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

- ***Informe de Auditoría de Tecnologías de Información.***
- ***Carta de Gerencia CG 1-2015 T.I.***
- ***Informe Final.***

San José, 02 de Mayo del 2016

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 2015 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 1-2015 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

Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad N° R-1153
Vence el 30 de septiembre del 2016.

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

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 diecinueve 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. Seguridad física del cuarto de servidores.
2. Inventario de hardware.
3. Inventario de software.
4. Estudios de vulnerabilidad.
5. Plan de Continuidad.
6. Plan de pruebas del plan de continuidad y capacitaciones.
7. Integración de Sistemas.
8. Procedimiento de uso, desecho y reutilización de equipo electrónico.
9. Metodología de proyectos de Tecnologías de Información.
10. Estándares para el desarrollo de sistemas.
11. Metodología de administración de riesgo de TI.
12. Informes de Auditoría Interna.
13. Políticas para el manejo de incidentes y problemas.
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. Modelo de arquitectura de la información.
18. Evaluaciones del desempeño de los colaboradores de tecnologías de información.
19. Seguimiento a cartas a gerencia anteriores.

1.3 Metodología

Para llevar a cabo este trabajo utilizamos una modalidad de entrevistas personalizadas a los funcionarios relacionados con la manipulación de los sistemas de información SIGAFONDO, Inversiones y TECAPRO, así como también con funcionarios de la Dirección de Tecnologías de Información que le prestan servicios al ***Fondo de Jubilaciones y Pensiones del Poder Judicial,*** con el fin de verificar el cumplimiento de la normativa aplicable en materia de tecnologías de la información, la cual sometemos a consideración de ustedes en esta carta de gerencia CG-I-2015.

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"

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. Seguridad física del cuarto de servidores.

El cuarto de servidores posee adecuados controles de seguridad, se han solucionado debilidades como por ejemplo la recarga de los extintores. A pesar de lo anterior, aún no se ha solucionado el tema del orden del cableado del cuarto de servidores, ver Oportunidad de Mejora 01 de la Carta de Gerencia del 2014 en la matriz de seguimiento y el Anexo III del presente informe.

2. Inventario de hardware.

Actualmente se cuenta con un inventario de los servidores y de las PC´s del Poder Judicial, considerando los equipos del Fondo (FPJ).

3. Inventario de software.

La Dirección de Tecnología de Información cuenta con la herramienta System Center Configuration Manager, la cual genera un inventario detallando por cada equipo de la organización del software instalado. Además, se cuenta con un inventario general de licencias.

4. Estudios de vulnerabilidad.

En noviembre del periodo 2015 se finalizó un estudio de vulnerabilidad de la red del Poder Judicial, mediante la cual trabaja el Fondo. En este momento se están implementado las acciones correctivas para solventar las debilidades encontradas. El Área de Seguridad de la Dirección de Tecnología de Información está llevando a cabo la tarea de seguimiento del cumplimiento de dichas acciones. Ver Hallazgo 03 de la Carta a Gerencia del 2007 en la matriz de seguimiento.

5. 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.

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

En el periodo 2015 se hicieron pruebas del plan de continuidad. 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.

7. Integración de Sistemas.

En la actualidad se está trabajando en el desarrollo de un nuevo Sistema Contable, mediante el cual se estarían automatizando e integrando procesos de contabilidad. Además, este sistema contable estaría integrando con otros sistemas, dentro de ellos el SIGAFONDO e Inversiones. Ver Hallazgo 01 de la Carta a Gerencia del 2005 y Hallazgo 01 de la Carta a Gerencia del 2009 en la matriz de seguimiento.

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

En la actualidad se cuenta con procedimientos para el uso, desecho y reutilización de equipo electrónico; sin embargo, estos no se han oficializado y no se están cumpliendo. Ver Hallazgo 04 de la Carta a Gerencia del 2011 en la matriz de seguimiento.

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 nuevos Sistema Contable.

10. Estándares 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 2015.

12. Informes de Auditoría Interna.

En el periodo 2015, la Auditoría Interna emitió recomendaciones en cuanto a la necesidad de cambiar la lógica en el cálculo de las jubilaciones y pensiones. Para ello se han tomado acciones en la designación de personal de la Dirección de Tecnología de Información y del Departamento de Gestión Humana. Según lo indicado por los usuarios, en este momento se está trabajando en los ajustes respectivos al Sistema SIGAFONDO para implementar las observaciones realizadas por la Auditoría Interna.

13. Políticas para el manejo de incidentes y problemas.

Se cuenta con un procedimiento para la gestión de incidentes. Además, se cuenta con una herramienta para la atención de los incidentes de tecnologías de información.

14. Plan de capacidad y desempeño.

Aún no se cuenta con un plan de la capacidad y desempeño. 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. A pesar de lo anterior, 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, se estarán integrando el resto de sistema 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 algunas debilidades en cuanto al cálculo de jubilaciones y la integración con el sistema SIGAGH respecto al proceso de aportes. Ver Hallazgos 03 y 04 del presente informe.
- Sistema de Inversiones: No se detectaron deficiencias en el sistema de Inversiones.

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; sin embargo, se nos indicó que el tema de clasificación de la información no le corresponde a dicha unidad. Dado lo anterior, al Asunto 01 de la Carta a Gerencia del periodo 2013 de la matriz de seguimiento, se le asigna como estado No Aplica con el fin de separar el tema de clasificación de la información del de seguridad móvil y definiendo nuevos hallazgos para este periodo. Ver Hallazgos 01 y 02 del presente informe.

17. Modelo de arquitectura de la información.

Se determinó que la Dirección de Tecnología de Información cuenta con un modelo de arquitectura de la información, en donde se documentan los datos organizacionales, los sistemas y procesos del Poder Judicial, contemplando así al Fondo. Además, se hace un mapeo entre datos, sistemas y procesos.

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

Actualmente se está llevando a cabo un proyecto para el desarrollo de una herramienta que permita evaluar el rendimiento de los funcionarios de tecnologías de información. Ver Hallazgo 01 de la Carta a Gerencia del periodo 2008 en la matriz de seguimiento.

19. Seguimiento a cartas a gerencia anteriores.

Se determinó que se cuenta con 3 recomendaciones corregidas, 10 en proceso, 2 pendientes y 1 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: AUSENCIA DE LINEAMIENTOS PARA LA CLASIFICACIÓN DE LA INFORMACIÓN EN EL FONDO DEL PODER JUDICIAL. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el Fondo del Poder Judicial no cuenta con lineamientos para clasificar la información de acuerdo a su criticidad. Se hizo solicitud de estos lineamientos al Departamento de Tecnología de Información y no se nos suministró, además se nos indicó que la definición de estos lineamientos no deben ser responsabilidad del área.

En este momento la Dirección de Tecnología de Información ha formulado un proyecto para la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) en el Poder Judicial, cubriendo así al Fondo, tomando como base la familia de estándares del ISO/IEC 27000. El estándar ISO/IEC 27002, parte de la familia ISO/IEC 27000, en su versión 2013 la cual se va a utilizar para establecer el SGSI, posee un objetivo de control referente a clasificación de la información, el cual contempla los siguientes dos controles:

- Directrices de clasificación.
- Etiquetado y manipulado de la información.
- Manipulación de activos.

Dado lo anterior, dentro del mismo proyecto de implementación del Sistema de Gestión de Seguridad de la Información, podría implementarse políticas, procedimientos y lineamientos para la clasificación, etiquetado y manipulación de la información.

Al no contar con lineamientos de cómo debe clasificarse la información y cómo debe manipularse según su criticidad, existe el riesgo de que datos confidenciales queden expuestos a personas no autorizadas.

CRITERIO:

El apartado 1.4, "Gestión de la seguridad de la información" 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 una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.".

RECOMENDACIONES:

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.

HALLAZGO 02:AUSENCIA DE POLÍTICAS Y LINEAMIENTOS PARA LA SEGURIDAD MÓVIL EN EL FONDO DEL PODER JUDICIAL. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el Fondo del Poder Judicial no cuenta con políticas para garantizar la seguridad en dispositivos móviles. Se hizo solicitud de estos lineamientos a la Dirección de Tecnologías de Información y se nos indicó que aún no existen, pero que para su elaboración se ha establecido un proyecto mediante el cual se implementará un Sistema de Gestión de Seguridad de la Información, contemplando así políticas para seguridad móvil.

Al no contar con lineamientos para regular el uso de dispositivos móviles y gestionar su seguridad, existe el riesgo de que los funcionarios del Fondo del Poder judicial expongan información de la organización a través de sus dispositivos.

CRITERIO:

El apartado 1.4, "Gestión de la seguridad de la información" 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 una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios.

Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad".

RECOMENDACIONES:

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

Con relación a Seguridad Móvil, mediante el Proyecto Nº 2015LA-000020-PROV de SGSI (Sistema de Gestión de Seguridad de la Información) se estarán implementando una serie de políticas, entre ellas una para uso de dispositivos móviles. Actualmente el proyecto se encuentra en la etapa de ejecución.

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. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el Sistema del Fondo de Jubilaciones y Pensiones del Fondo del Poder Judicial, posee un módulo denominado Aportes, mediante el cual se registra los aportes y el tiempo servido de los trabajadores asociados.

Durante la revisión del módulo, se verificó que, para la carga de los aportes y el tiempo servido de los trabajadores, el Departamento de Gestión Humana genera un reporte en MS Excel desde el sistema SIGAGH, y lo envían por correo electrónico al área del Subproceso de Ingresos y Cuentas por Cobrar del Fondo del Poder Judicial, en donde una persona encargada recibe el archivo, lo revisa, le da formato y luego lo convierte a un archivo .txt. Posterior al proceso anterior, se sube el archivo .txt al módulo de Aportes.

Al no estar integrado el SIGAGH y SIGAFONDO para la carga de la información de los aportes y tiempo servido, existe el riesgo de existan errores a la hora de manipular el archivo en MS Excel antes de cargarlo al sistema, o bien que se manipule la información que en él se almacena. Además, existe el riesgo de que la información de los aportes y tiempo servido de los trabajadores pueda ser expuesta y/o vulnerada ya que se está enviando por correo sin controles de cifrado o encriptación.

CRITERIO:

El apartado 1.4.4, "Seguridad en las operaciones y comunicaciones" 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 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."

RECOMENDACIONES:

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

La generación de Aportes de Empleados se encuentra automatizada, el único manejo que da el usuario es que en el Sistema del Fondo de Jubilaciones y Pensiones se realiza carga del archivo con los resultados de la generación del aporte obrero de empleados, este archivo es generado de manera automática por el Sistema de Gestión Humana. Los aportes de empleados y jubilados se llevan de forma automática en el Módulo de Aportes, en el cual se tienen los aportes unificados de empleados y jubilados para reportarlos a la SUPEN de forma mensual.

Además, existe una funcionalidad en el Sistema del Fondo de Jubilaciones que concilia los resultados de los Aportes contra el salario del empleado registrado en el Sistema de Gestión Humana.

Ver Anexo **"Módulo de Aportes"**.

HALLAZGO 04: DEBILIDADES EN LA AUTOMATIZACIÓN DEL CÁLCULO DE TIEMPO SERVIDO DE LOS COLABORADORES ASOCIADOS AL FONDO DEL PODER JUDICIAL. RIESGO MEDIO.

CONDICIÓN:

Se determinó que el sistema SIGAFONDO del Fondo del Poder Judicial, posee un módulo de cálculo de jubilaciones mediante el cual se calcula el monto a recibir por concepto de jubilación a un funcionario asociado al Fondo.

Para realizar el cálculo del monto de jubilación es requerido que se calcule el tiempo servido de un colaborador. Para calcular el tiempo servido se consideran los años que ha trabajado un colaborador; sin embargo, deben hacerse rebajos o ajustes a dicho tiempo considerando aspectos como por ejemplo permisos sin goce de salario que haya tenido un determinado funcionario.

El cálculo del tiempo servido se realiza en el módulo de Cálculo de Jubilaciones del SIGAFONDO; sin embargo, la información del tiempo servido previo al periodo 2004, se gestiona en el sistema SIP (sistema anterior al SIGAFONDO), por lo cual, cuando un funcionario con historial anterior al periodo 2004 decide jubilarse, entonces se debe extraer la información desde el SIP hasta el SIGAFONDO de manera automática y se integra con el tiempo servido posterior al 2004.

A pesar de la integración, el SIP no calcula correctamente el tiempo servido de acuerdo con las reglas del Fondo del Poder Judicial y llega información errónea al sistema SIGAFONDO. Por ejemplo, los permisos sin goce de salario deben restarse del total del tiempo servido y el SIP no hace esa resta. Cabe mencionar el que el Sistema SIGAFONDO sí se ajusta a las reglas actuales para el cálculo de tiempo servido. Dado lo anterior, las encargadas de la Unidad de Jubilaciones y Pensiones deben hacer una verificación manual del expediente del funcionario que requiera jubilarse, el cual se encuentra en digital, con el fin de verificar si la información del tiempo servido que brindó el SIP es correcta, en caso de que no sea así, efectúan los ajustes en el sistema SIGAFONDO para registrar el debido tiempo servido.

Al existir esta debilidad en el sistema SIP, cabe la posibilidad de que se incurra en un error a la hora de calcular el tiempo servido y por ende el cálculo de la jubilación, impactando así económicamente al Fondo del Poder Judicial o bien a sus beneficiarios. También al requerirse la verificación manual del expediente digital de los candidatos a jubilarse se pierde agilidad en el proceso de jubilación.

CRITERIO:

El apartado 3.2, “Implementación de software” 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 implementar el software

que satisfaga los requerimientos de sus usuarios y soporte efectivamente sus procesos, para lo cual debe:

a. Observar lo que resulte aplicable de la norma 3.1anterior.
b. Desarrollar y aplicar un marco metodológico que guíe los procesos de implementación y considere la definición de requerimientos, los estudios de factibilidad, la elaboración de diseños, la programación y pruebas, el desarrollo de la documentación, la conversión de datos y la puesta en producción, así como también la evaluación postimplantación de la satisfacción de los requerimientos.
c. Establecer los controles y asignar las funciones, responsabilidades y permisos de acceso al personal a cargo de las labores de implementación y mantenimiento de software.
d. Controlar la implementación del software en el ambiente de producción y garantizar la integridad de datos y programas en los procesos de conversión y migración.
e. Definir los criterios para determinar la procedencia de cambios y accesos de emergencia al software y datos, y los procedimientos de autorización, registro, supervisión y evaluación técnica, operativa y administrativa de los resultados de esos cambios y accesos.
f. Controlar las distintas versiones de los programas que se generen como parte de su mantenimiento."

RECOMENDACIONES:

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

Sobre este tema se debe aclarar que el Sistema Integrado de Personal SIP es un sistema obsoleto que dejó de funcionar desde el año 2004, por lo que la información de R.T.S no es una fuente de información automatizada y que además la Dirección de Gestión Humana mantiene esta información en expedientes, por lo que el SIP no es una solución, lo que se ha realizado son las migraciones según demanda acorde con las solicitudes y cálculos de jubilación que se deben aplicar. La Dirección de Tecnología desarrolló todas las aplicaciones que permiten a los usuarios de G.H. el ingreso de Reconocimientos de Tiempo Servido calculados fuera del Sistema, por lo que esta recomendación no aplica para la parte Técnica.

HALLAZGO 05: EL PROCEDIMIENTO DE RESPALDOS NO SE ENCUENTRA APROBADO. RIESGO BAJO.

CONDICIÓN:

Se determinó que la Dirección de Tecnología de Información posee un procedimiento documentado para la elaboración de respaldos; sin embargo, se nos indicó que éste fue remitido al Departamento de Planificación y aún no se ha aprobado. Además, se hizo solicitud de evidencia de los respaldos efectuados en el periodo 2015, para lo cual se nos suministró la bitácora de pruebas realizadas a los respaldos en el año 2015, haciendo constar que se están efectuando los respaldos, pero no se puede constatar la periodicidad en que se realizan o bien si se están realizando de manera estándar.

Al no contar con el procedimiento aprobado para realizar respaldos, existe el riesgo de que estos no se estén ejecutando en la periodicidad adecuada ni que se esté realizando el debido control al proceso de ejecución de respaldos.

CRITERIO:

El apartado 4.3, "Administración de los datos" 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 asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura".

RECOMENDACIONES:

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.

IV. MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

HALLAZGO	RECOMENDACIÓN	COMENTARIO DE ADMINISTRACIÓN	ESTADO
CG 2014			
HALLAZGO 01: AUSENCIA DE UN PROCEDIMIENTO PARA LA MIGRACIÓN DE DATOS EN EL FPJ. RIESGO MEDIO.	Desarrollar y aprobar formalmente un procedimiento para la administración y control de las migraciones de datos, el procedimiento debe de guiar, controlar y estandarizar los planes de migración de datos para cada proyecto que lo amerite.	El sistema del Fondo de Jubilaciones y Pensiones y el Sistema Contable utilizan la misma estructura para la definición del Plan de Migración. En el Sistema Contable aún se encuentra en proceso de definición de datos. Ver Anexo "**Planes de Migración**".	**CORREGIDO** Para los sistemas en desarrollo se establecen los planes de migración respectivos.
OPORTUNIDAD DE MEJORA 01: DEBILIDADES EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES Y UPS. RIESGO BAJO.	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.	Se revisa el centro de cómputo y se reordenan los cables eléctricos. Se revisan los extintores que se ubican en el centro de datos, se verifica que estén recargados y la próxima recarga será en octubre 2016 y 2019.	**PROCESO** Los extintores se encuentran recargados. El cableado del cuarto de servidores estaba siendo cambiado durante la visita de auditoría y aún se encuentra desordenado. Ver Anexo 3.

OPORTUNIDAD DE MEJORA 02: AUSENCIA DE UN PROCEDIMIENTO DE PLANEACIÓN PARA LA REVISIÓN DEL DESEMPEÑO Y CAPACIDAD DE LOS RECURSOS DE TI. RIESGO MEDIO.	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.	Para acatar estas recomendaciones se trabaja apegado al marco de trabajo definido en el PETIC, mediante el cual define los procesos y marco de trabajo mediante el plan 2015-2020. Se está en la definición, documentación de procesos.	**PENDIENTE** Aún no se ha implementado. Según lo indicado, cuando se implemente la herramienta Operation Manager de System Center se va a poder generar el respectivo plan de la capacidad y desempeño.

CG 2013			
HALLAZGO 01: NO SE CUENTA CON UN SITIO ALTERNO DE OPERACIONES. **RIESGO ALTO**	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 n - Planeamiento operativo y estratégico - Estructuración de un plan de migración a sitio alterno en caso de emergencia	Actualmente esta Dirección está ejecutando el proyecto Centro Alterno mediante convenio con el ICE, el cual cuenta con un Data Center Tier III definido por el Uptime Institute. El proyecto tiene un alcance de 8 servicios críticos en una primera fase, para luego continuar llevando más servicios en las siguientes etapas. Se está trabajando en el diseñó de recuperación en sitio alterno. Ver Anexo "**Centro Alterno de Datos**"	**PROCESO** Se está en proceso de ejecución de un proyecto para la implementación de un sitio alterno.

OTROS ASUNTOS			
ASUNTO 01: MEJORA DE PROCESOS DE CLASIFICACIÓN DE DATOS Y SEGURIDAD MÓVIL	***Se recomienda*** el establecimiento de políticas y procedimientos que le deleguen la responsabilidad al usuario creador de los datos o información electrónica o física, en cuanto al establecimiento de la criticidad o confidencialidad de los datos, esto para que el departamento de TI pueda realizar un trabajo más efectivo en término de seguridad para la custodia de los datos. Además se recomienda, la generación de una normativa interna, en cuanto al uso de los dispositivos móviles y realizar una valoración en cuanto a la usabilidad de estos dispositivos y la posibilidad de prohibir o mejorar la gestión de estos por parte del departamento de TI.	Como se indicó en el 2015 La clasificación de Datos no le corresponde a TI. Se solicita su reasignación. Con relación a Seguridad Móvil, mediante el Proyecto Nº 2015LA-000020-PROV de SGSI (Sistema de Gestión de Seguridad de la Información) se estarán implementando una serie de políticas, entre ellas una para uso de dispositivos móviles. Actualmente el proyecto se encuentra en la etapa de ejecución. Ver anexo **"Acta de Constitución del Proyecto(SGSI)"** **NOTA ACLARATORIA** Agregada en fecha 06/05/2016: Los adjuntos que se mencionan fueron	**NO APLICA** Se actualiza con los Hallazgos 01 y 02 del presente informe.

		aportados en el primer aporte que se realizó.	
CARTA 1-2012			
OTROS ASUNTOS A INFORMAR			
ASUNTO 01: NO SE CUENTA CON INVENTARIO DE SOFTWARE POR EQUIPO	***Se recomienda*** implementar la confección del inventario de licencias por equipo, utilizadas en el Fondo; manteniendo el mismo actualizado, ejerciendo un control adecuado que evite que se incida en una acción que vaya en contra de las leyes o contratos establecidos.	Actualmente la herramienta System Center Configuration Manager se encuentra implementada al 100% en todo el país, la cual permite realizar inventarios de software y hadrware de toda la plataforma tecnológica que soporta los servicios institucionales.	**CORREGIDO** Ya se cuenta con el inventario de licencias instaladas por equipo.

CARTA 1-2011			
HALLAZGO 2: LAS CUENTAS POR COBRAR DEL FONDO DEL PODER JUDICIAL NO SE LLEVAN EN UN SOLO SISTEMA INFORMÁTICO.	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.	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 febrero de 2016 se iniciaron las pruebas del Módulo de Cuentas por cobrar II Etapa, ambos módulos unifican las cuentas por cobrar que se llevan en el Poder Judicial. Se estima que la contratación concluirá en el mes de mayo de 2017. Ver Anexo "**Cronograma del Contrato Sist Contable**" Estado de la Recomendación: En Proceso.	**PROCESO** Se está en proceso de la implementación del nuevo Sistema Contable del Poder Judicial mediante el cual se implementaría la recomendación.

CARTA 1-2011			
HALLAZGO 4: NO SE CUMPLE CON LO MENCIONADO EN LA POLÍTICA PARA EL USO, DESECHO Y REUTILIZACIÓN DE MEDIOS ELECTRÓNICOS O IMPRESOS	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.	Se adjuntan los procedimientos: "Procedimiento para solicitud, entrega y uso de dispositivos de almacenamiento" junto con la guía correspondiente, "Procedimiento para reciclaje-destrucción de dispositivos de almacenamiento", "Procedimiento para devolución de dispositivos de almacenamiento". Ver Anexo "**Procedimientos para uso desecho y reutilización de medios electrónicos**". (**NOTA ACLARATORIA** Agregada en fecha 06/05/2016: Los adjuntos que se mencionan fueron aportados en el primer aporte que se realizó.)	**PENDIENTE** Los procedimientos suministrados aún no se encuentran aprobados y no hay evidencia de su cumplimiento.

CARTA 2009			
INTEGRACIÓN DE LOS DIFERENTES MÓDULOS.	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.	El Sistema Contable considera la Integración con el Sistemas de Inversiones y el Sistema del Fondo de Jubilaciones y Pensiones. Durante el 2015 se recibió a satisfacción los módulos de Libro de Bancos, Contabilidad General I Etapa, Cuentas por Cobrar I Etapa y Contabilidad General II Etapa al 31 de diciembre del 2015 se cerró con un avance de 58.97% del total de la contratación. Ver Anexo "**Informe de labores Diciembre Sist Contable**" Estado de la Recomendación: En Proceso.	**PROCESO** Está en proceso la implementación del nuevo sistema contable mediante el cual se llevaría a cabo la respectiva integración de los sistemas y módulos del Fondo del Poder judicial.

CARTA 2008			
HALLAZGO 1: NO SE REALIZAN EVALUACIONES SOBRE EL DESEMPEÑO DE LOS INTEGRANTES DEL ÁREA DE TI.		La empresa SearchJob entregó la segunda etapa del proceso de definición de indicadores. Se adjunta informe a modo de borrador ya que se están discutiendo algunos aspectos a mejorar. En este informe se observa la definición de roles y los indicadores propuestos para la valoración de carga de trabajo y rendimiento según cada rol. Ver Anexo: " **Borrador Evaluación del Rendimiento de Funcionarios DTI**".	**PROCESO** Se está llevando a cabo un proyecto para el desarrollo de un instrumento para la evaluación del rendimiento de los colaboradores de TI.

CARTA 2007			
HALLAZGO 3: NO SE HA IMPLEMENTADO UN ESTUDIO SOBRE LAS VULNERABILIDADES QUE PODRÍA TENER LA RED (ESTUDIO DE PENETRACIÓN).		En 2015 se finalizó con el proyecto del Pentest; con base en los resultados se tomaron acciones correctivas, y actualmente se da seguimiento en la resolución de hallazgos en conjunto con las demás áreas de la Dirección. Ver Anexo **"Informe de Cierre del Proyecto"**. **(<u>NOTA ACLARATORIA</u>** Agregada en fecha 06/05/2016: Los adjuntos que se mencionan anteriormente fueron aportados en el primer aporte que se realizó.) Adicionalmente se hacen análisis de vulnerabilidades a la infraestructura tecnológica con la herramienta que se adquirió en la	**PROCESO** Se llevó a cabo un estudio de pentest, el cual se finalizó. En este momento se están implementando las acciones correctivas para solventar las debilidades detectadas en el estudio.

		CONTRATACIÓN DIRECTA No. 2015CD-000531-PROVCD. Ver Anexo "**Contrato 2015CD-000531-PROVCD**". **(NOTA ACLARATORIA** Agregada en fecha 06/05/2016: Los adjuntos que se mencionan anteriormente fueron aportados en el primer aporte que se realizó.)	

CARTA *CG2-2006*			
HALLAZGO 3: EL SISTEMA DE CONTABILIDAD NO SE DESACTIVA O PARALIZA AUTOMÁTICAMENTE DESPUÉS DE HABER ESTADO CIERTO TIEMPO SIN SER UTILIZADO.		Durante el 2015 se recibieron a satisfacción los módulos de Libro de Bancos, Contabilidad General I Etapa, Cuentas por Cobrar I Etapa y Contabilidad General II Etapa. Según el cronograma del contrato, se estima que en el mes de mayo del 2017 se reciba a satisfacción el Desarrollo del Sistema Contable. Para lo cual se suministra evidencia del recibo a satisfacción de los módulos señalados Ver Anexo "**Módulos recibidos a satisfacción**". Estado de la Recomendación: En Proceso	**PROCESO** El control se implementaría en conjunto con el nuevo sistema contable.
HALLAZGO 4: EL SISTEMA DE CONTABILIDAD NO CUENTA CON UNA BITÁCORA ADECUADA, Y EL		En el Sistema del Fondo de Jubilaciones y Pensiones la recomendación fue atendida desde el año 2010. En cuanto al	**PROCESO** El sistema SIGAFONDO cuenta con las respectivas

SISTEMA DE PLANILLAS CARECE DE ESTA OPCIÓN DE SEGURIDAD.		Sistema Contable se encuentra en proceso de desarrollo por parte de la Empresa Babel, en el módulo de Seguridad del Sistema se encuentra implementada dicha recomendación, este módulo está desarrollado y en producción sin embargo depende de la puesta en marcha de los módulos del sistema contable para iniciar su utilización en el ambiente de producción.	bitácoras. El sistema contable actual no contempla bitácoras; sin embargo, el nuevo sistema estaría contemplando el control.

CARTA *CG 2-2005*			
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		Durante el 2015 se recibieron a satisfacción los módulos de Libro de Bancos, Contabilidad General I Etapa, Cuentas por Cobrar I Etapa y Contabilidad General II Etapa. Según el cronograma del contrato, se estima que en el mes de mayo del 2017 se reciba a satisfacción el Desarrollo del Sistema Contable. Para lo cual se suministra evidencia del recibo a satisfacción de los módulos señalados Ver Anexo **"Módulos recibidos a satisfacción**". Estado de la Recomendación: En Proceso.	**PROCESO** Mediante la implementación del nuevo Sistema Contable se estará llevando la integración con los otros sistemas del Fondo.

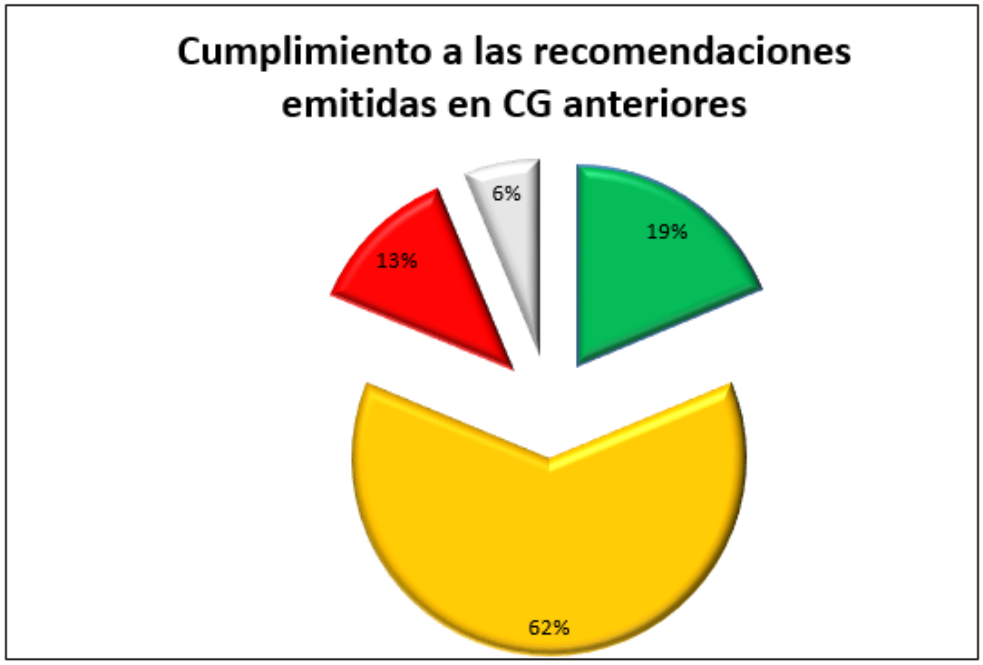
CARTA CG-1-2003			
HALLAZGO 6: EXISTE DEPENDENCIA DE LA EMPRESA TECAPRO, LO CUAL PODRÍA AFECTAR LA CONTINUIDAD DE LAS OPERACIONES		El nuevo Sistema de Contabilidad solventará esta situación, debido a que la contratación del sistema corresponde a un desarrollo a la medida, según las necesidades del Poder Judicial, para lo cual la Dirección de Tecnología se encargará del mantenimiento del sistema una vez que finalice el periodo de garantía que debe brindar la empresa. **Estado de la Recomendación: En Proceso**	**PROCESO** Con la implementación del nuevo sistema se eliminará la dependencia de TECAPRO. El nuevo sistema estará por un periodo de garantía en mantenimiento de la empresa BABEL, una vez finalizado el periodo, la Dirección de Tecnología de Información asumiría la tarea.

CARTA CG 1-2002			
El Departamento de informática del Poder Judicial no cuenta con una bitácora de acceso a la Red, en donde se despliegue información tal como nombre de usuario, fecha y hora de ingreso.		Se implementó la herramienta ADAudit la cual permite obtener bitácoras de acceso de los usuarios al dominio Poder-Judicial, fecha, hora de ingreso y nombre del equipo. La herramienta almacena un histórico de los últimos tres meses.	**CORREGIDO** Ya se cuenta con la bitácora de acceso a la red.

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

PERIODO	CORREGIDO	PROCESO	PENDIENTE	NO APLICA	TOTAL POR PERIODO
2014	1	1	1	0	**3**
2013	0	1	0	1	**2**
2012	1	0	0	0	**1**
2011	0	1	1	0	**2**
2009	0	1	0	0	**1**
2008	0	1	0	0	**1**
2007	0	1	0	0	**1**
2006	0	2	0	0	**2**
2005	0	1	0	0	**1**
2003	0	1	0	0	**1**
2002	1	0	0	0	**1**
TOTAL POR ESTADO	**3**	**10**	**2**	**1**	**16**

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



Recomendaciones	Corregidas	Proceso	Pendiente	N/A
16	3	10	2	1

V. ANEXOS

ANEXO I

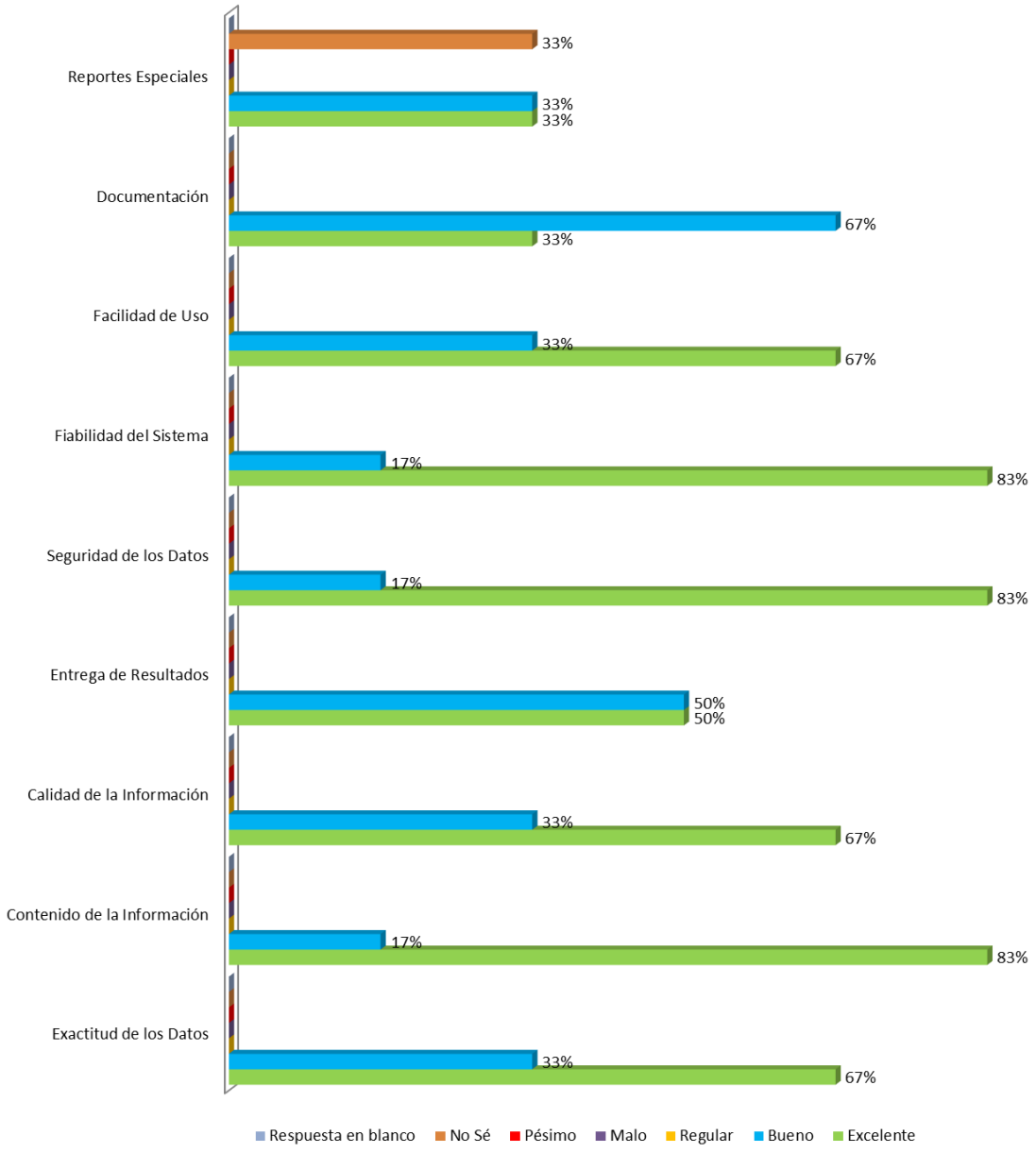
EVALUACIÓN FUNCIONAL A LOS SISTEMAS DE INFORMACIÓN IMPLANTADOS EN EL FONDO DEL PODER JUDICIAL

En este apartado se muestra el resultado de la evaluación realizada respecto a la calidad funcional de los sistemas de información implantados en el Fondo del Poder Judicial según la percepción de los usuarios finales.

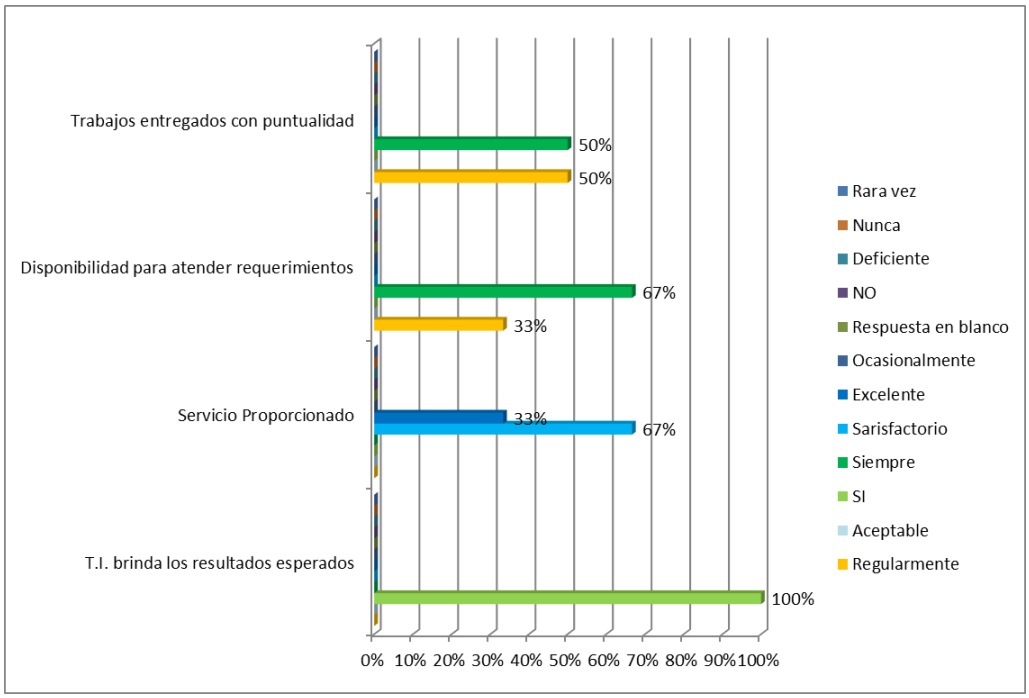
Los módulos evaluados y las personas entrevistadas en el proceso de evaluación de la calidad funcional se muestran en la tabla siguiente:

Sistema	***Módulo***	***Usuario***
Sistema Fondo de Jubilaciones y Pensiones del Poder Judicial	Aportes	Yorleny López Guevara.
	Deducciones	Esmeralda Hidalgo Ruíz Katherine Zamora Murillo
	Cálculo de jubilaciones	Priscilla Romero Calderón
	Cálculo de pensiones	Jennifer Carrillo Cárdenas
Inversiones	Inversiones	Suhey Sánchez Segura

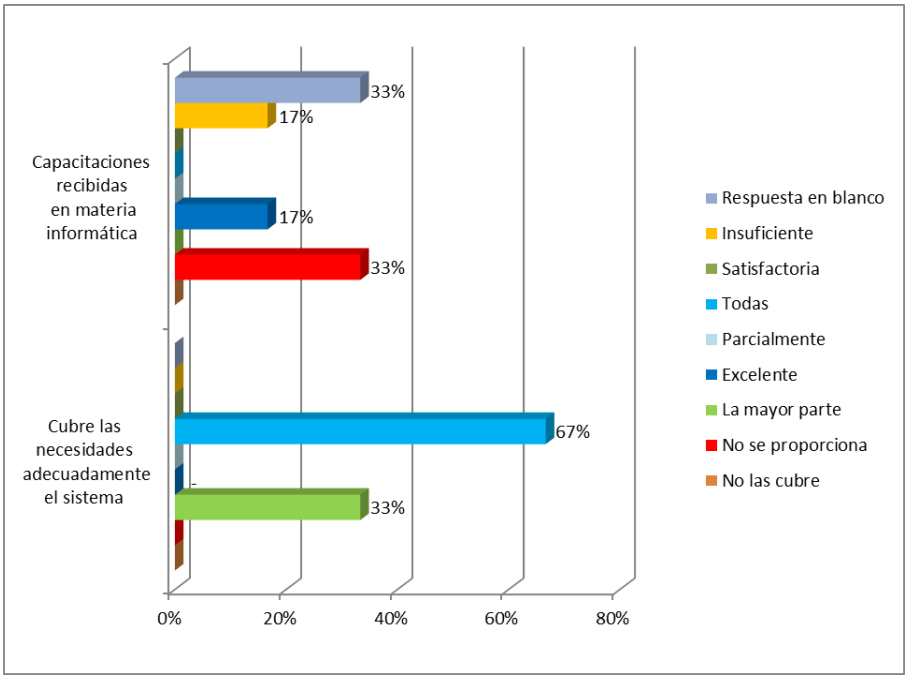
El detalle de la evaluación de la calidad funcional según usuarios al sistema que se encuentra actualmente en producción, se muestran en el gráfico siguiente:



Percepción de los usuarios finales respecto al servicio brindado por parte de la Dirección de Tecnología de Información.



Percepción de los usuarios finales respecto a si los sistemas de información del FPJ cubren satisfactoriamente las necesidades actuales de la Institución:



Mejoras indicadas por los usuarios de los sistemas de información

Aportes

- Mejorar la capacidad de los servidores en los que se encuentran instalados los sistemas

Deducciones

- El sistema se mantiene estable, no se requieren mejoras.

Cálculo de Jubilaciones y Pensiones

- Implementación de un sistema/módulo de reajustes de jubilaciones y pensiones.

ANEXO II

Análisis de Riesgos T.I.
Dirección de Tecnología de Información
Periodo 2015

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.

Centro computo		Condición	Vulnerabilidad		Comentarios	Observaciones	Tipo Riesgo
			Sí	No			
		Seguridad Física	SI	NO			
☐	☐	Proceso de autorización de ingreso	☐	√	Sí se posee la bitácora.		B
☐	☐	Personal interno y externo debidamente identificado (gafete)	☐	√	Sí se utiliza identificación.		B
☐	☐	Revisión de equipos de ingreso y salida	☐	√	Se lleva un control al ingreso al edificio.		B
☐	☐	Bitácoras de acceso al edificio y centro de cómputo	☐	√	Sí se manejan al centro de datos.		B
☐	☐	Acceso restringido a personal de informática definido	☐	√	Sí está restringido.		B
☐	☐	Una sola vía de acceso	☐	√	Hay una única vía de acceso en el cuarto de servidores.		B
☐	☐	Externos son acompañados por internos	☐	√	Sí lo realizan de esta forma.		B
☐	☐	Puerta de acceso segura	☐	√	Sí es segura.		B
☐	☐	Acceso con tarjeta electrónica al centro de datos	☐	√	En el cuarto de servidores se ingresa con tarjeta.		B
☐	☐	Alarmas de detección de intrusos	☐	√	Sí se maneja.		B
☐	☐	Monitoreo de la entrada por cámara de seguridad	☐	√	Sí hay cámaras en la entrada al cuarto de servidores.		B
☐	☐	Ubicación en un sitio seguro (lugares colindantes)	☐	√	Se encuentra en un quinto piso y hay ventanas.		B
☐	☐	Lugar completamente cerrado	√	☐	Hay ventanas en el cuarto de servidores.		B

		Paredes de concreto	√		Hay una pared de gypson.		B
		Cielo raso sellado		√	Está sellado.		B
		Equipos ubicados en rack		√	Los equipos están acomodados en racks.		B
		Los rack están asegurados		√	Sí están asegurados.		B
		Cableado de datos independiente del eléctrico		√	Sí es independiente.		B
		Cableado entubado y canaleteado		√	Sí está entubado.		B
		Cableado debidamente rotulado	√		Se está cambiando algún cableado por lo cual está desordenado y sin rotular.		B
		Hay un sitio alterno	√		No hay un sitio alterno.		A
		Instalación eléctrica					
		Hay pararrayos		√	Sí hay pararrayos.		B
		Circuito eléctrico independiente		√	Es independiente.		B
		Interruptor de emergencia en la sala de cómputo (palanca)		√	Sí cuenta con interruptor.		B
		Cableado eléctrico debidamente entubado o cubierta contra incendios		√	Sí se encuentra entubado.		B
		Conexión de los equipos a UPS		√	Si hay UPS.		B
		UPS ubicada en un sitio seguro		√	Sí se encuentra en un sitio seguro.		B
		Pruebas periódicas de la UPS (bitácora)		√	Se realizan durante la revisión de mantenimiento.		B
		UPS en contrato de mantenimiento preventivo y correctivo		√	Sí se maneja.		B
		Conexión a Planta eléctrica		√	Sí cuentan con una planta eléctrica.		B
		Planta eléctrica ubicada en un sitio seguro		√	Sí está en un sitio seguro.		B
		Pruebas periódicas de la planta eléctrica		√	Aún no se ha realizado pues entró en operación recientemente.		B

		Planta eléctrica en contrato de mantenimiento preventivo y correctivo		√	Posee mantenimiento preventivo-correctivo periódicamente.		B
		Luces de emergencia en el centro de cómputo o cercanías		√	Se cuenta con ellas.		B
		Pruebas periódicas de sistema de iluminación de emergencias		√	Sí se realizan.		B
		Instalación aire acondicionado					
		Equipo de aire acondicionado independiente para el centro de datos		√	Sí es independiente.		B
		Equipo de respaldo para el aire acondicionado		√	Se cuenta con aire acondicionado redundante.		B
		Contrato de mantenimiento preventivo y correctivo		√	Sí se posee.		B
		Control y monitoreo de humedad y temperatura		√	Sí se controla.		B
		Desastres Naturales					
		Brigada de emergencias		√	Sí hay una brigada.		B
		Capacitación del personal		√	Sí se han realizado.		B
		Rutas de evacuación y salidas de emergencia		√	Sí existen.		B
		Señalización		√	Sí está señalizado.		B
		Simulaciones periódicas		√	Se realizan cada 3 meses.		B
		Fácil acceso por Unidades de Bomberos	√		No es de fácil acceso por encontrarse en el piso 5.		B
		Sistemas de detección de humo/calor/fuego		√	Sí cuentan con sistema de detección de humo y extinción.		B
		Sistemas automáticos y manuales de alarma		√	Sí existen.		B

		Extinguidores cercanos portátiles (revisados al día)		√	Si hay extintores y revisados al día.		B
		Uso de aspersores	√		No se poseen; sin embargo se cuentan con 4 extintores dentro del cuarto de servidores.		B
		Pisos falsos		√	No se posee.		B
		Desnivel en el piso		√	No cuenta con desnivel.		B
		Fallas en Hardware					
		Redundancia de servidores críticos		√	Sí se maneja de manera virtual.		B
		Mantenimiento preventivo		√	Se da a nivel interno.		B
		Mantenimiento correctivo		√	Se da a nivel interno, y en ocasiones a nivel externo.		B
		Fallas en Software					
		Política de uso de recursos (prioridades en procesos)		√	Sí se maneja.		B
		Control de cambios		√	Se maneja control de cambios en software.		B
		Fallas en Comunicaciones					
		Redundancia de equipos y enlaces		√	Si existe.		B
		Mantenimiento preventivo		√	Sí se realiza.		B
		Mantenimiento correctivo		√	Sí se realiza.		B

		Respaldos y recuperación					
		Política de respaldos		√	Sí se posee.		B
		Procedimientos para respaldo y recuperación	√		No están aprobados los procedimientos de respaldos.		M
		Almacenamiento de información		√	Almacenados en el equipo de respaldos y en un sitio externo en una caja fuerte.		B
		Traslado de respaldos		√	Sí se maneja.		B
		Configuración de programas para respaldo		√	Sí se utilizan programas para respaldos.		B
		Ataques por virus					
		Política de antivirus		√	Sí se posee.		B
		Programa antivirus		√	Utilizan McAfee.		B
		Actualización del antivirus		√	Se actualiza automáticamente.		B
		Administración de incidentes y problemas		√	Sí se maneja.		B

		Intrusión					
		Política de acceso lógico		√	Manejan VPN para ciertas personas.		B
		Control de acceso a aplicaciones		√	Sí se maneja.		B
		Monitoreo de usuarios y accesos		√	Sí se realiza.		B
		Administración de Operaciones					
		Capacitación personal técnico		√	Sí se realizan.		B
		Segregación de funciones		√	Sí está segregado.		B

		Riesgos de la gestión de TI					
		¿Se tienen definido un plan estratégico para IT alineado con el de la organización?		√	Sí se posee.		B
		¿El Plan estratégico ha sido divulgado a los niveles que corresponde?		√	Sí está divulgado.		B
		¿Se tienen definidas las políticas y procedimientos para IT?	√		Sí se cuenta con procedimientos y políticas de TI, a pesar de ello algunos no se encuentran aprobados.		M
		¿Se tiene definido el apetito de riesgos para IT?	√		No está definido.		M
		¿Los riesgos que la organización se encuentra dispuesta a aceptar se encuentran aprobados formalmente por la Administración y el Comité de Auditoría?	√		Los riesgos están desactualizados.		M
		¿El mapa de riesgos es revisado y actualizado periódicamente?	√		En el 2015 no se revisaron y actualizaron los riesgos.		M
		¿La evaluación de riesgos considera elementos cualitativos y cuantitativos?	√		Sólo considera aspectos cualitativos.		B
		¿Los riesgos de IT son revisados con los usuarios del sistema?	√		Se han revisado y actualizado.		B
		¿Se han implementado anti virus y firewalls?		√	Si se han implementado.		B
		¿Se han establecido los protocolos para la realización de copias de seguridad?	√		Si existen pero no están aprobados.		B

		¿La seguridad de la información es un tema de seguimiento para la alta gerencia como para el Comité de Auditoría?	√		En este momento se ha formulado un proyecto para establecer un Sistema de Gestión de Seguridad de la Información.		M
		¿Las políticas y procedimientos relacionados con TI son revisados y actualizados periódicamente, considerando los cambios en la industria y la regulación externa?		√	Sí se encuentran actualizados.		B
		¿Se tiene definido el perfil para cada cargo de IT y los colaboradores vinculados cumplen con el mismo?		√	Sí se posee.		B
		¿Se tienen definido un plan estratégico para IT alineado con el de la organización?		√	Si se cuenta.		B
		¿Se tienen definidas y divulgadas las funciones y responsabilidades de cada colaborador del área?		√	Si están definidas.		B
		¿Las responsabilidades de cada nivel y colaborador, parten del principio de segregación de funciones?		√	Así se realiza.		B
		¿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?		√	Las jefaturas poseen los roles de administrador del sistema, y ellos aprueban y aplican cambios.		B
		¿Los usuarios de las herramientas conocen formalmente sus responsabilidades con el uso de las mismas?		√	Se posee manuales de usuario.		B
		¿Las herramientas de IT permiten tener la trazabilidad de las operaciones realizadas así como de los usuarios (logs)?		√	Sí se cuentan con bitácoras.		B
		¿Se monitorea el estado de los equipos (Hardware)?	√		Sí se realiza, a pesar de ello no se cuenta con un plan de capacidad y desempeño.		M
		¿La seguridad física de las instalaciones donde operan los equipos y personas de IT, es evaluada y revisada periódicamente, cumplimiento con los protocolos establecidos?		√	Sí se revisa.		B
		¿La organización desarrolla un plan de formación integral tanto para los miembros		√	Se ha sacado una campaña de cápsulas en donde se dan recomendaciones de seguridad a la organización.		B

		de IT como para los usuarios de la herramienta, orientado al uso, seguridad y ética en la utilización de las mismas?					
		¿Se han establecido indicadores de gestión que permitan medir el desempeño de las herramientas como de los colaboradores del área?	√		Actualmente se está llevando a cabo un proyecto para efectuar las evaluaciones del desempeño de los colaboradores de TI.		B
		¿Se han implementado planes de acción correctivos, para aquellos casos en que los indicadores presentar resultados inferiores a los esperados?	√		Aún no se han hecho evaluaciones.		B
		¿Se han adquirido pólizas de seguro para eventos de riesgos en el área de IT?	√		No se cuenta con pólizas de seguro que cubran los equipos críticos de la Institución.		M
		¿Cada proyecto de IT 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?		√	Existe una Comisión que valora el tema de riesgos en los proyectos.		B
		¿Se hace un seguimiento periódico al cumplimiento contractual de las obligaciones adquiridas por los proveedores de IT y dicho seguimiento es documentado?		√	Sí se realiza.		B
		¿Todos los cambios desarrollados en las aplicaciones y/o software son documentados y custodiados?		√	Sí se documentan.		B
		¿Se ha establecido el plan de continuidad para los procesos de IT?		√	Sí se ha establecido.		B
		¿Se solicita el apoyo de consultores externos para los proyectos estratégicos?		√	Sí se realiza.		B

		Los accesos son autorizados por un nivel superior.		√	Son autorizados por las jefaturas de las áreas usuarias.		B
		Los accesos otorgados son revisados periódicamente.		√	Sí se realiza.		B
		La asignación de los accesos parte de la segregación de funciones.		√	Así se realiza.		B
		Cada usuario tiene asignada una clave de composición alfa numérica y de mínimo 8 caracteres		√	Así se realiza.		B
		Se pueden rastrear las operaciones realizadas por los usuarios por medio de los logs		√	Sí se cuenta con el control.		B
		Se cuenta con una política de copias de seguridad y de restauración.	√		Sí la poseen, a pesar de ello, los procedimientos de respaldos no se encuentran aprobados.		M
		La información sensible se encuentra protegida de modificaciones no autorizadas.		√	Está protegida.		B
		Se cumplen con los niveles de seguridad físicos para los servidores.	√		El cableado se encuentra desordenado.		B
		Asignación de usuarios y claves personalizada		√	Así se realiza.		B
		Segregación de funciones entre los niveles que solicitan, realizan, aprueban y monitorean los cambios.		√	Sí existe la segregación.		B
		Alertas para los niveles que autorizan los cambios cuando los mismos se realizan.		√	Si existen.		B
		Las modificaciones en las bases son realizadas por un área independiente a la que utiliza la información.		√	Se gestiona de esa manera.		B
		Los cambios en la base permiten tener la trazabilidad de quien los realiza por medio de los logs.		√	Sí existen mecanismos para dar seguimiento.		B
		Se tiene un número reducido de administradores.		√	Así se gestiona.		B
		Se cuenta con un diccionario de datos para la base, identificando las relaciones internas que		√	Sí se tiene un diccionario de datos.		B

		tiene y los accesos de consulta o modificación.					
		Definición y documentación de la Política de Cambios	□	√	Sí se cuenta con la documentación.		B
		Segregación de funciones entre el desarrollador, aprobador y responsable de administrar en producción	□	√	Sí hay segregación de funciones.		B
		Aprobación del usuario final de los cambios.	□	√	Así se realiza.		B
		Asignación usuarios y permisos, previo requerimiento y aprobación del Director y/o Responsable del área que utiliza la aplicación.	□	√	Así se realiza.		B
		Reportes periódicos de los cambios que se consideran críticos en las aplicaciones, para validar su autorización por parte del nivel aprobador de los cambios.	□	√	Sí se maneja.		B
		Validación periódica de los cambios en permisos y asignación de usuarios por parte del nivel autorizador.	□	√	Sí se valida.		B
		Bloqueo de usuarios retirados, previa comunicación de Gestión Humana.	□	√	Sí se maneja.		B
		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.	□	√	Es responsabilidad de los administradores.		B
		Bloqueo de usuarios en vacaciones	√	□	Esto no se realiza.		B
		Identificación de los usuarios que realizan las transacciones, por medio de los Logs.	□	√	Sí se poseen logs.		B
		Certificaciones externas sobre la calidad del servicio prestado.	□	√	Mediante la SUPEN, la auditoría externa y la auditoría interna.		B
		Suscripción de un acuerdo sobre privacidad con el proveedor.	□	√	Sí se maneja.		B
		Plan de contingencia para migrar a otro servidor	√	□	Aún no se cuenta con un sitio alterno.		M
		Plan de capacitaciones en seguridad, para los usuarios con accesos más vulnerables.	□	√	Sí se han brindado.		B

		Cifrar las bases de datos más sensibles, junto con controles de monitoreo.		√	Sí se maneja, para claves y los archivos que envían las entidades deductoras.		B
		Limitar el acceso a los datos y/o solicitar mayores autenticaciones, de acuerdo al dispositivo y al lugar desde donde se ingresa.		√	Sí se realiza.		B
		Instalar en los dispositivos móviles parches que permitan aislar los datos de la compañía de los personales.	√		No se ha establecido la política de seguridad móvil.		M
		Se realizan pruebas periódicas sobre la recuperación de datos.		√	Sí se realiza.		B

ANEXO III

CABLEADO DEL CUARTO DE SERVIDORES