FONDO DE JUBILACIONES Y PENSIONES DEL PODER JUDICIAL (FONDO DEL PODER JUDICIAL)

- ***Informe de Auditoría de Tecnologías de Información.***
- ***Carta de Gerencia CG 1-2016 T.I.***
- ***Informe final***

San José, 03 de abril del 2017

Señores
Fondo de Jubilaciones y Pensiones del Poder Judicial

Estimados señores:

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa de tecnologías de información del período 2016 al ***Fondo de Jubilaciones y Pensiones del Poder Judicial*** con base en el examen efectuado notamos ciertos aspectos referentes al sistema de control interno y procedimientos de tecnologías de información, los cuales sometemos a consideración de ustedes en esta carta de gerencia CG 1-2016 T.I.

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 empleados en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos de sistemas.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)

Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2017.06.15 10:03:06 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad N° R-1153
Vence el 30 de setiembre del 2017.

"Exento de timbre de Ley número 6663 del Colegio de Contadores Públicos de Costa Rica, por disposición de su artículo 8."

ÍNDICE

INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN DEL FONDO DE JUBILACIONES Y PENSIONES DEL PODER JUDICIAL

I. INTRODUCCIÓN

1.1 Objetivo

Como objetivo primordial evaluamos y monitoreamos el entorno de Tecnologías de Información con el que cuenta el ***Fondo de Jubilaciones y Pensiones del Poder Judicial***. Específicamente, se trabajó sobre dieciocho áreas de evaluación, que constituyen el entorno que administra el Fondo dentro del conglomerado informático del Poder Judicial.

1.2 Alcance

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

1. Planeación estratégica de TI.
2. Seguridad física del cuarto de servidores.
3. Estudios de vulnerabilidad.
4. Plan de Continuidad.
5. Plan de pruebas del plan de continuidad y capacitaciones.
6. Gestión de respaldos.
7. Pruebas de restauración de los respaldos.
8. Procedimiento de uso, desecho y reutilización de equipo electrónico.
9. Metodología de gestión de proyectos de tecnologías de Información.
10. Metodología para el desarrollo de sistemas de información.
11. Metodología de administración de riesgo de TI.
12. Informes de Auditoría Interna.
13. Políticas para el manejo de incidentes.
14. Plan de capacidad y desempeño.
15. Sistemas de Información del Fondo de Jubilaciones y Pensiones del Poder Judicial.
16. Clasificación de datos y seguridad móvil.
17. Evaluaciones del desempeño de los colaboradores de tecnologías de información.
18. Seguimiento a cartas a gerencia anteriores.

1.3 Metodología

Para llevar a cabo este trabajo utilizamos una modalidad de solicitud de información acompañada de entrevistas y consultas a los funcionarios de la Dirección de Tecnologías de Información, y de otras áreas del Fondo que tuviesen relación alguna con tecnologías de información. Se efectuó un trabajo de seguimiento a recomendaciones de periodos anteriores, así como una verificación de cumplimiento de la normativa aplicable al ***Fondo de Jubilaciones y Pensiones del Poder Judicial,*** en materia de tecnologías de información, resultados que sometemos a su consideración en esta carta de gerencia CG-I-2016.

Además de formular preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los funcionarios entrevistados las evidencias de sus respuestas por medio de documentos escritos o en formato digital con el propósito de respaldar sus afirmaciones.

Cabe destacar que este trabajo está enfocado en evaluar la existencia de controles internos necesarios que garanticen la operación de los procesos administrativos automatizados del ***Fondo de Jubilaciones y Pensiones del Poder Judicial,*** más la confiabilidad y disponibilidad de los datos almacenados en los sistemas de cómputo instalados.

1.4 Normativas y criterios utilizados

Para la evaluación del control interno de los sistemas en producción y la administración, operatividad y servicios de T.I. utilizamos como referencia lo especificado en el documento **N-2-2007-CO-DFOE** "Normas técnicas para la gestión y el control de las Tecnologías de Información" emitido por la Contraloría General de la República.

II. DETALLE DE LOS PUNTOS EVALUADOS EN LAS DIFERENTES ÁREAS DE TECNOLOGÍAS DE INFORMACIÓN DEL FONDO DE JUBILACIONES Y PENSIONES DEL PODER JUDICIAL

A continuación, se detallan las conclusiones obtenidas producto de los puntos valorados:

1. Planificación estratégica de TI.

La Dirección de Tecnologías Información cuenta con un plan estratégico en materia tecnológica que contempla al Fondo de Jubilaciones y Pensiones del Poder Judicial. Este plan se encuentra alineado con el plan estratégico institucional.

Además, para el periodo 2016, la Dirección estableció un plan anual operativo mediante el cual se establecieron y cumplieron tareas que permitieron implementar parte del plan estratégico establecido.

2. Seguridad física del cuarto de servidores.

El cuarto de servidores posee adecuados controles de seguridad, y se ha mejorado el control. Se ordenó el cableado de red, y se recargaron 2 de los 4 extintores que se encuentran en la habitación, ver Oportunidad de Mejora 01 de la Carta de Gerencia del 2014 en la matriz de seguimiento y el Anexo I del presente informe.

3. Estudios de vulnerabilidad.

El Área de Telemática de la Dirección de Tecnologías de Información aplica la herramienta Mcafee Vulnerability Manager para efectuar estudios de seguridad de la red institucional.

Además, se efectúan seguimientos periódicos con el fin de validar que se ejecuten las acciones correctivas requeridas para solucionar las debilidades identificadas.

4. Plan de Continuidad.

Se determinó que se ha establecido un plan de contingencias y continuidad para el Fondo. Dicho plan posee una estructura adecuada, ya que contempla lo siguiente: objetivos, alcances, posibles situaciones críticas, acciones a ejecutar en caso de una contingencia y acciones posteriores a ella, además de los responsables.

Adicionalmente, se ha implementado un sitio alterno y se está en proceso de establecer los procedimientos de migración a este ante una posible contingencia. ver Hallazgo 01 de la Carta de Gerencia del 2013 en la matriz de seguimiento.

5. Plan de pruebas del plan de continuidad y capacitaciones.

Recientemente en enero del año 2017 se hicieron pruebas al plan de continuidad, y se determinó que los resultados de dichas pruebas fueron satisfactorios. Respecto a las capacitaciones, se detalló que los usuarios no tienen participación en el plan establecido, su ejecución depende de labores técnicas las cuales son ejecutadas por TI, y la capacitación que este personal requiere lo recibe a la hora de ejecutar las pruebas.

6. Gestión de respaldos.

Se cuenta con un procedimiento para la ejecución de respaldos, y estos se están llevando a cabo; sin embargo, el procedimiento sigue sin aprobar. Ver Hallazgo 05 de la Carta de Gerencia del 2015 en la matriz de seguimiento.

7. Pruebas de restauración de los respaldos

Existe un documento de control en donde se registran las pruebas de restauración de los respaldos, el cual evidencia que se ejecutaron dichas pruebas en el periodo 2016.

8. Procedimiento de uso, desecho y reutilización de equipo electrónico.

En la actualidad no se cuenta con procedimientos para el uso, desecho y reutilización de equipo electrónico; sin embargo, este proceso se estaría contemplando como parte del Sistema de Gestión de Seguridad de la Información. Ver Hallazgo 01 del presente informe.

9. Metodología de proyectos de Tecnologías de Información.

Se cuenta con una metodología de gestión de proyectos de tecnologías de información, la cual posee una estructura adecuada. Esta metodología se está cumpliendo a través de su aplicación en el proyecto de implementación del nuevo Sistema Financiero-Contable.

10. Metodología para el desarrollo de sistemas.

Se determinó que se cuenta con una metodología de desarrollo de software la cual contempla lo siguiente: análisis del sistema, plan de pruebas, diseño, implementación y cierre. Además, se cuentan con estándares de programación y bases de datos. Esta metodología y estándares se están cumpliendo a través de su aplicación en la implementación del nuevo Sistema Contable.

11. Metodología de administración de riesgo de TI.

Se determinó que la Dirección de Tecnología de Información gestiona sus riesgos a partir de la metodología institucional SEVRI. Se determinó que posee una estructura adecuada, ya que en dicha metodología se identifican los riesgos, se analizan con base en probabilidad e impacto, se evalúa la funcionalidad de los controles y posterior a ello se hace una evaluación de los riesgos luego de la aplicación de los controles. Los riesgos de tecnologías de información fueron actualizados para el periodo 2016.

12. Informes de Auditoría Interna.

En el periodo 2016, la Auditoría Interna emitió recomendaciones en cuanto a tecnologías de información. Actualmente se lleva un control del cumplimiento de las recomendaciones, aún no se han implementado, pero se encuentran dentro del plazo establecido por la Auditoría Interna.

13. Políticas para el manejo de incidentes y problemas.

Se cuenta con un procedimiento para la gestión de incidentes; sin embargo, el documento no se ha aprobado y por lo cual no se ha implementado aún. Ver Hallazgo 02 del presente informe.

14. Plan de capacidad y desempeño.

Aún no se cuenta con un plan de la capacidad y desempeño. El Área de Soporte Técnico estará efectuando dicho plan; sin embargo, no han formalizado una fecha. Ver Oportunidad de Mejora 02 de la Carta a Gerencia del 2014 en la matriz de seguimiento.

15. Sistemas de Información del Fondo de Jubilaciones y Pensiones del Poder Judicial.

En este momento se cuenta con tres sistemas en el Fondo del Poder Judicial.

- Sistema Contable (TECAPRO): Este sistema se mantiene sin cambios respecto a periodos anteriores. Está en proceso de desarrollo un nuevo Sistema Contable, mediante el cual se solucionarían las debilidades del sistema TECAPRO y se eliminaría la dependencia del proveedor de dicha aplicación. Además, mediante el nuevo sistema el cual estaría en producción en el año 2017, se estarán integrando el resto de sistemas del Fondo del Poder Judicial. Ver Hallazgo 02 de la Carta a Gerencia del 2011, Hallazgo 01 de la Carta a Gerencia del 2009, Hallazgo 03 y 04 de la Carta a Gerencia del 2006, Hallazgo 01 de la Carta a Gerencia del 2005 y Hallazgo 06 de la Carta a Gerencia del 2003 en la matriz de seguimiento.
- Sistema Fondo de Jubilaciones y Pensiones del Poder Judicial: Este sistema en la actualidad se mantiene estable, en fase de mantenimiento en caso de que surjan nuevos requerimientos de los usuarios. A pesar de lo anterior, existen una debilidad en cuanto al cálculo de jubilaciones, para lo cual se está coordinando para dar el respectivo tratamiento. Por otro lado, existe una debilidad en la integración del sistema con el SIGAGH respecto al proceso de aportes, la cual no puede ser subsanada en el corto plazo debido a deficiencias en la cantidad de personal que ejecuta el proceso. Ver Hallazgos 03 y 04 respectivamente de la Carta a Gerencia del 2015.
- Sistema de Inversiones: El sistema no ha sufrido cambios significativos respecto a periodos anteriores y no se han detectado deficiencias.

En cuanto a la seguridad de los sistemas, los tres manejan el tema de su autenticación mediante el active directory, el cual posee los controles de seguridad adecuados.

16. Clasificación de datos y seguridad móvil

Aún no se cuenta con políticas y procedimientos para la clasificación de datos y seguridad móvil. En este momento la Dirección de Tecnología de Información está implementando un Sistema de Gestión de Seguridad de la Información mediante el cual indican que se estaría contemplando el tema de seguridad móvil y clasificación de datos. Ver Hallazgos 01 y 02 de la Carta a Gerencia del periodo 2015 en la matriz de seguimiento

17. Evaluaciones del desempeño de los colaboradores de tecnologías de información.

Actualmente se cuenta con un procedimiento para la evaluación del desempeño de los colaboradores de la Dirección de Tecnologías de Información; sin embargo, dicho procedimiento no se aplicó en el periodo 2016. Ver Hallazgo 03 del presente informe y el Hallazgo 01 de la Carta a Gerencia del periodo 2008 en la matriz de seguimiento.

18. Seguimiento a cartas a gerencia anteriores.

Se determinó que se cuenta con 1 recomendación corregida, 9 en proceso, 4 pendientes y 3 en estado no aplica. Lo anterior evidencia que se han ejecutado acciones para atender las recomendaciones emitidas por la auditoría externa al Fondo del Poder Judicial respecto a tecnologías de información. Ver Matriz de Seguimiento.

III. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: INCUMPLIMIENTO DE LA POLÍTICA PARA LA GESTIÓN DE ACTIVOS DE HARDWARE. RIESGO MEDIO.

CONDICIÓN:

Se determinó que la Dirección de Tecnologías de Información (DTI) cuenta con una política para la gestión de activos de hardware. Dicha política establece que la DTI debe velar por el cumplimiento de políticas y reglamentos para llevar a cabo una adecuada eliminación de los activos. Además, la misma indica que la DTI debe gestionar un proceso para eliminar información de medios de almacenamiento antes de desechar, trasladar o donar algún equipo.

Sin embargo, se nos indicó que no se cuenta con una política o procedimiento para la eliminación de activos. Por otro lado, se comentó que se está en el proceso de implementación de un sistema de gestión de seguridad de la información el cual contemplaría los controles correspondientes al uso, desecho y reutilización de medios electrónicos o impresos. Ante la ausencia de dichos controles a nivel de la DTI, se aplican los mecanismos que establece el reglamento para control y uso de activos institucionales.

Al no contar con un procedimiento para el uso, reutilización y desecho de activos e información, se dificulta gestionar los activos de TI de la manera correcta, y no se define un proceso para borrar la información de forma segura, por lo que no se tiene un control ni la garantía de que los datos han sido eliminados satisfactoriamente. Además, al no contar con un debido proceso de eliminación de información, existe el riesgo de generar fuga de información confidencial durante el proceso de desecho del equipo, así mismo, compromete datos de suma importancia para la Institución.

CRITERIO:

Según el apartado 1.4.4 "Seguridad en las operaciones y comunicaciones" del proceso 1.4 "Gestión de la seguridad de la información" presente en la normativa técnica para la gestión y el control de las Tecnologías de Información N-2-2007-CO-DFOE, establece que: "La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe:

a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.
c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus."

Además, el apartado (E) "Eliminación" presente en la política GTI-10202102 "Gestión de activos de hardware" la cual establece lo siguiente: "La Dirección de Tecnología velará por que se cumpla con todas las políticas y reglamentos institucionales pertinentes para una adecuada eliminación de los activos. Como parte de esto debe:

1. Crear y mantener un proceso para la eliminación de los datos de los discos y la memoria permanente antes del desecho, traslado o donación de equipos.
2. Coordinar con las instancias correspondientes, para que, en los procesos de destrucción y desecho de activos tecnológicos, se implementen medidas amigables con el ambiente.
3. Comunicar a los órganos correspondientes, para que se efectúe la actualización de los registros relacionados con el control de activos institucionales."

RECOMENDACIÓN:

A la Dirección de Tecnologías de Información:

Establecer una política o procedimiento para el uso, desecho o reutilización de medios que gestionan información, cumpliendo con lo establecido en la política para la gestión de activos de hardware. Para ello se debe considerar al menos lo siguiente:

a. Identificar y/o definir los medios que se utilizan para almacenar y transportar información.
b. Definir el proceso de custodia de la información.
c. Alinear el procedimiento para el almacenamiento de la información con el marco de seguridad establecido.
d. Definir el proceso para eliminar la información de forma definitiva, de tal modo que no existan medios para recuperarla.

HALLAZGO 02: NO SE CUENTA CON UN PROCEDIMIENTO VIGENTE Y APROBADO PARA LA GESTIÓN DE INCIDENTES Y PROBLEMAS DE T.I. RIESGO BAJO.

CONDICIÓN:

Se determinó que la Dirección de Tecnologías de Información (DTI) cuenta con un procedimiento para la gestión de incidentes y problemas de TI, el cual fue desarrollado mediante la licitación 2016LA-000008-PROV con la empresa Deloitte. Sin embargo, dicho procedimiento aún no se ha implementado dado que dicha contratación aún se encuentra en ejecución. Dado lo anterior, la DTI no cuenta con un procedimiento que se encuentre activo para la gestión de incidentes y problemas de TI.

Al no poseer un procedimiento formal para atención de incidentes y problemas activo y en operación, no se garantiza que se dé una adecuada administración de los mismos, ni que se esté tratando los incidentes bajo un estándar o proceso establecido, con la prioridad adecuada. Lo anterior genera un riesgo de recurrencia en los incidentes y podría no capturarse el aprendizaje necesario. Además, al no identificar los incidentes que puedan ocasionar problemas de TI, podría afectar la continuidad de los servicios de TI.

CRITERIO:

Según el apartado 4.5 "Manejo de Incidentes" presente en la normativa técnica para la gestión y el control de las Tecnologías de Información N-2-2007-CO-DFOE: "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.".

RECOMENDACIONES:

A la Dirección de Tecnologías de Información:

1. Dar seguimiento al contrato con Deloitte para asegurar que los tiempos de entrega se den según lo acordado y evitar atrasos en la entrega de los productos, con el fin de implementar y capacitar al personal oportunamente.

2. Girar instrucciones para que una vez que el procedimiento se encuentre finalizado y sea completamente funcional, sea implementado inmediatamente por el área responsable.

3. Llevar a cabo un proceso de sensibilización con los usuarios de las tecnologías de información en el Fondo de Jubilaciones y Pensiones del Poder Judicial, de manera tal que conozcan y sepan ejecutar el procedimiento de gestión de incidentes que se desarrolle.

HALLAZGO 03: NO SE EFECTUARON EVALUACIONES SOBRE EL RENDIMIENTO DE LOS COLABORADORES DE TI EN EL PERIODO 2016. RIESGO BAJO.

CONDICIÓN:

Se determinó que el Fondo de Jubilaciones y Pensiones del Poder Judicial cuenta con un procedimiento para la evaluación del rendimiento o desempeño de los colaboradores de la Dirección de Tecnologías de Información (DTI). Dicho procedimiento se elaboró en mayo del 2016, sin embargo, según lo comentado por la administración, aún no se ha aplicado a los funcionarios de la DTI.

Al no contar con evaluaciones del desempeño, se dificulta la identificación de las debilidades en las habilidades del personal que labora en la DTI y no se puede determinar las áreas en las que el personal requiere capacitación. Por lo tanto, existe el riesgo de que el personal presente bajo rendimiento y no se identifique si la carga de trabajo se distribuye adecuadamente, por lo que dificultaría llevar a cabo una planificación efectiva de las acciones correctivas que se deban aplicar.

CRITERIO:

Según el apartado 2.4 "Independencia y recurso humano de la Función de TI" presente en la normativa técnica para la gestión y el control de las Tecnologías de Información N-2-2007-CO-DFOE: "El jerarca debe asegurar la 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.".

RECOMENDACIONES:

A la Dirección de Tecnologías de Información:

1. Ejecutar el procedimiento para la evaluación del rendimiento de los colaboradores de la DTIC al menos una vez al año.

2. Elaborar un plan de capacitación considerando las acciones correctivas para el personal de T.I., los cuales hayan obtenido una baja calificación en la evaluación del desempeño.

IV. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CG 2015	
HALLAZGO 01: AUSENCIA DE LINEAMIENTOS PARA LA CLASIFICACIÓN DE LA INFORMACIÓN EN EL FONDO DEL PODER JUDICIAL.	
RECOMENDACIÓN	***A la Dirección Ejecutiva del Fondo del Poder Judicial en coordinación con la Dirección de Tecnologías de Información*** 1. Incluir dentro del proyecto de implementación del SGSI la implementación de políticas, procedimientos y demás lineamientos para el clasificado, etiquetado y manipulación de la información, ya sea en medios físicos o digitales. 2. Valorar responsabilidades en la administración del SGSI, con el fin de determinar lo siguiente: a. El responsable de coordinar la implementación y mantenimiento del SGSI. b. El responsable de evaluar el cumplimiento de las políticas de seguridad de la información y de los lineamientos establecidos en el SGSI. 3. Involucrar a todas las áreas del Fondo del Poder Judicial en el proyecto, aunque se esté liderando desde la Dirección de Tecnologías de Información.
COMENTARIOS DE LA ADMINISTRACIÓN	Al respecto, considera esta Dirección que dicha recomendación no le compete, en razón que el Sistema de Gestión de Seguridad de la Información, corresponde a la Dirección a su cargo, por lo que mucho le solicitará valorar la posibilidad de incluir el alcance para incluir el ámbito administrativo dentro de la contratación, con el fin de dar cumplimiento a la solicitud de la Auditoría Externa.
ESTADO	**PENDIENTE** Según lo comentado por el Área de Seguridad, el ámbito del proyecto para la implementación de un SGSI es en el área jurisdiccional, por lo que no incluye el área administrativa. Sin embargo, una vez finalizado el proyecto, se evaluará si el proyecto se puede extender a toda la Institución, incluyendo el Fondo de Jubilaciones y Pensiones del Poder Judicial. No obstante, para que el proyecto sea exitoso se requiere la colaboración de la Dirección Ejecutiva y demás dependencias de la Institución.
HALLAZGO 02: AUSENCIA DE POLÍTICAS Y LINEAMIENTOS PARA LA SEGURIDAD MÓVIL EN EL FONDO DEL PODER JUDICIAL.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información*** 1. Verificar que dentro del proyecto de implementación del SGSI se contemple el tema de seguridad móvil y que involucre al Fondo del Poder Judicial. 2. Establecer una política de seguridad móvil con el fin de documentar los controles de seguridad que deben implementarse e indicar a las áreas usuarias la manera en que deben utilizar los dispositivos móviles y sus restricciones en la organización. También puede considerarse la implementación de lineamientos de seguridad móvil dentro de una política de seguridad de la información general, en vez de una política propia para el tema. 3. Verificar periódicamente que se cumpla con la política o lineamientos establecidos para la seguridad móvil. Se deben documentar los resultados de las evaluaciones realizadas.

COMENTARIOS DE LA ADMINISTRACIÓN	El SGSI va a dar como resultado la Declaratoria de Aplicabilidad, de esto puede surgir una política que podrá hacerse extensiva a todo el desarrollo móvil, pero de nuevo, conviene recordar que el SGSI tiene un alcance especificado en el contrato.
ESTADO	**PENDIENTE** No se cuenta con políticas o procedimientos para la seguridad móvil. Según lo comentado por el Área de Seguridad, al finalizar la implementación del SGSI para el área jurisdiccional, se puede evaluar la extensión del alcance a toda la Institución.
HALLAZGO 03: EL SISTEMA SIGAFONDO NO ESTÁ INTEGRADO CON EL SIGAGH PARA LA CARGA DE LOS APORTES DE LOS TRABAJADORES ASOCIADOS AL FONDO DEL PODER JUDICIAL.	
RECOMENDACIÓN	***Al Departamento de Financiero Contable en coordinación con la Dirección de Tecnología de Información*** 1. Evaluar la factibilidad de integrar el Sistema SIGAGH con el Sistema SIGAFONDO, considerando aspectos económicos y de seguridad de los datos. Logrando que la información de aportes y reconocimiento de tiempo servido sea extraída desde SIGAGH al SIGAFONDO sin la necesidad de que se envíen archivos por correo y que estos deban ser manipulados para darles formato. 2. En caso de no poderse lograr la integridad por aspectos técnicos, se debe documentar la justificación de por qué no se va a hacer la integración entre ambos sistemas.
COMENTARIOS DE LA ADMINISTRACIÓN	Por medio de correo electrónico del 16/03/2017, se remite a la Dirección de Tecnología de la Información la boleta 161-TI-2017, la cual se solicita requerimiento de mejora e integración del Sistema SIGAFONDO y el SIGAGH.
ESTADO	**PROCESO** El Macroproceso Financiero Contable está coordinando con la Dirección de Tecnologías de Información para subsanar la debilidad identificada en el presente hallazgo. Adicionalmente, se debe coordinar con otras áreas que participan en el proceso.
HALLAZGO 04: DEBILIDADES EN LA AUTOMATIZACIÓN DEL CÁLCULO DE TIEMPO SERVIDO DE LOS COLABORADORES ASOCIADOS AL FONDO DEL PODER JUDICIAL.	
RECOMENDACIÓN	***A la Dirección de Gestión Humana en coordinación con la Dirección de Tecnología de Información*** 1. Evaluar la posibilidad de migrar la información correspondiente al tiempo servido de los funcionarios asociados al Fondo del Poder Judicial que se encuentra en el sistema SIP al sistema SIGAFONDO, con el fin de que este último efectúe el cálculo total del tiempo servido, considerando que este sistema sí calcula correctamente el tiempo servido de acuerdo con las reglas actuales del Fondo. De considerarse factible, debe llevarse a cabo la migración. 2. En caso de que no se encuentre factible implementar la migración, debe valorarse implementar los ajustes necesarios al SIP con el fin de que éste efectúe correctamente el cálculo de tiempo servido. 3. De no ser factible implementar las recomendaciones anteriores, debe documentarse la justificación de por qué no se van a implementar.
COMENTARIOS DE LA ADMINISTRACIÓN	En relación con las recomendaciones 1 y 2 sobre la posibilidad de migrar la información correspondiente al tiempo servido de los funcionarios asociados al Fondo de Jubilaciones y Pensiones del Poder Judicial que se encuentra en el SIP al sistema SIGAFONDO,

	para que se pueda efectuar el cálculo del tiempo servido en los estudios de jubilaciones y pensiones en el Módulo de Jubilaciones y Pensiones; resulta imposible ya que como bien indica Tecnología de Información en el correo de fecha 07 de marzo 2017 el Sistema Integrado de Personal SIP es un sistema obsoleto que dejó de funcionar desde el 01 de marzo del 2004. Por otra parte, para poder migrar esa información de todos los funcionarios asociados al Fondo del Poder Judicial que tengan registros antes del 01 de marzo del 2004 en el Sistema Integrado de Personal SIP, deberá realizarse antes un estudio puntualizado del tiempo servido para cada funcionario judicial de manera individual y determinar el tiempo servido antes del 01 de marzo de 2004, utilizando la información del SIP y el expediente personal. En este caso, resulta imposible atenderlo pues no hay capacidad instalada para realizar esta tarea, dado que el procedimiento actual es registrar este tiempo de conformidad con las gestiones de jubilación que se han ido presentando en el tiempo al momento de la solicitud de jubilación, como parte del proceso de Jubilaciones y Pensiones, dado que la información no está automatizada en el Sistema SIGAFONDO. Si bien es cierto, el SIGAFONDO cuenta con un Módulo de Reconocimiento de Tiempo Servido que permite registrar el tiempo servido de un funcionario en el Estado y sus instituciones públicas y que empezó a funcionar en el 2010. Este Módulo de Reconocimiento de Tiempo Servido registra el tiempo a reconocer en otras instituciones del estado para anuales y jubilación, o bien sólo para anualidades y el monto que debe reintegrar al Fondo de Jubilaciones y Pensiones del Poder Judicial, según la norma vigente. Asimismo, también permite registrar los Reconocimientos de Tiempo Servido, que antes de la puesta en funcionamiento no se calcularon en su momento por el sistema SIGAFONDO. De ahí, que el sistema permite registrar y calcular el tiempo por el sistema o fuera del mismo, lo que conlleva a determinar el total del tiempo servido de un funcionario judicial, considerando el tiempo laborado en el Poder Judicial y el reconocido en otras Instituciones públicas del Estado. Sin embargo, lo correspondiente al tiempo que registra en el SIP un funcionario judicial, siempre será sujeto de estudio.
ESTADO	**NO APLICA** El sistema que llevaba el control del tiempo servido por colaborador es muy obsoleto por lo que dificulta realizarle cambios. Además, se requiere realizar un estudio por cada funcionario para determinar el tiempo servido, según lo contenido en el SIP y el expediente personal, y no se cuenta con el personal suficiente para realizar dichos estudios. Por lo que, el cálculo se realiza al momento de la solicitud de jubilación de un determinado funcionario bajo demanda.
HALLAZGO 05: EL PROCEDIMIENTO DE RESPALDOS NO SE ENCUENTRA APROBADO.	
RECOMENDACIÓN	***Al Departamento de Planificación*** 1. Revisar y aprobar el procedimiento de respaldos con el fin de formalizar este proceso. ***A la Dirección de Tecnología de Información*** 2. Efectuar los ajustes requeridos al procedimiento de respaldos para su aprobación, según las observaciones que pueda efectuar eventualmente el Departamento de Planificación.
COMENTARIOS DE LA ADMINISTRACIÓN	Se adjunta la última versión del procedimiento de administración de respaldos. Ver Anexo "**Procedimientos de Respaldos**". Pendiente aprobación por parte del Departamento de Planificación.

ESTADO	**PENDIENTE** El procedimiento para la administración de respaldos se encuentra pendiente de aprobación.
CG 2014	
OPORTUNIDAD DE MEJORA 01: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES Y UPS.	
RECOMENDACIÓN	1. Ordenar los cables eléctricos dentro del cuarto de servidores. 2. Cumplir con la recarga del extintor ubicado en el cuarto de UPS, según la periodicidad establecida.
COMENTARIOS DE LA ADMINISTRACIÓN	Se adjuntan fotografías tomadas el día 08 de marzo 2017 del Centro Datos Principal, ubicado en el I Circuito Judicial SJ. Se revisan los extintores que se ubican en el centro de datos, Vencieron en octubre 2016 y fueron reportados el año pasado a Salud Ocupacional, los pusieron en el plan de mantenimiento. Ver anexo "**Fotografías del cuarto de servidores**"
ESTADO	**PROCESO** Durante la revisión del centro de datos, se identificaron 4 extintores, los cuales presentaban las siguientes fechas de próximas recargas: • 05/2019 • 10/2015 • 05/2019 • Oct 2016 Aún existen dos extintores sin recargar.
OPORTUNIDAD DE MEJORA 02: AUSENCIA DE UN PROCEDIMIENTO DE PLANEACIÓN PARA LA REVISIÓN DEL DESEMPEÑO Y CAPACIDAD DE LOS RECURSOS DE TI.	
RECOMENDACIÓN	1. Definir un proceso y un marco de trabajo para el desarrollo, revisión y ajuste del plan del desempeño y la capacidad. 2. Considerar lo siguiente (actual y futuro) en el desarrollo del plan del desempeño y la capacidad: a. Requerimientos de cliente. b. Prioridades del negocio. c. Objetivos del negocio. d. Impacto en el presupuesto. e. Uso de recursos. f. Tendencias de capacidades de TI y de la industria, incluyendo: i. Desempeño de la aplicación. ii. Tecnología, disponibilidad y confiabilidad. iii. Desempeño, capacidad y soporte a usuarios. iv. Planeación de la continuidad y de contingencias. v. Consideraciones de privacidad de datos y seguridad. 3. Desarrollar y mantener el plan del desempeño y la capacidad de manera oportuna, y asegurar que este documentado y acordado

	por los interesados (stakeholders), alineado a los SLAs y registrado apropiadamente.
COMENTARIOS DE LA ADMINISTRACIÓN	Se adjuntó un proceso que fue definido mediante contratación junto con los resultados, hasta el momento no se ha aplicado. Ver anexo "**Procedimiento Evaluación Desempeño**".
ESTADO	**PENDIENTE** Se cuenta con un procedimiento para la evaluación del desempeño de los colaboradores de la DTI, sin embargo, no se han elaborado planes de capacidad y desempeño de la plataforma tecnológica (infraestructura, red, sistemas, etc.).
CG 2013	
HALLAZGO 01: NO SE CUENTA CON UN SITIO ALTERNO DE OPERACIONES.	
RECOMENDACIÓN	Trabajar en conjunto con la dirección institucional en la contratación, creación o formulación de un sitio alterno de procesamiento de datos, donde se cuente como mínimo: - Estudios de factibilidad. - SLAs y tiempos deseados de "UPT ME" por parte de la Institución. - Planeamiento operativo y estratégico. - Estructuración de un plan de migración a sitio alterno en caso de emergencia.
COMENTARIOS DE LA ADMINISTRACIÓN	Se adjunta contrato establecido con el ICE, estudio de factibilidad y plan de implementación. Ver anexo "**Sitio Alterno**". Se encuentra en confección el Protocolo de Activación del Centro Alterno (corresponde al plan de migración en caso de emergencia).
ESTADO	**PROCESO.** Se cuenta con un sitio alterno para el procesamiento de datos, sin embargo, aún se encuentra en desarrollo el proceso para la migración a dicho sitio.
CG 2011	
HALLAZGO 2: LAS CUENTAS POR COBRAR DEL FONDO DEL PODER JUDICIAL NO SE LLEVAN EN UN SOLO SISTEMA INFORMÁTICO.	
RECOMENDACIÓN	Continuar con el desarrollo de la segunda etapa del SIGAFONDO, el cual contempla el desarrollo de una aplicación de contabilidad para el Poder Judicial, integrada con las diferentes aplicaciones del Fondo, es deseable incorporar dentro del sistema contable un módulo de cuentas por cobrar, con el fin de unificar el proceso de estas cuentas.
COMENTARIOS DE LA ADMINISTRACIÓN	La Contratación del Sistema Contable del Poder Judicial inició el 02 de julio del 2014, la cual está conformada por 11 entregables. El Módulo de Cuentas por Cobrar I Etapa se recibió durante el último trimestre del 2015, en el mes de mayo de 2016 se recibió a satisfacción Módulo de Cuentas por cobrar II Etapa, ambos módulos unifican las cuentas por cobrar que se llevan en el Poder Judicial. A partir del 01 de marzo del 2017, inició la etapa de "Paralelo y Pruebas Integrales", Se estima que la contratación concluirá en el mes de agosto de 2017. Ver Anexo "**Cronograma del Contrato Sist Contable 2017**".
ESTADO	**PROCESO** El hallazgo será subsanado con la implementación del sistema Financiero-Contable.

HALLAZGO 4: NO SE CUMPLE CON LO MENCIONADO EN LA POLÍTICA PARA EL USO, DESECHO Y REUTILIZACIÓN DE MEDIOS ELECTRÓNICOS O IMPRESOS.	
RECOMENDACIÓN	Cumplir lo que indica la política para el uso, desecho y reutilización de medios electrónicos o impresos con información, con la finalidad de prevenir la difusión, modificación, substracción o destrucción de los datos del Poder Judicial.
COMENTARIOS DE LA ADMINISTRACIÓN	Esta política no existe. No obstante, recientemente la Comisión Gerencial de Tecnologías de Información, avaló que la siguiente política llamada "Gestión de Activos de hardware" fuera elevada para aprobación de la Corte Plena. Dentro de ella, en el ítem E, se indica literalmente lo siguiente: "E. Eliminación. La Dirección de Tecnología velará por que se cumpla con todas las políticas y reglamentos institucionales pertinentes para una adecuada eliminación de los activos. Como parte de esto debe: 1. Crear y mantener un proceso para la eliminación de los datos de los discos y la memoria permanente antes del desecho, traslado o donación de equipos. 2. Coordinar con las instancias correspondientes, para que, en los procesos de destrucción y desecho de activos tecnológicos, se implementen medidas amigables con el ambiente. 3. Comunicar a los órganos correspondientes, para que se efectúe la actualización de los registros relacionados con el control de activos institucionales. " Adicionalmente a esto, se está conduciendo un proyecto para la confección de un Sistema de Gestión de la Seguridad de la Información, que se encuentra en la fase V y dentro de cuyos resultados, se encuentra la "Declaración de aplicabilidad" (SOA por sus siglas en inglés). Se adjunta Informe de Avance número 12 de dicho proyecto y el documento Gestión de Activos de hardware. Ver Anexo "11-Gestiones relacionadas al proceso de desecho y reutilización de medios electo impresos".
ESTADO	**NO APLICA** No se cumple con los lineamientos establecidos en la política GTI-10202102 Gestión de Activos de Hardware. Se le asigna el estado de NO APLICA y se actualiza la condición en un el Hallazgo 01 del presente informe.
CG 2009	
INTEGRACIÓN DE LOS DIFERENTES MÓDULOS.	
RECOMENDACIÓN	A la fecha se encuentra pendiente en el Fondo de Jubilaciones y Pensiones del Poder Judicial la integración en los sistemas de Contabilidad, Planillas de Jubilados y Pensionados y el de Inversiones. Cabe destacar que aún se trabaja en la implementación del proyecto SIGAFONDO permitiendo integración entre los diferentes módulos que la componen.
COMENTARIOS DE LA ADMINISTRACIÓN	El Sistema Contable considera la Integración con el Sistemas de Inversiones y el Sistema del Fondo de Jubilaciones y Pensiones. Al 31 de diciembre del 2016 se cerró con un avance de 85,47% del total de la contratación. Durante el 2016 se recibieron a satisfacción los siguientes módulos: • Quinto Entregable: Cuentas por Cobrar II Etapa, recibido a satisfacción en mayo 2016. • Sexto Entregable: Cuentas por Pagar I Etapa, recibido a satisfacción en agosto 2016. • Sexto Entregable: Cuentas por Pagar II Etapa, recibido a satisfacción en octubre 2016. • Séptimo Entregable: Cajas, recibido a satisfacción en Noviembre del 2016.

	• Noveno Entregable: Interfaces Externas, recibido a satisfacción en diciembre del 2016. • Décimo Entregable: Conciliaciones, recibido a satisfacción en diciembre 2016. En cuanto a las Horas de Acompañamiento, durante el 2016 se recibieron a satisfacción un total de 767. Ver Anexo "**Informe de labores Diciembre Sist Contable**".
ESTADO	**PROCESO** El hallazgo será subsanado con la implementación del sistema Financiero-Contable.
CG 2008	
HALLAZGO 1: NO SE REALIZAN EVALUACIONES SOBRE EL DESEMPEÑO DE LOS INTEGRANTES DEL ÁREA DE TI.	
RECOMENDACIÓN	
COMENTARIOS DE LA ADMINISTRACIÓN	Se adjuntó un proceso que fue definido mediante contratación junto con los resultados, hasta el momento no se ha aplicado. Ver anexo "**Procedimiento Evaluación Desempeño**".
ESTADO	**NO APLICA** Se cuenta con un procedimiento para la evaluación del desempeño; sin embargo, aún no se ha implementado. Para actualizar la condición, el presente hallazgo no aplica y se actualiza con el Hallazgo 03 del presente informe.
CG 2007	
HALLAZGO 3: NO SE HA IMPLEMENTADO UN ESTUDIO SOBRE LAS VULNERABILIDADES QUE PODRÍA TENER LA RED (ESTUDIO DE PENETRACIÓN).	
RECOMENDACIÓN	
COMENTARIOS DE LA ADMINISTRACIÓN	La Sección de Telemática aplica una vez al mes un análisis de vulnerabilidades sobre la solución de equipos críticos de comunicación de la plataforma de comunicaciones. Lo anterior con un equipo especializado para dicha función por lo que constantemente se está en verificación y acciones correctivas según el resultado obtenido. Siendo información confidencial, los informes y la descripción de la solución que se utiliza, se solicita la visita en sitio e inspección en lugar, donde un profesional le puede presentar y explicar el trabajo constante que se realiza en el análisis de vulnerabilidades en la Red del Poder Judicial. Favor coordinar la visita o inspección si procede, con el compañero Bertony Jiménez, de Telemática.
ESTADO	**CORREGIDO.** Se cuenta con una herramienta para la identificación, análisis y seguimiento de vulnerabilidades en la red. Mensualmente se remite el informe a los responsables de subsanar las debilidades identificadas.
CG 2006	
HALLAZGO 3: EL SISTEMA DE CONTABILIDAD NO SE DESACTIVA O PARALIZA AUTOMÁTICAMENTE DESPUÉS DE HABER ESTADO CIERTO TIEMPO SIN SER UTILIZADO.	

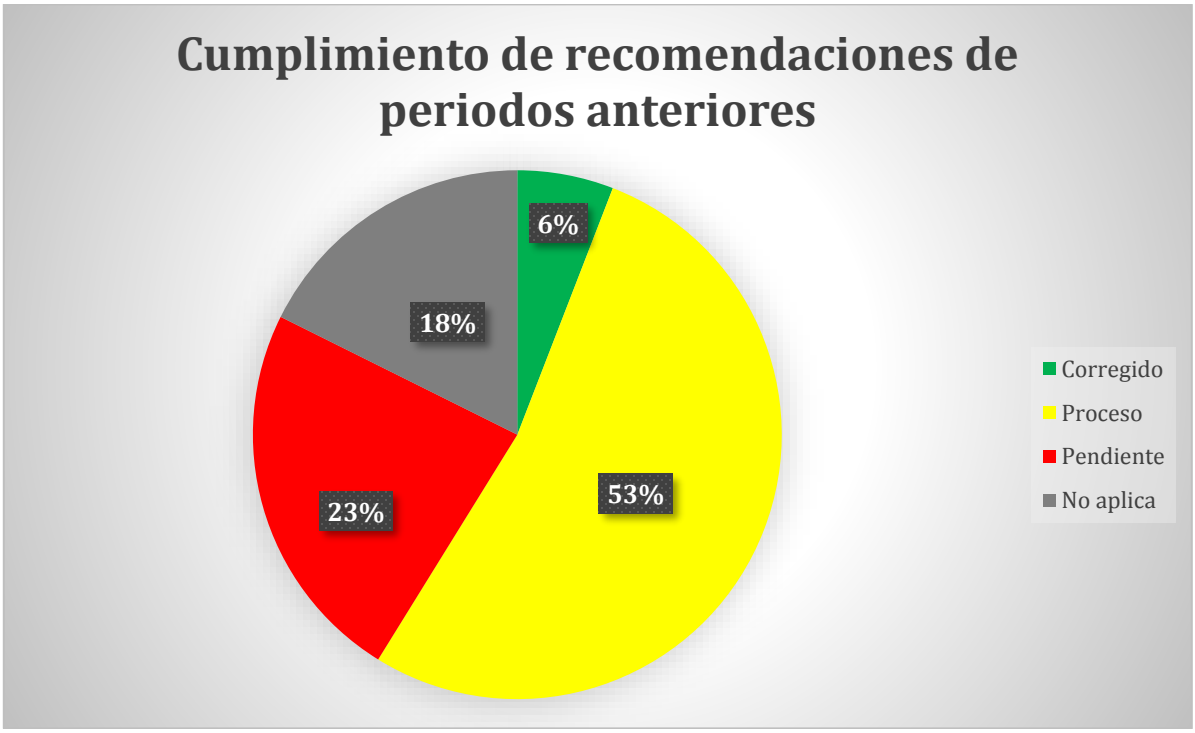
RECOMENDACIÓN	
COMENTARIOS DE LA ADMINISTRACIÓN	Durante el 2016 se recibieron a satisfacción los siguientes módulos: • Quinto Entregable: Cuentas por Cobrar II Etapa, recibido a satisfacción en Mayo 2016. • Sexto Entregable: Módulo de Cuentas por Pagar I Etapa, recibido a satisfacción en Agosto 2016. • Sexto Entregable: Módulo de Cuentas por Pagar II Etapa, recibido a satisfacción en Octubre 2016. • Séptimo Entregable: Cajas, recibido a satisfacción en Noviembre del 2016. • Noveno Entregable: Interfaces Externas, recibido a satisfacción en Diciembre del 2016. • Décimo Entregable: Conciliaciones, recibido a satisfacción en Diciembre 2016. En cuanto a las Horas de Acompañamiento, durante el 2016 se recibieron a satisfacción un total de 767. Ver Anexo "**Módulos Recibidos a Satisfacción 2016**".
ESTADO	**PROCESO** El hallazgo será subsanado con la implementación del sistema Financiero-Contable.
HALLAZGO 4: EL SISTEMA DE CONTABILIDAD NO CUENTA CON UNA BITÁCORA ADECUADA, Y EL SISTEMA DE PLANILLAS CARECE DE ESTA OPCIÓN DE SEGURIDAD.	
RECOMENDACIÓN	
COMENTARIOS DE LA ADMINISTRACIÓN	En el Sistema del Fondo de Jubilaciones y Pensiones la recomendación fue atendida desde el año 2010. En cuanto al Sistema Contable se encuentra en la Etapa de Paralelo y Pruebas Integrales, en el módulo de Seguridad del Sistema se encuentra implementada dicha recomendación. Aplicada en el Sistema de Fondo de Jubilaciones y Pensiones. En proceso en el Sistema Contable la Etapa de Paralelo y Pruebas Integrales.
ESTADO	**PROCESO** El hallazgo será subsanado con la implementación del sistema Financiero-Contable.
CG 2005	
HALLAZGO 1: LOS SISTEMAS ACTUALES NO ESTÁN INTEGRADOS POR LO QUE LAS ACTUALIZACIONES DE LAS BASES DE DATOS SE REALIZAN EN FORMA INDEPENDIENTE MEDIANTE PROCESOS MANUALES DE HOJAS DE CONTROL DE EXCEL.	
RECOMENDACIÓN	
COMENTARIOS DE LA ADMINISTRACIÓN	El Sistema Contable considera la Integración con el Sistemas de Inversiones y el Sistema del Fondo de Jubilaciones y Pensiones. Al 31 de diciembre del 2016 se cerró con un avance de 85,47% del total de la contratación. Durante el 2016 se recibieron a satisfacción los siguientes módulos: • Quinto Entregable: Módulo de Cuentas por Cobrar II Etapa, recibido a satisfacción en Mayo 2016. • Sexto Entregable: Módulo de Cuentas por Pagar I Etapa, recibido a satisfacción en Agosto 2016. • Sexto Entregable: Módulo de Cuentas por Pagar II Etapa, recibido a satisfacción en Octubre 2016. • Séptimo Entregable: Módulo de Cajas, recibido a satisfacción en Noviembre del 2016.

	• Noveno Entregable: Módulo de Interfaces Externas, recibido a satisfacción en Diciembre del 2016. • Décimo Entregable: Módulo de Conciliaciones, recibido a satisfacción en Diciembre 2016. En cuanto a las Horas de Acompañamiento, durante el 2016 se recibieron a satisfacción un total de 767. Ver Anexo "**Módulos Recibidos a Satisfacción 2016**".
ESTADO	**PROCESO** El hallazgo será subsanado con la implementación del sistema Financiero-Contable.
CG 2003	
HALLAZGO 6: EXISTE DEPENDENCIA DE LA EMPRESA TECAPRO, LO CUAL PODRÍA AFECTAR LA CONTINUIDAD DE LAS OPERACIONES	
RECOMENDACIÓN	
COMENTARIOS DE LA ADMINISTRACIÓN	En el caso de TECAPRO se tiene un contrato de mantenimiento para que se garantice la atención por parte de la empresa, en este caso se tiene el riesgo y se mitiga con el contrato de mantenimiento. Adicionalmente el sistema TECAPRO puede registrar asientos de días anteriores por lo que el tiempo de atención por parte de la empresa tiene un bajo impacto. Debido a que el sistema TECAPRO se actualizó con la última versión, se cuenta con una herramienta que opera correctamente en los equipos con Sistema operativo actualizado, y el contrato de mantenimiento garantiza las actualizaciones de las versiones. Solucionada a través de un proceso de mitigación de riesgo en la continuidad del servicio.
ESTADO	**PROCESO** Se cuenta con un contrato para el desarrollo de un nuevo sistema Financiero-Contable, el cual va a sustituir el sistema actual. A febrero del presente año el sistema se encuentra a un 85% aproximadamente de su implementación, y se espera que concluya en agosto del 2017. Después de su implementación, el sistema posee un año de garantía por parte de la empresa desarrolladora para brindar el soporte y mantenimiento requerido, el cual pasaría a manos de la DTI cuando este finalice.

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

PERIODO	CORREGIDO	PROCESO	PENDIENTE	NO APLICA	TOTAL POR PERIODO
2015	0	1	3	1	**4**
2014	0	1	1	0	**2**
2013	0	1	0	0	**1**
2011	0	1	0	1	**2**
2009	0	1	0	0	**1**
2008	0	0	0	1	**1**
2007	1	0	0	0	**1**
2006	0	2	0	0	**2**
2005	0	1	0	0	**1**
2003	0	1	0	0	**1**
TOTAL POR ESTADO	**1**	**9**	**4**	**3**	**17**

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



V. ANEXOS

ANEXO I Extintores vencidos

Anexo II Análisis de Riesgos Tecnologías de Información
Periodo 2016

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.

A. SEGURIDAD FÍSICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.1	Proceso de autorización de ingreso		✓	Se cuenta con un procedimiento para el ingreso al centro de datos.		B
A.2	Personal interno y externo debidamente identificado (gafete)		✓	Los usuarios cuentan con gafete.		B
A.3	Revisión de equipos de ingreso y salida		✓	Se lleva un control de activos para equipo nuevo y se generan boletas de registro para equipo que sale del sitio.		B
A.4	Bitácoras de acceso al edificio y centro de cómputo		✓	Se cuenta con una bitácora de ingreso al centro de datos.		B
A.5	Acceso restringido a personal de informática definido		✓	Sí se tiene restringido el acceso, si alguna persona desea solicitar el acceso al centro de datos, debe realizar una solicitud formal.		B
A.6	Una sola vía de acceso		✓	Sí hay una sola vía de acceso.		B
A.7	Externos son acompañados por internos		✓	Sí se acompaña a terceros.		B
A.8	Puerta de acceso segura		✓	Se cuenta con una puerta de acero con cerradura magnética.		B
A.9	Acceso con tarjeta electrónica al centro de datos		✓	Se debe acceder al centro de datos con tarjeta electrónica (gafete).		B
A.10	Alarmas de detección de intrusos		✓	Se cuenta con sensores de movimiento.		B
A.11	Monitoreo de la entrada por cámara de seguridad		✓	Se cuenta con cámara de seguridad en la entrada al sitio.		B
A.12	Ubicación en un sitio seguro (lugares colindantes)		✓	Se ubica en el 5to piso, dentro del área de TI.		B
A.13	Lugar completamente cerrado		✓	Existen ventanas de vidrio temperado.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
A.14	Paredes de concreto		✓	Dos paredes son de cemento y las otras dos son de un material contra fuego (no son de cemento).		B
A.15	Cielo raso sellado		✓	Sí está sellado.		B
A.16	Equipos ubicados en rack		✓	Sí están ubicados en racks.		B
A.17	Los racks están asegurados		✓	Sí están asegurados.		B
A.18	Cableado de datos independiente del eléctrico		✓	Sí es independiente.		B
A.19	Cableado entubado y canaleteado		✓	Ambos tipos de cables están entubados o canaleteados.		B
A.20	Cableado debidamente rotulado		✓	El cableado sí está rotulado o etiquetado.		B
A.21	Hay un sitio alterno		✓	Se cuenta con un contrato con el ICE.		B

B. INSTALACIÓN ELÉCTRICA

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
B.1	Hay pararrayos		✓	Sí se cuenta con pararrayos		B
B.2	Circuito eléctrico independiente		✓	Sí es independiente.		B
B.3	Interruptor de emergencia en la sala de cómputo (palanca)		✓	El centro de datos cuenta con interruptores para emergencia, asimismo se cuenta con un interruptor principal fuera del sitio.		B

B.4	Cableado eléctrico debidamente entubado o cubierta contra incendios		✓	Sí está entubado.		B
B.5	Conexión de los equipos a UPS		✓	Sí se tiene conexión a UPS.		B
B.6	UPS ubicada en un sitio seguro		✓	Se encuentran en el sótano.		B
B.7	Pruebas periódicas de la UPS (bitácora)		✓	Servicios generales en coordinación con el área de infraestructura.		B
B.8	UPS en contrato de mantenimiento preventivo y correctivo		✓	Sí se encuentran en mantenimiento.		B
B.9	Conexión a Planta eléctrica		✓	Sí se cuenta con planta eléctrica.		B
B.10	Planta eléctrica ubicada en un sitio seguro		✓	La planta eléctrica se encuentra fuera del edificio y es vigilada por los oficiales de seguridad.		B
B.11	Pruebas periódicas de la planta eléctrica		✓	Se realizan pruebas junto al mantenimiento.		B
B.12	Planta eléctrica en contrato de mantenimiento preventivo y correctivo		✓	Se encuentra en mantenimiento por la empresa FONT.		B
B.13	Luces de emergencia en el centro de cómputo o cercanías		✓	Hay luces de emergencia para exteriores o fuera del centro de datos.		B
B.14	Pruebas periódicas de sistema de iluminación de emergencias		✓	Sí se realizan pruebas.		B

C. INSTALACIÓN AIRE ACONDICIONADO

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
C.1	Equipo de aire acondicionado independiente para el centro de datos		✓	Sí es independiente.		B
C.2	Equipo de respaldo para el aire acondicionado		✓	Se cuenta con 5 aires acondicionados.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
C.3	Contrato de mantenimiento preventivo y correctivo		✓	Sí se realiza mantenimiento preventivo y correctivo bajo un contrato.		B
C.4	Control y monitoreo de humedad y temperatura		✓	Sí se realiza mantenimiento preventivo y correctivo bajo un contrato.		B

D. DESASTRES NATURALES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
D.1	Brigada de emergencias		✓	A lo interno del Poder Judicial hay brigada en coordinación con Salud ocupacional.		B
D.2	Capacitación del personal		✓	Sí se realizan capacitaciones.		B
D.3	Rutas de evacuación y salidas de emergencia		✓	Cada piso y sección tiene definido un protocolo de evacuación y puntos de reunión.		B
D.4	Señalización		✓	Sí está señalizado.		B
D.5	Simulaciones periódicas		✓	Sí se realizan simulacros.		B
D.6	Fácil acceso por Unidades de Bomberos		✓	Sí es de fácil acceso.		B
D.7	Sistemas de detección de humo/calor/fuego		✓	Se cuenta con detectores de humo.		B
D.8	Sistemas automáticos y manuales de alarma		✓	Sí se cuenta con alarmas manuales.		B
D.9	Extinguidores cercanos portátiles (revisados al día)	✗		Se cuenta con 4 extintores en el centro de datos, pero solo dos se encuentran recargados.		B
D.12	Uso de aspersores	✗		No se cuenta con aspersores.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
D.11	Pisos falsos		✓	No se cuenta con piso falso, el cableado se maneja sobre canaletas en la parte superior del centro de datos.		B
D.12	Desnivel en el piso		✓	No hay desnivel en el piso, sin embargo, este se encuentra en un 5to piso, por lo que no hay vulnerabilidad de inundaciones.		B

E. FALLAS HARDWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
E.1	Redundancia de servidores críticos		✓	Se cuenta con redundancia de equipo solo para la parte crítica.		B
E.2	Mantenimiento preventivo		✓	El área de infraestructura se encarga del mantenimiento. Además, los proveedores de los equipos realizan mantenimiento cada 3 meses.		B
E.3	Mantenimiento correctivo		✓	Cada 3 meses se le da mantenimiento al equipo.		B

F. FALLAS SOFTWARE

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
F.1	Política de uso de recursos (prioridades en procesos)		✓	Se cuenta con una política institucional para el uso de recursos tecnológicos para los usuarios. Para el centro de datos hay una política para la gestión de los recursos de los equipos.		B
F.2	Control de cambios		✓	Se cuenta con un procedimiento para la gestión de cambios en TI.		B

G. FALLAS EN COMUNICACIONES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
G.1	Redundancia de equipos y enlaces	✗		Sí hay redundancia de equipos, sin embargo, no hay redundancia de enlaces. Según lo comentado, hay un proyecto para obtener un segundo enlace de conexión como redundancia.		B
G.2	Mantenimiento preventivo		✓	Se le da mantenimiento preventivo y correctivo por parte de los proveedores de los equipos.		B
G.3	Mantenimiento correctivo		✓	Se le da mantenimiento preventivo y correctivo por parte de los proveedores de los equipos.		B

H. RESPALDOS Y RECUPERACIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
H.1	Política de respaldos		✓	Se cuenta con un procedimiento para la administración de respaldos.		B
H.2	Procedimientos para respaldo y recuperación		✓	Se cuenta con un procedimiento para la administración de respaldos.		B
H.3	Almacenamiento de información		✓	Se utilizan discos y cintas para almacenar respaldos.		B
H.4	Traslado de respaldos		✓	Los respaldos se envían a una sede que está ubicada en San Joaquín de Flores.		B
H.5	Configuración de programas para respaldo		✓	Se utiliza Data Domain para gestionar los respaldos.		B

I. ATAQUES POR VIRUS

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
I.1	Política de antivirus		✓	Se maneja una suite de seguridad con políticas preestablecidas.		B
I.2	Programa antivirus		✓	Se utiliza McAfee.		B
I.3	Actualización del antivirus		✓	Se utiliza una consola para administrar los equipos y se encarga de la distribución de las actualizaciones.		B
I.4	Administración de incidentes y problemas		✓	Hay un centro de atención el cual gestiona los incidentes reportados y los escala a la DTI para su revisión. En caso de no encontrar solución se escala al proveedor Consulting Group para su gestión.		B

J. INTRUSIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
J.1	Política de acceso lógico		✓	Se utiliza un formulario para solicitar los accesos. Para accesos de Active Directory son atendidos a través del centro de atención.		B
J.2	Control de acceso a aplicaciones		✓	Los accesos son aprobados por los coordinadores o jefaturas inmediatas.		B
J.3	Monitoreo de usuarios y accesos		✓	Los sistemas poseen bitácoras para monitorear los movimientos de los usuarios.		B

K. ADMINISTRACIÓN DE OPERACIONES

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
K.1	Capacitación personal técnico		✓	Cada año se gestionan reservas presupuestarias y se dan cursos entre abril y agosto de capacitaciones requeridas. El personal capacitado se encarga de retroalimentar a los demás funcionarios.		B
K.2	Segregación de funciones		✓	Sí hay segregación de funciones.		B

L. RIESGOS DE LA GESTIÓN DE TI

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.1	¿Se tienen definido un plan estratégico para TI alineado con el de la organización?		✓	Se cuenta con un PETI alineado a la organización.		B
L.2	¿El Plan estratégico ha sido divulgado a los niveles que corresponde?		✓	Se divulga a lo interno a través de la intranet y se realizan reuniones trimestrales. A lo externo se realizan talleres, a través del Área de Prensa y se sube la página web institucional.		B
L.3	¿Se tienen definidas las políticas y procedimientos para TI?		✓	Sí se cuenta con la definición de políticas y procedimientos.		B
L.4	¿Se tiene definido el apetito de riesgos para TI? (Nivel de riesgo que la Institución quiere aceptar)		✓	Los riesgos se tratan de tal forma que lleguen a un nivel aceptable.		B
L.5	¿Los riesgos que la organización se encuentra dispuesta a aceptar se encuentran aprobados formalmente por la Administración y el Comité de Auditoría?		✓	Son evaluados por Control Interno, además, los de nivel aceptable no deben ser aprobados (por el bajo nivel), pero son controlados por un Equipo de Riesgos de la DTI.		B
L.6	¿El mapa de riesgos es revisado y actualizado periódicamente?		✓	Se realizan revisiones anuales de los riesgos.		B
L.7	¿La evaluación de riesgos considera elementos cualitativos y cuantitativos?		✓	Sí se consideran ambos criterios.		B
L.8	¿Los riesgos de TI son revisados con los usuarios del sistema?		✓	Durante la revisión de los riesgos de la DTI, hay participación de las áreas involucradas.		B
L.9	¿Se han implementado anti virus y firewalls?		✓	Sí se cuenta con estos dispositivos o programas de software.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.10	¿Se han establecido los protocolos para la realización de copias de seguridad?		✓	Se cuenta con un procedimiento para la realización de respaldos, posteriormente, los dispositivos de almacenamiento se trasladan a un sitio externo.		B
L.11	¿La seguridad de la información es un tema de seguimiento para la alta gerencia como para el Comité de Auditoría?		✓	A través de las recomendaciones según el plan de trabajo de la Auditoría Interna. La DTI está en proceso de conformar un área de dirección y control para el seguimiento interno a los marcos internos para la parte del Gobierno de TI con COBIT 5.		B
L.12	¿Las políticas y procedimientos relacionados con TI son revisados y actualizados periódicamente, considerando los cambios en la industria y la regulación externa?		✓	Cada año se realizan revisiones y actualizaciones de los riesgos.		B
L.13	¿Se tiene definido el perfil para cada cargo de TI y los colaboradores vinculados cumplen con el mismo?		✓	Se cuenta con un manual descriptivo de puestos.		B
L.14	¿Se tienen definidas y divulgadas las funciones y responsabilidades de cada colaborador del área?		✓	Sí se realiza de esta manera.		B
L.15	¿Las responsabilidades de cada nivel y colaborador, parten del principio de segregación de funciones?		✓	Sí existe segregación de funciones en la DTI.		B
L.16	¿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?		✓	Cada área de la Institución tiene asignado un administrador de la seguridad del sistema, los cuales se encargan de esta función.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.17	¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de las mismas?		✓	Se realizan capacitaciones iniciales.		B
L.18	¿Las herramientas de TI permiten tener la trazabilidad de las operaciones realizadas, así como de los usuarios (logs)?		✓	Sí se cuenta con bitácoras en los sistemas de información.		B
L.19	¿Se monitorea el estado de los equipos (Hardware)?		✓	Se monitorea mensualmente a través de la herramienta Vulnerability Manager, sin embargo, aún no se cuenta con un plan de capacidad y desempeño.		B
L.20	¿La seguridad física de las instalaciones donde operan los equipos y personas de TI, es evaluada y revisada periódicamente, cumplimiento con los protocolos establecidos?	✗		El centro de datos es monitoreado todos los días por el área de seguridad. Además, todos los días el personal de Soporte Técnico revisa presencialmente si hay daños en el equipo o hay alguna anomalía. No obstante, no se cuenta con políticas de seguridad física.		B
L.21	¿La organización desarrolla un plan de formación integral tanto para los miembros de TI como para los usuarios de la herramienta, orientado al uso, seguridad y ética en la utilización de las mismas?		✓	Para la parte de seguridad de los sistemas, la DTI se encarga de dar la capacitación al encargado del sistema.		B
L.22	¿Se han establecido indicadores de gestión que permitan medir el desempeño de las herramientas como de los colaboradores del área?	✗		Se realizó una contratación para el diseño de un procedimiento, sin embargo, aún no se ha implementado.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.23	¿Se han implementado planes de acción correctivos, para aquellos casos en que los indicadores presentan resultados inferiores a los esperados?	✗		El procedimiento no se ha implementado.		B
L.24	¿Se han adquirido pólizas de seguro para eventos de riesgos en el área de TI?		✓	No se cuenta con pólizas, sin embargo, el equipo crítico posee redundancia y recibe mantenimiento correctivo y preventivo.		B
L.25	¿Cada proyecto de TI tienen definidos y documentos los riesgos tanto de su desarrollo como de la puesta en marcha, así como tiene la proyección de recursos financieros a invertir?		✓	Se definen los riesgos en el plan de dirección del proyecto, según lo establecido en la metodología.		B
L.26	¿Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de TI y dicho seguimiento es documentado?		✓	Se realiza una revisión de productos para dar la aceptación de los mismos, además, se cuenta con SLAs con proveedores.		B
L.27	¿Todos los cambios desarrollados en las aplicaciones y/o software son documentados y custodiados?		✓	Se cuenta con un procedimiento para la gestión de cambios en TI.		B
L.28	¿Se ha establecido el plan de continuidad para los procesos de TI?		✓	Se cuenta con un plan de continuidad para el SIGAFJP.		B
L.29	¿Se solicita el apoyo de consultores externos para los proyectos estratégicos?		✓	Sí se solicita apoyo a externos.		B

M. SISTEMAS DE INFORMACIÓN

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.1	Los accesos son autorizados por un nivel superior.		✓	Hay un encargado en cada área que se encarga de esta labor.		B
M.2	Los accesos otorgados son revisados periódicamente.		✓	Existen lineamientos para que los dueños de la información revisen el uso adecuado de los permisos de los usuarios.		B
M.3	La asignación de los accesos parte de la segregación de funciones.		✓	Sí hay segregación de funciones.		B
M.4	Cada usuario tiene asignada una clave de composición alfa numérica y de mínimo 8 caracteres		✓	Sí es de esta forma.		B
M.5	Se pueden rastrear las operaciones realizadas por los usuarios por medio de los logs		✓	Los sistemas sí cuentan con bitácoras.		B
M.6	Se cuenta con una política de copias de seguridad y de restauración.		✓	Se cuenta con un procedimiento para la elaboración de respaldos de información.		B
M.7	La información sensible se encuentra protegida de modificaciones no autorizadas.		✓	Existen métodos de autenticación de por medio para acceder a la información. Además, se restringen los permisos de acceso a la información.		B
M.8	Se cumplen con los niveles de seguridad físicos para los servidores.		✓	No se detectaron debilidades significativas en el centro de datos.		B
M.9	Asignación de usuarios y claves personalizada		✓	Las credenciales de los usuarios sí son personalizadas.		B
M.10	Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.		✓	Se cuenta con niveles de atención de usuarios. Además, sí existe segregación de funciones entre los que gestionan el cambio.		B
M.11	Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.		✓	Se manejan boletas de aceptación antes de pasarlos a producción. Se alertan a través de correo electrónico.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.12	Las modificaciones en las bases de datos son realizadas por un área independiente a la que utiliza la información.		✓	Sí es de esta manera.		B
M.13	Los cambios en la base de datos permiten tener la trazabilidad de quien los realiza por medio de los logs.		✓	Sí se cuentan con logs.		B
M.14	Se tiene un número reducido de administradores.		✓	Sí es de esta manera.		B
M.15	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.		✓	Se cuenta con un diccionario de datos.		B
M.16	Definición y documentación de la Política de Cambios		✓	Se cuenta con un procedimiento para la gestión de cambios.		B
M.17	Segregación de funciones entre el desarrollador, aprobador y responsable de administrar en producción		✓	Sí hay segregación de funciones.		B
M.18	Aprobación del usuario final de los cambios.		✓	Se manejan boletas de aceptación antes de pasarlos a producción.		B
M.19	Asignación usuarios y permisos, previo requerimiento y aprobación del Director y/o Responsable del área que utiliza la aplicación.		✓	Hay un encargado de la seguridad por área que se encarga de esta labor.		B
M.20	Reportes periódicos de los cambios que se consideran críticos en las aplicaciones, para validar su autorización por parte del nivel aprobador de los cambios.		✓	Se manejan boletas de aceptación antes de pasarlos a producción.		B
M.21	Validación periódica de los cambios en permisos y asignación de usuarios por parte del nivel autorizador.		✓	Hay un encargado de la seguridad por área que se encarga de esta labor.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
M.22	Bloqueo de usuarios retirados, previa comunicación de Gestión Humana.		✓	Sí se bloquea, según lo indique cada área.		B
M.23	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.		✓	El encargado de la seguridad por cada área se encarga de administrar y revisar accesos.		B
M.24	Bloqueo de usuarios en vacaciones		✓	Sí se bloquea, según lo indique cada área.		B
M.25	Identificación de los usuarios que realizan las transacciones, por medio de los Logs.		✓	Los sistemas cuentan con bitácoras.		B
M.26	Certificaciones externas sobre la calidad del servicio prestado.		✓	Se realizan auditorías externas anualmente para validar procesos de TI.		B
M.27	Suscripción de un acuerdo sobre privacidad con el proveedor.		✓	Se cuentan con cláusulas de confidencialidad con externos.		B
M.28	Plan de contingencia para migrar a otro servidor		✓	Se cuenta con un plan de continuidad para el SIGAFPJ.		B
M.29	Plan de capacitaciones en seguridad, para los usuarios con accesos más vulnerables.		✓	La DTI brinda capacitación sobre seguridad al encargado de la seguridad en cada área.		B
M.30	Cifrar las bases de datos más sensibles, junto con controles de monitoreo.		✓	Se cifra la contraseña de los usuarios y la conexión a bases de datos.		B
M.31	Limitar el acceso a los datos y/o solicitar mayores autenticaciones, de acuerdo al dispositivo y al lugar desde donde se ingresa.		✓	Se utilizan clientes de aplicaciones para el acceso remoto, considerando las medidas de seguridad necesarias.		B
M.32	Instalar en los dispositivos móviles parches que permitan aislar los datos de la compañía de los personales.		✓	La información no está disponible para dispositivos móviles.		B
M.33	Se realizan pruebas periódicas sobre la recuperación de datos.		✓	Sí se realizan pruebas de los respaldos.		B