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

- ***Carta de Gerencia CG 2-2012***
- ***Informe de Auditoría de Sistemas y Tecnologías de Información.***
- ***Informe Final***

San José, 22 de Marzo del 2013

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 2012 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 1-2012.

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 Nº 1649
Póliza de fidelidad Nº 0116 FIG 0007
Vence el 30 de setiembre del 2013.

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

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

TRABAJO REALIZADO

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 trabajo sobre dieciséis áreas de evaluación, que constituyen el entorno que administra el Fondo dentro del conglomerado informático del Poder Judicial. Lo anterior según lo especificado en el documento **SP-A-060** "Circular sobre los trabajos que deben realizar los auditores externos de los regímenes básicos y fondos de pensiones complementarios especiales supervisados por la Superintendencia de Pensiones".

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. Seguridad lógica de los sistemas de información.
9. Capacitaciones en materia de seguridad de la información.
10. Procedimiento de uso, desecho y reutilización de equipo electrónico.
11. Metodología de proyectos de Tecnologías de Información.
12. Estándares para el desarrollo de sistemas.
13. Metodología de gestión de la calidad.
14. Metodología de administración de riesgo de TI.
15. Evaluaciones de desempeño de los funcionarios de TI.
16. Informes de Auditoría Interna.
17. Seguimiento formal de las pistas de auditoría.
18. Seguimiento a Cartas de Gerencia Anteriores.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de entrevistas personalizadas a los funcionarios relacionados con los sistemas de información de contabilidad, inversiones, planillas, activos fijos, cuentas por cobrar así como también con los encargados de telemática, soporte y bases de datos que le prestan servicios al ***Fondo de Jubilaciones y Pensiones del Poder Judicial,*** aplicando los aspectos que evalúan el cumplimiento de la normativa vigente establecida en el documento **SP-A-060** emitido por la SUPEN el cual se denomina "Circular sobre los trabajos que deben realizar los auditores externos de los regímenes básicos y fondos de pensiones complementarios especiales supervisados por la Superintendencia de Pensiones".

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 a 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.

a. Ambiente de Control

- Revisión de la funcionalidad de los sistemas de información utilizados en el ***Fondo del Poder Judicial*** como el soporte brindado a dichos sistemas de información. Además evaluamos el estado actual del proyecto SIGAFONDO.

- Revisión de la existencia de Manuales de sistemas al usuario final y políticas en el uso adecuado de los sistemas de información que se encuentran en producción en el ***Fondo del Poder Judicial***.

b. Auditoría de Sistemas Externas Anteriores

Analizamos los informes de sistemas externa (cartas de gerencia anteriores), archivados en el ***Fondo de Jubilaciones y Pensiones del Poder Judicial***, con el fin de dar seguimiento a las principales observaciones, hallazgos y recomendaciones emitidas en estas instancias.

c. Normativas y criterios utilizados

Para la evaluación del control interno de los sistemas en producción y la administración, operatividad y servicios utilizamos como referencia lo especificado en el documento **SP-A-060** "Circular sobre los trabajos que deben realizar los auditores externos de los regímenes básicos y fondos de pensiones complementarios especiales supervisados por la Superintendencia de Pensiones y lo establecido en las **N-2-2007-CO-DFOE** "Normas técnicas para la gestión y el control de las Tecnologías de Información"

DETALLE DE LOS PUNTOS A EVALUAR EN LAS DIFERENTES ÁREAS DE TECNOLOGÍAS DE INFORMACIÓN DEL FONDO DE JUBILACIONES Y PENSIONES DEL PODER JUDICIAL

A continuación se detallan los aspectos evaluados según lo indicado por la SUPEN en su circular SP-A-060, así como los resultados a los mismos por el área evaluada:

1. Seguridad Física del cuarto de servidores

El 18 de marzo del 2013, se realizo el recorrido en el cuarto de servidores del Fondo de Jubilaciones y Pensiones del Poder Judicial, pudiéndose determinar que se mantienen en dicho cuarto importantes medidas de seguridad como lo son: detectores de humo y humedad, extintor, aire acondicionado, bitácora de ingreso, apertura de puerta con tarjeta, entre otros.

2. Inventario de hardware.

Se determinó que a la fecha de la presente auditoría, ya se cuenta con un sistema automatizado para el registro y control del inventario de hardware. Dicho sistema es administrado por la Proveeduría; además es importante indicar que el inventario se mantiene actualizado ya que de forma anual se actualiza y cuando se considere necesario.

3. Inventario de software.

Durante la presente auditoría no se evidenció la existencia de un inventario de software por equipo del Fondo. **Ver Asunto a Informa 1.**

Comentarios de la Administración:
La recomendación emitida forma parte de los requerimientos que se tienen proyectados desarrollar en el 2013 Módulo de Activos Intangibles del Sistema Catálogo de Activos Fijos. CAF

4. Manuales de usuario y técnicos de los sistemas.

Se cuenta con los manuales de usuario y manuales técnicos de los diferentes sistemas utilizados en el Fondo de Jubilaciones y Pensiones del Poder Judicial. Los mismos se encuentran actualizados, incluyen las principales opciones del sistema y presentan facilidad de uso para los usuarios finales.

5. Estudios de vulnerabilidad de la red.

Durante la presente auditoría no se entregó documentación que respalde la ejecución de estudios de vulnerabilidad de red durante el periodo 2012, por tanto la atención de la recomendación emitida mediante el HALLAZGO 3: NO SE HA IMPLEMENTADO UN ESTUDIO SOBRE LAS VULNERABILIDADES QUE PODRÍA TENER LA RED (ESTUDIO DE PENETRACIÓN) de la Carta de Gerencia del 2007 se mantiene pendiente.

6. Plan de Continuidad.

El Plan de Contingencias de TI entregado, evidencia que este fue emitido en febrero del 2010 y no se evidencia a la fecha de la presente auditoría que este haya sido revisado o bien modificado. Por otra parte se evidencia la ejecución de las pruebas del plan de continuidad, las cuales se ejecutaron del 12 al 19 de marzo del 2012, en las misma participaron funcionarios tanto del Departamento de TI como funcionarios involucrados en el proceso de otros Departamentos del Fondo, se indica que los resultados obtenidos fueron satisfactorios. De acuerdo a lo mencionado se considera corregida la atención del HALLAZGO 1: NO EXISTE EVIDENCIA DOCUMENTAL SOBRE LA REALIZACIÓN DE PRUEBAS AL PLAN DE CONTINUIDAD DEL SIGA-FONDO DE JUBILACIONES Y PENSIONES NI CON CAPACITACIONES REALIZADAS A DICHO PLAN incluido en la Carta de Gerencia del 2011.

7. Prueba de los respaldos de información.

No se entrego evidencia sobre la ejecución de las pruebas a los respaldos de información durante el periodo 2012. Por otra parte la Jefatura de Soporte Técnico indico que dichas pruebas no se ejecutan. **Ver hallazgo 01**.

Comentarios de la Administración:
Actualmente los respaldos del Fondo de Jubilaciones se llevan en cinta y en el disco duro de un servidor, los respaldos a disco se tienen desde el 2010, por lo que también pueden ser utilizados en caso de ser requeridos.

Adicionalmente, se está definiendo un medio alterno de respaldos con el fin de no depender únicamente de los respaldos en cinta, debido a la imposibilidad material de realizar pruebas en el equipo, pues estos servidores se utilizan 24/7 para efectuar respaldos de todos los sistemas del Poder Judicial. Actualmente el tamaño de cada respaldo del SIGA-FJP es aproximadamente de 170 MB, los cuales se estarían incluyendo en un CD y enviándose de manera mensual para custodia, se llevará un control con las pruebas realizadas previo a su remisión para ser custodiados. La Sección de Soporte Técnico será la encargada de realizar los respaldos y enviarlos a custodia, la Sección de Sistemas de Información se encargará de realizar las pruebas de los respaldos para asegurarse del correcto funcionamiento.

8. Integración de Sistemas

De acuerdo al documento facilitado y que contiene el estudio de factibilidad del nuevo Sistema Contable del Poder Judicial, se incluye el módulo de Cuentas por Cobrar, considerando la unificación de cuentas. De acuerdo, a lo indicado anteriormente es posible indicar que el proceso de atención a la recomendación emitida en la Carta de Gerencia del 2011, mediante el HALLAZGO 2: LAS CUENTAS POR COBRAR DEL FONDO DEL PODER JUDICIAL NO SE LLEVAN EN UN SOLO SISTEMA INFORMÁTICO se encuentra en proceso.

Por otra parte, en la Carta de Gerencia del 2009 deja reflejado mediante el hallazgo INTEGRACIÓN DE LOS DIFERENTES MÓDULOS, que no existe integración entre los sistemas de Contabilidad, Planillas de Jubilados y Pensionados y el de Inversiones, sobre este asunto igualmente se evidencia en el estudio de factibilidad los requerimientos necesarios para corregir esta situación. Es importante indicar que el proyecto de la implementación del Sistema Contable se encuentra en la etapa de análisis y diseño y además ya se encuentran preseleccionadas las empresas que desarrollarán dicho proyecto.

9. Evaluación de los sistemas utilizados en el Fondo.

Se efectuó una evaluación de la funcionalidad de los principales sistemas utilizados en el Fondo de Jubilaciones y Pensiones del Poder Judicial, en conjunto con los usuarios expertos en cada caso. El detalle de los resultados se muestra en el **Anexo 1 EVALUACIÓN FUNCIONAL A LOS SISTEMAS DE INFORMACIÓN IMPLANTADOS EN EL FONDO DEL PODER JUDICIAL.**

Comentarios de la Administración:
Sobre este aspecto, se aceptan las mejoras que informaron los usuarios para el Sistema de Inversiones, las mismas están siendo consideradas en el alcance del nuevo proyecto de inversiones. Así mismo, las mejoras sugeridas por los usuarios al Sistema de Contabilidad y al Sistema de Cuentas por Cobrar, forman parte de los requerimientos del Sistema Contable del Poder Judicial, el cual se encuentra en las etapas de análisis y diseño.

10. Capacitaciones de Seguridad de la Información.

Tomando como referencia el respaldo de las capacitaciones realizadas durante el periodo 2012 referente seguridad de la información. Es posible indicar que se realizaron capacitaciones mediante correo electrónico relacionadas con la contraseña de ingreso a los sistemas y a la red institucional y sobre el modulo de seguridad de los sistemas. De acuerdo a lo anterior se considera corregida la atención de la recomendación emitida en la Carta de Gerencia del 2011 mediante el HALLAZGO 3: NO SE IMPARTEN CAPACITACIONES EN MATERIA DE SEGURIDAD INFORMÁTICA A LOS FUNCIONARIOS DEL FONDO DEL PODER JUDICIAL.

11. Procedimiento uso, desecho y reutilización medios electrónicos.

No se entregó el respaldo de la existencia de un procedimiento referente al uso, desecho y reutilización de medios electrónicos, tal y como lo indica la política que debería existir. Por tanto se mantiene pendiente la atención de la recomendación emitida mediante el HALLAZGO 4: NO SE CUMPLE CON LO MENCIONADO EN LA POLÍTICA PARA EL USO, DESECHO Y REUTILIZACIÓN DE MEDIOS ELECTRÓNICOS O IMPRESOS incluido en la Carta de Gerencia del 2011.

12. Metodología de la gestión de proyectos.

Se cuenta con una Metodología para la Gestión de Proyectos formalmente aprobada en julio del 2011, en dicha metodología se incluyen los siguientes aspectos: fases o etapas de proyectos, recursos a utilizar, productos a obtener en cada etapa, definición de riesgos y responsabilidades, políticas o normas a cumplir con la metodología, entre otras.

En el documento facilitado sobre el estudio de factibilidad del Proyecto que se está ejecutando para desarrollar e implementar el Sistema Contable, se evidencia la aplicación de esta metodología.

13. Políticas, estándares y procedimientos de desarrollo.

Se evidenció la implementación de las diferentes políticas, metodologías y procedimientos relacionados con el desarrollo de sistemas. Los cuales corresponden a:

- Definición de Estándares de la Base de Datos.
- Estándares Programación Depto TI-PJ.
- Lista de Estándares de los Sistemas de Información.
- Manual Técnico - Propuesta para Estándar.
- Metodología de Análisis.
- Metodología de Diseño.
- Metodología para Diseño de Manual Técnico
- Metodología para Diseño de Manuales.
- Plan de Pruebas-Estándar 30-10-2012.

14. Metodología de gestión de la calidad.

Se evidencia de acuerdo al respaldo facilitado, se evidencia que se ha definido una metodología para asegurar la gestión de la calidad de los diferentes procesos que se ejecutan por tecnologías de información. Dicha metodología se basa en una serie de formularios, controles, actas y minutas de reuniones, entre otros.

15. Metodología de gestión de riesgos.

En el segundo semestre del 2012, se aplicó la metodología definida para la administración de riesgos relacionados con tecnologías de la información. En la misma se evidencia la ejecución de procesos como lo son: identificación de riesgos, identificación de fuentes de los riesgos, efectos que pueden generar y las alarmas de activación de los diferentes riesgos. Además en la misma se incluyen los controles o acciones a ejecutar con el propósito de disminuir la probabilidad de la materialización de los mismos.

16. Evaluaciones de desempeño.

En la Carta de Gerencia del 2008, se indicó mediante el HALLAZGO 1: NO SE REALIZAN EVALUACIONES SOBRE EL DESEMPEÑO DE LOS INTEGRANTES DEL ÁREA DE TI, se dejo evidenciado que no se realizan evaluaciones sobre el desempeño de los funcionarios del Departamento de TI. Debido a lo indicado por el Departamento de TI, referente a las evaluaciones de desempeño de los colaboradores de dicho Departamento. Se indica además que la metodología aplicada se basa en la ejecución de proyectos y que además el Departamento de Gestión Humana se encuentra trabajando para una propuesta de evaluación institucional se considera en proceso el estado de la recomendación.

17. Seguimiento formal de las pistas de auditoría.

Se verificó que el Departamento de Tecnologías de Información diseñaron los reportes y funcionalidades necesarias que le permite al usuario verificar los movimientos realizados en el sistema, los cuales son almacenados en las bitácoras de transacciones y de procesos. No obstante, no se ha definido formalmente quien debe dar seguimiento a las pistas de auditoría, cabe mencionar que esta actividad es responsabilidad de las áreas usuarias. De acuerdo a lo anterior se considera que la atención del **HALLAZGO 5: NO EXISTE SEGUIMIENTO DE LAS PISTAS DE AUDITORÍA** emitido en la Carta de Gerencia del 2007 se encuentra en proceso**.**

Comentarios de la administración:
Se remitirá un oficio a los Departamentos Usuarios para que le den seguimiento a las pistas de Auditoría por medio de la utilización de las consultas y reportes de las bitácoras de procesos y transacciones suministradas por el SIGA-FJP.

18. Informes de Auditoría Interna.

Durante el periodo 2012, la Auditoría Interna del Fondo emitió 5 informes, relacionados directa e indirectamente con tecnologías de información, en los cuales se informan los resultados obtenidos en la evaluación de los estados financieros, seguimiento a cartas de gerencia anteriores, seguimientos a informes de auditoría interna, entre otros. Se entrego respaldo que evidencia que el Departamento de Tecnologías de Información esta brindado atención de las recomendaciones y condiciones identificadas.

HALLAZGOS Y RECOMENDACIONES IDENTIFICADAS

HALLAZGO 01: NO SE EJECUTAN PRUEBAS A LOS RESPALDOS DE INFORMACIÓN. RIESGO ALTO

CONDICIÓN:
Se evidencia mediante correos y comunicados oficiales, que se definió que las pruebas a los respaldos de información deben realizarse conforme lo establece el Plan de Contingencias. No obstante, de acuerdo a lo indicado por la Jefatura de Soporte Técnico dichas pruebas no se realizan; además no se entrego documentación que demuestre la ejecución de dichas pruebas.

CRITERIO:
En la Circular Nº1163-DTI-2012 se comunicó lo siguiente "Las pruebas de recuperación de bases de datos se harán conforme a la periodicidad establecida en el plan de contingencias de cada uno de los sistemas. Por ejemplo, si se estableció en el plan de contingencia como periodicidad para realizar las pruebas cada seis meses, las pruebas de restauración de respaldos igualmente se realizarán con esa regularidad. En el caso de respaldos de datos de los servidores de archivos se probará dos veces al mes de manera aleatoria"

Además en el Plan de Contingencias se establece " Para la verificación de las cintas de respaldos el día viernes de cada semana durante la tarde se revisarán las cintas que llegaron de San Joaquín, mediante una restauración inicial a disco duro de los respaldos de las bases de datos con una antigüedad de 4 semanas."

RECOMENDACIÓN:
Iniciar con la práctica de ejecutar las pruebas a los respaldos de información tal y como lo establece la normativa interna. Con el propósito de asegurar la continuidad del negocio en caso de presentar alguna circunstancia o contingencia que afecte la información de las diferentes transacciones de los sistemas utilizados en el Fondo.

COMENTARIOS DE LA ADMINISTRACIÓN:
Actualmente los respaldos del Fondo de Jubilaciones se llevan en cinta y en el disco duro de un servidor, los respaldos a Disco se tienen desde el 2010, por lo que también pueden ser utilizados en caso de ser requeridos.
Adicionalmente, se está definiendo un medio alterno de respaldos con el fin de no depender únicamente de los respaldos en cinta, debido a la imposibilidad material de realizar pruebas en el equipo, pues estos servidores se utilizan 24/7 para efectuar respaldos de todos los sistemas del Poder Judicial. Actualmente el tamaño de cada respaldo del SIGA-FJP es aproximadamente de 170 MB, los cuales se estarían incluyendo en un CD y enviándose de manera mensual para custodia, se llevará un control con las pruebas realizadas previo a su remisión para ser custodiados. La Sección de Soporte Técnico será la encargada de realizar los respaldos y enviarlos a custodia, la Sección de Sistemas de Información se encargará de realizar las pruebas de los respaldos para asegurarse del correcto funcionamiento.

OTROS ASUNTOS A INFORMAR

ASUNTO 01: NO SE CUENTA CON INVENTARIO DE SOTWARE POR EQUIPO

Durante el proceso de auditoría se determinó que no se cuenta con un inventario detallado de las licencias por equipo, lo que no permite tener un adecuado control de las mismas. Lo anterior, deja evidenciado que no hay certeza de las aplicaciones instaladas en los equipos; esta condición hace que se presenten situaciones como:

- Brechas en cumplimiento de las condiciones de los proveedores.
- Exposiciones comerciales y contractuales de adquisición.
- Las soluciones automatizadas que no están en línea con los planes a corto y largo plazo de la organización
- Insuficiente calidad del software en soluciones adquiridas.
- Falta de control de los costes.

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.

Comentarios de la Administración:
La recomendación emitida forma parte de los requerimientos que se tienen proyectados desarrollar en el 2013 Módulo de Activos Intangibles del Sistema Catálogo de Activos Fijos. CAF

ANEXO 1

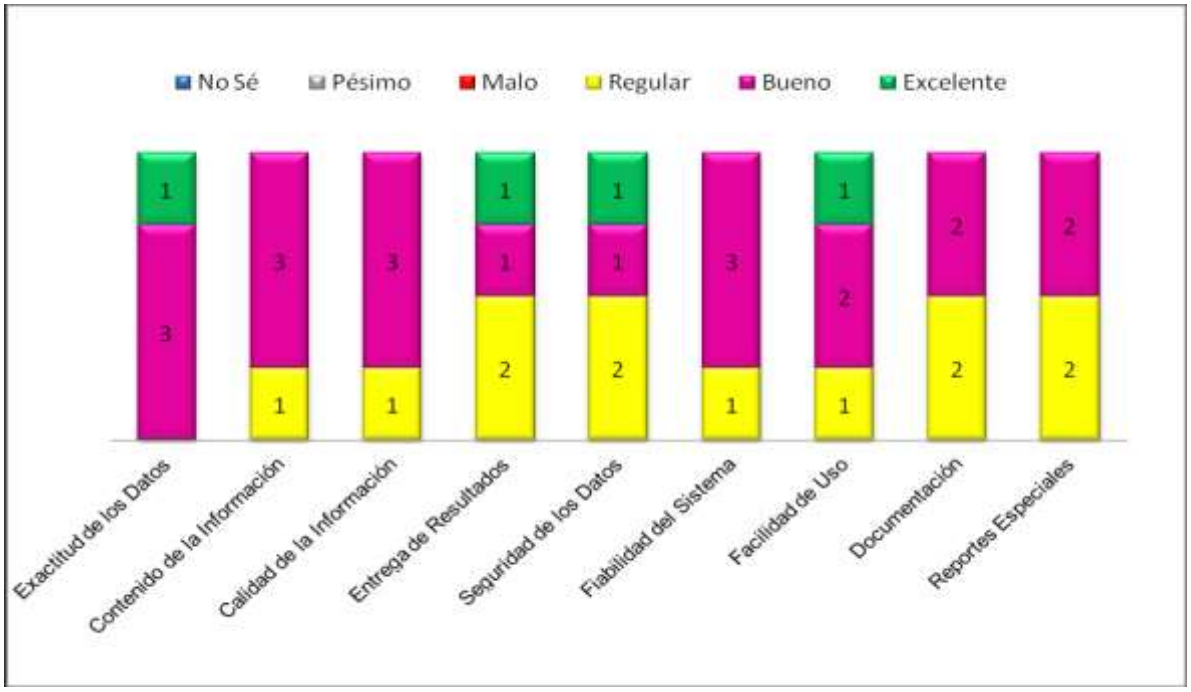
EVALUACIÓN FUNCIONAL A LOS SISTEMAS DE INFORMACIÓN IMPLANTADOS EN EL FONDO DEL PODER JUDICIAL

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.

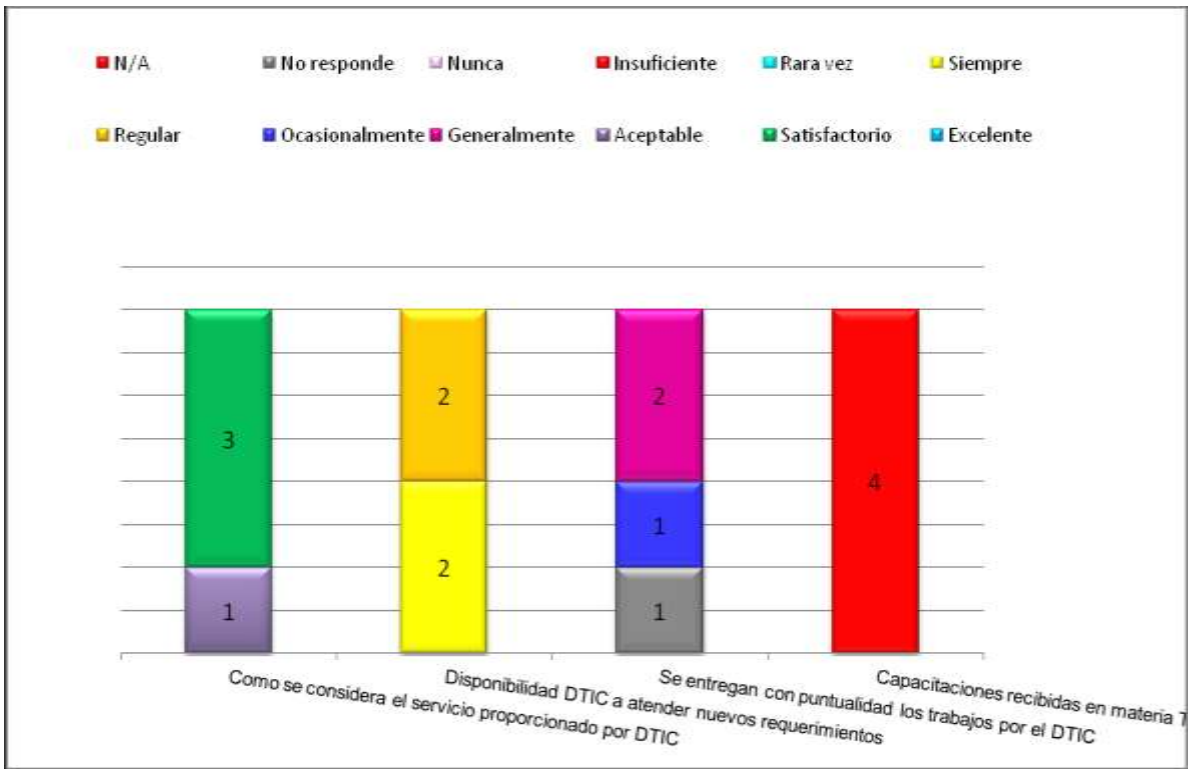
Los módulos evaluados y las personas entrevistadas en el proceso de evaluación de la calidad funcional se muestran en la tabla siguiente:

Nombre del Funcionario	***Sistema a Valorar***
Inversiones	Michael Mena Peñaranda
Inversiones	Floribel Campos Solano
Contabilidad	Kattia Vargas Pérez
Cuentas por Cobrar	Arelis Santos Carazo

a. 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:



b. Percepción de los usuarios finales respecto al servicio brindado por parte de Departamento de Tecnologías de Información.



c. Comentarios o mejoras por parte de los usuarios referentes a la valoración de los sistemas de información:

Inversiones:

- Mejora en el proceso de registro de las inversiones, de modo que sea un proceso más ágil y automatizado, que permita una mejor interacción del usuario.
- Integración con los diferentes sistemas que se están desarrollando, así como la implementación de aprobaciones electrónicas.

Contabilidad

- Integración de sistemas.

Cuentas por Cobrar

- En lo que corresponde a cuentas por cobrar por RTSFPJ a empleados que pasan a ser jubilados que el sistema hale el monto actualizado de la cuenta por cobrar, en virtud que solo hala la deuda inicial, sin discriminar si esta ha sido cancelada o abonada.

MATRIZ DE SEGUIMIENTO A CARTAS DE GERENCIA ANTERIORES

CARTA 1-2011			
HALLAZGO	**RECOMENDACIÓN**	**COMENTARIO DE LA ADMINISTRACIÓN**	**ESTADO**
HALLAZGO 1: NO EXISTE EVIDENCIA DOCUMENTAL SOBRE LA REALIZACIÓN DE PRUEBAS AL PLAN DE CONTINUIDAD DEL SIGA-FONDO DE JUBILACIONES Y PENSIONES NI CON CAPACITACIONES REALIZADAS A DICHO PLAN	Realizar de forma regular las pruebas al plan de contingencias del SIGA-FONDO documentando el procedimiento y resultado de las pruebas efectuadas. Además se debe asegurar que todos las partes involucradas reciban sesiones de capacitación de forma regular debidamente documentadas respecto a los procesos, roles y responsabilidades en caso de un contingente, con la finalidad de verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia. También el plan de continuidad debe abarcar todas las áreas del Fondo del Poder Judicial.	Se remiten las pruebas realizadas al Plan de Continuidad de Tecnología de Información durante los años 2012 y 2013. Ver Anexo "Pruebas al Plan de Continuidad del SIGA-FJP"	**CORREGIDA**

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.	En el Sistema Contable del Poder Judicial se contempla el módulo de Cuentas por Cobrar, en el cual se unifica el proceso de dichas cuentas.	**PROCESO** De acuerdo al documento que contiene el estudio de factibilidad del nuevo Sistema Contable del Poder Judicial, se incluye el módulo de Cuentas por Cobrar, considerando la unificación de cuentas.
HALLAZGO 3: NO SE IMPARTEN CAPACITACIONES EN MATERIA DE SEGURIDAD INFORMÁTICA A LOS FUNCIONARIOS DEL FONDO DEL PODER JUDICIAL.	Incluir dentro de los planes de capacitación la formación, entrenamiento y los contenidos necesarios para que el personal del Fondo del Poder Judicial conozca las políticas, procedimientos, normativas de Tecnologías de Información, riesgos, amenazas y uso de Tecnologías de Información. Dicho plan debe contar con el debido apoyo presupuestario. Además es conveniente implementar los mecanismos necesarios para monitorear el debido cumplimiento los lineamientos establecidos.	Como parte de la puesta en marcha del proyecto SIGA-Fondo de Jubilaciones y Pensiones se capacitó a los usuarios, en relación con la seguridad del sistema, esquema de seguridad y uso de claves. Así mismo, la Dirección de Tecnología de Información con el apoyo del Departamento de Prensa y Comunicación ha informado por medio de la Intranet a los funcionarios del Poder Judicial las políticas de Seguridad Informática. Finalmente, se han realizado campañas informativas con la colaboración del Departamento de Prensa y Comunicación en la que se indica a los empleados del Poder Judicial la obligatoriedad de cambiar las contraseñas y las medidas de seguridad que deben de tomarse en cuenta para definir las claves. Ver anexo "Capacitaciones sobre la Seguridad de la Información"	**CORREGIDO**

		Tal y como se indicó en el Apartado 6 de este oficio**,** en la visita realizada por parte de su Despacho se informó que durante el proceso de implantación del SIGA-FJP se realizaron capacitaciones a los usuarios involucrados con aspectos de seguridad del sistema.	
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.	Si bien es cierto no se ha promulgado un reglamento específico que materialice esta política sí se han realizado esfuerzos para cumplirla. En este sentido se puede indicar que para la destrucción del papel se tiene una campaña de reciclaje que culmina con la destrucción del papel en las instalaciones de Kimberly-Clark, empresa con la que se tiene el respectivo acuerdo de confidencialidad. Con respecto al desecho de los discos duros, las computadoras que se donan son preparadas previamente por personal de la Sección de Soporte Técnico quienes como parte del proceso eliminan la información que hay en los discos. Se buscan alternativas para desechar adecuadamente elementos como los CDs y DVDs. La Dirección de Tecnología tiene como política no recomendar la utilización de dispositivos como llaves USB dado que representan una vulnerabilidad.	**PROCESO** A la fecha de la presente auditoría, no se ha desarrollado un procedimiento referente al uso, desecho reutilización de medios electrónicos de manera cumplir con lo indicado en la política. Sin embargo, de acuerdo a lo indicado por el Departamento de TI si se aplican medidas para el tratamiento de los medios electrónicos.

		Tal y como se informa en el apartado 7 del presente oficio, los desechos electrónicos del Poder Judicial se están entregando para reciclaje por parte del Departamento de Proveeduría, y se está en puertas la firma de un convenio con el Instituto Tecnológico de Costa Rica, para el manejo responsable de este tipo de bienes.	
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 del Poder Judicial, el cual se encuentra en la Etapa de Análisis y Diseño considera la integración con el Sistema de Inversiones y el SIGA-Fondo de Jubilaciones y Pensiones. Ver apartado "Interfases Internas" del Anexo " Respaldo de las gestiones para las cuentas por cobrar".	**PROCESO** Como ya se ha indicado, el proyecto del nuevo Sistema Contable del Poder Judicial, se encuentra en la etapa de análisis y diseño. Además en el estudio de factibilidad se evidencia la inclusión de Contabilidad, Planillas de Jubilados, Pensionados e inversiones.

CARTA 2008			
HALLAZGO 1: NO SE REALIZAN EVALUACIONES SOBRE EL DESEMPEÑO DE LOS INTEGRANTES DEL ÁREA DE TI.		Sería inexacto decir que no se evalúa el desempeño de los funcionarios ya que la organización de la Dirección de TI se orienta al manejo por proyectos y bajo esta óptica el rendimiento de cada miembro de un equipo es evaluado por su líder y está en relación directa con el cumplimiento de las metas que se establezcan. Las jefaturas de cada área a su vez dan seguimiento a los proyectos y la Dirección de TI integra los esfuerzos de las diferentes áreas. La institución desechó su sistema de evaluación del personal dado que no daba los resultados requeridos; el Departamento de Gestión Humana trabaja en la propuesta de un nuevo sistema de evaluación del rendimiento. No se considera apropiado implementar un sistema paralelo al institucional por lo que se está a la espera de lo que se defina para todos los funcionarios de la institución.	**PROCESO** Debido a lo indicado por el Departamento de TI, referente a las evaluaciones de desempeño de los colaboradores de dicho Departamento. Detallando que la metodología aplicada se basa en la ejecución de proyectos y que además el Departamento de Gestión Humana se encuentra trabajando para una propuesta de evaluación institucional se considera en procesos el estado de la recomendación.
El Departamento de T.I. del Fondo de Jubilaciones y Pensiones del Poder Judicial no cuenta con una herramienta automatizada para realizar un inventario al equipo de cómputo	Es recomendable que el departamento de tecnologías de la información del Fondo de Jubilaciones y Pensiones del Poder Judicial, realice el inventario del equipo de cómputo con una herramienta automatizada para agilizar este proceso y poder llevar un mejor control del mismo.	La información del Inventario del Equipo de cómputo se lleva a través del sistema CAF Catálogo de Activos Fijos del Poder Judicial. Ver anexo "Inventario de Hardware".	**CORREGIDA** El Sistema CAF desde el 2009 está en producción, debido a las necesidades que se van presentando se le ha realizado mejoras.

			No obstante, el inventario se sigue realizando de forma manual y posteriormente se alimenta el Sistema CAF.
CARTA 2007			
HALLAZGO 3: NO SE HA IMPLEMENTADO UN ESTUDIO SOBRE LAS VULNERABILIDADES QUE PODRÍA TENER LA RED (ESTUDIO DE PENETRACIÓN).		Para el 2012 se incluyó el presupuesto para realizar la contratación de un test de vulnerabilidad de la red por parte de una consultora externa sin embargo los fondos debieron utilizarse para atender necesidades más urgentes. Es importante acotar que durante el 2012 sí se gestionó el cambio de los principales equipos de seguridad perimetral de la institución, cambio que se está realizando en estos días. También es importante hacer notar que se cuenta con un área de seguridad informática encargada de monitorear el comportamiento de la red con el fin de detectar comportamientos anormales que pudieran indicar la presencia de un hacker en la red. Y por último debe señalarse que la red institucional es una sola por lo que no es posible separar los esfuerzos que se hacen en la red del Fondo de Pensiones de los que se hacen para el resto de la red. Se continúa en un proceso constante de análisis de posibilidades de mejora en la seguridad informática de la institución. Para el 2013 se incluyó nuevamente el contenido para el test de	**PENDIENTE** A pesar de que se han realizado gestiones para contratar la ejecución de un estudio de vulnerabilidad de la red, se han presentado inconvenientes para que esta se realice. Por tanto se mantiene pendiente la atención de la recomendación.

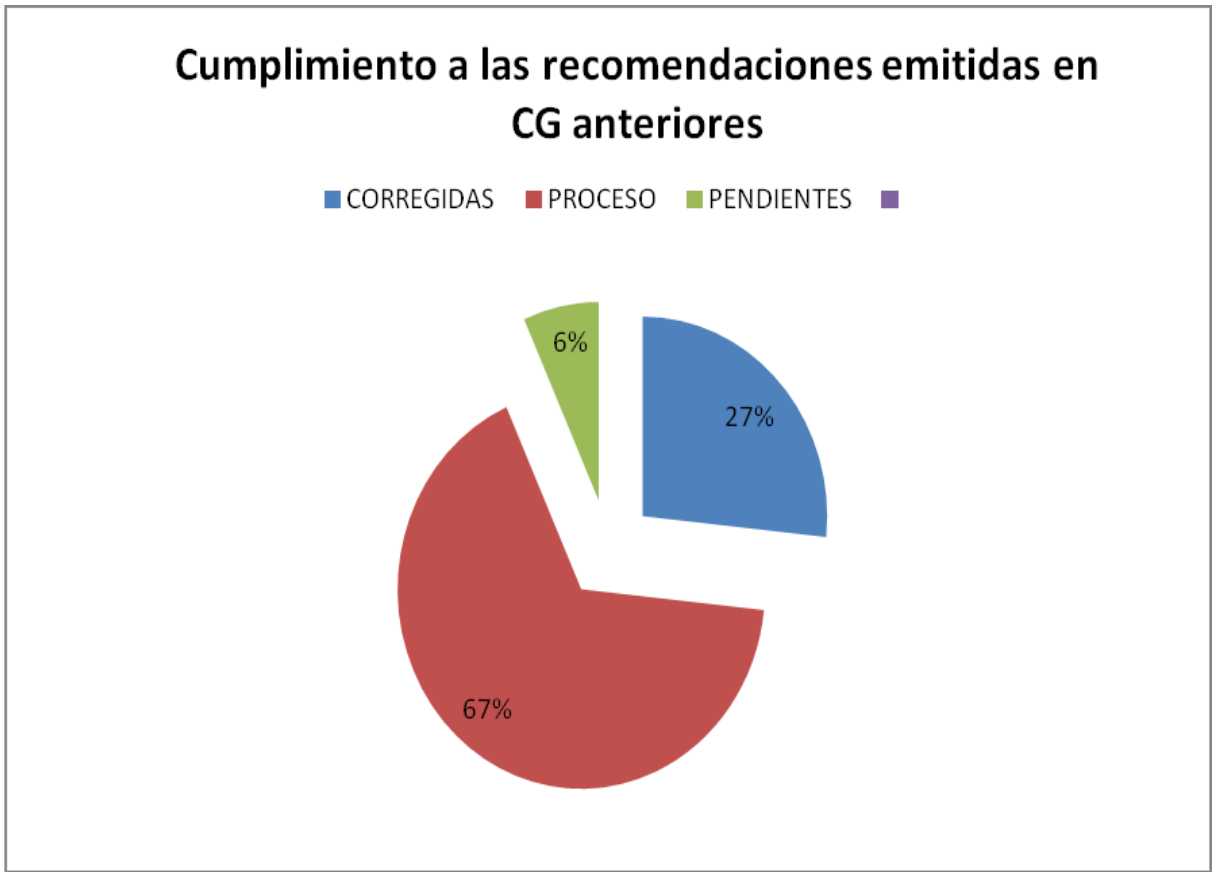
		penetración, sin embargo, este presupuesto debió utilizarse ya en la contratación urgente de la migración del active directory institucional de Windows 2003 a Windows 2008; se analiza la posibilidad de reponer este contenido para realizar la contratación del test de penetración.	
HALLAZGO 5: NO EXISTE SEGUIMIENTO DE LAS PISTAS DE AUDITORÍA.		Dirección de Tecnología diseñó los reportes y funcionalidades necesarias que le permite al usuario verificar los movimientos realizados en el sistema, los cuales son almacenados en las bitácoras de transacciones y de procesos. Por lo tanto el seguimiento a las pistas de auditoría debe ser dirigida a los Departamentos Usuarios. Según lo señalado en el apartado 8 del presente oficio, se solicita que dicha recomendación sea dirigida a las áreas usuarias del SIGA-FJP, así mismo se informa que la Auditoría Interna del Fondo de Jubilaciones utiliza el "Generador de informes del SIGA-Fondo de Jubilaciones y Pensiones" para dar seguimiento a las situaciones especiales que identifiquen en el sistema.	**PROCESO** A pesar de que se ya se implementaron las pistas de auditoría en los sistemas, no se ha definido formalmente el responsable de dar seguimiento a las mismas. Esta actividad debe ser ejecutada por parte de las áreas usuarias como "dueños" de los datos

CARTA *CG2-2006*			
HALLAZGO 1: LOS SISTEMAS DE CONTABILIDAD Y DE PLANILLAS NO CUENTAN CON UN PROCESO DE CAMBIO DE CLAVE AUTOMÁTICO CORRECTO.		La seguridad del Sistema del Fondo de Jubilaciones y Pensiones del Poder Judicial se lleva por medio del Active Directory, por lo que en cumplimiento a las mejores prácticas en la gestión de la seguridad de usuarios, los sistemas de información en el Poder Judicial utilizan seguridad integrada, esto implica, que con el mismo usuario y clave de la red del Poder Judicial los funcionarios se autentican en los diversas herramientas tecnológicas que apoyan su función. Siendo así, las políticas de cambio de contraseña en los sistemas de información son las mismas que los utilizados en la red de la institución. Es por esto que durante el año 2012 se analizó la importancia de activar políticas de contraseñas seguras e informar a la población judicial la importancia y responsabilidad que cada uno tiene en la seguridad de la información. En el mes de octubre y noviembre se publicó una campaña al respecto, se adjuntan los correos electrónicos enviados por el Departamento de Prensa. Así mismo, a partir del 4 de marzo del presente año, se activa la política de cambio de contraseña cada tres meses.	**CORREGIDA** Además de lo indicado por la Administración, durante la evaluación de los sistemas se determinó la implementación del cambio de clave automático.

HALLAZGO 3: EL SISTEMA DE CONTABILIDAD NO SE DESACTIVA O PARALIZA AUTOMÁTICAMENTE DESPUÉS DE HABER ESTADO CIERTO TIEMPO SIN SER UTILIZADO.		El nuevo Sistema de Contabilidad solventará esta situación por medio de controles de desactivación de las sesiones que no están en uso. Sobre este hallazgo se aclara que los aspectos relacionados con las mejoras en la Seguridad del Sistema TECAPRO han sido cubiertas en por el Módulo de Seguridad del Fondo de Jubilaciones y Pensiones, por lo que esta recomendación ya fue acatada y se encuentra en proceso de implantación.	**PROCESO** No se ha corregido la debilidad indicada en el sistema actual de Contabilidad. Se indica que será incorporado en el nuevo sistema.
HALLAZGO 4: EL SISTEMA DE CONTABILIDAD NO CUENTA CON UNA BITÁCORA ADECUADA, Y EL SISTEMA DE PLANILLAS CARECE DE ESTA OPCIÓN DE SEGURIDAD.		El nuevo Sistema de Contabilidad solventará esta situación por medio de bitácoras de procesos y bitácoras de transacciones que se implementan por medio del módulo de seguridad. Sobre este tema se aclara que las recomendaciones emitidas sobre las Bitácoras de Seguridad del Sistema TECAPRO han sido cubiertas en por el Módulo de Seguridad del Fondo de Jubilaciones y Pensiones, por lo que esta recomendación ya fue acatada y se encuentra en proceso de implementación en el nuevo sistema contable.	**PROCESO** No se ha corregido la debilidad indicada en el sistema actual de Contabilidad. Se indica que será incorporado en el nuevo sistema.

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		El sistema SIGA-Contabilidad estará integrado con el Sistema de Inversiones y el SIGA-Fondo de Jubilaciones y Pensiones, sin embargo contarán con bases de datos independientes. La información necesaria para cada proceso se obtendrá en forma directa desde cada base de datos origen. En cuanto a la integración de los sistemas del Fondo de Jubilaciones y Pensiones del Poder Judicial se entregó evidencia en el **"Estudio de Factibilidad"** que el Sistema Contable considera la integración solicitada, dicho sistema se encuentra en la Etapa de Análisis y Diseño. Por lo indicado, se solicita que se actualice el citado hallazgo al estado en Proceso.	**PROCESO** No se ha realizado la corrección de la debilidad.
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 será adquirido por medio de un desarrollo a la medida. Ver el documento "Estudio de Factibilidad del Sistema Contable del Poder Judicial", en la cual el Poder Judicial será el responsable de dar mantenimiento al sistema una vez que finalice el periodo de garantía de la contratación de la programación.	**PROCESO** Como ya se ha indicado está en proceso el desarrollo a la medida del nuevo sistema Contable, que corregirá la dependencia con la empresa TECAPRO.

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		Actualmente se encuentra en la Proveeduría, las especificaciones técnicas para que una consultora apoye el proceso de migración a la plataforma Windows 2008, con la que se tiene proyectado activar estas opciones.	**PROCESO** Se está trabajando en las gestiones para corregir la inexistencia de una bitácora de ingreso a la red.

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

CORREGIDAS	**4**
PROCESO	**10**
PENDIENTES	**1**