FONDO DE RETIRO, AHORRO Y PRÉSTAMO - FRAP
CAJA COSTARRICENSE DEL SEGURO SOCIAL – CCSS

- **Informe Auditoría de Tecnologías de Información**
- **Carta de Gerencia TI 2019**
- **Informe final**

San José, 07 de febrero del 2020.

Señores
Fondo de Retiro, Ahorro y Préstamo - CCSS

Estimados señores:

Según nuestro contrato de servicios, efectuamos nuestra visita de auditoría externa del período 2019 al Fondo de Retiro, Ahorro y Préstamo de la Caja Costarricense del Seguro Social, con base en el examen efectuado notamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en el manual de "Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE)" de la Contraloría General de la República, y los Objetivos de Control para la Información y Tecnología Relacionada CobiT®, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2019.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a funcionarios o colaboradores en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos de tecnologías de información.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

MARIO RICARDO MONTENEGRO GUILLEN (FIRMA)
Firmado digitalmente por MARIO RICARDO MONTENEGRO GUILLEN (FIRMA)
Fecha: 2020.02.17 10:24:09 -06'00'

Lic. Ricardo Montenegro Guillén
Contador Público Autorizado No.5607
Póliza de Fidelidad No. 0116 FIG 7
Vence el 30 de setiembre del 2020.

"Timbre de Ley número por ¢25.00 del Colegio de Contadores Públicos de Costa Rica, se adhiere y cancela en el original".

TABLA DE CONTENIDO

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN

I. INTRODUCCIÓN

1.1 OBJETIVO

Como parte de la evaluación a los estados financieros del Fondo de Retiro, Ahorro y Préstamo de la Caja Costarricense de Seguro Social (en adelante FRAP), procedimos a realizar la evaluación de los controles generales de la gestión de Tecnología de Información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos a la luz de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, emitidas por la Contraloría General de la República y los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés), y en general las mejores prácticas de la industria de Tecnología de Información.

1.2 ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

- Evaluación general del control interno en materia de T.I. del FRAP.
- Cumplimiento de políticas y procedimientos establecidos por la Dirección de Tecnologías de Información y Comunicaciones en el FRAP.
- Seguimiento a cartas de gerencia anteriores.

1.3 METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la Dirección de Tecnologías de Información y Comunicaciones de la C.C.S.S., y la administración del FRAP.

Además, formulamos preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los colaboradores las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

1.4 LIMITACIONES AL ALCANCE

No se suministró la información de los contratos establecidos con proveedores externos de TI y su respectivo seguimiento.

II. HALLAZGOS

HALLAZGO 01: AUSENCIA DE UN PROCEDIMIENTO PARA LA GESTIÓN DE INCIDENTES DE TI. RIESGO BAJO.

CONDICIÓN:

Se determinó que el Área de Tecnologías de Información del FRAP no cuenta con un procedimiento para la gestión de incidentes de TI. De acuerdo con la información suministrada, se cuenta con los respectivos SLAs y un registro de incidentes, no obstante, no se suministró un procedimiento que respalde la labor de gestión del proceso.

Al no poseer un procedimiento formal para atención de incidentes, no se garantiza que se dé una adecuada administración de estos, minimizando el riesgo de recurrencia y procurando la captura del conocimiento y el aprendizaje necesario.

CRITERIO:

Según el proceso **DSS02 "Gestionar Peticiones e Incidentes de Servicio"** presente en el marco de referencia COBIT 5 la organización debe: "*Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes*".

RECOMENDACIONES:

Al Área de TI del FRAP:

1. Elaborar un procedimiento o metodología para la gestión de incidentes de TI, el cual debe considerar al menos:

    a. Priorización (según el impacto y urgencia)
    b. Modelos de incidentes para errores conocidos.
    c. Registro de soluciones temporales.
    d. Casos en los que requiere ejecutar acciones de recuperación.
    e. Documentar la resolución del incidente y evaluar si se almacena como fuente conocimiento.
    f. Notificación a los involucrados sobre la solución del incidente.
    g. Informes periódicos de estado de los incidentes reportados.

2. Presentar ante la Dirección de Tecnologías de Información y Comunicación el respectivo procedimiento para su valoración y aprobación.

III. SEGUIMIENTO A CARTAS A GERENCIA ANTERIORES

Carta de Gerencia 2018	
HALLAZGO 01: DEFICIENCIAS EN LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información y Comunicaciones:*** 1. Revisar y valorar la actual política seguridad de la información y demás procedimientos y normas referentes a la seguridad de modo que se actualicen con base en un análisis de riesgos. Esta revisión y actualización se debe realizar al menos una vez al año. 2. Realizar revisiones periódicas para verificar el cumplimiento de la política de seguridad de la información en el FRAP, de modo que se pueda identificar las principales deficiencias sobre la misma e implementar las medidas adecuadas, entre ellas la capacitación de los usuarios en caso de ser requerido. 3. Presentar la actualización de los documentos sobre seguridad de la información ante la Comité Gerencial de Tecnologías de Información de modo que se realice la respectiva aprobación y divulgación.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante oficio DFRAP-2019-1126 con fecha 16/12/2019, se traslada a la DTIC para su respectivo descargo.
ESTADO	**PENDIENTE** No se brindó información sobre las gestiones realizadas para atender las deficiencias de la política de seguridad de la información.
HALLAZGO 02: AUSENCIA DE UN LINEAMIENTO PARA LA EVALUACIÓN DE CONTROL INTERNO DE TI EN EL FRAP.	
RECOMENDACIÓN	***A la administración del FRAP:*** 1. Establecer un lineamiento para evaluar el control interno de TI, donde se incluya: a. Objetivo. b. Regulaciones. c. Descripción de la metodología. d. Responsabilidad. e. Seguimiento. f. Políticas y procedimientos abarcados. g. Informes de control. 2. Cumplir con el lineamiento establecido, realizar las evaluaciones periódicamente y documentar las inconsistencias detectadas. 3. Realizar los planes de acción necesarios para corregir las inconsistencias detectadas.

	4. La administración del FRAP debe de garantizar la implementación del lineamiento establecido en materia de control interno de TI.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante oficio DFRAP-2019-1126 con fecha 16/12/2019, se traslada a la DTIC para su respectivo descargo.
ESTADO	**PENDIENTE** No se evidenció la existencia de este lineamiento.
HALLAZGO 03: DEFICIENCIAS EN LA GESTIÓN DE LICENCIAS DE SOFTWARE DEL FRAP.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información y Comunicaciones:*** 1. Mantener un inventario de licencias adquiridas en el FRAP de modo que se tenga un control de las licencias que se encuentran disponibles y/o en uso. 2. Mantener un control del software instalado en cada una de las terminales de los usuarios del FRAP, de modo que se puede verificar en cualquier momento que software poseen los equipos de los usuarios. 3. Verificar periódicamente si el software instalado en los equipos se encuentra dentro de la lista de software permitido por la institución y si las licencias utilizadas se encuentran bajo control de la DTIC. En caso de identificar software no permitido o licencias no controladas, se debe realizar un proceso de mantenimiento para desinstalar dichos programas.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante la herramienta institucional SCCM (System Center Configuration Manger) con la aplicación CCSS Enterprise Remote Access / Configuration Manager Control en el reporte (Software 02E - Installed software on a specific computer) se brinda el respectivo seguimiento y control periódico al software instalado en cada computadora.
ESTADO	**PENDIENTE** Se identificó software instalado el cual no se encuentra registrado en el inventario de otros programas ni en la lista de software autorizado por la administración de la CCSS.
HALLAZGO 04: DEFICIENCIAS EN EL PROCESO DE GESTIÓN DE CAMBIOS.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información y Comunicaciones:*** 1. Elaborar un procedimiento para la gestión de cambios para otros tipos (no solo sistemas de información), como servicios de TI, procesos, infraestructura, etc. Para ello, se debe considerar: a. La descripción del procedimiento de cambios que tome en cuenta: i. Impacto del cambio (según categoría y priorización).

	ii. Proceso de cambios de emergencia. iii. Estado del cambio. iv. Revisión post-implementación. v. Riesgos asociados al cambio. vi. Plan de implementación (incluyendo un cronograma). vii. Aprobación del solicitante. b. Un control de cambios que incluya la fecha, la versión, responsable y los involucrados. c. Costos relacionados a la implementación del cambio. d. Alcance del cambio. e. Métricas o indicadores para medir la calidad del cambio.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante oficio DFRAP-2019-1126 con fecha 16/12/2019, se traslada a la DTIC para su respectivo descargo.
ESTADO	**PENDIENTE** Se identificó la existencia de un marco de trabajo para el mantenimiento de sistema basado en la metodología SCRUM, emitido por la Dirección de TI de la CCSS. Dicho documento describe el aseguramiento de calidad, roles, aplicación del proceso scrum, aprobaciones y proceso de pase a producción. No obstante, el proceso aún sigue orientado a sistemas de información y no a cambios de TI en general.
HALLAZGO 05: NO SE EVIDENCIÓ LA EXISTENCIA DE MANUALES TÉCNICOS PARA LOS SISTEMAS DE INFORMACIÓN DEL FRAP.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información y Comunicaciones:*** 1. Desarrollar manuales técnicos para los sistemas de información utilizados en el FRAP en donde se describa detalladamente la estructura de estos, así como la codificación, componentes, funcionamiento, librerías utilizadas, interfaces, procesos, fórmulas o cualquier otro componente utilizado en los sistemas. 2. Mantener los manuales técnicos actualizados según la implementación de cambios que se le realicen a los sistemas. Se debe revisar periódicamente que dichos manuales se mantengan actualizados y aprobados.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante oficio DFRAP-2019-1126 con fecha 16/12/2019, se traslada a la DTIC para su respectivo descargo.
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.

HALLAZGO 06: NO SE EVIDENCIÓ LA REALIZACIÓN DE PRUEBAS A LOS RESPALDOS DE INFORMACIÓN.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información:*** 1. Mantener un registro de las bitácoras de las pruebas realizadas a los respaldos del FRAP, los cuales contemplen aspectos como los siguientes: a. Fecha y hora de la prueba de recuperación. b. Detalle de la prueba de recuperación. c. Responsable. d. Resultado (si fue exitoso o no). e. Observaciones.
COMENTARIOS DE LA ADMINISTRACIÓN	Mediante oficio DFRAP-2019-1126 con fecha 16/12/2019 se traslada a la DTIC para su respectivo descargo.
ESTADO	**PENDIENTE** Se evidenció la existencia de un procedimiento para la gestión de respaldos. Además, se suministró evidencia de los respaldos realizados de las bases de datos y documentos de los usuarios. No obstante, no se evidenció la realización de pruebas sobre estos respaldos.
HALLAZGO 07: NO SE CUENTA CON UN PROCEDIMIENTO PARA LA GESTIÓN DE ROLES Y PERMISOS DE LOS USUARIOS FORMALMENTE DOCUMENTADO.	
RECOMENDACIÓN	***Al encargado de TI del FRAP en conjunto con las áreas usuarias:*** 1. Definir la periodicidad con la cual se debe de realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben de generar. ***Al encargado de TI del FRAP:*** 2. Contar con un procedimiento para la gestión de roles y permisos de los usuarios en los sistemas de información el cual incluya al menos: a. Proceso para crear la solicitud para el registro de nuevos usuarios, modificar o eliminarlos y otorgar permisos. b. Colaboradores autorizados de realizar las solicitudes. c. Periodicidad con la cual se debe de realizar el monitoreo de los usuarios y sus permisos, así como los reportes que se deben de generar, según lo acordado con las áreas usuarias.

COMENTARIOS DE LA ADMINISTRACIÓN	Mediante oficio DFRAP-2019-1127 con fecha 17/12/2019 se traslada al Área Beneficio por Retiro al Lic. Luis Alexis Bermúdez Bejarano para su respectivo descargo y atención.
ESTADO	**EN PROCESO** Se evidenció la existencia de un procedimiento para la gestión de perfiles de usuario, con fecha de febrero de 2020. Dado a que este proceso es muy reciente, no se cuenta con evidencia de las respectivas revisiones.
Carta de Gerencia 2017, 2016 y 2015	
1. Necesidades de TIC del FRAP no contempladas en la estrategia.	
RECOMENDACIÓN	Continuar con la ejecución del debido proceso iniciado por la Dirección del Fondo de Retiro, Ahorro y Préstamo. Una vez que éste se dé por aprobado es necesario que se realicen todas las actividades pertinentes que garanticen la debida gestión de la TIC, alineando ésta con las necesidades del negocio.
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019
ESTADO	**PENDIENTE** Aún no se ha desarrollado el plan estratégico de TI del FRAP.
2. Deficiencias en la Gestión de Pistas de Auditoría.	
RECOMENDACIÓN	Gestionar las actividades necesarias que permitan contar con una aplicación informática integral que contenga las pistas de auditoría necesaria sobre las operaciones claves para el negocio.
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019 Enfatizando que en el desarrollo del sistema integrado del FRAP en los módulos de Inversiones y contabilidad si se han desarrollado e incorporado estos controles. Actualmente la Dirección del FRAP en coordinación con la Subárea Sistemas Financieros Administrativos se encuentra en un proceso en torno al seguimiento e implementación del paralelo para la automatización del módulo de inversiones y contable con el objetivo de dejar de utilizar la herramienta en FOX que genera los estados financieros y realizar todos los procesos desde el sistema integrado del FRAP, el cual contempla estos controles.
ESTADO	**EN PROCESO** Se identificó la existencia de un procedimiento para la revisión de las pistas de auditoría. Además, se suministró un correo electrónico en el cual se envía a las áreas usuarias, no obstante, no se suministró la respuesta de los usuarios, por lo que no se evidencia que se haya efectuado la revisión.

3. Falta de Documentación para la totalidad de Aplicaciones.	
RECOMENDACIÓN	Como parte del desarrollo de la solución informática integral para el FRE; se deberá documentar, según los estándares institucionales, los procedimientos necesarios vinculantes a dicha solución.
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019 Enfatizando que los sistemas que se han desarrollado recientemente sí han incorporado documentación al respecto.
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
4. Falta de Integridad entre módulos.	
RECOMENDACIÓN	El desarrollo de la solución informática para el FRE; debe considerar todas las funcionalidades que le permitan automatizar de manera integral las operaciones y generación de estados financieros que el FRE necesita para su gestión.
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
5. Debilidades en los Sistemas Automatizados del FRE.	
RECOMENDACIÓN	Dentro de la solución informática integral que se desarrolle, será necesario contemplar todos los controles que permitan tener una seguridad razonable que la información que se gestione en el sistema tiene la integridad, confiabilidad y confidencialidad necesaria en los procesos de entrada, procesamiento y salida de información.
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019 • Actualmente se realiza una carga al sistema contable FOX mediante un archivo TXT, el cual contiene información referente a asientos automáticos y estados financieros generados desde el sistema automatizado del FRAP. • Se sigue utilizando el sistema contable en FOX como sistema generador de la información final. • Se utilizan procesos manuales únicamente para la elaboración de los asientos manuales.

ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
6. Vulnerabilidad en la Seguridad del Sistema.	
RECOMENDACIÓN	La solución informática integral que se desarrolle deberá asumir los esquemas de seguridad y acceso establecidos en las políticas institucionales definidas por la Dirección de Tecnología de información de la CCSS.
COMENTARIOS DE LA ADMINISTRACIÓN	Hallazgo: La utilización de procesos carga de archivos, detallado en los puntos anteriores, y las debilidades en la gestión de acceso que tiene la aplicación desarrollada en la herramienta FOX, exponen a la información a sufrir violaciones en su integridad, confiabilidad y confidencialidad. Pendiente de Atender al 16-12-2019
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
7. Vulnerabilidad en la Seguridad del Sistema con respecto al registro de bitácoras de control y de auditoría	
RECOMENDACIÓN	Gestionar las actividades necesarias que permitan contar con una aplicación informática integral que contenga las pistas de auditoría necesaria sobre las operaciones claves para el negocio.
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019 Enfatizando que los sistemas que se han desarrollado recientemente sí han incorporado controles al respecto.
ESTADO	**EN PROCESO** Se identificó la existencia de un procedimiento para la revisión de las pistas de auditoría. Además, se suministró un correo electrónico en el cual se envía a las áreas usuarias, no obstante, no se suministró la respuesta de los usuarios, por lo que no se evidencia que se haya efectuado la revisión.
8. Debilidades en la Generación automática de reportes para SUPEN y revisión de datos.	
RECOMENDACIÓN	Como parte del desarrollo de la solución informática integral, se deberá desarrollar los procesos automáticos necesarios que garanticen que la información de los estados financieros y demás información solicitada por la SUPEN se elabore sin que medie procesos manuales.

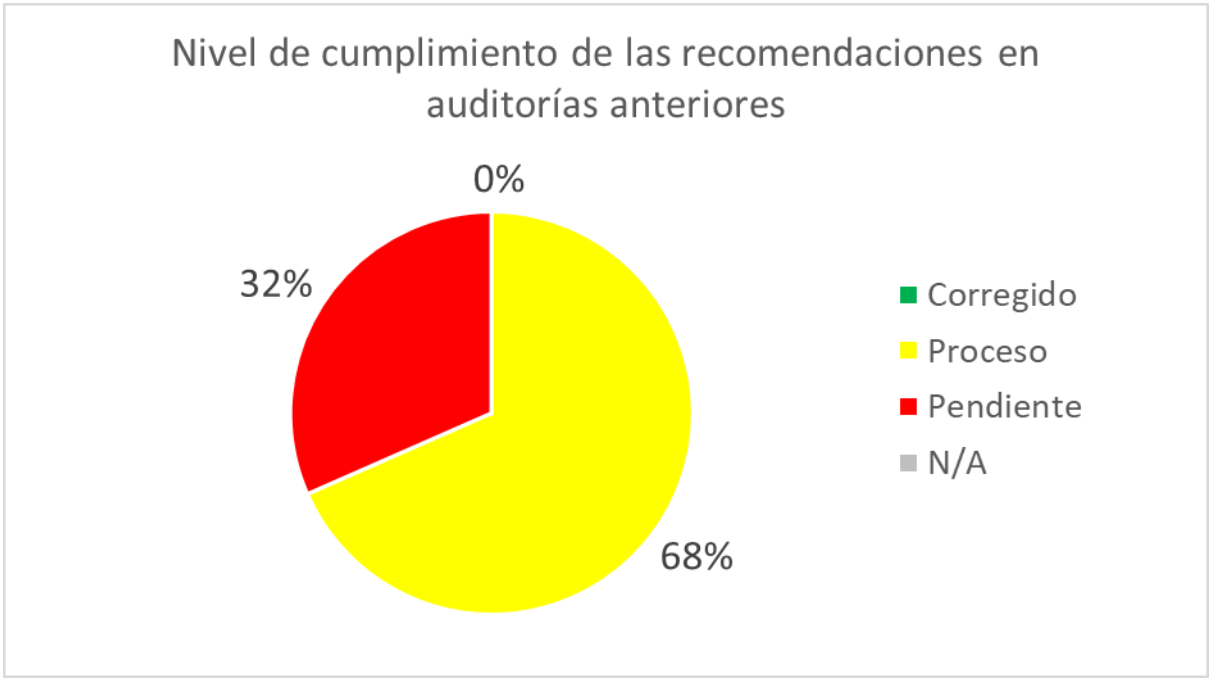
COMENTARIOS DE LA ADMINISTRACIÓN	Pendiente de Atender al 16-12-2019 Actualmente no se digitaliza la información, se realiza una carga al sistema contable FOX mediante un archivo TXT el cual contiene información referente a asientos automáticos y estados financieros generados desde el sistema automatizado del FRAP. El riesgo operativo (factor humano) inmerso en este proceso sería que se cargue un archivo diferente al que genera el sistema integrado del FRAP.
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
Carta de Gerencia 2014	
1. Se carece de pistas de auditoría para la base de datos y un encargado de su revisión	
RECOMENDACIÓN	No indica.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** El Sistema Integrado del FRAP cuenta con las respectivas pistas de auditoría, no obstante, aún se utiliza el sistema FOX el cual no posee esta característica.
2. Actualmente se encuentra implementando el módulo de inversiones, el cual no está integrado en la contabilidad y los asientos contables a fin de mes deben de ser digitalizados en el sistema contable.	
RECOMENDACIÓN	No indica.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
3. Se requiere un aplicativo que integre los módulos requeridos para el procesamiento de la información del Fondo. Por el momento se carece de interfaces gráficas, configuración de campos, controles de validación, ayuda en línea para funcionarios.	
RECOMENDACIÓN	No indica.
COMENTARIOS DE LA ADMINISTRACIÓN	

ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.
4. No se cuenta con un sistema integrado para revisar el esquema de seguridad de los módulos que lo integran. Se ejecutan controles manuales de sus archivos en Excel.	
RECOMENDACIÓN	No indica.
COMENTARIOS DE LA ADMINISTRACIÓN	
ESTADO	**EN PROCESO** Se han realizado esfuerzos por migrar e integrar los sistemas, no obstante, aún no se ha finalizado el proyecto.

A continuación, se resume por periodo el cumplimiento de las recomendaciones emitidas en periodos anteriores:

PERIODO	CORREGIDO	EN PROCESO	PENDIENTE	NO APLICA	TOTAL
2018	0	2	5	0	**7**
2017 / 2016 / 2015	0	7	1	0	**8**
2014	0	4	0	0	**4**
TOTAL	**0**	**13**	**6**	**0**	**19**

A continuación, se resume el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores de manera gráfica:



IV. APÉNDICES

APÉNDICE 01: ANÁLISIS DE RIESGOS TI

Periodo 2019

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio ☑	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo ☑	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

ID	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
1	Política de respaldos		✓	Sí se posee.		B
2	Procedimientos para respaldo y recuperación		✓	Sí se posee		B
3	Traslado de respaldos		✓	Si se maneja		B
4	Configuración de programas para respaldo		✓	Sí se maneja.		B
5	¿Se tienen definido un plan estratégico para TI alineado con el de la organización?	✗		No se evidenció la existencia de un plan estratégico u operativo de TI para el FRAP.		M
6	¿El Plan estratégico ha sido divulgado a los niveles que corresponde?	✗		No se evidenció la existencia de un plan estratégico u operativo de TI para el FRAP.		M
7	¿Se tienen definidas las políticas y procedimientos para TI?	✗		No se tiene documentado el proceso para la gestión de incidentes.		B
8	¿Se han implementado antivirus y firewalls?		✓	Sí se han implementado.		B
9	¿Se han establecido los protocolos para la realización de copias de seguridad?		✓	Sí se han establecido.		B
10	¿La seguridad de la información es un tema de seguimiento para la alta gerencia como para el Comité de Auditoría?	✗		No se le da seguimiento a la seguridad de la información.		M

11	¿Las políticas y procedimientos relacionados con TI son revisados y actualizados periódicamente, considerando los cambios en la industria y la regulación externa?	✗		Se identificó que el documento de cambios no se actualiza desde el periodo 2016 y el proceso de respaldos desde el periodo 2017.		M
12	¿Se tiene definido el perfil para cada cargo de IT y los colaboradores vinculados cumplen con el mismo?		✓	Sí se cuenta con un manual de puestos.		B
13	¿Se tienen definidas y divulgadas las funciones y responsabilidades de cada colaborador del área?		✓	Sí se tienen definidas. Además, se realizan evaluaciones del desempeño al personal.		B
14	¿Las responsabilidades de cada nivel y colaborador, parten del principio de segregación de funciones?		✓	Sí se maneja.		B
15	¿La creación de usuarios y la asignación de los permisos y/o perfil en los aplicativos es solicitada y aprobada formalmente por cada líder de área?		✓	Así se realiza. La jefatura del FRAP se encarga de asignar permisos.		B
16	¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de las mismas?		✓	Sí se maneja dentro de la Política de Seguridad de la Información.		B
17	¿Las herramientas de TI permiten tener la trazabilidad de las operaciones realizadas, así como de los usuarios (logs)?	✗		El SIFRAP cuenta con bitácoras, no obstante, el FOX no.		M

18	¿Se monitorea el estado de los equipos (Hardware)?		✓	Se les brinda mantenimiento periódico a los equipos.		B
19	¿La seguridad física de las instalaciones donde operan los equipos y personas de TI, es evaluada y revisada periódicamente, cumplimiento con los protocolos establecidos?		✓	Los servidores del FRAP se encuentran en CODISA el cual es certificada como Tier III.		B
20	¿Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de TI y dicho seguimiento es documentado?		✓	Se cuenta con un contrato activo de TI para el FRAP, el cual se le da seguimiento cada 4 meses. La primera revisión aún no se ha realizado dado que el contrato se realizó en octubre del presente año.		B
21	¿Todos los cambios desarrollados en las aplicaciones y/o software son documentados y custodiados?		✓	Se cuenta con una herramienta para la gestión de los cambios.		B
22	¿Se ha establecido el plan de continuidad para los procesos de TI?		✓	Sí se posee.		B
23	¿Se solicita el apoyo de consultores externos para los proyectos estratégicos?		✓	Sí se solicita cuando es requerido.		B
24	Los accesos son autorizados por un nivel superior.		✓	Así se realiza.		B
25	Los accesos otorgados son revisados periódicamente.	✗		El procedimiento de gestión de roles y permisos es muy reciente, por lo que no se pudo evaluar su implementación.		B

26	La asignación de los accesos parte de la segregación de funciones.		✓	Así se realiza.		B
27	Cada usuario tiene asignada una clave de composición alfanumérica y de mínimo 8 caracteres	✗		Se identificaron deficiencias en la seguridad lógica de los sistemas.		M
28	Se pueden rastrear las operaciones realizadas por los usuarios por medio de los logs	✗		El sistema FOX no posee bitácoras, el SIFRAP sí las posee.		M
29	Se cuenta con una política de copias de seguridad y de restauración.		✓	Se cuenta con políticas de respaldos y restaurado		B
30	La información sensible se encuentra protegida de modificaciones no autorizadas.		✓	Mediante la gestión de roles y perfiles, y control de acceso.		B
31	Se cumplen con los niveles de seguridad físicos para los servidores.		✓	Se cumple con esta condición.		B
32	Asignación de usuarios y claves personalizada	✗		Se cumple con esta condición, no obstante, hay deficiencias de seguridad lógica.		M
33	Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.		✓	Sí se maneja.		B
34	Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.		✓	Se controlan a través de una herramienta.		B

35	Las modificaciones en las bases de datos son realizadas por un área independiente a la que utiliza la información.		✓	Se cumple con esta condición.		B
36	Los cambios en la base de datos permiten tener la trazabilidad de quien los realiza por medio de los logs.	✗		El sistema FOX no cumple con esta condición.		M
37	Se cuenta con un diccionario de datos para la base de datos, identificando las relaciones internas que tiene y los accesos de consulta o modificación.		✓	Sí se maneja.		B
38	Definición y documentación de la Política de Cambios	✗		Se cuenta con SCRUM para cambios en sistemas, pero no se evidenció de un proceso de cambios para TI en general.		M
39	Aprobación del usuario final de los cambios.		✓	Se gestiona a través de una herramienta, la cual lleva el control de la aprobación del cambio.		B
40	Asignación usuarios y permisos, previo requerimiento y aprobación del director y/o responsable del área que utiliza la aplicación.		✓	Se cumple con esta condición		B
41	Validación periódica de los cambios en permisos y asignación de usuarios por parte del nivel autorizador.		✓	La asignación de permisos en los sistemas se realiza por parte de la jefatura.		B

42	Revisión periódica de la compatibilidad de los accesos otorgados de acuerdo con el reporte de funciones de Gestión Humana y el principio de segregación de funciones.	✗		No se evidenció la revisión periódica de los perfiles de usuario.		M
43	Identificación de los usuarios que realizan las transacciones, por medio de los Logs.	✗		El FOX no cuenta con esta característica.		M
44	Certificaciones externas sobre la calidad del servicio prestado.		✓	Se realizan auditorías de forma anual y se manejan procesos internos para la validación de la calidad del servicio que brinda TI.		B
45	Plan de contingencia para migrar a otro servidor		✓	Sí se posee.		B
46	Plan de capacitaciones en seguridad, para los usuarios con accesos más vulnerables.	✗		No se le da seguimiento a la política de seguridad.		M
47	Se realizan pruebas periódicas sobre la recuperación de datos.	✗		No se suministró evidencia.		M

--- Última Línea ---