Fondo de Jubilaciones y Pensiones del Poder Judicial

- ***Informe de Auditoría de Tecnologías de Información.***
- ***Carta de Gerencia CG-TI 2019***
- ***Informe Final.***

San José, 21 de febrero del 2020

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 2019 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-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 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: 2020.03.06 11:28:33 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad N° 0116 FIG 7
Vence el 30 de setiembre del 2020.

"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 las 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:

A. Sistemas de información del FPJ.
B. Gestión de perfiles de usuario en los sistemas de información.
C. Atención de requerimientos de usuario.
D. Gestión de respaldos de información.
E. Gestión de la capacidad y disponibilidad de la plataforma tecnológica.
F. Gestión de la continuidad de TI.
G. Evaluación del desempeño de los colaboradores de la DTIC.

1.3 Metodología

Para llevar a cabo este trabajo utilizamos una modalidad de solicitud de información 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. Efectuamos 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-TI 2019.

Además de formular preguntas sobre la existencia de controles informáticos, en todos los casos necesarios solicitamos a los funcionarios 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 información implementados.

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 y en general las sanas prácticas en materia tecnológica.

1.5 Limitaciones al alcance

Durante el presente estudio no se presentaron limitaciones al alcance.

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:

A. Sistemas de información del FPJ.

Se indicó por parte de la DTIC lo siguiente:
"Con respecto al FJP según el oficio 835, CLÁUSULA TERCERA: "En relación con los sistemas de información del Fondo de Jubilaciones, Contabilidad y Sistema de Inversiones, la Dirección de Tecnología brindará el soporte, atención de incidentes y las mejoras estrictamente necesarias, las cuales deberán ser elevadas a la Comisión Gerencial de Tecnología para su respectiva valoración, deberá ser considerado la disponibilidad del recurso".

Con respecto al sistema contable: "El Consejo Superior en sesión N° 90-19, Artículo LXXXIII, acordó: Suspender el cronograma de trabajo del Sistema Contable del 2019 y Cambiar el cronograma de trabajo del 2020 del Sistema Contable, con el fin de atender las modificaciones necesarias en el sistema para aplicar el cambio de catálogo contable, solicitado por la Superintendencia de Pensiones (SUPEN). Ver anexo 5. Integración, se adjunta oficio 835".

Cabe mencionar que se cuenta con los respectivos procedimientos para la revisión y administración de bitácoras del sistema. No obstante, al no realizar las respectivas mejoras al sistema, se determina que el hallazgo asociado (H01 - 2018) se encuentra en proceso.

B. Gestión de perfiles de usuario en los sistemas de información.

Se identificó la existencia de procedimientos y manuales para la gestión de este proceso. Además, se evidenció que se realizan revisiones dos veces al año, por lo tanto, no se identificaron deficiencias de gestión.

C. Atención de requerimientos de usuario.

Se identificó la existencia de un procedimiento para la gestión de peticiones de usuario. Dicho procedimiento posee asociado un conjunto de lineamientos o políticas y una ficha de proceso, el cual se asocia al proceso de COBIT DSS02 y la respectiva matriz RACI. Dichos procedimientos cuentan con una estructura adecuada y están alineados a las recomendaciones de las buenas prácticas.

D. Gestión de respaldos de información.

Se identificó la existencia de respaldos, no obstante, no se cuenta con un procedimiento formalmente establecido para el proceso, el cual defina responsabilidades, roles, medios de almacenamiento, tiempo de resguardo (antigüedad de los respaldos), envío de respaldos y periodicidad, entre otros. Además, los procedimientos no establecen un plan o periodicidad para ejecutar las respectivas pruebas. Ver hallazgo 01.

E. Gestión de la capacidad y disponibilidad de la plataforma tecnológica.

Se identificó la existencia de un procedimiento y un plan para la gestión de la capacidad y disponibilidad de los recursos de la plataforma tecnológica. Sin embargo, no se evidenció que estos documentos se encuentren aprobados, ni se suministró evidencia de cumplimiento. Por lo tanto, la oportunidad de mejora asociada (OM02 - 2014) se encuentra en proceso.

F. Gestión de la continuidad de TI.

Se determinó que aún no se cuenta con un plan de continuidad de servicios de TI para el FPJ. Cabe mencionar que se cuenta con un plan de contingencia tanto para el fondo como para inversiones, los cuales son los planes con los que se ha contado desde periodos anteriores.

En cuanto al avance del plan de continuidad, en octubre del periodo 2019 se desarrolló el respectivo BIA. De acuerdo con el cronograma de trabajo, se espera terminar el plan durante el cuarto trimestre del periodo 2021. Por lo tanto, el hallazgo asociado (H03 - 2017) se encuentra en proceso de implementación.

G. Evaluación del desempeño de los colaboradores de la DTIC.

Se identificó la existencia de procedimientos y políticas para la gestión del recurso humano. Dichos documentos contemplan los lineamientos sobre la definición de indicadores y métodos para evaluar el desempeño de los colaboradores de TI. Cabe mencionar que ya se han definido algunas herramientas e indicadores, no obstante, aún no se encuentran implementados ya que apenas se ha concluido la etapa de diseño del proyecto. Por lo tanto, el hallazgo H03 – 2016 se encuentra en proceso.

III. HALLAZGOS Y RECOMENDACIONES

HALLAZGO 01: DEFICIENCIAS ENCONTRADAS EN LOS PROCEDIMIENTOS DE RESPALDOS Y RECUPERACIÓN DE DATOS DEL FONDO DEL PODER JUDICIAL. RIESGO BAJO.

CONDICIÓN:

a. Sobre el procedimiento para la generación de los respaldos de la información del Fondo del Poder Judicial:

Según lo indicado por la Dirección de Tecnología de la Información y Comunicación (DTIC) los respaldos se realizan de manera automática y en el momento que se crea una base de datos cuenta con un Job que detecta y genera el esquema de respaldos. No obstante, no se cuenta con un procedimiento que respalde lo antes mencionado que permita verificar el cumplimiento, responsables de verificar los respaldos, periodicidad entre otros aspectos.

Sin embargo, se logró identificar un archivo de la gestión de respaldos de enero a diciembre del 2019. En el reporte se detalla el nombre de la base de datos en este caso Siga FJP Reconocimiento, fecha de inicio del respaldo, fecha de finalización del respaldo, fecha de caducidad (NULL), tamaño del respaldo, nombre del conjunto de respaldos y descripción.

b. Sobre el procedimiento para la recuperación de la información del Fondo del Poder Judicial:

Se cuenta con un procedimiento para la restauración de respaldos mediante solicitud de la persona usuaria con el objetivo de restaurar un archivo, carpeta, aplicación entre otros. Con respecto a la base de datos, la DTIC cuenta con un procedimiento para la restauración de respaldos de base de datos donde establece los pasos a seguir para restaurar los respaldos de la base de datos mediante una solicitud por parte del encargado de base de datos, en caso de emergencia o cuando este lo requiera. Sin embargo, el documento no posee un plan de pruebas de restauración de respaldos que se ejecute de manera periódica.

Al no contar con un procedimiento formal para la realización de respaldos de la información y la ejecución de pruebas de recuperación de manera periódica, existe el riego de que no se pueda recuperar la información debido a incidentes no esperados, la incapacidad de actuar de forma inmediata y asegurar la continuidad del procesamiento de los datos.

CRITERIO:

El proceso **4.3 "Administración y operación de la plataforma tecnológica"** presente en el documento N-2-2007-CO-DFOE Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la República menciona: "*La organización debe*

mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:

a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.
b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.
c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.
d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas.
e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro.
f. Mantener separados y controlados los ambientes de desarrollo y producción.
g. Brindar el soporte requerido a los equipos principales y periféricos.
h. Definir formalmente y efectuar rutinas de respaldo, custodiar los medios de respaldo en ambientes adecuados, controlar el acceso a dichos medios y establecer procedimientos de control para los procesos de restauración.
i. Controlar los servicios e instalaciones externos.".

RECOMENDACIONES:

A la Dirección de Tecnología de la Información y Comunicación:

1. Documentar el procedimiento para los respaldos de información, considerando los siguientes aspectos:
    a. Plan de respaldo.
    b. Cuáles datos se deben incluir.
    c. Medios de soporte a utilizar (discos duros, cintas, etc.).
    d. Tipos de respaldos (parciales, incrementales, etc.).
    e. Cantidad de copias a realizar.
    f. Donde guardarlas.
    g. Quienes los manejan.
    h. Verificación del respaldo.
    i. Periodicidad de los respaldos (mensual, semanal, diaria, etc.)

2. Establecer un plan de pruebas de restauración de respaldos en donde por cada tipo de respaldo se indique lo siguiente:
    a. Periodicidad de las pruebas.
    b. Responsable.
    c. Resultados
    d. Acciones ejecutadas cuando las pruebas resultaron insatisfactorias.

IV. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CG 2018	
HALLAZGO 01: OPORTUNIDADES DE MEJORA IDENTIFICADAS EN LOS SISTEMAS DEL FPJ.	
RECOMENDACIÓN	***A la Dirección de Tecnología de la Información:*** 1. Evaluar la parametrización y configuración de la seguridad lógica de los sistemas de información con el fin de asegurar que se cumplan con los siguientes aspectos: a. Los sistemas sólo deben permitir la existencia de una sesión de usuario a la vez. Valorar que cuentas de usuario no requieren tener múltiples sesiones abiertas y restringirlas a una sola. b. Implementar mecanismos para el uso de contraseñas temporales para los casos en que los usuarios deseen reestablecer la contraseña o se crean nuevos usuarios. El usuario debe cambiar la contraseña tras su primer uso. ***A la Dirección de Tecnología de la Información en conjunto con las áreas usuarias:*** 2. Realizar un proceso de revisión con las áreas usuarias con el fin de poder identificar las necesidades de integración y automatización de procesos, de modo que se pueda subsanar las oportunidades de mejora indicadas en la condición del hallazgo. ***A las áreas usuarias en conjunto con la Dirección de Tecnología de la Información:*** 3. Evaluar incorporar en el procedimiento propuesto para la revisión de pistas o bitácoras, la periodicidad en que se efectuarán, y así verificar que los procesos del negocio y accesos se encuentran dentro de lo esperado.
COMENTARIOS DE LA ADMINISTRACIÓN	Evidencia aportada: Acta del Consejo Superior N°090-2019, oficio 835-2020, lineamiento L-DTIC-001 Uso de las credenciales de usuario y contraseñas, Circular 11-DTI-2017, correo electrónico del coordinador de la Unidad de Seguridad Informática, se adjuntan también los procedimientos para la revisión de pistas de auditoría correspondientes a los sistemas del FJP y de Contabilidad del Poder Judicial.
ESTADO	**EN PROCESO** En relación con la parametrización de las contraseñas de los sistemas del Fondo del Poder Judicial, se determinó los siguientes aspectos: **a. Cantidad de sesiones simultáneas que pueden poseer los usuarios:** La Dirección de Tecnología de la Información y Comunicación (DTIC) menciona que en el oficio 835, CLÁUSULA TERCERA: "n relación con los sistemas de información del Fondo de Jubilaciones, Contabilidad y Sistema de Inversiones, la Dirección de Tecnología brindará el soporte, atención de

	incidentes y las mejoras estrictamente necesarias, las cuales deberán ser elevadas a la Comisión Gerencial de Tecnología para su respectiva valoración, deberá ser considerado la disponibilidad del recurso". **b. Uso de contraseñas temporales cuando se requiera crear un usuario o restablecer una contraseña:** Se determinó que se restablece la contraseña y permite activar la opción para que le solicite al usuario el cambio de contraseña en el siguiente inicio de sesión, ambas opciones se realizan de manera individual por cada cuenta de usuario y no por una configuración ya establecida. **c. Vencimiento de la contraseña:** Se identificó la opción en la política del AD, sin embargo, cuenta con 0 días. Además, se comprobó que cuenta con un Sistema Administrador de contraseñas se notifica mediante correo a los usuarios que incumple con cambiar cada 90 días la contraseña según lo establecido en el lineamiento para el uso de las credenciales de usuario y contraseñas (L-DTIC-001). Para dicho control cuentan con un Sistema Administrador de contraseñas. La notificación establecer los requisitos mínimos que debe considerar para la nueva contraseña. **d. Tamaño de la contraseña:** Se comprobó en la política del AD que el tamaño mínimo de la contraseña es de 8 caracteres. **e. Complejidad de la contraseña:** Se identificó que se encuentra habilitada la política en el AD que la contraseña debe cumplir los requisitos de complejidad establecidos. **f. Histórico de contraseñas:** Se determinó en la política del AD que exige un histórico de 8 contraseñas recordadas. Es importante mencionar que la Dirección de Tecnología de la Información y Comunicación cuenta con un lineamiento para el uso de las credenciales de usuario y contraseñas (L-DTIC-001) En relación con las gestiones realizadas para subsanar las deficiencias encontradas en CG de periodos anteriores, la Dirección de Tecnología de la Información y Comunicación menciona lo siguiente: • El oficio 835, CLÁUSULA TERCERA:" En relación con los sistemas de información del Fondo de Jubilaciones, Contabilidad y Sistema de Inversiones, la Dirección de Tecnología brindará el soporte, atención de incidentes y las mejoras estrictamente necesarias, las cuales deberán ser elevadas a la Comisión Gerencial de Tecnología para su respectiva valoración, deberá ser considerado la disponibilidad del recurso". • Con respecto al sistema contable: "El Consejo Superior en sesión N° 90-19, Artículo LXXXIII, acordó: Suspender el cronograma de trabajo del Sistema Contable del 2019 y Cambiar el cronograma de trabajo del 2020 del Sistema Contable, con el fin de atender las modificaciones necesarias en el sistema para aplicar el cambio de catálogo contable, solicitado por la Superintendencia de Pensiones (SUPEN)".

Además, se les consultó a los usuarios sobre la condición identificada en la Carta de Gerencia del periodo 2018 para los sistemas SCI, SIGA-FPJ y SIGA-CONTA. En respuesta los usuarios mencionaron lo siguiente:

Sistema	Comentario
Sistema Integrado de Carteras de Inversión (SCI)	Según lo indicado por el usuario se mantiene la condición, sin embargo, se remitió a la Dirección de Tecnología de Informática el GIS No. IM-718719-2-205598 (reporte de mejora), para que se realicen los cambios correspondientes, es importante indicar que este GIS no se había remitido anteriormente, pero si estaba en espera del trámite respectivo, en virtud de que estaba en espera de la finalización del proceso de integración de los requerimientos de SUPEN (nuevo catálogo contable y cambios relacionados en los sistemas).
SIGA-FPJ	Según lo indicado por el usuario se mantiene la condición.
SIGA-CONTA	Según lo indicado por el usuario se mantiene la condición, sin embargo, se tiene previsto trabajar a finales del 2020 y principios del 2021 con el DTIC para subsanar la deficiencia indicada.

Por último, se determinó que el Consejo Superior del Poder Judicial en sesión No. 32-19, celebrada el 9 de abril de 2019, artículo XXXVII, acordó modificar la circular N° 40-2019 aprobada en la sesión Nº 9-19 celebrada el 05 de febrero del 2019, artículo LV, acogió referente al "Procedimiento para la administración de bitácoras de los sistemas del Poder Judicial" elaborado en enero del 2019 y en la lista de reportes o consultas disponibles por sistema para revisar la bitácora de transacciones se incluye el Sistema de Fondo de Jubilaciones y Pensiones del Poder Judicial. Sin embargo, el procedimiento no define la periodicidad en la que el Usuario encargado de oficina debe realizar las revisiones a la bitácora de las transacciones del sistema, a pesar de que se identificó en el reporte de Bitácora de Transacciones (SIGA-FPJ) las revisiones de los 4 trimestres del 2019. Es importante mencionar que la labor de revisión y depuración de acciones de los diferentes usuarios del sistema se inició en 04/02/2020, debido a que los reportes no se encontraban disponibles en el menú del SIGA-FJP.

Además, el procedimiento para la administración de bitácoras en cuanto a las revisiones periódicas de los movimientos realizados en el sistema del Fondo de Jubilaciones y Pensiones elaborado en marzo del 2017, no se encuentra actualizado.

CG 2017	
HALLAZGO 03: AUSENCIA DE UN PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN ACTUALIZADO PARA EL FONDO DEL PODER JUDICIAL.	
RECOMENDACIÓN	***A la Dirección de Tecnologías de Información:***

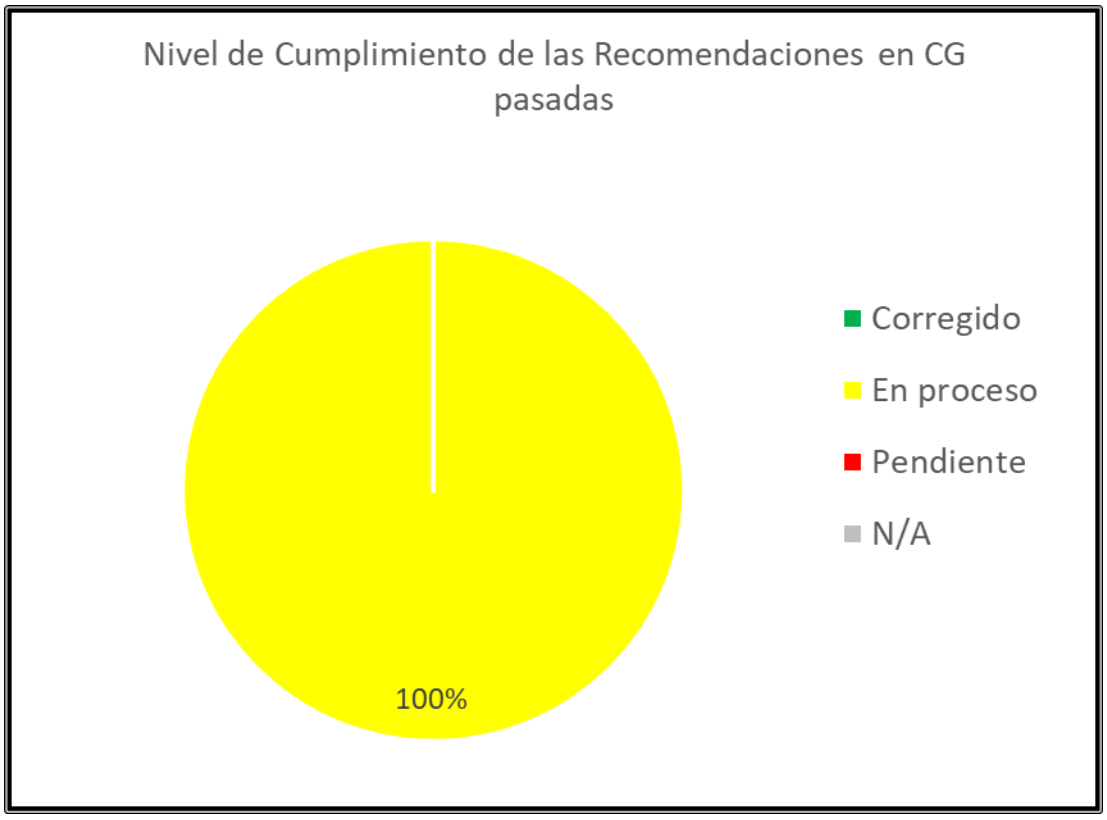
	1. Actualizar el plan de continuidad de TI considerando las actividades necesarias para garantizar la disponibilidad y continuidad de las tecnologías de información que soportan las operaciones del Fondo. 2. Presentar ante el órgano respectivo, el plan de continuidad de TI para su respectiva aprobación. 3. Realizar pruebas periódicas del plan de continuidad según lo establecido en el plan de pruebas. Se deben documentar los resultados y en caso de detectar áreas de mejora, se deben aplicar al plan oportunamente. 4. Capacitar al personal involucrado sobre el plan de continuidad, asegurando que los involucrados conozcan sus roles y responsabilidades en caso de requerir activar el plan.
COMENTARIOS DE LA ADMINISTRACIÓN	Evidencia aportada: BIA Institucional (Análisis de Impacto de Negocio), cronograma del proyecto de Continuidad de los Servicios, evidencia de las capacitaciones, y planes de contingencia de los sistemas del FJP y de Inversiones. El plan de Continuidad de los servicios institucionales se encuentra en proceso de construcción, al momento de esta evaluación, se cuenta con el BIA aprobado por los órganos superiores correspondientes. Debe recordarse que la DTIC le brinda servicios tecnológicos a todo el Poder Judicial y por convenio al FJP, por lo que los resultados, procesos, modelos e instrumentos que genere el proyecto que se está gestionando, aplican de igual forma al Fondo.
ESTADO	**EN PROCESO** Aún se encuentra en desarrollo el plan de continuidad de TI. De acuerdo con el cronograma suministrado, se tiene planificada la finalización en el periodo 2021.
CG 2016	
HALLAZGO 03: NO SE EFECTUARON EVALUACIONES SOBRE EL RENDIMIENTO DE LOS COLABORADORES DE TI EN EL PERIODO 2016.	
RECOMENDACIÓN	***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.
COMENTARIOS DE LA ADMINISTRACIÓN	Evidencia aportada: modelo de evaluación del desempeño por competencias (institucional), modelo de gestión humana por competencias (institucional), documentación del diseño del proceso APO07 Gestionar los Recursos Humanos, el cual contiene un apartado referente al tema de evaluación del desempeño (documento y lineamiento del proceso APO07), control de horas efectivas.

	Ahora bien, sobre esta evaluación, existe un plan institucional para que se vaya adoptando el modelo, aunque como puede observarse, ya se ha venido coordinando con Gestión Humana.
ESTADO	**EN PROCESO** Se identificó la existencia de los respectivos procedimientos, no obstante, aún el proyecto no ha finalizado. Según lo indicado por la DTIC, se acaba de concluir la etapa de diseño del proyecto.
CG 2014	
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	Evidencia aportada: documentación del proceso BAI04 Gestionar la disponibilidad y capacidad, y el plan para la gestión de la capacidad.
ESTADO	**EN PROCESO** Se cuenta con los respectivos lineamientos, no obstante, no se suministró evidencia de su aprobación ni de cumplimiento.

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

PERIODO	CORREGIDO	PROCESO	PENDIENTE	NO APLICA	TOTAL
2018	0	1	0	0	**1**
2017	0	1	0	0	**1**
2016	0	1	0	0	**1**
2014	0	1	0	0	**1**
TOTAL	**0**	**4**	**0**	**0**	**4**

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



V. APÉNDICE

APÉNDICE I: Análisis de Riesgos Tecnologías de Información 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.

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
A.14	Paredes de concreto		✓	Las paredes son de concreto.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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
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 2 extintores en el centro de datos, los cuales se encuentran recargados.		B
D.12	Uso de aspersores		✓	Se cuenta con aspersores.		B
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 y redundancia de enlaces.		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 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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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 antivirus y firewalls?		✓	Sí se cuenta con estos dispositivos o programas de software.		B
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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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
L.17	¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de estas?		✓	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 cuenta con una unidad de monitoreo la cual da seguimiento a los eventos que presentan la infraestructura de hardware y comunicaciones.		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.		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 estas?		✓	Para la parte de seguridad de los sistemas, la DTI se encarga de dar la capacitación al encargado del sistema.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
L.22	¿Se han establecido indicadores de gestión que permitan medir el desempeño de las herramientas como de los colaboradores del área?	✗		Se cuenta con un procedimiento para la evaluación de la capacidad y disponibilidad, sin embargo, no se evidenció su implementación.		B
L.23	¿Se han implementado planes de acción correctivos, para aquellos casos en que los indicadores presentan resultados inferiores a los esperados?	✗		El proceso aún no se ha aplicado.		B
L.24	¿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.25	¿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 estos, además, se cuenta con SLAs con proveedores.		B
L.26	¿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.27	¿Se ha establecido el plan de continuidad para los procesos de TI?	✗		Se cuenta con un plan de contingencia para el FPJ y su respectivo BIA. No obstante, aún no se ha desarrollado el plan de continuidad.		M
L.28	¿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 alfanumérica 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
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

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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
M.22	Bloqueo de usuarios retirados, previa comunicación de Gestión Humana.		✓	Sí se bloquea, según lo indique cada área.		B

Centro de Cómputo	Condición	Vulnerabilidad ✗ - ✓		Comentarios	Observaciones	Tipo de riesgo
		SÍ	NO			
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 contingencias 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 con el 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

--- Última línea ---