularse, considerando las particularidades de cada entidad supervisada, en atención a su naturaleza, complejidad, modelo de negocio, volumen de operaciones, criticidad de sus procesos y la dependencia tecnológica. Cualquier otra particularidad o aspecto puede ser considerada por la entidad supervisada o por la Superintendencia. Los procesos del marco de gestión de TI que no aplican para su modelo de negocio deberán ser justificados razonadamente mediante un estudio técnico.*
>
> *Cuando la gestión de TI sea tipificada como corporativa, la entidad puede coordinar, aplicar y mantener un único marco de gestión de TI corporativo, el cual debe contemplar los riesgos de TI establecidos en la gestión integral de riesgos aprobada por el órgano de dirección de cada una de las entidades.*
>
> *De acuerdo con las necesidades de supervisión, el riesgo identificado, o cuando se determine que el marco de gestión de TI no es acorde a las particularidades de la entidad supervisada, las Superintendencias pueden requerir, mediante resolución razonada, la inclusión de procesos en el marco de gestión de TI establecido por las entidades supervisadas"*

Con ese propósito, la Junta Administrativa del FRAP aprobó el establecimiento del "Marco de Gestión TIC del Fondo de Retiro de Empleados" tal y como lo menciona en el inciso g del apartado "Antecedentes" de dicha normativa interna, al citar:

> *"El Fondo de Retiro de los Empleados de la CCSS en conjunto con la Dirección del FRAP desarrolló un estudio técnico con el fin de determinar el marco de gestión en TIC. Por lo anterior mediante oficio DFRAP-0020-2020 se eleva el estudio técnico para aprobación y visto bueno a la Dirección de Tecnologías Información y Comunicaciones de la Caja Costarricense de Seguro Social el cual remite el oficio DTIC-0301-2020 el cual indica, cito textual:*

(… Al respecto, de manera atenta y respetuosa me permito indicarle que esta Dirección a través de las unidades técnicas realizó el estudio técnico de Marco de Gestión en TIC del FRE alineado al modelo de entrega de servicios TIC, desarrollado por nuestra unidad y aprobado por el Consejo Tecnológico. En ese sentido, esta Dirección avala dicho estudio técnico.)

La validación anterior expuesta se realizó de manera conjunta con la Dirección de Tecnologías Información y Comunicaciones de la Caja Costarricense de Seguro Social, para determinar el alcance de responsabilidades de la DTIC y del FRE en materia de la gestión tecnológica, considerando que la DTIC constituye el órgano responsable de la gestión tecnológica institucional y por tanto el FRE debe acatar los lineamientos que al respecto se establecen en calidad de usuario de los servicios institucionales de tecnología que brinda a la CCSS."

En ese orden de ideas, la normativa interna denominada "Marco de Gestión TIC del Fondo de Retiro de Empleados" actualmente ha oficializado la versión 2.0 y fue publicada en marzo de 2023.

2- OBSERVACIONES

Dado lo expuesto anteriormente a continuación, se presentan las siguientes observaciones, con el propósito de que sean analizadas por esa Administración Activa para definir y/o implementar estrategias destinadas a mantener y perfeccionar el marco de gestión TIC en la Institución.

- Considerando que existen normas que refieren a la necesidad de establecer un marco de gobernanza y gestión TI, tales como las emitidas por el Consejo Nacional de Supervisión del Sistema Financiero, Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT); resulta necesario alinear esfuerzos para integrar requerimientos y aplicar una correcta priorización de las actividades orientadas a brindar el cumplimiento normativo.

  La relevancia de lo mencionado radica en que la DTIC lidera el Proyecto de Gobernanza y Gestión de las TI en la CCSS. No obstante, dicha iniciativa aún no finaliza; por ello, el FRE debió diseñar su propio marco de gestión en TI para acatar lo establecido en el Reglamento General de Gestión de la Tecnología de Información, como parte de un requerimiento a entidades supervisadas y reguladas dentro del sistema financiero costarricense.

- En virtud de los requerimientos que se le presentan a la CCSS en materia de establecer e implementar un marco de gobierno y gestión TI, resulta necesario obtener una comunicación y colaboración apta por parte del equipo de trabajo Institucional (representación de negocio y técnica).

  Lo anterior, por parte de las diferentes instancias involucradas, la DTIC como ente rector de tecnologías en la CCSS y la Dirección del FRAP, en conjunto con otras áreas relevantes para ejercer el cumplimiento del marco normativo.

En ese sentido, el alinear esfuerzos: compartir avances y metas; y tomar decisiones conjuntas para avanzar en la implementación del marco de gestión TI, promueve una visión compartida y una mejor comprensión referente a superar los desafíos presentes.

- El "Reglamento General de Gestión de la Tecnología de Información" del Consejo Nacional de Supervisión del Sistema Financiero (CONASSIF), establece en su artículo 11 la realización de Auditorías Externas de TI para las unidades supervisadas. En este sentido, resulta de vital importancia que durante el desarrollo de estas evaluaciones (en las etapas de planificación, ejecución y comunicación de resultados) se integre según corresponda a la Dirección de Tecnologías de Información y Comunicaciones como parte del equipo. Esto se debe a que los temas abordados no solo conciernen al FRE, sino que también se refieren a una situación institucional vinculada con el gobierno y la gestión de las TI.

3- CONSIDERACIONES FINALES

Se ha formalizado un "Marco de Gestión en TIC del Fondo de Retiro de Empleados (FRE) de la Caja Costarricense de Seguro Social" con el propósito de respaldar el cumplimiento de la normativa dictada por el Consejo Nacional de Supervisión del Sistema Financiero, el cual es aplicable únicamente para un área específica de la CCSS.

No obstante, cabe señalar que el requerimiento de implementar el marco de gobierno y gestión TIC en la CCSS (alcance institucional), hasta ahora no ha sido posible.

A ese respecto, la necesidad se pretende atender por medio del Proyecto de Gobernanza y Gestión de las TIC, el cual es dirigido por la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

Por tanto, es importante que el proyecto considere al FRE como una unidad beneficiaria de su implementación. En este sentido, resulta fundamental para la DTIC alinear los requerimientos del FRE con los objetivos actuales del programa "Gobierno y Gestión de las TIC". De esta manera, se logrará la consolidación y estandarización de los requisitos, objetivos, procesos y demás aspectos relacionados con el Marco de Gestión en TIC.

Además, dado el contexto de las exigencias actuales en materia de TI provenientes de entidades externas a la CCSS, resulta esencial que la Dirección del FRAP se comunique e incluya al ente rector TIC para obtener su asesoría en lo correspondiente. De igual manera, la DTIC debe brindar su apoyo en lo referente al cumplimiento normativo relacionado con tecnologías de información.

En ese sentido, se insta a la Administración a supervisar rigurosamente el cumplimiento de las normas en tiempo y forma, así como a acelerar la entrega de resultados del Proyecto de Gobernanza y Gestión de las TI, asegurándose de seguir la planificación establecida. Asimismo, encontrando un equilibrio adecuado entre las diversas regulaciones y garantizar el cumplimiento de todas las exigencias relacionadas con la gestión de las TIC.

Para abordar dicha situación, es importante contar con un enfoque integral y estratégico que permita identificar las áreas de convergencia entre los diferentes marcos normativos y buscar puntos de integración. Esto implica una evaluación cuidadosa de las regulaciones y requisitos aplicables, así como la implementación de políticas y procesos que sean coherentes con ambos conjuntos de regulaciones siempre que sea posible.

Por lo anterior, se informa a esa Administración Activa, a fin de aportar elementos de juicio adicionales que coadyuven a la adecuada toma de decisiones, para que se realice una valoración de los aspectos señalados, y se fortalezcan las medidas de control interno.

Al respecto, se deberá informar a esta Auditoría Interna sobre las acciones ejecutadas para administrar el riesgo y brindar la atención de la situación comunicada, a partir del recibido de este documento

Atentamente,

AUDITORÍA INTERNA

OLGER SANCHEZ CARRILLO (FIRMA)

Firmado digitalmente por OLGER SANCHEZ CARRILLO (FIRMA)
Fecha: 2023.08.03 17:26:51 -06'00'

M. Sc. Olger Sánchez Carrillo
Auditor

OSC/RJS/RAHM/OMG/lbc

C. Auditoría-1111

Referencia: ID-95625