Junta de Protección Social

INFORME DE AUDITORÍA INTERNA AI JPS N° 01-2015

ÁREA DE SISTEMAS

TEMA:

"SEGUIMIENTO DE RECOMENDACIONES GIRADAS POR EL ÁREA DE SISTEMAS DE LA AUDITORÍA INTERNA, MEDIANTE INFORMES Y ADVERTENCIAS EMITIDAS A TRAVÉS DE NOTAS"

PREPARADO POR:

ING. VIVIANA RIVERA BARRANTES
PROFESIONAL III

15 DE ENERO DE 2015

DIRIGIDO A:

GERENCIA GENERAL

COPIA:

DEPARTAMENTO DE TECNOLOGÍA DE LA INFORMACIÓN
DEPARTAMENTO CONTABLE PRESUPUESTARIO
DEPARTAMENTO DE RECURSOS MATERIALES

INDICE

RESUMEN EJECUTIVO

Informe de Auditoría Interna AI JPS N° 01-2015

Esta Auditoría incluyó dentro del Programa de Trabajo para el Área de Auditoría de Sistemas del año 2014, un estudio sobre el seguimiento de recomendaciones giradas mediante informes, así como, las advertencias emitidas a través de notas.

El objetivo general del informe, consistió en verificar si los Departamentos que conforman la Administración Activa de la Junta de Protección Social han cumplido con las recomendaciones y advertencias emitidas por el Área de la Auditoría de Sistemas.

El alcance del presente estudio abarcó las recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, en los siguientes informes:

- AI JPS N° 22-2012 *"Verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la Junta de Protección Social por medio de los socios comerciales".*

- AI JPS N° 04-2013 *"Manejo del fondo y la bolsa para el pago de premios de la lotería pega millones en la determinación de utilidades".*

- AI JPS N° 05-2013 *"Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante Informes AI JPS N° 26-2011 y advertencias emitidas mediante notas".*

- AI JPS N° 17-2013 *"Estudio sobre las compras de equipos de cómputo realizadas a Componentes El Orbe, S.A, comprendidas entre los periodos 2009, 2010 y 2011 inclusive".*

Además, abarca las advertencias giradas por esta Auditoría Interna durante el año 2013 y el primer semestre del 2014.

Dentro de los resultados del estudio se determinó:

➢ Del total de recomendaciones giradas en los informes previamente citados, se comprobó que de 103 recomendaciones, 51 fueron cumplidas, 25 están parcialmente cumplidas y 27 se encuentran pendientes.

- De 27 recomendaciones que se encuentran pendientes, 7 pertenecen al Informe AI JPS N° 22-2012, 2 al Informe AI JPS N° 4-2013, 13 al Informe AI JPS N° 05-2013 y 5 al Informe AI JPS N° 17-2013

- De las 26 advertencias realizadas por el área de Auditoría de Sistemas, se determinó que a la fecha del informe se encuentran 13 de ellas cumplidas, 2 parcialmente cumplidas y 11 se encuentran pendientes.

Es importante mencionar, que las recomendaciones y advertencias emitidas en las diferentes notas e informes están dirigidas a fortalecer el control interno de la Institución.

1. INTRODUCCIÓN

1.1 Origen de la auditoría

El siguiente estudio corresponde al Programa de Trabajo del Área de Auditoría de Sistemas del año 2014.

1.2 Objetivo general

Verificar si las unidades administrativas que conforman la Junta de Protección Social, han cumplido con las recomendaciones y advertencias que fueron giradas por el Área de la Auditoría de Sistemas.

1.3 Alcance de la auditoría

El estudio abarcó las recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, a través de los informes AI JPS N° 22-2012 *"Verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la junta de protección social por medio de los socios comerciales"*, AI JPS N° 04-2013 *"Manejo del fondo y la bolsa para el pago de premios de la lotería pega millones en la determinación de utilidades"*, AI JPS N° 05-2013 *"Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante Informes AI JPS N° 26-2011 y advertencias emitidas mediante notas"*, AI JPS N° 17-2013 *"Estudio sobre las compras de equipos de cómputo realizadas a Componentes El Orbe, S.A, comprendidas entre los periodos 2009, 2010 y 2011 inclusive"*, además de las advertencias giradas por medio de notas por esta Auditoría Interna durante el período 2013 y el primer semestre del 2014.

1.4 Metodología

Para el presente estudio, el Área de Sistemas utilizó la siguiente metodología:

1. Revisión de la documentación recibida de la Administración Activa, donde informan acerca del cumplimiento de las recomendaciones que se giraron en los informes, para verificar el cumplimiento de las mismas.

2. Revisión de la documentación recibida de la Administración Activa, referente a las advertencias giradas a través de notas, para verificar el cumplimiento de las mismas.

3. Solicitar a las diferentes áreas del Departamento de Tecnologías de Información, la documentación necesaria para verificar cada una de las recomendaciones emitidas por la Auditoría de Sistemas.

4. Se efectuaron consultas a los responsables de las funciones de la Administración Activa y se verificó la información tanto física como de datos, para determinar el cumplimiento de las recomendaciones.

5. Las actividades fueron realizadas de acuerdo con la normativa aplicable al ejercicio de la Auditoría.[1]

1.5 Normativa sobre deberes en el trámite de Informes de Auditoría.

De conformidad con lo que establece la Contraloría General de la República, se transcriben los artículos Nº 36, 37, 38 y 39 de la Ley General de Control Interno Nº 8292, publicada en La Gaceta Nº 169 de 04 de setiembre del 2002.

> ***"Artículo 36.- Informes dirigidos a los titulares subordinados***
>
> *Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
>
> *a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.*
>
> *b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de*

[1] Norma 205.7 del Manual de Normas Generales de Auditoría para el Sector Público y Norma 1.3.3 de las Normas para el ejercicio de la Auditoría Interna en el Sector Público.

recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."

"Artículo 37.- Informes dirigidos al jerarca

Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente."

"Artículo 38.- Planteamiento de conflictos ante la Contraloría General de la República

Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.

La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, Nº 7428, de 7 de setiembre de 1994."

www.jps.go.cr • Tel.: (506) 2527 2000 • Apdos.: 1979-1000 / 592-1000 • San José, Costa Rica

Artículo 39.- Causales de responsabilidad administrativa

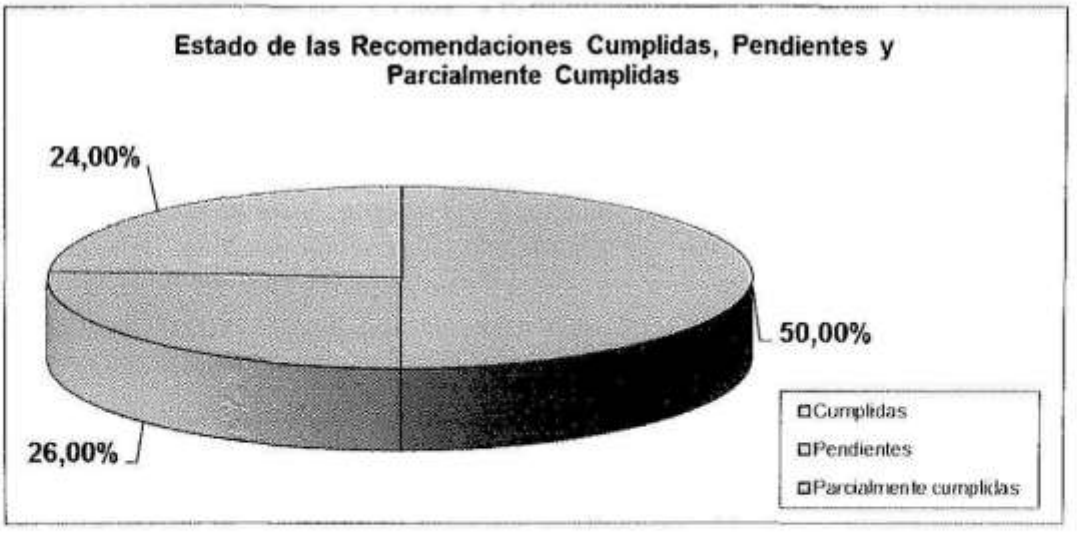
El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios...."

2. RESULTADOS DEL ESTUDIO

A. Al verificar el cumplimiento de las recomendaciones giradas en los diferentes informes, según el período indicado en el alcance de este informe, se comprobó que del 100% de estas recomendaciones un 50% fueron cumplidas, un 24% se encuentran parcialmente cumplidas y el 26% aún están pendientes (Ver Anexo 1, y Anexo 2). El siguiente cuadro muestra el detalle de lo citado:

Estado de la recomendación	Cantidad de recomendaciones	% de cumplimiento
Cumplidas	51	50%
Parcialmente cumplidas	25	24%
Pendientes	27	26%
Total de recomendaciones	**103**	**100%**

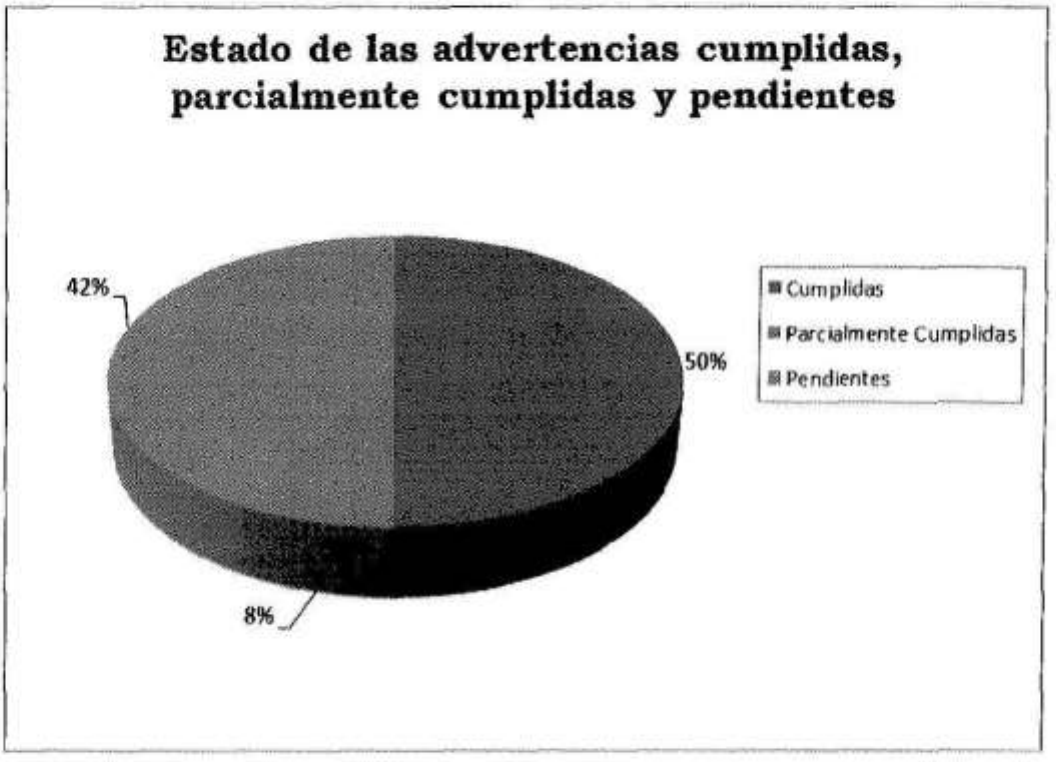
Adicionalmente presentamos en forma gráfica, el estado de las recomendaciones según el cuadro anterior:



B. De las advertencias emitidas por el Área de Sistemas de la Auditoría Interna, según el alcance de este estudio, se determinó que del 100% de éstas un 50% fueron cumplidas, un 8% se encuentran parcialmente cumplidas y el 42% aún están pendientes (Ver Anexo N° 3 y Anexo N° 4). El siguiente cuadro presenta el detalle de lo antes citado:

Estado de las advertencias	Cantidad de advertencias	% de cumplimiento
Cumplidas	13	50%
Parcialmente cumplidas	2	8%
Pendientes	11	42%
Total de Advertencias	**26**	**100%**

A continuación, presentamos en forma gráfica, el estado de las advertencias según el cuadro anterior:



C. Es importante mencionar, que del total de las 103 recomendaciones, 26 forman parte del informe AI JPS N° 22-2012, 13 pertenecen al informe AI JPS N° 4-2013, 52 al informe AI JPS N° 05-2013 y 12 al informe AI JPS N° 17-2013.

El siguiente resumen, muestra para cada informe y por unidad administrativa, la cantidad de recomendaciones que se encuentran cumplidas, parcialmente cumplidas y pendientes: (Ver un detalle ampliado en Anexo 5)

Cantidad de recomendaciones cumplidas, parcialmente cumplidas y pendientes, por Informe y por Departamento

Informes		Recursos Materiales			Informática			Contabilidad			Total
		PC	C	P	PC	C	P	PC	C	P	
22-2012	Verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la junta de protección social por medio de los socios comerciales.				3	16	7				26
4-2013	Manejo del fondo y la bolsa para el pago de premios de la lotería pega millones en la determinación de utilidades.							2	8	3	13
05-2013	Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante Informes AI JPS N° 26-2011 y advertencias emitidas mediante notas.				17	22	13				52
17-2013	Estudio sobre las compras de equipos de cómputo realizadas a Componentes El Orbe S.A, comprendidas entre los periodos 2009, 2010 y 2011 inclusive.	1	4	4	1	1	1				12
	Total:	1	4	4	21	39	21	2	8	3	103

Simbología
PC = Parcialmente Cumplida
C = Cumplida
P = Pendiente

En relación con los puntos citados, es importante indicar lo que establece la Ley General de Control Interno N° 8292 publicada en La Gaceta N° 169 del 4 de setiembre del 2002, en lo que interesa:

Capítulo III, La Administración Activa;

SECCION I;

"1. ***Deberes del jerarca y los titulares subordinados***
Artículo 12.- Deberes del jerarca y de los titulares subordinados en el sistema de control interno...

c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan."

Capítulo IV,

SECCION IV,

Informes de auditoría interna:

*"Artículo 36. – **Informes dirigidos a los titulares subordinados.** Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:*
a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados.

b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además, deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas

propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes.

c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda."

3. CONCLUSION

Del total de 103 recomendaciones giradas por la Auditoría Interna a través de los informes, 27 recomendaciones aún no habían sido cumplidas y 25 estaban parcialmente cumplidas, esto para un total de 52 recomendaciones, lo que indica que un 49% de las mismas no habían sido cumplidas en su totalidad.

En el caso de las advertencias giradas, de un total de 26, 11 se encuentran pendientes y 2 están parcialmente cumplidas, de igual forma, esto señala que casi un 50% de éstas, no se encuentran totalmente cumplidas.

Es importante indicar que las recomendaciones y advertencias pendientes de cumplir o parcialmente cumplidas no son solamente de los años 2013 y 2014, algunas de ellas vienen pendientes de años anteriores, manteniendo dicho estatus, lo anterior, señala una falta de interés por parte de la jefatura del Departamento de Tecnologías de la Información, por cumplir la totalidad de las recomendaciones y advertencias.

Asimismo, el señor Ronald Ortíz Méndez, mediante nota I-328 del 15 de marzo del año 2013 (dirigida al señor Francisco Ibarra Arana), indica que algunas recomendaciones fueron cumplidas y otras se cumplirían en el año 2014, no obstante, según este seguimiento, todavía existen recomendaciones sin cumplir.

Es importante mencionar que, la aplicación de las recomendaciones, permite fortalecer la estructura de control interno, misma que se encuentra inmersa en las diferentes funciones que se llevan a cabo en nuestra Institución. Se colabora con la Administración Activa, por cuanto los informes que lleva a cabo esta Auditoría Interna, ayudan al logro de los objetivos y metas institucionales establecidas en el Plan Anual Operativo, así como para la protección del Patrimonio Público.

4. RECOMENDACIONES

Al señor Milton Vargas Mora, Gerente General, con base en el presente informe se solicita:

1. Girar instrucciones por escrito a los señores Ronald Ortiz Méndez, Jefe del Departamento de Tecnología de la Información, Rafael A. Oviedo Chacón, Jefe a.i. del Departamento de Contabilidad y Presupuesto y a la señora Mary Valverde Vargas, Jefe a.i. Departamento de Recursos Materiales, para que procedan al cumplimiento de las recomendaciones y advertencias pendientes de aplicar que se detallan en el Anexo N° 1 y Anexo N° 2 conforme lo establece la Ley General de Control Interno.

2. Solicitar a los señores Ronald Ortiz Méndez, Jefe del Departamento de Tecnología de la Información, Rafael A. Oviedo Chacón, Jefe a.i. del Departamento de Contabilidad y Presupuesto y Mary Valverde Vargas, Jefe a.i. Departamento de Recursos Materiales el cronograma de cumplimiento de las mismas, en un plazo no mayor a diez días hábiles, con copia a esta Auditoría Interna.

5. OBSERVACIONES DE LA ADMINISTRACIÓN

El día 15 de enero de 2015, se realizó la conferencia de resultados del presente informe, en la Sala de Sesiones de Junta Directiva, por parte de la Administración Activa asistió el señor Milton Vargas Mora, al cual le fueron presentados los resultados del estudio, contándose además con la participación del señor Ronald Ortiz Mendez, Jefe del Departamento de Informática, y por esta Auditoría Interna asistieron la señora Viviana Rivera Barrantes y el señor Jose Wong Carrion.

Al finalizar la comunicación del estudio, se consignaron las siguientes observaciones en el *"Acta de Conferencia de Resultados"*:

1. Valorar el uso de la firma digital, para lo cual el Departamento de Tecnología de la Información realizará un estudio de costo - beneficio.

2. El Departamento de Tecnología de la Información verificará el alcance de la contratación adjudicada a la empresa Deloitte para que realizara el

seguimiento de recomendaciones debido a que en apariencia no todos los informes fueron contemplados.

Licda. Viviana Rivera Barrantes, MAP
Profesional III

Lic. José Wong Carrion
Jefe Área de Sistemas

MBA. Rodrigo Carvajal Mora
Subauditor Interno

ANEXO N° 1

Detalle de las recomendaciones emitidas por el Área de Sistemas de la Auditoría Interna (Pendientes y Parcialmente Cumplidas)

Informe AI JPS N° 32-2010 Estudio sobre la verificación de la seguridad en la comunicación de datos entre los entes externos y la institución, relacionada con los productos que comercializa la junta de protección social

Dirigido a: Departamento Tecnologías de la Información **Fecha** 28 de diciembre, 2010

Recomendación	Estado de la recomendación	Seguimiento
A. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO ALTO		
2.Validación de usuarios en Sitio Web. Se recomienda realizar una implementación de un segundo factor de autenticación para los usuarios en línea del tipo contraseña de un solo uso (One Time Password OTP), además, otra opción de validación recomendada es una infraestructura de llave pública (Public Key Infrastructure, PKI) que soporte la utilización de Firma Digital (DS – Digital Signature) para validar las transacciones que realiza cada uno de los clientes una vez autenticados en el sitio transaccional. Adicionalmente, es necesario que se facilite a los usuarios del servicio información sobre las ventajas que tiene el conocer los riesgos de seguridad asociados al uso de la aplicación, así como la importancia de mantener sus equipos debidamente actualizados con las recomendaciones del vendedor del producto (ISO 27002 8.2.2.).	Parcialmente Cumplida	A través del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se citó: *"1. Se deshabilitó el sitio web transaccional http://secure.jps.go.cr/jpsvirtual/login.html ya que dicho sitio dejo de ser utilizado por la Institución.* *2. Se implementó la plataforma Citrix que dentro de sus funcionalidades realiza el cambio de premios, despachar lotería, entre otros. Esta plataforma posee un mecanismo de autenticación basado en tres pasos (ver evidencia adjunta) lo que refuerza el mecanismo de seguridad y/o de acceso a la plataforma.* *3. Se Implementó a partir de febrero de 2014 un programa de capacitación y sensibilización con el fin de concientizar a los usuarios sobre los peligros y riesgos de seguridad presentes en el uso de las Tecnologías de Información, y para proporcionar las herramientas y mecanismos para prevenir los diversos riesgos en materia de seguridad de la información"* *"Los sitios web de cajeros y agencias tienen listo el pase a producción por parte del departamento de TI para su migración a la plataforma Citrix, sin embargo por parte del Banco de Costa Rica se ha puesto resistencia indicando que se deben ejecutar una serie de pruebas de parte del Banco.*

		El día 3 de Julio del 2014 se efectuó una sesión con personeros del área de mesa de ayuda y seguridad informática del Banco de Costa Rica con el fin de lograr migrar los sitios web de cajeros y agencias a la plataforma Citrix para los cajeros del BCR. De parte de la JPS se informa que todo está listo y por parte del Banco se está a la espera. En dicha sesión se atendieron las consultas de los personeros de TI del BCR con respecto a la plataforma Citrix y finalmente se estaría esperando el aval del Banco para realizar la migración." En la revisión efectuada a la tabla *"SG_Usuarios"* del 26 de agosto, se comprobó que existen varios usuarios que no están utilizando firma digital, así como tampoco socios comerciales, entre ellos están: **Codigo Usuario** / **Login** / **Nombre1** / **Apellido1** / **Firma Digital** 3983 / 02-0650-0836 / Laura / Vargas / N 3796 / 01-1126-0419 / Ingrid / Martinez / N 3749 / 06-0299-0801 / Yury / Castillo / N 3728 / 07-0132-0158 / Benjamín / Cáceres / N 3722 / 01-1506-0467 / Fabian / Amador / N 3683 / 01-1550-0839 / Yorlyn / Mora / N 3675 / 02-0362-0962 / Raul / Guzmán / N 3647 / 01-0556-03970104 / Linny / Villalobos / N 3648 / 01-0556-03970105 / Adriana / Villegas / N Si bien es cierto, a nivel interno en su mayoría se está utilizando la firma digital, aún en los puntos de ventas para cambios de premios, no poseen un segundo factor de autenticación.
3.Infraestructura del sitio transaccional. Establecer una protección de tres capas en la zona desmilitarizada (DMZ), así como analizar la posibilidad de instalar equipos (Sistemas de Detección de Intrusiones) de tal manera que estas sean validadores del contenido de los paquetes que trasiegan por la red, identificando de esta manera la probabilidad de que un paquete malicioso se	Parcialmente Cumplida	A través del oficio GG.1847-2014 del 8 de agosto del 2014 del Informe adjunto *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, se respondió: *"1. La implementación de la nueva de red (cambio en ubicación del centro de datos y actualización de equipos de red) demuestra la actual arquitectura de red basada en capas y segmentada con la creación de redes*

encuentra dentro de la red que pueda comprometer los servicios el cual se ofrecen. Desligar la responsabilidad de temas de seguridad de la Dirección de Tecnología de Información. Contar con personal especializado en temas de seguridad y con experiencia en entidades financieras y procesos de aseguramiento transaccional de sitios Web. Llevar a cabo las gestiones necesarias para establecer una Sección de Seguridad de la Información que sea la encargada de los temas de seguridad en la infraestructura, esta unidad debe reportar directamente a la Junta Directiva de la Institución y contar con las herramientas de capacitación y equipos recomendados para su gestión, así mismo, debe ser el ente encargado de monitorear los servicios en un modelo de 24/7/365 dada la actividad de la Institución.		*virtuales privadas (VPN). En la topología de red se muestra la segmentación de la red y la separación de la infraestructura de servidores, red LAN interna, firewall y las sucursales. (Ver imagen de topología de la red adjunta). La estructura actual posee dos niveles de seguridad con el firewall basado en una arquitectura en clúster y el equipo controlador de entrega F5.* *2. Se han desarrollado las gestiones necesarias por parte de la Dirección de Tecnologías de la Información para establecer la Sección de Seguridad de la Información dentro de la organización. De acuerdo con el Plan Estratégico de TI (PETI) 2014-2017 se adiciono dentro del organigrama del departamento de TI el área de Seguridad de la Información, no obstante la alta gerencia no ha avalado la plaza para el oficial de seguridad de TI. Por lo tanto se implementó una iniciativa por parte de la Dirección de TI de realizar una contratación externa con un proveedor con experiencia en trabajos de seguridad de la información para gestionar reforzar y obtener retroalimentación en el tema de seguridad. Se está a la espera de recibir la aprobación de dicha plaza para disponer de un funcionario en la ejecución de labores de seguridad de la información y la definición de la estrategia de ejecución de las funciones a realizar.* *El funcionario a cargo de la seguridad de TI, es importante que cuente con al menos alguna certificación que lo capacite en el área de seguridad de TI. La organización debe analizar la viabilidad y lo que mejor se apega a sus objetivos estratégicos, si desligar lo oficina de seguridad de la información del área de TI o bien incluida dentro de dicha unidad organizativa (Es importante tener clara la diferencia entre seguridad de la información y seguridad informática, ver sección de glosario). La alta dirección debe reflexionar sobre el aval de la plaza de seguridad de la información, independientemente de donde se situé jerárquicamente. Si es indispensable que la JPS cuente con personal especialista en el tema de seguridad de la información dentro de la Junta de Protección Social. Destacar que la decisión no es del departamento de Tecnologías de Información, ya que es un tema que trasciende a nivel de la alta dirección."* Pese, a que el Departamento de Tecnologías de Información ha mejorado la infraestructura tecnológica aún no sea establecido una Sección de Seguridad de la Información donde además ofrezca un servicio de 24/7/365.

7.Debilidades en los parámetros de contraseña

Realizar un análisis de los parámetros de contraseña activos en los software de sistemas (Sybase, Sun Solaris, Windows Server 2008 y Aplicación Web transaccional) donde se especifique los parámetros a utilizar en estas. A continuación se presenta la recomendación de parámetros:

Política	Valor
Longitud mínima contraseña	seis o más
Máximo contraseña edad (en días)	30 a 90
Edad mínima de la contraseña (en días)	0 a 1
Contraseña historia tamaño	seis o más
Complejidad contraseña	Activado
Bloqueo de umbral (intentos fallidos)	tres

Pendiente

Al extraerse la información de la base de datos, sobre los usuarios del Departamento de Tecnologías de la Información, se detectó lo siguiente:

- *Usuarios con la longitud mínima de contraseña:* 6 (Configurada por su valor por defecto).
- *Expiración del password:* 0 (Configurada por su valor por defecto, no permite verificar el vencimiento de contraseñas).

En la configuración de la base de datos del comando *"sp_configure"*, se observó que aún hay parámetros con su valor por defecto:

Parameter Name	Default	Memory Used	Config Value	Run Value	Unit	Type
auditing	0	0	1	1	switch	dynamic
check password for digit	0	0	0	0	switch	dynamic
minimum password length	6	0	6	6	bytes	dynamic
allow remote access	1	0	1	1	switch	dynamic

- *Minimum password length:* los campos de *"valor"* y *"run"* poseen el valor por defecto en 6 cuando lo recomendable es 8.
- *Check password for digit:* los campos de *"valor"* y *"run"* poseen el valor por defecto en 0 lo cual indica que la complejidad de las contraseñas no está activa.

En la consulta realizada a la base de datos el 26 de agosto del 2014, a través del parámetro *"sp_helpserver"* con el fin de detectar cual servidor posee conexión remota, se determinó que existen 4 servidores, en donde ya no se está utilizando el modelo de encriptación *"RPC modelo de seguridad A"* ni el recomendado según la sana práctica *"Modelo de seguridad RPC B"* como puede observarse:

Name	Network_name	Class	Status
NODO1	NODO1	local	no timeouts, no net password encryption, writable , enable login redirection
NODO1_XP	NODO1_XP	RPCServer	no timeouts, no net password encryption, writable , enable login redirection
NODO2_BS SYB_BACK UP	NODO2_BS	ASEnterprise	timeouts, no net password encryption, writable , enable login redirection
NODO1	NODO1_BS	[NULL]	

Por medio del reporte *"Informe de Usuarios por Perfil que contenga 'seguridad'"* con fecha 27 de octubre del 2014, se evalúo cuales usuarios se encontraban como administradores de la Web Transaccional y se determinó que existen usuarios que están definidos como administradores, entre ellos están: *"Jairo Cruz Sibaja, Luis Ramírez Arroyo, Randall Espinoza Flores, Ronald Ortiz Méndez"*, siendo algunos de estos funcionarios analistas. Mediante oficio GG.1847-2014 del 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se indicó:

> *"... Para este punto cabe indicar que esta plataforma de web transaccional ya no existe y su funcionalidad se deshabilito."*

8.Cuentas de usuario asociadas a ex-funcionarios. Inactivar los usuarios indicados en el punto No. 8 de Resultados del Informe 32-2010 denominado *"Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social"*.	Parcialmente Cumplida	Al revisar los datos de la tabla RH_Empleados, se comprobó que 3 personas estaban inactivas en dicha tabla, pero a su vez se encontraban activos en la tabla syslogins. Ellos son:

Codigo Empleado	Suid	Nombre Empleado	Estado Puesto
1094	5382	Thompson Rodriguez Carlos Manuel	I

<table>
<tr>
<td>Realizar una revisión de la totalidad de los usuarios de la plataforma de tecnología, para identificar si existen usuarios adicionales a los indicados en el punto 8 de Resultados del Informe 32-2010 denominado "Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social", que deban ser deshabilitados.

Coordinar con el Área de Recursos Humanos, el proceso a seguir cuando se presente la salida de un funcionario.</td>
<td></td>
<td>
<table>
<tr><td>855</td><td>5375</td><td>Salazar Sanchez Edgar</td><td>I</td></tr>
<tr><td>522</td><td>4196</td><td>Jimenez Quiros Lilliana M</td><td>I</td></tr>
</table>
</td>
</tr>
<tr>
<td><u>9.Debilidades en la seguridad de la información en los contratos con socios comerciales y canales de distribución.</u>
Fortalecer las medidas de seguridad indicadas en los contratos con los socios comerciales y canales de distribución para brindar una protección adecuada tanto a la Junta de Protección Social y a los Socios Comerciales.</td>
<td>Pendiente</td>
<td>En relación con las cédulas jurídicas, se determina por medio de un muestreo de la tabla "syslogins" el día 2 de octubre del 2014, que existen diferentes números de cédula para un mismo socio comercial:

Así mismo, en la tabla syslogins actualizada al 2 de octubre del 2014, se encontraron los siguientes:
<table>
<tr><th>Status</th><th>Name</th><th>Fullname</th></tr>
<tr><td>0</td><td>L03033703130101</td><td>Alberto Vargas Royo (socio)</td></tr>
<tr><td>0</td><td>L03033703130201</td><td>Alberto Vargas Royo (socio)</td></tr>
<tr><td>0</td><td>L0112800486</td><td>Alejandro Fernandez Diaz (soci</td></tr>
<tr><td>0</td><td>L0112810486</td><td>Alejandro Fernandez Diaz (soci</td></tr>
<tr><td>0</td><td>L031011921110401</td><td>Cadico Taras (Socio Comercial)</td></tr>
<tr><td>0</td><td>L031011921110201</td><td>Cadico Tejar (socio Comercial)</td></tr>
<tr><td>0</td><td>L01041704410101</td><td>Carlos Cruz Chan (Socio C)</td></tr>
<tr><td>0</td><td>L01041704410201</td><td>Carlos Cruz Chan (Socio C)</td></tr>
<tr><td>0</td><td>L031014290220101</td><td>Cellsoft (socio)</td></tr>
<tr><td>0</td><td>L031014290220102</td><td>Cellsoft (socio)</td></tr>
<tr><td>0</td><td>L031014290220103</td><td>Cellsoft (socio)</td></tr>
<tr><td>0</td><td>L0110770563</td><td>Cindy Coronado Duarte (BCR)</td></tr>
<tr><td>0</td><td>L0113420259</td><td>Cindy Coronado Duarte (BCR)</td></tr>
<tr><td>0</td><td>L030040566010102</td><td>Coopeflores San Joaquin (socio</td></tr>
<tr><td>0</td><td>L030040566010105</td><td>Coopeflores San Joaquin (socio</td></tr>
<tr><td>0</td><td>L030040566010106</td><td>Coopeflores San Joaquin (socio</td></tr>
<tr><td>0</td><td>L030040566010107</td><td>Coopeflores San Joaquin(socio)</td></tr>
</table>
</td>
</tr>
</table>

		0	L0204520942 Edgar Espinoza Jiménez BCR
		0	L0401820506 Edgar Espinoza Jiménez BCR
		0	L01042303910101 Gallinita Feliz (socio)
		0	L01042303910102 Gallinita Feliz (socio)
		0	L01042303910103 Gallinita Feliz (socio)
		0	L01042303910104 Gallinita Feliz (socio)
		0	L01042303910202 Gallinita Feliz (socio)
		0	L0102550799 Gonzalo Lizano Vindas
		0	L0102250799 Gonzalo Lizano Vindas (SIAB)
		0	L0401110581 Guillermo Sancho Loaiza Heredi
		0	L0108520221 Guillermo Sancho Loaiza Herred
		0	L0110080257 Jason Barrantes Zamora (BCR)
		0	L0207250291 Jason Barrantes Zamora (BCR)
		0	L0303140674 Jorge Rosales Gordon (socio)
		0	L03031406740103 Jorge Rosales Gordon SC 03
		0	L03031406740104 Jorge Rosales Gordon SC 04
		0	L0112410191 Karen Valverde Solis (socio)
		0	L030040566010103 Karen Valverde Solis (socio)
		0	L0113530783 Karol Jimenez Umaña (SIAB)
		0	L0502640301 Karol Jimenez Umaña (SIAB)
		0	L0302660721 Luis Ramirez Vargas (BCR)
		0	L0106970985 Luis Ramírez Vargas BCR
		0	L0112150521 Orlando Gomez Gamboa (socio)
		0	L01121505210101 Orlando Gomez Gamboa (socio)
		0	L0800930013 Rosa Chacon Gadea (BCR)
		0	L0207480513 Rosa Chacón Gadea (BCR)
		0	L0206110238 Sara Quesada Garita (BCR)
		2	L0206110235 Sara Quesada Garita BCR
		2	L0119580306 Usuario para backup
		0	backup_user Usuario para backup
		0	L0203390680 Victor Ramirez Rojas
		0	L0205650707 Victor Ramirez Rojas (socio)
		0	L0401440164 Victor Vargas Oviedo (socio)

		0 L0300405660010109 Victor Vargas Oviedo (socio) 0 L0104500195 David Navarro Hernandez 0 L0109500620 David Navarro Hernández 0 L0113090087 David Soto Rodriguez (BCR) 0 L0109480066 David Soto Rodriguez (BCR) 0 L0108617709 Diego Paez Burgos (BCR) 0 L0801000656 Diego Paez Burgos BCR Por otro lado, a través del oficio I 54-13 del pasado 22 de enero del 2013 se incluyó la cláusula vigésima sétima que se suscribe con los socios comerciales, la cual indica: *"... la Junta le suministra al SOCIO COMERCIAL y a cada uno de los autorizados por este, una clave de identificación o PIN individual y secreta. ..."*
B. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO MEDIO		
10.Protección contra código malicioso. Se debe considerar realizar revisiones y actualizaciones del software antivirus en forma diaria. Además configurar esta herramienta para que cubra todos los sistemas y equipos existentes en la red, con esto apoyara la gestión en temas de seguridad y prevención de software malicioso que pueda llevar a mayores situaciones incidentales en la infraestructura. Efectuar un estudio de costo beneficio con la finalidad de establecer un proceso de revisión mínima mensual en los equipos de los socios comerciales que se conectan a la red, para evaluar el estado de la seguridad local de los equipos y sus puntos de acceso a internet. Del resultado de dicho estudio enviar copia a la Auditoría Interna. Implementar herramientas de análisis de vulnerabilidades para los diferentes sistemas y roles existentes en la red.	Parcialmente Cumplida	En el oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el Departamento de Tecnologías de la Información"*, donde se respondió: *"1. Se implementó un proceso de monitoreo diario con el programa antivirus con el fin operar proactiva y reactivamente en eventos o incidentes que reporte dicho sistema con el fin mantener a la organización protegida del malware, equipos debidamente actualizados y toma de acciones correctivas. Los equipos que pertenecen a la Junta de Protección Social y que se encuentran en el dominio institucional cuenta los controles de seguridad antimalware respectivamente activos.* *2. Con el fin de salvaguardar la seguridad institucional se habilito para los socios comerciales una campaña de consejos de seguridad de la información con el fin de salvaguardar la seguridad institucional en los sistemas institucionales a los que acceden (cambio de premios, despacho loterías).* *3. Se desarrolló y ejecutó un análisis de vulnerabilidades a toda la plataforma tecnológica institucional incluidas las sucursales mediante el uso de la herramienta de análisis de vulnerabilidades Nessus. Adicionalmente se hizo una revisión aleatoria pare determinar el*

<table>
<tr>
<td></td>
<td></td>
<td>software instalado en los equipos. A raíz de esta revisión se estableció una política a nivel de active director que únicamente los usuarios con privilegios pueden instalar software. (Ver anexo 37 – Estado de instalación de software autorizado)"

En la revisión efectuada al anexo 37 señalado anteriormente, indica:

"Durante la revisión se determinó la presencia de equipos que aún mantienen el sistema operativo Windows XP. Es preocupante aún la gran cantidad de equipos que cuenta con este sistema operativo..."

Por lo que, se procedió a consultar el listado de equipos con Windows XP, y se determinó que aún existen máquinas con este sistema operativo.

Asimismo, en el análisis de vulnerabilidades Nessus, se comprobó las siguientes vulnerabilidades:

1. Equipos con S.O. Windows XP
2. Versión de open SSH vulnerable
3. Mikro Tik Roter OS Sin Contraseña
4. Múltiples vulnerabilidades en Servicio Samba
5. Versión vulnerable de PHP
6. Versión HP System Management HomePage
7. Debilidades en Certificados SSL

Además, no se logró comprobar si el Departamento de Tecnologías de la Información realizó el estudio de costo beneficio, para realizar la revisión de los equipos de los socios comerciales, los cuales se conectan a la red institucional.</td>
</tr>
<tr>
<td><u>13.Roles de la base de datos sybase sin contraseña.</u>
Realizar un análisis de la ausencia de contraseñas en los roles definidos en el motor de base de datos, asignar la contraseña respectiva y guardar los password en sobres sellados y autorizados por la Jefatura del Departamento de Informática.</td>
<td>Parcialmente Cumplida</td>
<td>Al hacer una revisión el 26 de agosto del 2014 a la tabla "syssrvroles" se comprobó que los siguientes roles no poseen contraseñas:

<table>
<tr><th colspan="2">Name</th></tr>
<tr><td>sa_role</td><td>mon_role</td></tr>
<tr><td>sso_role</td><td>js_admin_role</td></tr>
<tr><td>oper_role</td><td>messaging_role</td></tr>
<tr><td>sybase_ts_role</td><td>js_client_role</td></tr>
<tr><td>navigator_role</td><td>js_user_role</td></tr>
<tr><td>replication_role</td><td>webservices_role</td></tr>
</table>
</td>
</tr>
</table>

dtm_tm_role	keycustodian_role
ha_role	Sa_serverprivs_role

Por otro lado, en el oficio GG.1847-2014 del 8 de agosto del 2014 del Informe adjunto *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, se respondió:

> *"1. Se realizó en un ambiente de pruebas un análisis del resultado de la implementación del cifrado en los demás roles de la base de datos. El estudio efectuado determino la pérdida en la continuidad del servicio del motor de base de datos y afectación en la conexión con la consola de aplicaciones. En los anexos 18 y 19 se adjuntan los análisis efectuados y la determinante de la no aplicación del cifrado a los roles. ..."*

- En el anexo número 18 del informe citado, relacionado con la funcionalidad de los roles a nivel de Sybase, emitido por el señor Joaquín Casaw de la empresa Corporación Informática ODS S.A., mencionó:

> *"El asignar un password a los roles implica un nivel adicional de seguridad. Si un login tiene un role asignado y este no tiene password todas las funcionalidades del role quedan automáticamente activas con solo ingresar. ... Si el role tiene un password tendría además de conocer el password del login que conocer el password del role.*
> *Un inconveniente es que para activar el password de un role es necesario digitar el password y alguien podría estar observando y capturarlo.*
>
> *Herramientas como el DBArtisan abren una sesión por cada ejecución de comando de manera que tendrían que activar el role cada vez que ejecuten algo que necesite de los privilegios de un role.*
> *...*
>
> *Se debe tener cuidado con aplicaciones existentes que realicen tareas que necesiten de los privilegios de algún role como creación de logines y cambios de passwords puesto que al asignarles un*

		password al role este debe ser activado antes de ejecutar los comandos." • Asimismo, en el anexo número 19 del informe anterior, sobre el Estudio de la implementación de password a los roles de la BD, se citó: *"Ante esto se tomó la valoración de la configuración en otras bases de datos Sybase y la práctica no acostumbra a utilizar password en los roles, sin embargo si se toman las medidas de seguridad como las anteriores con el fin de proteger el acceso al motor de bases de datos.* *... la asignación de los password a los roles conllevaría afectar la continuidad en el servicio que presta el departamento de Tecnologías de Información , no obstante lo aportado por el área de seguridad es tomar las medidas anteriormente descritas con el fin de salvaguarda la seguridad del motor de base de datos. ..."* Al hacer una revisión del justificante para no incorporar la contraseña en los roles, no se consideró que las razones dadas sean suficientes para no acatar dicha recomendación, dado que se está poniendo en riesgo la seguridad de los datos, por lo que, tal y como lo señala el señor Casaw, el incorporar dicha contraseña, vendría más bien a ocasionar un nivel de seguridad adicional, el cual en vez de perjudicar la información, ayuda a protegerla. No obstante, se rescata el hecho de que el Departamento de Tecnología de la Información haya contratado una empresa externa para solucionar hallazgos encontrados por esta Auditoría, no obstante es importante que dicho Departamento tome en consideración las medidas definidas por esta, con el fin de cumplir con los controles de seguridad.
14.Debilidades en la asignación de roles sa_role y sso_role. Realizar un análisis de los roles y privilegios de los funcionarios para que estos se encuentren acorde a la naturaleza y funciones del puesto, en caso de no estarlo revocar estos permisos de forma inmediata.	Pendiente	A través del oficio GG.1847-2014 del 8 de agosto del 2014 del Informe adjunto *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, se respondió: *"1. Se deshabilito el usuario L0119580306 y sc007xdBuser del motor de base de datos.* *2. Se deshabilito al usuario mmasis los roles que no le correspondían, asignando únicamente los roles que le competen a su función."*

<table>
<tr>
<td></td>
<td></td>
<td>En la revisión efectuada al informe 05-2013 "Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante Informe AI JPS N° 26-2011 y advertencias emitidas mediante notas.", específicamente esta recomendación, se observó los usuarios mmasis, L0119580306, sc007xdBuser. Al hacer la comprobación de los usuarios con role sa_role y sso_role de la base de datos actualizada al 2 de octubre del 2014, se detectó que los usuarios mmasis, sc007xdBuser se encuentran activos, y por otro lado, al comparar la información actual con respecto al informe anterior, se observó la inclusión del usuario backup_user asignado a estos roles; con relación al usuario L0119580306 se encuentra inactivo, lo cual significa que en cualquier momento podría volverse activar.</td>
</tr>
<tr>
<td><u>16.Usuarios finales asociados a la tabla master.</u>
Realizar un análisis de los usuarios mencionados en el punto No. 16 de resultados del Informe 32-2010 denominado "Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social", para verificar que sus funciones se encuentren asociadas a tablas adecuadas y pertenezcan a tablas creadas por defecto del motor de base de datos Comunicar a la Auditoría Interna sobre el resultado de este análisis.</td>
<td>Pendiente</td>
<td>En la consulta realizada a la base de datos "master" el 2 de octubre del 2014, se comprobó que existen cuentas activas, se debe recordar que únicamente los usuarios administradores deben tener acceso. Así mismo, en dicha lista se muestran usuarios que no corresponden a funcionarios institucionales. Los que se identificaron son:
<table>
<tr><th>Suid</th><th>Status</th><th>Accdate</th><th>Name</th><th>Fullname</th></tr>
<tr><td>1</td><td>0</td><td>26/09/2011</td><td>Sa</td><td>[NULL]</td></tr>
<tr><td>4989</td><td>0</td><td>27/07/2012</td><td>master_maint</td><td>[NULL]</td></tr>
<tr><td>4988</td><td>0</td><td>27/07/2012</td><td>jps_maint</td><td>[NULL]</td></tr>
<tr><td>5421</td><td>0</td><td>01/10/2014</td><td>L0114890279</td><td>[NULL]</td></tr>
<tr><td>5422</td><td>0</td><td>01/10/2014</td><td>L0115740779</td><td>[NULL]</td></tr>
<tr><td>5423</td><td>0</td><td>01/10/2014</td><td>L0115240273</td><td>[NULL]</td></tr>
<tr><td>5424</td><td>0</td><td>01/10/2014</td><td>L0503730746</td><td>[NULL]</td></tr>
<tr><td>3</td><td>0</td><td>08/05/2012</td><td>Replica</td><td>administrador de replicación</td></tr>
</table>
En el informe 05-2013 "Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante Informe AI JPS N° 26-2011 y advertencias emitidas mediante notas.", de esta recomendación no se observaron los números de cédulas antes descritos.

Por otro lado, en el oficio GG.1847-2014 del 8 de agosto del 2014 se</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>adjuntó el Informe "Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información", donde se indicó:

"... Por lo tanto no existe algún tipo de amenaza, sin embargo por estética si se efectuó el cambio a la base de datos de seguridad.
Este punto únicamente se dejaron los usuarios asociados a la tabla master que así lo requerían de acuerdo a la funcionalidad dentro del motor de la Base de datos."

Con base en lo anterior, se comprobó que a pesar de que dejaron usuarios en la tabla master ("sa", "master_maint", "jps_maint", "replica") otros fueron creados.</td>
</tr>
<tr>
<td><u>17.Existencia de usuarios genéricos y duplicados.</u>
Se recomienda realizar un análisis de las cuentas de usuario genéricas y duplicadas identificadas en el punto N° 17 de Resultados del Informe 32-2010 denominado "Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social", valorando su mantención o eliminación de acuerdo a las funciones dentro del software de sistema y crear una lista de las cuentas genéricas que no se pueden eliminar, con el fin de documentar el usuario responsable de dicha cuenta y la función por la cual se mantiene. Comunicar a la Auditoría Interna sobre el resultado de este análisis.</td>
<td>Pendiente</td>
<td>En la revisión efectuada a las tablas SG_Usuarios y syslogins, se comprobó:

• Usuarios duplicados.
• Números de cédulas asociadas a usuarios inexistentes.
• Logins que no corresponden a ningún número de cédula.
• Funcionarios no existentes.
• Cédulas relacionadas con otras personas.

A continuación, se detalla los datos encontrados en la tabla SG_Usuarios actualizada al 26 de agosto del 2014:

<table>
<tr><th>Código Usuario</th><th>Nombre1</th><th>Apellido1</th><th>Login</th><th>Estado</th></tr>
<tr><td>1091</td><td>Eugenia</td><td>Angulo</td><td>L0105090454</td><td>A</td></tr>
<tr><td>1228</td><td>Eugenia</td><td>Angulo</td><td>L0105090459</td><td>A</td></tr>
<tr><td>1642</td><td>Evelyn</td><td>Guillen</td><td>L111300318</td><td>A</td></tr>
<tr><td>864</td><td>Evelyn</td><td>Guillen</td><td>L0111660674</td><td>A</td></tr>
<tr><td>3236</td><td>Freddy</td><td>Artavia</td><td>L020551038</td><td>A</td></tr>
<tr><td>3225</td><td>Freddy</td><td>Artavia</td><td>L0205510389</td><td>A</td></tr>
<tr><td>35</td><td>Prueba</td><td>Prueba</td><td>L0109990999</td><td>A</td></tr>
<tr><td>3418</td><td>Prueba</td><td>Prueba</td><td>L0101110111</td><td>A</td></tr>
<tr><td>3643</td><td>Prueba</td><td>Prueba</td><td>L0202340567</td><td>A</td></tr>
<tr><td>3642</td><td>Prueba</td><td>Prueba</td><td>L0202220225</td><td>A</td></tr>
</table>
</td>
</tr>
</table>

3419	Prueba01	Prueba01	L10202220222	A
1517	Victoria	Rojas	L0105900197	A
2409	Victoria	Rojas	L15901970101	A
2594	Ricardo	Guzman	L0109130062	A
1182	Ricardo	Guzmán	L0109130621	A
3159	Rosa	Chacón	L0800930013	A
1980	Rosa	Chacón	L027480513	I
2143	Rosa	Chacón	L0207480513	I
2428	Victor	Ramírez	L0205650707	A
1905	Victor	Ramírez	L0203390680	A
34	Ivannia	Quesada	L1	E
36	Ivannia	Quesada	L0701230219	E

Por otro lado, se detallan los usuarios genéricos activos de la base de datos Sybase, de la tabla *"syslogins"*:

Suid	Status	Name	Fullname
5421	0	L0114890279	[NULL]
5422	0	L0115740779	[NULL]
5423	0	L0115240273	[NULL]
5424	0	L0503730746	[NULL]
5022	0	L114570671	Reina Sanchez Acuña
4787	0	L0111900814	[NULL]
4835	0	L0111170029	[NULL]
4852	0	L0503160750	[NULL]
4861	0	L0290370633	[NULL]
4875	0	L503340189	[NULL]
4954	0	L0115030621	[NULL]
5002	0	L0110080861	[NULL]
5006	0	L0108700848	[NULL]
5009	0	L0113700434	[NULL]
5033	0	L2060900551	[NULL]
5364	0	L0603390460	[NULL]
5370	0	L0126980530	[NULL]
5076	0	L0700950330	[NULL]
5124	0	L0207250201	[NULL]

		5331 0 L0402210976 [NULL] 5160 0 L0103590378 [NULL] 5168 0 L0112170087 [NULL] 5172 0 L0105770952 [NULL] 5279 0 L105420744 [NULL] 5288 0 L402270315 [NULL] 5289 0 L402170682 [NULL] 1707 2 L0119580306 Usuario para backup
19.Ausencia de revisiones periódicas de las bitácoras de auditoría. Diseñar y elaborar la política y el procedimiento de revisiones periódicas de las bitácoras de auditoría, así como la frecuencia de ejecución de esta. Donde quede evidencia del equipo revisado, persona ejecutora del proceso, análisis realizado y su resultado, fecha de ejecución y firma de autorización de la Jefatura del Departamento de Informática. Para el establecimiento del procedimiento, se debe diseñar una estrategia de monitoreo que permita identificar en función del riesgo que representa para la entidad el componente de la infraestructura (servidor, base de datos, equipo de comunicación), la frecuencia de monitoreo y a qué equipos se aplicaría dicho monitoreo. Adicionalmente, cuando la estrategia esté finalizada, determinar si el Departamento de Informática requiere de un software para la administración de dicho proceso.	Parcialmente Cumplida	A través del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se actualizó la política "2250 09 PR-04-2013 Procedimiento para el Control de Cumplimiento en Seguridad de la Información" que documenta el procedimiento para el control de la revisión de bitácoras o registros de logs en donde se detalla las acciones a ejecutar* *2. Se habilitó la configuración en las propiedades del active directory de las pistas de auditoría correspondientes.* *3. Se implementaron las bitácoras de registro de acceso al centro de datos y acceso a los equipos de telecomunicaciones."* Por otro lado, se señaló, en ese mismo oficio: *"La aplicación de un software para la gestión de registros o logs, podría permitir correlacionar eventos y determinar un mejor análisis de la información, proceso que podría ejecutarse en forma manual, no obstante automatizada es menos susceptible a errores. Las directivas de auditoría se encuentran habilitadas en los sistemas, sin embargo el proceso de revisión debe ejecutarse manualmente."* En la revisión de las directivas de auditoría del active directory se comprobó que las mismas se encuentran habilitadas. No obstante, no se comprobó la existencia de una estrategia de monitoreo, que permita identificar en función del riesgo el

		componente de la infraestructura, la frecuencia de monitoreo y a qué equipos se aplicaría dicho monitoreo. Por otro lado, en el procedimiento *"2250 09 PR-04-2013 Procedimiento para el Control de Cumplimiento en Seguridad de la Información"* se describe el Control para revisión de bitácoras o registro de logs, donde se detalla los siguientes procesos a realizar por parte del encargado de producción de TI: *" 1.1 Llevar una bitácora o registro de logs de los componentes críticos para la Junta (Base de datos Sybase, active directory , equipos de comunicación, control de acceso al data center y departamento de informática).* *1.1. Llevar un control semanal de dichas bitácoras con el fin de detectar posibles anomalías y documentar las mismas en donde quede la sustantividad de la revisión, persona ejecutora del proceso y la fecha de ejecución.* *1.2. Remitir mediante un oficio o correo electrónico las anomalías que se detecten en los diferentes registros o logs, a la jefatura del departamento de TI."* En la consulta realizada el día 28 de noviembre del 2014 al señor Jairo Cruz Sibaja, quien se encuentraba como encargado de producción de TI, de acuerdo a lo manifestado por el señor Ronald Ortiz, jefe del Departamento de Tecnologías de la Información, mencionó que los puntos citados en el procedimiento descrito no se están llevando.
20.Usuarios finales y genéricos como Administradores del Sistema. Realizar un análisis de los usuarios identificados en el punto N° 20 del Informe 32-2010 denominado *"Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social"* de resultados y proceder a revocar o mantener los privilegios de estos. Asimismo, desarrollar una lista donde quede evidencia de los usuarios autorizados para esta función.	Parcialmente Cumplida	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se configuró únicamente como usuarios administradores del active directory Jairo Cruz (Oficial de Seguridad de TI), Randall Espinoza (Soporte TI), Ronald Ortiz (Dirección de TI), Luis Ramirez (Producción de TI). Ver anexo 23 – Usuarios admins del active directory. Así mismo con acceso al escritorio remoto únicamente a estos funcionarios.*

		2. Se bloqueó la cuenta krbtgt que se encuentra en el grupo de replicación de contraseña RODC. Esta cuenta al encontrarse deshabilitada no puede hacer uso." Al efectuar la revisión al *"active directory"* el día 12 de noviembre, se comprobó que los usuarios con acceso al escritorio remoto serían *"bcampbell", "jcruz", "rortiz"*, siendo este primero diferente al hallazgo encontraron mediante oficio GG.1847-2014.
21.Debilidades en la seguridad física y ambiental. Fortalecer el cumplimiento de la política de seguridad en la administración y control ambiental del centro de cómputo, con el fin aplicar correctamente los controles ahí indicados. Establecer un funcionario como encargado de supervisar el cumplimiento de esta política. Modificar la infraestructura física del datacenter principal, con el fin de eliminar los focos de riesgo indicados en la condición.	Parcialmente Cumplida	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, respondiéndose: *"1. Se trasladó el centro de datos principal a un nuevo sitio con categoría Tier II. El nuevo centro de datos cuenta con un mecanismo de autenticación biométrico y es de acceso restringido, cuenta con un sistema para el control del mantenimiento de la temperatura, extintor, cámaras de monitoreo y de suelo elevado.* *2. Se implementó en el centro de datos adicionalmente al mecanismo de acceso biométrico una bitácora manual para el registro de la actividad a realizar para cada funcionario que acceda al data center.* *3. Se implementó una bitácora de acceso en el sitio alterno con un formato o estándar de registro que contempla la fecha (dd-mm-aaaa), hora de ingreso, hora de salida, nombre completo de la persona que realiza la visita, empresa o departamento dentro de la Junta, razón o motivo de la visita y firma de la persona.* *4. Se implementó una bitácora de acceso para el departamento de Tecnologías de Información para el registro de personal externo e interno con un formato o estándar de registro que contempla la fecha (dd-mm-aaaa), hora de ingreso, hora de salida, nombre completo de la persona que realiza la visita o hace el ingreso al departamento, razón o motivo de la visita y firma de la persona.* *5. Se implementaron racks en cada uno de los pisos para albergar los dispositivos de telecomunicaciones de acuerdo al segmento de red al que pertenecen con estructuras con todas las medidas de seguridad respectivas.* *6. Se eliminó el cable UTP que se encontraba expuesto en la entrada al auditorio.*

		7. Se implementaron medidas de seguridad física con la implantación de llavines o cerraduras en los racks que contienen los equipos de la red institucional y que son únicamente de acceso al personal autorizado. A continuación se detallan los racks: *1-) Rack Mercadeo Enlace Inalámbrico cerrado* *2-)Rack Mezanini cerrado* *3-) Rack Piso 3 cerrado* *4-) Rack Piso 4 Cerrado* *5-) Rack Piso 5 Cerrado* *8-) Rack Sótano casetilla de guarda cerrado.* *8. Se implementó protección al cableado de red UTP de acuerdo a las buenas prácticas en los racks institucionales."* En la columna de comentarios del oficio citado, se señaló: *"Nota: En el edificio del almacén se encontró un rack, mismo que no cuenta con las buenas prácticas de seguridad, Al respecto el departamento de TI no ha logrado solucionar este aspecto por cuanto no se ha de finido claramente lo que se va a realizar con los usuarios ubicados en este edificio, pues de hacerlo sin esta definición desencadenaría el gasto de recursos institucionales importantes."* Esta recomendación se da como Parcialmente Cumplida, hasta que el Departamento de Tecnologías de la Información resuelva el tema del rack ubicado en el edificio del almacén y cumpla con las buenas prácticas de seguridad.
C. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO BAJO		
23.Existencia de Usuarios sin el estándar de creación. Para los usuarios indicados en el punto N° 23 de los Resultados del Informe 32-2010 denominado *"Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social"*, se recomienda inactivarlos y generar un nuevo usuario que se ajuste al estándar institucional descrito en la oportunidad de mejora.	Pendiente	El oficio GG.1847-2014 del 8 de agosto del 2014 posee adjunto el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se deshabilitaron las cuentas sin justificación de los siguientes usuarios que no cumplen con el estándar de creación de cuenta L+ Cedula en el motor de Base de Datos:* *-Seguriternet (SUID 1498) ,activapremioespecialinternet(SUID 4257) , pruebas (SUID 1697) , TELT06 (SUID 968) , L011119109 (SUID 1928) , aelectronica (SUID 4562) , conectividad7_capacitacion,*

pruebas_jps_r_cal (SUID 3454), L0909990999 (SUID 1665)"

En la revisión efectuada a la base de datos *syslogins* se comprobó que existen usuarios en su mayoría activos que no cumplen con el estándar del Departamento de Tecnologías de la Información, además algunos de los usuarios definidos no poseen el nombre correspondiente del funcionario. Por ejemplo:

Suid	Status	Name	Fullname
3398	2	consulta_web	Consultas Sitio Web
3652	0	webelectronica	Web Electrónica
4072	0	secureconectividad	accesoaccessserver
5278	0	crm_jps	Administrador CRM
5175	0	gtech	gtech
4437	0	rortiz	Ronald Ortiz Mendez Administra
1755	0	jpsivr	sistema de voz
1	0	sa	[NULL]
4989	0	master_maint	[NULL]
4988	0	jps_maint	[NULL]
3	0	replica	[NULL]
1253	0	sac2003	Soporte Cementerios
4802	0	sc007xdbuser	Acceso
3007	0	dbmon	[NULL]
4885	0	L01053208110101	[NULL]
1070	0	segcementerios	Acceso Seguridad Cementerios
955	0	SYSSQL	Del Sistema
5342	0	jcruz	Jairo Cruz
1634	0	lramirez	Luis Ramirez Arroyo
1657	0	mmasis	Maynor Masis Castillo
1087	0	seguridad_jps	Soporte seguridad de sistemas
5120	0	backup_user	Usuario para backup
2	0	probe	[NULL]

		1078 2 JDJD01 Iris Mata Secre de actas 3096 2 intefbene Interface sistema IntefBenefic intefpresu 2 intefpresu Interface_modulosintef_presu 871 2 sac2000 Producción adm cementerios 3398 2 sacwebuser Usuario internet sacdb2003
24.Firewall de Sistema Operativo Windows inactivo. Se recomienda realizar un proceso de activación de los muros de fuego ("Firewall") que proporciona el proveedor de servicios en el sistema operativo y modificar el estándar de configuración para incluir la activación del firewall.	Pendiente	El pasado 8 de agosto del 2014 por medio del oficio GG.1847-2014, se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se implementó la habilitación o activación de la configuración del firewall en los equipos Windows de los usuarios finales sin embargo no aparece como habilitado (ver explicación en la columna de Comentarios/Observaciones).* *Nota: El antivirus Karpersky impide habilitar el firewall de Windows debido a reglas de restricción del antivirus que internamente maneja las directivas y restricciones de seguridad. Habilitar el firewall no permitiría ejecutar el antivirus en los equipos finales, sin embargo el antivirus de acuerdo a sus reglas maneja las directivas de seguridad para solventar. No obstante se hizo la prueba a nivel de active directory pero el antivirus no dejaba aplicarlo."* En la revisión efectuada al estado del antivirus del active directory el día 12 de noviembre del 2014 se comprobó que estaba inhabilitado. Por lo que, dada la explicación mediante oficio GG.1847-2014, el Departamento de Tecnologías de la Información debe valorar alternativas de antivirus ante esta situación, o bien, realizar un estudio donde se señala las ventajas o desventajas en cuanto a seguridad de mantener desactivado el firewall, a causa de que el antivirus no lo permite.

Informe AI JPS N° 31-2010 Estudio relacionado con una revisión general de usuarios en los servidores Institucionales.

Dirigido a: Departamento de Tecnologías de la Información **Fecha** 27 de diciembre de 2010

<table>
<tr><th>Recomendación</th><th>Estado de la recomendación</th><th>Seguimiento</th></tr>
<tr><td colspan="3">A los Departamentos de Tecnologías de la Información y Desarrollo del Talento Humano:</td></tr>
<tr><td>1. El Departamento de Informática deberá localizar en los Servidores Institucionales, a todas las personas que ya no laboran para la Junta de Protección Social y que permanecen con cuenta de correo electrónico y que aún aparecen como usuarios en el Active Directory; asimismo, y en conjunto con el Departamento de Recursos Humanos, se recomienda establecer un procedimiento manual o automatizado para que Recursos Humanos comunique en forma oportuna a Informática de todas aquellas personas que dejen de laborar para la Institución por cualquier circunstancia o se trasladen a otra unidad administrativa, ya sean interinos o en propiedad y éste pueda llevar a cabo las exclusiones y movimientos correspondientes. (Punto único del Apartado I y punto A. del Apartado II del Informe JPS N° 31-2010 denominado "Estudio relacionado con una revisión general de usuarios en los servidores Institucionales").</td><td>Pendiente</td><td>En la revisión efectuada de los funcionarios inactivos de la tabla "RH_Empleados" contra el correo institucional, se comprobó que los siguientes se encuentra activos en el directorio de correo:

<table><tr><th>Cód.Empl.</th><th>Nombre</th></tr><tr><td>352</td><td>Salazar Mora Gerardo</td></tr><tr><td>626</td><td>Peralta Sandí Maritza</td></tr><tr><td>667</td><td>Mora Valdez Carmen María</td></tr><tr><td>873</td><td>Roldan Vargas Marlon</td></tr><tr><td>965</td><td>Castro Gonzalez Mainor</td></tr><tr><td>967</td><td>Villalobos Jimenez Edgardo</td></tr><tr><td>972</td><td>Rojas Castrillo Jessica</td></tr><tr><td>1087</td><td>Solorzano Zumbado Samanta</td></tr><tr><td>1088</td><td>Campos Vargas Carmen Nidia</td></tr></table>
Por medio de los oficios DTH-1474-2014, DTH-1033-2014, RRHH-1949-2013, RRHH-1455-2013, RRHH-1444-2013, RRHH-1270-2013, RRHH-1038-2013, RRHH-0864-2013, RRHH-0829-2013, RRHH-0528-2013, RRHH-0476-2013, RRHH-0184-2013, RRHH-0076-2013, el Departamento de Desarrollo de Talento Humano le comunicó al Departamento de Tecnologías de la Información sobre la salida de ex funcionarios.

En el oficio GG.1847-2014 del 8 de agosto del 2014 se adjuntó el Informe "Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información", donde se respondió:

" 1. Se configuró en el active directory la estandarización para mantener los datos completos en los campos correspondientes a:
Apellidos (AMBOS), nombre completo y la descripción de los usuarios que no la contengan completa. De acuerdo al listado (ver Anexo 24 – Mantenimiento de Lista de</td></tr>
</table>

Empleados JPS) se procedió actualizar en el controlador de dominio la información personal correspondiente y además de la nueva unidad organizativa a la que pertenece el funcionario.

2. Se implementó a partir del año 2013 el nuevo formato para crear usuarios en el active directory correspondiente al siguiente estándar: L+numCédula"

Al hacer la revisión en el active directory se comprobaron diferentes estándares a continuación se presentan:

Nombre
Luis Gustavo Chacarria Masis
mflores
mvfernandez
rbarrantesm
L0206920250

Al verificar los colaboradores que ingresaron después del 2013, se comprobó que algunos no cumplen con dicho estándar, entre ellos están:

Cod.	Nombre	F.Ingreso	Usuario
1085	Araya Romero Gabriela	10/12/2013	Gabriela Araya Romero
1086	Solano Herrera Cynthia	10/12/2013	Cynthia Solano Herrera
1100	Herrera Bolaños Persi	18/08/2014	Persi Francisco Herrera Bolaños
851	Mena Ulloa Andrea	01/07/2014	amena
996	Flores Tencio Mauricio	14/04/2014	mflores
1082	Siles Alfaro Patricia	20/11/2013	Patricia Siles Alfaro
1083	Brenes Guerrero Arelys	20/11/2013	Arelys Brenes Guerrero
1084	Chavarria Masis Luis Gustavo	20/11/2013	Luis Gustavo Chavarria Masis
			Meybelyn Chavarría Ramos
			Nestor Villalobos Briceño

Los siguientes usuarios aparecen activos en el active directory, pero inactivos en la tabla RH_Empleados:

Nombre	Nombre para mostrar	F.Ingreso
L0113180144	Samanta Solorzano Zumbado	8-1-2014

<table>
<tr><td></td><td></td><td>El usuario jsaenz "Johana Vanessa Sáenz Leitón" de la Agencia Heredia, no aparece en la lista de Recursos Humanos

Existen Sub departamentos creados en Unidades que no corresponden tales como:

<table><tr><th>Departamentos</th><th>Sub departamentos</th></tr><tr><td rowspan="2">Tecnologías de Información</td><td>BCR</td></tr><tr><td>Socios Comerciales</td></tr></table></td></tr>
<tr><td colspan="3">Al Departamento de Tecnologías de la Información:</td></tr>
<tr><td>2. Efectuar un estudio relacionado con el horario de acceso a los sistemas por parte de los funcionarios y determinar cuáles horas pueden ser restrictivas para el ingreso a esos sistemas, lo anterior, previa consulta a las Jefaturas de las diferentes unidades administrativas de la Institución, con la finalidad de no obstaculizar sus labores cuando éstas deban realizarse fuera de horarios de oficina. (Punto B. del Apartado II del Informe JPS N° 31-2010 denominado "Estudio relacionado con una revisión general de usuarios en los servidores Institucionales").</td><td>Parcialmente Cumplida</td><td>Con base en la revisión efectuada al horario definido en el "active directory" en relación al horario permitido por las jefaturas de los diferentes Departamentos, se comprobó que a pesar de que enviaron oficios señalando el horario de cada funcionario, esto no se cumplió, a continuación se detallan:

<table><tr><th>Funcionario</th><th>Circular</th><th>Fecha</th><th>Horario</th></tr><tr><td>Shirley Jimenez Matamoros</td><td>AC-120-2012</td><td>19-3-2013</td><td>M6am – 12mn</td></tr><tr><td>José Pérez Obaldía</td><td>DPV-172-2013</td><td>18-3-2013</td><td>L a V 8am a 17pm</td></tr><tr><td>Sara Morales Sanchez</td><td rowspan="2">DRC-351-13</td><td rowspan="2">19-3-2013</td><td rowspan="2">L a V 8:15am a 7pm</td></tr><tr><td>Eugenia Mora Barrantes</td></tr><tr><td>Patricia Morales Salazar</td><td>DRC-351-13</td><td>19-3-2013</td><td>L a V 6:45am a 5pm</td></tr><tr><td>Andrés Araya Jimenez</td><td rowspan="4">DRC-351-13</td><td rowspan="4">19-3-2013</td><td rowspan="4">L a V 7am a 5pm</td></tr><tr><td>Mauricio Flores Tencio</td></tr><tr><td>Mileidy Jimenez Matamoros</td></tr><tr><td>Teresa Corrales López</td></tr><tr><td>Elizabeth Solis Jinesta</td><td rowspan="2">AI-134</td><td rowspan="2">20-3-2013</td><td rowspan="2">L a V 6:30am a 11pm</td></tr><tr><td>Andrés Martinez Porras</td></tr><tr><td>Marcia Salazar Vargas</td><td>DA-203-2013</td><td>18-3-2013</td><td>L a V 7:30am a 4:30pm</td></tr><tr><td>Manuel Loría Vargas</td><td>DA-203-2013</td><td>18-3-2013</td><td>L a V 7am a 7pm</td></tr><tr><td>Freddy Guzman Jimenez</td><td>SSG-035</td><td>18-3-2013</td><td>L a V 7am a 18:30pm</td></tr><tr><td>David Arista Martinez</td><td rowspan="2">IV-J-073-2013</td><td rowspan="2">18-3-2013</td><td rowspan="2">L a V 8am a 17:30pm</td></tr><tr><td>José Palma Mora</td></tr><tr><td>Vanessa Vega Astorga</td><td>DFC-187-2013</td><td>8-4-2013</td><td>L a V y D 7 am a 19pm</td></tr><tr><td>Rafael Oviedo Chacón</td><td>DFC-187-2013</td><td>8-4-2013</td><td>L a V y D 7 am a 20pm</td></tr><tr><td>Ileana Alfaro Granados</td><td rowspan="2">RRHH-0463-2013</td><td rowspan="2">3-4-2013</td><td rowspan="2">L a V 6 am a 19pm</td></tr><tr><td>Olman Brenes Brenes</td></tr></table></td></tr>
</table>

		María Solano Gonzalez			
		Andrea Mena Ulloa	A.S.916-2013	3-4-2013	L a V 7am a 7pm
		María Delgado Morales	A.S.916-2013	3-4-2013	L a V 7am a 7pm
		Jairo Arce Esquivel Kimberly Barquero Aguilar Victor Campos Miranda Kenneth Obando Masis Carlos Rivas Espinoza Cesar Rojas Rivera Miguel Valverde Fernández	T-SC-660-2013	27-3-2013	L, M, J 7:30 a 5pm K, V 7:30am a 7:30pm D 3:30 a 7:30pm
		Jorge Villalobos Fonseca	DP.402-2013	21-3-2013	L a V 7:30am a 5pm
		José Siles Barboza Auxiliadora Martinez Salas Vesalio Coto Mora Ligia Quiros Mena	JPS-Suc-Car-246-2013	19-3-2013	L, M 7:30am a 5pm K, V 8am a 6pm J 8am a 5pm D 4pm a 7pm
		Florinda Gonzalez	JPS-Suc-Car-246-2013	19-3-2013	L a V 7:30am a 7pm D 4pm a 7pm
		Odilie Loría Solano Maritza Muñiz Ramírez	T-234	4-4-2013	L a V 6am a 8pm
		Iris Estrada Masis	T-234	4-4-2013	L, M, J 7am a 7pm K, V 7am a 8pm D 3:30pm a 7:30pm
		Rodolfo Hernández Gutiérrez	T-234	4-4-2013	L a V 6am a 8pm
		Martha Herra Sirias	T-234	4-4-2013	L, M, J 7am a 5pm K, V, D 7am a 8pm
		Juan Mora Ureña	T-234	4-4-2013	L a V, D 7am a 8pm
		Luis Huertas Fernández	T-234	4-4-2013	L a V, D 7am a 8pm
		L (Lunes), K (Martes), M (Miércoles), J (Jueves), V (Viernes)			
3. Establecer estándares en la información contenida en el "Active Directory" específicamente en "Description" y "Display Name", completando en ambos casos la información contenida en ellos. (Punto D. del Apartado II del Informe JPS Nº 31-	Pendiente	En la revisión efectuada para algunos usuarios del active directory, se comprobó que existen campos sin llenar tales como: *"Nombre para Mostrar"*, *"Descripción"*, *"Teléfono del Trabajo"*, *"Dirección del Correo"*. A continuación se detalla:			
		Departamento	**Nombre**	**Nombre para Mostrar**	**Descripción**	**Teléfono del Trabajo**	**Dirección de Correo**

2010 denominado *"Estudio relacionado con una revisión general de usuarios en los servidores Institucionales"*).		Administración de CampoSantos	L0303970708			X
		Gerencia General	lmoraga		X	
			emadriz		X	
			Persi Francisco Herrera Bolaños		X	X
		Recursos Materiales	amena		X	X
			acamacho			X
			grodriguez		X	
		Salud Ocupacional	caguilar		X	
		Agencia Puntarenas	Arelys Brenes Guerrero			X
			Luis Gustavo Chavarria Masis			X
			Patricia Siles Alfaro			X
		Comunicación y relaciones públicas	jlarias		X	X
		Contraloría de Servicios	Mónica Aguirre Gómez	X	X	X
			Erin Melissa Montero Castro		X	X
		Plataforma de Servicio al Cliente San José	Cristian Sanchez Sanchez			X
			kbarquero		X	
		Agencia Pérez Zeledón	Cinthya Solano Herrera			X
			Gabriela Araya Romero			X
		Gerencia de Desarrollo Social	squiros		X	

		Planificación Institucional	Ana Cristina Garro Sanchez (PRAC)		X	X
			Juan Pablo Durán Nuñez		X	X
			Laura Vargas Chacon	X	X	X
			rmarchena		X	
		Junta Directiva	Delia Villalobos Alvarez		X	X
			mroman		X	
		Sorteos	aarias		X	
			gmunoza		X	X
		Gerencia Administrativa Financiera	L0601610106		X	X
		Contable Presupuestario	hsanabria			X
		Producción	agarcia		X	X
			Luis Diego Fuentes	X	X	X
			rarguedas		X	X
		FOMUVEL	Cindy Madrigal Lautoche		X	X
			Jessica Salas Gomez		X	X
			Karla Solis Cruz		X	X
		Mercadeo	Raquel Artavia Roman		X	X
		Auditoría Interna	rrojasr			X
		Servicios Administrativos	Gilberto Chacón Sarmiento		X	X
		Agencia de Alajuela	nloria			X

		Asejups	Jurgen Chinchilla Avendaño	X	X	X
			Yoselyn Calvo Jimenez	X	X	X
		IPL	cnavarro			X
		Administración de Loterías	gcespedes		X	X
			L0206920250			X
			tgonzalez		X	
		Prosoft	Meybelyn Chavarría Ramos		X	X
			Nestor Villalobos Briceño		X	X
		Gestión Social	Carmen Nidia Campos Vargas		X	X
			L011318144		X	
		Deloitte	Luis Pinedo Cabrera		X	X
		Gerencia de Operaciones	dzunigah		X	X
4. Corregir los aspectos descritos en los puntos E, F y G del Apartado II del Informe JPS N° 31-2010, de tal manera que: no se repitan funcionarios en una misma unidad administrativa, no aparezca un mismo funcionario en diferentes unidades simultáneamente y que no se encuentren funcionarios anotados en departamentos donde no laboran.	Pendiente	Por otro lado, se observó que no hay concordancia entre la lista facilitada por el Departamento Desarrollo del Talento Humano y Tecnologías de la Información, dado que existen usuarios que están registrados en departamentos que no les corresponde, por ejemplo:				

Depto. Active Directory	Usuario	Nombre	Observación
Gerencia General	larayaa	Laura Araya Arias	En Rec. Hum. aparece en Gerencia de Operaciones
	lmoraga	Laura Patricia Moraga Vargas	En Rec. Hum. aparece en Gerencia de Operaciones
	lrojas	Lilliana Rojas Segura	En Rec. Hum. aparece en Gerencia Gerencia con el

			nombre Carmen
Agencia Puntarenas	rvargas	Raúl Vargas Montenegro	En Rec. Hum. aparece en Suc. Cartago
Sorteos	kvalderrama	Katya Valderrama Castellón	En Rec. Hum. aparece en Administración de Loterías
Ventas	cmora	Carmen Mora Valdez	En Rec. Hum. aparece en Comunicación y Relaciones Públicas
Servicios Administrativos	jsoto	John Cesar Soto Espinoza	En Rec. Hum. aparece en Sucursal Pérez Zeledón
	laraya	Luis Rodríguez Araya	En Rec. Hum. aparece en Gerencia General, Rodríguez Araya María Lidia
	smorales	Sara Morales Sánchez	En Rec. Hum. aparece en Gerencia General
Agencia de Alajuela	mherra	Martha Patricia Herra Sirias	En Rec. Hum. aparece en Sucursal Heredia
Administración de loterías	cvalverde	Carlos Luis Valverde Meza	En Rec. Hum. aparece en Ventas
	kchacon	Kembly Chacón Brenes	En Rec. Hum. aparece en Sorteos
Agencia de Heredia	jsaenz	Johanna Vanessa Sáenz Leitón	En Rec. Hum. aparece en Ventas
Gerencia de Operaciones	gcenteno	Geovanny Centeno Espinoza	En Rec. Hum. aparece en Plat. Servicio al Cliente SJ
	jmora	Juan Alberto Mora Ureña	En Rec. Hum. aparece en Tesorería
	lhuertas	Luis Alberto Huertas Hernández	En Rec. Hum. aparece en Tesorería
	yfonseca	Yadira Fonseca Alvarado	En Rec. Hum. aparece en Junta Directiva

Estudio: 29-2010 "Seguimiento de recomendaciones giradas por el área de sistemas de la Auditoría Interna"
Este informe incluye los Informes N° 06-2008, N° 07-2009 y N° 10-2009, según el siguiente detalle:

Informe AI JPS N° 06-2008 Estudio sobre la verificación de la seguridad en el manejo de las transferencias electrónicas de fondos y la seguridad, integridad y consistencia de la información contenida en las bases de datos institucionales referentes al manejo de las loterías.

Dirigido a: Departamento de Tecnologías de la Información **Fecha** 19 de junio, 2008

Recomendación	Estado de la recomendación	Seguimiento
4. Se recomienda que se establezcan contratos de confidencialidad con el proveedor que da mantenimiento al sistema de información InTEF y se documenten las normas, políticas y procedimientos para la administración de este tipo de contratos, para que de esta forma queden claramente establecidos los alcances y los procedimientos en el entorno de seguridad que deben acatar los proveedores ante la institución.	Parcialmente Cumplida	Por medio del oficio RM. 1467-2014 del 1 de octubre del 2014 el Departamento de Recursos Materiales menciona los contratos a los que se les aplicaría dicha cláusula, así además con respecto a la cláusula N°2010LN-000002-PROV, citó *"... esta licitación no posee cláusula de confidencialidad. Tal como se ha explicado en otras ocasiones para procedimientos en etapa de ejecución, de requerir efectuar una modificación en los mismos el Departamento Administrador del contrato debe solicitarlo basados en las condiciones establecidas en el artículo 200 del Reglamento a la Ley de Contratación Administrativa. No sucede lo mismo en los nuevos procedimientos a los cuales se le ha incorporado de previo."*, a continuación las licitaciones que no poseen la cláusula de confidencialidad: N°2010LN-000002-PROV *"Contratación de Servicios de Mantenimiento Sistema de Administración de Loterías"* N°2010LA-000019-PROV *"Adquisición de Licencias Motor Base de Datos Sybase 15.0 ó Superior"* • Recursos Materiales menciona: *"En este caso no procedía la incorporación de dicha cláusula dado que la compra fue ejecutada en el año 2010 y la solicitud corresponde al 14 de febrero del año 2012."*
17. Considerar, establecer un proceso de capacitación enfocada al	Parcialmente	Por medio del oficio GG.1847-2014 del pasado 8 de agosto

entorno de seguridad para el o los funcionario(s) encargado(s) de la base de datos, y poder, a un corto plazo, y en complemento con la recomendación anterior, implementar una seguridad administrada directamente desde el motor de base de datos.	Cumplida	del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1- Se desarrolló un plan de recursos humanos para el área de TI para el período 2014-2017 en donde se detallan las necesidades y el cronograma de planteamiento para la capacitación con alcance a todos los procesos del área de TI. En el mismo se hace: enfoque a los procesos de seguridad informática. Durante el primer semestre del presente año algunos funcionarios ya iniciaron con el proceso de capacitación. Para el segundo semestre del 2014 se continuará con el plan de capacitación para los funcionados del departamento. (Ver anexo #9)."* Se observó el plan de recursos humanos, no obstante no se logró determinar dicho cumplimiento.
19. Se analizó de forma general, las actividades de los perfiles actuales que tiene la Junta de Protección Social para el Departamento de Informática y se recomienda que se haga un estudio para establecer más claramente la necesidad de la Institución en aspectos de especialistas (tecnólogos), que se enfoquen más a actividades de control y seguridad de los procesos informáticos de la Institución. Debemos recordar que los servicios informáticos de una entidad como la Junta de Protección Social de San José, en la actualidad, han pasado ha ser servicios de misión crítica para la continuidad de las operaciones cotidianas, por lo cual debemos establecer un mayor enfoque en aspectos de clasificación y preparación de los funcionarios que laboran dentro de ese Departamento.	Pendiente	A través del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"... Se ha solicitado a la Gerencia la aprobación del Oficial de Seguridad de TI, sin embargo la respuesta no ha sido positiva, ..."* Por otro lado, se señaló en ese mismo oficio lo siguiente: *"... 2. Se cuenta con un estándar de creación para logins en el motor de base de datos que corresponde a L+NumCédula. Debido a dicho estándar, no se crea ningún tipo de distinción entre usuarios internos, externos u otros debido al cumplimiento del estándar de creación definido internamente. No obstante si se puede tener una distinción o diferenciación entre los funcionarios institucionales y los externos de acuerdo a un script de base de datos que maneja el área de Producción de TI. ..."*

<table>
<tr><td></td><td></td><td>Al verificar la tabla syslogins se observaron usuarios con el estándar "L+NumCédula", sin embargo en dicha base de datos, no existe un campo donde se defina quien es funcionario de la Junta y quien es Socio Comercial. Ya que anotarlo en el campo denominado "fullname" no corresponde, dado que éste es un campo para la descripción del nombre de la persona, no para identificar si es funcionario institucional o no.</td></tr>
<tr><td>20. Revisar los contratos de outsourcing actuales y los que se pretendan establecer a corto plazo, con el propósito de reorientarlos adecuadamente de tal modo que se incorporen una serie de procedimientos de control y seguridad, tales como, la firma de contratos de confidencialidad y definición de políticas de seguridad para el acceso a la información institucional.</td><td>Parcialmente Cumplida</td><td>En la revisión efectuada a distintas compras directas y licitaciones abreviadas se comprobó que de 12 carteles consultados, 4 de ellos no poseen la cláusula de confidencial:
<table><tr><th>No poseen cláusula de confidencialidad</th></tr><tr><td>N°2014CD-000336 PROV-01 "Compra e Instalación de un dispositivo de almacenamiento de alta disponibilidad".</td></tr><tr><td>N°2014CD-000271-PROV-01 "Implementación llave en mano de Software de Seguimiento de Informes de Auditoría, sesiones de Junta Directiva y Administración de Proyectos según PMBOK."</td></tr><tr><td>N°2010LN-000002-PROV "Contratación de Servicios de Mantenimiento Sistema de Administración de Loterías"</td></tr><tr><td>N°2010LA-000019-PROV "Adquisición de Licencias Motor Base de Datos Sybase 15.0 ó Superior"</td></tr></table></td></tr>
<tr><td>21. Establecer un programa de capacitación en materia de seguridad en los sistemas para el Departamento de Informática, y asimismo hacer extensivo a todo el personal de la Institución, aquellos aspectos que le competen y puedan mejorar la seguridad, permitiendo una formación a mediano plazo en ese tema. La seguridad de la información es un tema que en la actualidad ha tomado mucha fuerza debido al incremento de los delitos informáticos. Una Institución como la Junta de Protección Social que debe estar siempre a la vanguardia e innovación, no escapa a este problema, pero estamos en un momento donde se pueden tomar las decisiones</td><td>Parcialmente Cumplida</td><td>De acuerdo con la información adjunta en el oficio GG.1847-2014 del 8 de agosto del 2014, se comprobó la existencia de "Reglas de oro" al iniciar sesión, basadas en la seguridad de TI, así como también, a través de correo electrónico "Mesa de Ayuda <mesa_ayuda@jps.go.cr>" se observó que el Departamento de TI, envía a los funcionarios correos acerca del tema de seguridad de TI.</td></tr>
</table>

para establecer e implementar las mejores prácticas. Un ejemplo de estándares de seguridad a seguir el ISO-27001.		

Informe 07-2009 Seguimiento de recomendaciones giradas por la Auditoría Interna al Departamento de Informática en el Informe N° 08-2006 referente a "Estudio relacionado con la página Web de la Junta de Protección Social de San José"

Dirigido a: Departamento de Tecnologías de la Información **Fecha:** 20 de abril, 2009

Recomendación	Estado de la recomendación	Seguimiento
1. Revisar y corregir el error que presenta en el submenú de "Organización" específicamente en el área de Auditoría donde el formulario para ingresar denuncias no se despliega. Así como agregar una guía de cómo llegar a presentar una denuncia a través de esta sección del menú (Punto A del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Pendiente	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información, se respondió: *"Algunos de los formularios se encuentran en proceso de actualización debido a que el área de Tecnologías de la Información no es responsable de dicho contenido ..."* El día 22 de setiembre del 2014 se consultó la página web de la Junta de Protección Social, comprobándose que la misma se encuentra idéntica a la consultada el 20 de noviembre del 2012, pese a que por medio del oficio 1 172-12 del pasado 16 de febrero del 2012 el señor Ronald Ortiz, indicó: *"Atendido nuevo sitio"* Actualmente, la página web no posee el formulario para ingresar denuncias, así como tampoco una guía de como presentar una denuncia. Por otro lado, con respecto al área para tramitar denuncias, el contacto que se muestra es el señor Carlos Luis Artavia Vega, Administrador de la Sucursal de Alajuela y no el responsable de tramitar denuncias.
9. Valorar la posibilidad de incorporar en la Sección de Cementerios del sitio Web, la siguiente información:	Parcialmente Cumplida	En el oficio GG.1847-2014 del 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*,

» Incluir dentro de la Sección de Cementerios, un apartado donde se puedan consultar las propiedades disponibles para su arriendo, así como también sus ubicaciones y sus precios.		donde se respondió: *"La información contenida en la sección de cementerios se encuentra en proceso de la generación de un script que retome la correcta información.* *El control para la solución fue emitido, se encuentra en proceso de ejecución."* En la revisión efectuada al sitio web, se logró observar la lista de propiedades disponibles para los cementerios central y metropolitano, no obstante, dicha información no se encuentra actualizada, ni separada por cementerio.
» Asignar un "número de identificación" y "palabra clave" a los arrendatarios de propiedades, con la finalidad de que con estos datos puedan consultar su saldo de financiamiento en la compra de nichos o si tiene pagos pendientes de mantenimiento, cerciorarse del monto correspondiente. (Punto E. del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Pendiente	A través del oficio I 172-12 del 16 de febrero del 2012 el señor Ronald Ortiz señaló: *"Se implementará"* No obstante, esto aún no ha sido realizado, dado que en la revisión efectuada a la página web se comprobó que la misma no posee *"número de identificación"* y *"palabra clave"* para los arrendatarios de propiedades.

Informe 10-2009 Seguimiento de recomendaciones giradas por los despachos de auditores externos Carvajal y Colegiados y Castillo-Dávila, Asociados

Dirigido a: Departamento de Tecnologías de la Información **Fecha:** 30 de junio 2009

Recomendación	Estado de la recomendación	Seguimiento
III. Planeación estratégica en Tecnologías de Información **Recomendación para el hallazgo N° 1:** *"Es fundamental que la organización posea un plan estratégico institucional que permita elaborar un plan estratégico de tecnologías de información que esté debidamente alineado. Sin embargo, mientras se formalice dicho instrumento, se recomienda que en el seno del comité informático se solicite a las diferentes áreas que definan sus necesidades de servicios y sistemas con un horizonte de 3 años para construir un portafolio de aplicaciones a construir y que el Departamento de Informática elabore una propuesta de la visión tecnológica que necesitará la organización tomando en consideración esas necesidades, así como los cambios que necesariamente deben darse para evitar la obsolescencia tecnológica. Dicha propuesta podría considerar elementos como los mencionados previamente en este informe".*	Parcialmente Cumplida	Se comprobó por medio del oficio TI 1308-13 del 2 de diciembre del 2013, que el Plan Estratégico en Tecnologías de Información se encuentra actualizado, sin embargo el mismo no se mostró aprobado por la Gerencia.
IV Organización de la función de TI **Recomendación para el hallazgo N° 1:** *"Se recomienda valorar la conveniencia de efectuar un proceso de reestructuración del departamento de Informática de manera que su organización funcional se adecue al tipo de servicios que en la actualidad debe administrar el área y se pueda disponer de plazas y funcionarios que realicen labores fundamentales como la*	Parcialmente Cumplida	Esta Auditoría comprobó que el señor Ronald Ortiz, designó al funcionario Bruce Campbell como oficial de seguridad mediante oficio I 1227-11 del 23 de noviembre del 2011; no obstante se comprobó que esa Dependencia promovió la Contratación Directa 2013CD-000515-PROV-01, al realizar la consulta sobre la justificación de contratar los servicios de un oficial de seguridad si ya contaban con un funcionario responsable, el señor Ortiz a través del oficio respondió TI 1420-13 del 23 de diciembre del 2013, respondió:

<table>
<tr>
<td>administración de bases de datos o la administración de la seguridad de información".</td>
<td></td>
<td>"... pese a que en el año 2009, se ha solicitado por parte de este Departamento la creación de una plaza de oficial de seguridad informático, al día de hoy no se cuenta con la misma formalmente creada con los deberes y obligaciones correspondientes ..."

Con el Plan Estratégico de TI 2014-2017, en la estructura organizacional de TI se define el puesto de seguridad informática, sin embargo dicho plan no se encuentra aprobado, por lo que no se puede tomar, como una estructura autorizada.</td>
</tr>
<tr>
<td>VIII. Capacitación

Recomendación para el hallazgo N° 1:

"Elaborar un programa de capacitación con un horizonte mínimo de 24 meses que permita actualizar en áreas sensibles el conocimiento del personal del departamento y hacer las previsiones presupuestarias necesarias para lograr que dicho programa de capacitación pueda llevarse a la práctica".</td>
<td>Parcialmente Cumplida</td>
<td>De acuerdo con el oficio DTH-1553-2014 del pasado 3 de octubre del 2014, se observó que el programa de capacitación del periodo 2012 a cumplir en el 2013, no fue cumplido.
Por otro lado, en el programa de capacitación del periodo 2013 a cumplirse en el 2014, los funcionarios del Departamento de Tecnologías de la Información no llevaron ningún curso, no obstante en la planificación de la capación estratégica del periodo 2014, y para el año en curso se observó que se llevaron algunos cursos, tales como:

<table>
<tr><th>Actividad</th><th>Fechas</th></tr>
<tr><td>Perspectiva de la Factura Electrónica para el 2014 – Oficio TI-83-2014</td><td>12-02-2014</td></tr>
<tr><td>Curso Itil Fondations V3 Oficio TI-219-2014</td><td>31 de marzo al 07 de abril, 2014 (24 horas)</td></tr>
<tr><td>Windows Server 2012 Administración</td><td>11 al 25 de agosto, 2014 (40 horas)</td></tr>
</table>
</td>
</tr>
</table>

Informe AI JPS N° 22-2012 Estudio sobre la verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la junta de protección social por medio de los socios comerciales

Dirigido a: Departamento de Tecnologías de la Información, Gerencia Administrativa Financiera **Fecha** 20 de diciembre, 2012

Recomendación	Estado de la recomendación	Seguimiento
1- Se recomienda tener equipo destinado para el monitoreo continuo de las comunicaciones, especialmente en los equipos utilizados para las conexiones a Internet.	Parcialmente Cumplida	En el gráfico *"Junta de Protección Social de San José C295137-006"* se puede observar la existencia de un equipo específico para el monitoreo de las conexiones con Internet, no obstante no se visualizó una bitácora donde se refleje las alertas por la saturación del enlace con Internet así como el constante monitoreo de estas.
2- Se recomienda agregar comentarios informativos en la configuración del switch de capa 3.	Pendiente	De acuerdo con la documentación enviada por el señor Ronald Ortiz el día 5 de agosto por medio de correo electrónico, correspondiente al documento Core-Sotano-R1-05-08-2014 se comprobó que el mismo no posee ningún comentario realizado por el Departamento de Tecnología de la Información.
8- Se recomienda optimizar la distribución del cableado de las salas de cómputo y comunicaciones de manera organizada y rotularlo de acuerdo a un estándar preestablecido que permita identificar a qué equipos se encuentran conectados.	Parcialmente Cumplida	En la revisión efectuada el día 26 de agosto del 2014 en compañía del señor Jairo Cruz al centro de datos de la Junta de Protección, se comprobó la existencia de equipos y cableados rotulados, no obstante algunos de ellos estaban rotulados con masking tape, se observó además la distribución de otros equipos sin estar debidamente señalizados. Se recuerda lo mencionado por la norma ANSI / TIA / EIA-606 *"Administración estándar para la Infraestructura de Telecomunicaciones de Edificios Comerciales"* en el apartado de etiquetado: *"Definición: El etiquetado es la marca de un elemento de una infraestructura de telecomunicaciones con el identificador apropiado y otra información relevante.* *El etiquetado puede producirse de dos maneras. Las etiquetas pueden ser agregadas al elemento, o, el propio elemento puede*

		ser marcado directamente. *Etiquetado será:* ☐ *fijado al elemento a ser administrado o* ☐ *marcado directamente sobre el elemento que se administra.* *Vea la sección 8.2 de la documentación de las normas originales de los requisitos de etiquetado."* **(Texto traducido del original)**
9- Debido a la sensibilidad de las transacciones realizadas en la aplicación para realizar apuestas deportivas, se recomienda hacer uso de un segundo factor de autenticación como por ejemplo certificados digitales instalados en los puntos de ventas autorizados.	Pendiente	Los puntos de venta no poseen el uso de certificados digitales, asimismo a través del oficio I 54-13 del pasado 22 de enero del 2013, se menciona: *"... En el caso de que la Junta determine a futuro la utilización del mecanismo de validación y acceso a través de firma digital, los costos de adquisición de los dispositivos lectores y firma digital propios del SOCIO COMERCIAL serán asumidos por este último.* *..."*
12- Se recomienda la implementación de un mecanismo que permita cifrar las credenciales de acceso antes de ser enviadas del cliente al servidor a través del uso de un puerto seguro como 443 (https) o cifrados a nivel de la aplicación a través del uso del algoritmo MD5.	Parcialmente Cumplida	A través del comando *"netstat -noa"* se comprobó la dirección remota *"37.252.228.18:443"* en estado *"ESTABLISHED"*, asimismo por medio de la dirección *"https://www.google.com"* se logró verificar que dicho sitio si es seguro, no obstante, al consultar la página de la *"https://correo.jps.go.cr"* esta se mostró como un sitio no seguro.
21- Se recomienda usar un algoritmo de cifrado robusto que genere ID de sesiones de usuario de forma aleatoria, de tal manera que no sean tan predecibles como los citados en el punto 21 de este informe.	Pendiente	Los días 5 y 25 de agosto del 2014 se consultó el certificado de seguridad, por medio de la página web https://apps.jps.go.cr/Citrix/XenApp/site/default.aspx, comprobándose que lo correspondiente al campo *"Id. de clave="* está de forma fija y no dinámica, como se indicó en dicha recomendación.
22- Se sugiere recomendar a los Socios Comerciales la activación del protector de pantalla con contraseña, debido a que la no activación del mismo representa un riesgo para la aplicación de la Junta de	Pendiente	No se observó ninguna circular o información donde se esté recomendando al socio comercial a utilizar protectores de pantalla con contraseña.

Protección Social.		
23- Se recomienda sugerir a los Socios Comerciales no instalar aplicaciones que representen un riesgo para la seguridad del equipo desde donde se realizan las apuestas deportivas.	Pendiente	No se observó ninguna circular o información donde se esté recomendando al socio comercial a no instalar aplicaciones que representen un riesgo para la seguridad del equipo.
24- Recomendar a los Socios Comerciales mantener actualizado sus programas de antivirus a fin de mantener protegido el equipo de código malicioso.	Pendiente	No se observó ninguna circular u otra documentación donde se esté recomendando al socio comercial mantener actualizados sus programas de antivirus.
25- Recomendar a los Socios Comerciales dejar la práctica de tener la contraseña y nombre de usuario escritas en papel en lugares visibles, indicándoles los riesgos asociados de mantener dicha práctica.	Pendiente	No se observó ninguna circular u otra documentación donde se esté recomendando al socio comercial mantener la contraseña y nombre de usuario en lugares seguros, que no estén expuestos a ninguna persona.

Informe AI JPS N° 04-2013 Manejo del fondo y la bolsa para el pago de premios de la Lotería Pega Millones en la determinación de utilidades

Dirigido a: Gerencia General, Gerencia Administrativa Financiera, Departamento de Contable Presupuestario y Departamento de Administración de Loterías **Fecha** 23 de enero, 2013

Recomendación	Estado de la recomendación	Seguimiento
3. Crear las cuentas contables necesarias y segregar la Bolsa para el Pago de Premios por modalidad de acierto, lo cual permite reflejar los saldos en forma independiente, de esta forma es como debe acumularse y pagarse según la normativa (Resultado 2.1.1).	Parcialmente Cumplida	Por medio del oficio G.0664-2013 del pasado 21 de marzo del 2013, en el cronograma de implementación de las recomendaciones, en lo que se refiere a la columna de observaciones para la recomendación número tres, se señaló: *"Desde el punto de vista contable no se segrega el registro por modalidad de aciertos ya que se considera que esta información la posee el Sistema de Lotería Electrónica según reporte denominado "Resumen de premios de pega millones". Así como el documento "Resumen Liquidación de Lotería de cada sorteo"."* A través del oficio AI-417 del 21 de junio del 2013 esta Auditoría, mencionó: *"...* 1. *El saldo de la Bolsa que refleja el Sistema de Lotería Electrónica no coincide con el saldo de la cuenta contable, lo anterior en virtud de que como se indicó en este Informe, la mecánica de registro utilizada por el Departamento de Contabilidad y Presupuesto, no muestra a una fecha dada el saldo real acumulado de dicha Bolsa.* *Tal diferencia entre ambos saldos, no hace funcional señalar que la segregación de la Bolsa del registro contable puede obtenerse mediante el Sistema de Lotería Electrónica.* 2. *No se debe dejar de lado que el artículo N° 11 del Reglamento de Juegos de Lotería Electrónica establece la*

acumulación en forma independiente por cada modalidad de acierto.

3. *Un registro contable pertinente, proporciona al usuario de la información financiera los elementos necesarios para conocer la situación económica a una fecha determinada. El poder establecer con base en los registros contables ...*"

Ante esto, el señor Rafael Angel Oviedo Chacón, jefe ai del Departamento de Contable Presupuestario, en oficio DCP-1597 del 27 de agosto del 2013, indicó:

"Con la finalización del juego "Pega Millones en mayo del 2013, esta recomendación no procede por lo que será aplicada al juego lotto.

Se creará un auxiliar en el cual se detallarán las modalidades de pago.

Para junio se dio apertura a tres cuentas en el catálogo contable: Bolsa, premios por pagar y reserva."
"

Se observa en el catálogo contable al 28 de noviembre del 2014 la existencia de cuentas contables correspondientes a los premios por pagar, la bolsa y la reserva, todas para el juego Lotto, por lo que se atiende la recomendación de crear las cuentas contables necesarias, a continuación se señalan:

"2.1.4.01.99.99.9.11 Premios por pagar - Loteria Electronica (Lotto)
2.1.4.01.99.99.9.20 Bolsa Lotto 54%
2.1.4.01.99.99.9.22 Reserva Lotto 1%"

Asimismo, la creación de la cuenta contable *"2.1.4.01.99.99.9.23 Premios no cobrados Lotto"*, la cual no refleja movimientos, por lo que esta Auditoria Interna no considera relevante la existencia de esta cuenta contable, dado que la cuantía de los premios no cambiados se reflejará como un saldo en la cuenta

		"2.1.4.01.99.99.9.11 Premios por pagar - Loteria Electronica (Lotto)", se documenta el caso de la liquidación del sorteo de Lotto No. 1391 del 12 de febrero del 2014, donde el monto de los premios ganados ascendió a ¢8,857,000 y los premios cambiados fueron de ¢8,014,000 quedando un saldo de premios no cambiados por ¢843,000. No obstante, lo referente a la segregación de la bolsa por modalidad de acierto no se encuentra aún implementada, se aporta por parte del Departamento Contable Presupuestario la solicitud de servicios No. 1469-2013 del 09 de setiembre del 2013 al Departamento de Tecnologías de Información para desarrollar dicha segregación.
10. Se proceda a trasladar contablemente a la cuenta de la Bolsa para el Pago de Premios de la Lotería Pega Millones, la acumulación de premios no acertados de la Lotería "Pega 6" contenidos en el saldo de ¢2,552,967.50 (dos millones quinientos cincuenta y dos mil novecientos sesenta y siete colones con 50/100) acumulado al 31 de diciembre de 2009 y trasladado a la cuenta de patrimonio 3.1.4.01.01.01 "Resultado Acumulado de Periodos Anteriores" (Resultados 2.1.1 y 2.2.2).	Pendiente	La suma de la bolsa del juego Pega 6 *(con base en el oficio DCP-589 del 11 de mayo del 2012 estaba por ¢1.450.357,25; compuesto por un monto de 1,309,946.11 monto establecido hasta el sorteo No. 358 y ¢140,411.14 del No. 358 al No. 397)* que se tenía incluida en la bolsa contable de ¢2,552,967.50 reflejada al 31 de diciembre del 2009, no fue trasladada a la bolsa de Pega Millones. Actualmente, el juego de Pega Millones no existe, por lo cual la Administración debe decidir si traslada esta suma al fondo de Lotto (existe criterio legal mediante oficio AL-408 del 27 de abril del 2012 que señala: *"... cuando esta Institución realiza una modificación normativa de uno de estos juegos, debe tener presente que eventualmente la norma que se está derogando ya ha generado derechos para la generalidad de los consumidores del producto..."*).
11. Se valore por parte de la Administración el destino de los recursos citados en el punto anterior, dado que los mismos debieron formar parte del premio acertado al realizarse el sorteo No. 518 del 05 de mayo del 2012 (Resultados 2.1.1 y 2.2.2).	Pendiente	Al hacer la revisión, se observó que aún la Administración no ha decidido que destino darle a dichos recursos.
12. Se ajuste contablemente el registro del gasto de premios por los seis aciertos realizado mediante Comprobante N° 21514 del 31 de mayo de 2012 (premios entre los sorteos de Pega Millones No 398 al N° 518), dado que el saldo de ¢2,552,967.50 (dos millones quinientos cincuenta y dos mil novecientos sesenta y siete colones con 50/100) señalado en la recomendación N° 10, incluye el monto	Parcialmente Cumplida	En la revisión realiza por esta Auditoría, se comprobó que Contabilidad elaboró el comprobante No. 28253 con fecha contable 31 de julio del 2013, sin embargo lo hace por la totalidad de los ¢2,552,967.50, cuando debió hacerse sólo por lo correspondiente a Pega Millones, es decir ¢1.102.610.25 según DCP-589 del 11 de mayo del 2012. Pese a que el movimiento de

de los premios no acertados entre los sorteos N° 398 al N° 451, por lo que ya había sido afectado al gasto de premios según el procedimiento de registro de la Bolsa de Premios empleado por el Departamento de Contabilidad y Presupuesto hasta el 31 de diciembre del 2009. Lo anterior, conlleva eliminar este monto del saldo reflejado en la cuenta de patrimonio 3.1.4.01.01.01 "Resultado Acumulado de Periodos Anteriores" (Resultados 2.1.1, 2.2.1 y 2.2.2).		los ¢2,552,967.50 se encuentra afectado en la liquidación del juego 1320 (neteado con los 25, 0 millones, mencionado en la recomendación No. 9), esa cifra no es correcta, ya que este monto incluye tanto lo correspondiente al juego Pega 6 como Pega Millones. Este Departamento señaló que afectó las utilidades en el sorteo No. 1320, no obstante no se visualiza este ajuste en la liquidación mencionada.
13. Se recuerde a los funcionarios del Departamento de Loterías y del Departamento de Contabilidad y Presupuesto su responsabilidad de realizar un adecuado manejo del Fondo y la Bolsa para el Pago de Premios de la Lotería Pega Millones, tanto en las liquidaciones de los sorteos como en los registros contables.	Pendiente	El día 12 de diciembre del 2014, ante la consulta planteada por esta Auditoría: *"Poseen alguna circular, correo u otro donde se les comunique a los funcionarios de contabilidad y loterías, sobre la responsabilidad de un adecuado manejo del fondo y la bolsa aplicable al nuevo juego Lotto?"*, vía correo electrónico al Departamento de Contabilidad, este último mencionó: *"... se analizó con los funcionarios encargados del registro del fondo del departamento de Contabilidad y Presupuesto y se coordinó con Tecnologías de Información para su control, lo indicado como respuesta a este punto:* *"**R/**Se realizó la solicitud de informática número 823 del 28 de Junio del 2013, en la que se solicitó la creación de la liquidación para los juegos de la Lotería Electrónica Lotto, la cual incorpora el control del pozo acumulativo, la bolsa y la reserva (se adjunta liquidación del sorteo número 1321 del 05 de Junio del 2013). "* *No se conoce de la existencia de Circular, correo u otro en donde se indique la responsabilidad de un adecuado manejo del fondo y la bolsa aplicable al nuevo juego Lotto."* **(El subrayado no es del original)** Con base en lo anterior, se observa que el departamento de Contabilidad no ha girado instrucciones a los funcionarios del Departamento Administración de Loterías y del Departamento Contable Presupuestario, recordándole la responsabilidad de realizar un adecuado manejo del Fondo y la Bolsa para el Pago de Premios de la Lotería Pega Millones, tanto en las liquidaciones de los sorteos como en los registros contables.

Informe AI JPS N° 17-2013 Estudio sobre las Compras de Equipos de Cómputo realizadas a Componentes El Orbe S.A., Comprendidas entre los períodos 2009, 2010 Y 2011 inclusive

Dirigido a: Departamento de Tecnologías de la Información, Departamento de Recursos Materiales **Fecha** 20 de noviembre, 2013

Recomendación	Estado de la recomendación	Seguimiento
Recursos Materiales		
5. Solicitar al Departamento de Informática, que incorpore en el Sistema del Registro de Proveedores una herramienta eficaz que notifique al encargado del mantenimiento del Registro de Proveedores, con una antelación mínima de quince días, la fecha de expiración de la inscripción del proveedor, de tal forma que el funcionario de proveeduría pueda informar a los proveedores con suficiente antelación para que procedan con la actualización de su información, en caso contrario, si el proveedor no actualiza la información, excluirlo del registro correspondiente, las actualizaciones al registro de proveedores deberán quedar documentadas mediante correo electrónico, fax o cualquier mecanismo que el Departamento de Proveeduría considere conveniente (Ver punto N° 3.4.2 del apartado Resultados del Estudio).	Pendiente	Mediante oficio AI-666 del 5 de setiembre del 2014 dirigido al señor Milton Vargas Mora, Gerente General, se citó: *"...* *No obstante, el interés de esta Auditoría Interna es que no sean invitados a contrataciones los proveedores que no actualicen su inscripción. Se solicita indicar el mecanismo que será empleado para la inactivación (si se estableció como un procedimiento para el encargado del registro o bien el sistema lo realiza en forma automática), así como la copia de las respectivas "Mesas de ayuda" tramitadas."* En cumplimiento con esta recomendación el señor Milton Vargas Gerente General, a través del oficio GG-2430-2014 del pasado 29 de setiembre de 2014, adjuntó el Anexo 1 *"GG-2224-2014"* del 16 de setiembre del 2014, emitiendo la siguiente instrucción: *"6- En los casos donde vence el plazo de inscripción lo que corresponderá es la exclusión del registro de proveedores, según artículo N° 124 del Reglamento de Contratación Administrativa. La figura de la inactivación procede según articulo N° 123 del Reglamento de Contratación Administrativa, en los casos donde un proveedor sin justa causa no participe en procesos de contratación habiendo sido invitado en tres ocasiones, o bien cuando se negare actualizar la información cuando la Administración así lo haya pedido* *No obstante lo requerido es que no sean invitados a contrataciones los proveedores que no actualicen su inscripción."*

		Por otro lado, por medio del Anexo 2 *"RM-1413-2014"* de ese mismo oficio GG-2430-2014 se mencionó: *"6. Mediante mesa de ayuda 405 se está solicitando al Departamento de Tecnologías de la Información que se alerte al proveedor dos meses antes de la expiración con el fin de que actualice su registro oportunamente.* *Se confecciona una mesa de ayuda (ver copia adjunta) para que se incorpore en el sistema que cada vez que un proveedor no participe se le haga una anotación y se le envíe una advertencia por correo y que el sistema lo inactive a la tercera vez. No obstante, se hace la advertencia que esta medida puede disminuir el número de proveedores en el Registro lo que cual en un momento dado puede ocasionar inconvenientes."* El 21 de noviembre del 2014 se verificó el estado de la solicitud de servicio número 0405-2014, y aún se encuentra en *"Asignado en Proceso"* por el Departamento de Tecnología de la Información, por otro lado, si bien es cierto, en dicha solicitud se señala que se informe al proveedor de que debe actualizar sus datos, también debe ser comunicado el responsable del mantenimiento del Registro de Proveedores, y en los caso en que el proveedor no tenga correo, será responsabilidad del encargado del mantenimiento informarles. Así también, donde se cita *"3-SE COLOQUE EN CONDICION "INACTIVOS" A TODOS AQUELLOS PROVEEDORES QUE SE INVITEN Y NO PARTICIPEN."*, es importante mencionar que la inactivación será hasta la tercera vez de que se invitan y éstos no participan.
6. Incorporar en el Manual de Procedimientos, un mecanismo adecuado en donde se establezca la rotación de los proveedores para ser invitados en los procesos de contratación, garantizando una apropiada participación (Ver punto N° 3.4.2 del apartado Resultados del Estudio).	Pendiente	Por medio del oficio AI-666 del 5 de setiembre del 2014, esta Auditoria indicó: *"Emplear un mecanismo aleatorio elegido automáticamente por el sistema, no garantiza una adecuada rotación de los proveedores, lo pertinente es fijar criterios tales como los sugeridos por el legislador, como el orden cronológico entre otros."* **(El subrayado no es del Original)**

		Mediante el oficio GG-2430-2014 del pasado 29 de setiembre de 2014, el señor Milton Vargas Gerente General, citó: *"La rotación tiene como propósito dar oportunidad a todos los proveedores inscritos, ya que actualmente se escogen en forma aleatoria, con la invitación a la totalidad de los proveedores, no solo se cumple con la recomendación de la Auditoría Interna, sino que se supera porque no solo se invitan todos los proveedores sino que le da más transparencia al proceso.* *De estar de acuerdo la Auditoria Interna con la sugerencia anterior sobre invitar a todos los proveedores, se procedería a eliminar el punto 2 de la mesa de servicio N°405-2014 (Adjunta al ANEXO 6)."* Tal y como se señaló en el oficio AI-666 no se recomienda la rotación de los proveedores a invitar, por lo que se acoge lo mencionado por la Gerencia sobre invitar a la totalidad de los proveedores, siendo un proceso más transparente. Asimismo, el mecanismo que ha utilizar, deberá ser incorporado en el Manual de Procedimientos.
7. Tramitar en caso de ser requerido, las eventuales consultas ante la Asesoría Legal, con el propósito de establecer los mecanismos a utilizar, a efectos de recuperar las sumas cobradas de menos en las multas establecidas por incumplimientos con el plazo de entrega del bien contratado, ya sea a los proveedores o bien a los funcionarios responsables, así como gestionar y dar seguimiento a dicho proceso, informando de las gestiones a esa Gerencia General y a esta Auditoría Interna (Ver puntos N° 3.4.3.1 y N° 3.4.3.2 del apartado Resultados del Estudio).	Parcialmente Cumplida	Mediante oficio GG-2225-2014 del pasado 10 de setiembre de 2014, el señor Milton Vargas Mora, Gerente General, señalo: *"... lo citado en el Acta 29-30 JULIO. Obedece al segundo caso, correspondiente a la Contratación Directa 2010CD-0573-Prov, en donde el proveedor entregó parte de los componentes del equipo en forma posterior al vencimiento del plazo de entrega.* *...* *Por lo cual es necesario conocer su criterio sobre lo anteriormente expuesto por la Auditoría Interna.* *..."* En relación a la respuesta emitida por la Asesora Jurídica la señora Marcela Sánchez Quesada, a través del oficio AJ-1013 del 16 de setiembre del 2014, mencionó:

		"... lo que corresponde es determinar por medio de un procedimiento administrativo, sustanciado a la luz de lo establecido en el ordinales 93 y 98 de la Ley de Contratación Administrativa y consecuentemente en el artículo 308 siguientes y concordantes de la Ley General de la Administración Pública No.6227 del 2 de mayo de 1978, para determinar si por parte de uno o varios funcionarios de la institución que intervinieron en ese proceso, se incurrió en algún tipo de responsabilidad tanto disciplinaria como pecuniaria... *No se puede dejar de mencionar, que en caso de no estar debidamente individualizadas e identificadas las personas y los hechos sobre los que se deba realizar la intimación e imputación de cargos respectivo, la Administración tiene la facultad de ordenar una investigación preliminar que le brinde los elementos necesarios para llevar a cabo el procedimiento administrativo correspondiente."* Dado lo anterior, se observa que la Gerencia se encuentra analizando la apertura de un procedimiento administrativo en caso de ser necesario.
8. Establecer la sanción de apercibimiento sobre los proveedores que incumplan con el plazo de entrega del bien (Ver punto N° 3.4.3.1 del apartado Resultados del Estudio).	Pendiente	Por medio del oficio AI-666 del 5 de setiembre del 2014, esta Auditoría señaló: *"Se solicita copia del documento o procedimiento mediante el cual se materializó el acatamiento de esta recomendación."* El señor Milton Vargas Gerente General, a través del oficio GG-2430-2014 el pasado 29 de setiembre de 2014, mencionó: *"Dado que nuestra Unidad acata la recomendación de la Auditoría interna a partir del mes de julio del presente año, para la aplicación de inhabilitaciones en los casos de reincidencia, no es posible remitir documentación al respecto puesto que aún no se han presentado situaciones en las que debamos aplicar este mecanismo sancionatorio."* Por lo tanto, dado que al 3 de diciembre del 2014, no ha sido recibida ninguna copia sobre el cumplimiento de esta

		recomendación, la misma queda pendiente, hasta verificar el acatamiento de la misma.
10. Realizar los pasos del proceso de contratación en forma apropiada, de forma tal que no se omitan verificaciones o cumplimientos vitales en este trámite de adquisiciones (Ver punto N° 3.4.3.2 del apartado Resultados del Estudio).	Pendiente	En el oficio GG-2430-2014 del pasado 29 de setiembre de 2014, el señor Milton Vargas, señaló: *"Para atender lo expuesto se emitieron los oficios GG-2223-2014 (ANEXO 3) y GG-2379-2014 (ANEXO 4) y para lo que nos ocupa se recibió la circular 08-2014 de Recursos Materiales (ANEXO 8) que remite lo solicitado."* En la revisión efectuada a los anexos citados en el oficio anterior, no se muestran los pasos del proceso de contratación en forma apropiada, tal y como lo menciona esta recomendación.
Tecnologías de la Información		
2. Verificar que, las especificaciones técnicas indicadas en el cartel coincidan con las características entregadas por el proveedor, esto antes de recibir el equipo. (Ver punto N° 3.1.2 del apartado Resultados del Estudio).	Pendiente	Por medio del oficio AI-666 del 5 de setiembre del 2014 esta Dependencia señaló: *"Se solicita **aportar copia del procedimiento de recepción de bienes** a que se hizo referencia, así como **el documento u otro** mediante el cual fue puesto a conocimiento de las unidades que reciben bienes."* La documentación aún no ha sido recibida por esta Auditoría.
3. Determinar el costo promedio en el mercado del bien por adquirir, de tal manera que se adjudiquen ofertas donde el precio no se desvíe en forma importante de este promedio de mercado (Ver punto N° 3.4.1 del apartado Resultados del Estudio).	Parcialmente Cumplida	Por medio del oficio AI-666 del 5 de setiembre del 2014 esta Dependencia señaló: *"Se solicita aportar el documento u otro donde se estableció este nuevo procedimiento, no se omite manifestar que **debe ser de aplicación en la totalidad de los casos donde se reciba una única oferta** de contratación, y no solo en los casos en que la única oferta supere el presupuesto autorizado."* Ante lo anterior, el señor Milton Vargas, Gerente General, a través del oficio GG-2430-2014 del 29 de setiembre del 2014 citó: *"El documento requerido es la suscripción del Acta 29-30 Julio,*

		de la cual la Auditoria Interna tiene copia; sin embargo para reiterar lo expuesto en el acta, se emitió el oficio GG-2224-2014 al área de Recursos Materiales y Tecnologías de la Información. ***(Anexo 1)"*** En el Anexo 1 mencionado, hace referencia al oficio GG-2224-2014 del 16 de setiembre del 2014, donde al señor Ronald Ortiz jefe de Tecnologías de la Información se le gira la siguiente instrucción: *"5- En la totalidad de los casos (no solo en los que casos en que la única oferta supere el presupuesto autorizado) en que se reciba una única oferta de contratación, deberá determinarse el costo promedio en el mercado del bien por adquirir. (Según lo indicado en el Acta 29-30 Julio en la página 5 para la recomendación 3"* Al hacer la verificación a los expedientes números N° 2014LA-000004-PROV *"Adquisición de computadoras de escritorio y portátiles"*, y N° 2014CD-000336-PROV-01 *"Compra e Instalación de un dispositivo de almacenamiento de alta disponibilidad."* se comprobó que no se incluyó ningún oficio en donde se incorpore el costo promedio en el mercado del bien por adquirir, pese a la instrucción girada por medio del oficio GG-2224-2014.

ANEXO N° 2

Detalle de las recomendaciones emitidas por el Área de Sistemas de la Auditoría Interna (Cumplidas)

Informe AI JPS N° 32-2010 Estudio sobre la verificación de la seguridad en la comunicación de datos entre los entes externos y la institución, relacionada con los productos que comercializa la junta de protección social

Dirigido a: Departamento Tecnologías de la Información **Fecha** 28 de diciembre, 2010

<table>
<tr><th>Recomendación</th><th>Estado de la recomenda-ción</th><th>Seguimiento</th></tr>
<tr><td colspan="3">D. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO ALTO</td></tr>
<tr><td>4.Estado de Certificados SSL (Secure Socket Layer).
Realizar un estudio con la finalidad de analizar la posibilidad de utilizar certificados altamente seguros para los sitios transaccionales, doffnde la sana práctica indica que debe ser Clase A+ (Solo Cifrados de Seguridad Excelente) para la protección de la información que es procesada por la web transaccional y enviar copia de dicho estudio a Auditoría Interna.

A continuación la tabla que indica cuales son las mejores prácticas de este certificado:
<table>
<tr><td>DH-DSS-AES256-SHA</td><td>Excellent Security</td><td>All of the excellent security ciphers utilize 256 bit AES keys for encryption. This cipher uses fixed Diffie Hellman for key exchange and DSS for authentication.</td></tr>
<tr><td>DH-RSA-AES256-SHA</td><td>Excellent Security</td><td>Similar to the one above, this one uses RSA for authenticationi</td></tr>
<tr><td>DHE-DSS-</td><td>Excellent Security</td><td>The next two ciphers are similar to the previous two respectively</td></tr>
</table>
</td><td>Cumplida</td><td>El pasado 8 de agosto del 2014 por medio del oficio GG.1847-2014, se adjuntó el Informe "Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información", en el cual respondieron:

"1. Se deshabilitó el sitio web transaccional http://secure.jps.go.cr/jpsvirtual/login.html ya que dicho sitio dejo de ser utilizado por la Institución. No obstante los sitios web de cajas y agencias aún se mantienen en producción y los mismos presentan una clase A- sin embargo se encuentran en plan de migración hacia la plataforma Citrix, por lo que los certificados SSL se aplicaran en caso de que se desista del plan de migración con el fin de no incurrir en el gasto de recursos.
2. Se implementó la plataforma Citrix que dentro de sus funcionalidades realiza el cambio de premios, despachar loteria, entre otros. Esta plataforma posee un mecanismo de autenticación basado en tres pasos (ver Anexo 01 – Pasos de mecanismo de autenticación) lo que refuerza el mecanismo de seguridad de acceso a la plataforma."

"En caso de no efectuar la migración de los sitios web de cajas y agencias, se implementará mediante el uso de la herramienta IIS Crypto los certificados SSL de acuerdo a las buenas prácticas.
Adicionalmente se efectuó un análisis sobre el estado de los certificados SSL de los diversos sitios web con el fin de estudiar el grado de fiabilidad</td></tr>
</table>

	AES256-SHA		differing only in their use of ephemeral Diffie Hellman for key exchange which for reasons explained above is considered to be more secure	
	DHE-RSA-AES256-SHA	Excellent Security	Using ephemeral Diffie Hellman for key exchange and RSA for authentication, this cipher is similar the one above	
	AES256-SHA	Excellent Security	The standard excellent security cipher uses a 256 bit AES encryption key and RSA for both key exchange and authentication	
	Se recomienda la utilización de un segundo factor de autenticación para los usuarios en línea del tipo contraseña de un solo uso (One Time Password OTP). Además, otra opción de validación recomendada es una infraestructura de llave pública (Public Key Infrastructure, PKI) que soporte la utilización de Firma Digital (DS - Digital Signature) para validar las transacciones que realiza cada uno de los clientes una vez autenticados en el sitio transaccional y así contar con todas las ventajas que ofrece la utilización de Firmas Digitales.			*de las plataformas web. (ver anexo 36 – Análisis sobre el estado de los certificados SSL)"* Adicional a lo anterior, dentro del resultado del anexo 36 – Análisis sobre el estado de los certificados SSL se señaló: *"... El cifrado RC4 es débil y la única razón para justificar su habilitación suele ser la mitigación del ataque BEAST que si es un riesgo alto y continua siendo aún una amenaza. Además el cifrado RC4 al deshabilitarlo podría afectar el servicio de conexión entre el cliente y el servidor, por lo que su deshabilitación no debe efectuarse a la ligera.* *Aún el riesgo no es crítico, sin embargo con los cambios tecnológicos y aumento de amenazas informáticas en un futuro se podría convertir en un riesgo crítico para la organización, por lo que se recomienda la habilitación de una plataforma de pruebas para realizar el experimento de la deshabilitación del cifrado RC4 y de la opción forward secrecy y observar la capacidad de respuesta* *...* *Los resultados anteriores retroalimentan el estado del grado de los certificados de los sitios institucionales, por lo que se afirma la Junta de Protección Social se encuentran deniro de un rango aceptable, destacando si la importancia de las oportunidades de mejora. Adicionalmente cabe destacar que para la plataforma citrix el reforzamiento del proceso de autenticación se basa en un mecanismo de doble autenticación lo que permite contar con un control más robusto de acceso."* Esta Auditoría da por cumplida esta recomendación en el entendido de que se encuentra el certificado dentro de un rango aceptable, sin embargo es importante que tomen en cuenta el cifrado RC4 dado que es débil y podría provocar en un futuro un riesgo institucional.
	5.Ausencia de un servidor de pruebas y desarrollo. Se recomienda: o Separar físicamente el ambiente de desarrollo y pruebas del ambiente de producción. o Eliminar del ambiente de producción en todas las bases de		Cumplida	En el oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, respondiéndose: *"1. Se separó el ambiente de desarrollo del ambiente de producción con el fin de aplicar las mejores prácticas y minimizar la posibilidad de manipulación y pérdida de integridad, confidencialidad y disponibilidad*

datos de pruebas. o Aplicar una revisión de accesos al ambiente de producción (sistema operativo y base de datos), para asegurar que el personal de desarrollo no posea acceso a este ambiente.		*de la información. Se eliminó el acceso de los funcionados internos no autorizados y usuarios externos al ambiente de producción dejando únicamente a los usuarios rortiz, lramirez, mmasis y jcruz con acceso al ambiente de producción esto de acuerdo a la labor de sus funciones.* *El ambiente de desarrollo es un ambiente de pruebas en el que llenen acceso los analistas desarrolladores para la ejecución de las pruebas de desarrollo que posteriormente serán instaurados en el ambiente de producción"* En la revisión efectuada, se observó que existen dos servidores uno de pruebas utilizado por los programadores y otro para el ambiente de producción.
6.Analista programadores con acceso al servidor de producción. Eliminar los accesos de los analistas programadores al ambiente de producción.	Cumplida	En el oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, indicando: *"1. Se eliminaron los accesos de consulta y de modificación de los analistas programadores al ambiente de producción. Únicamente los usuarios lramirez, mmasis, jcruz y rortiz tienen acceso, debido a la responsabilidad de sus funciones en el departamento de Tecnologías de Información. Esta recomendación fue acogida con el fin de cumplir con las buenas prácticas de manipulación de la información"* En la verificación realizada a los programadores Zúrika Ruíz Gonzáles, Saulo Villalobos Figueroa, se comprobó que no tenían acceso al ambiente de producción.
E. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO MEDIO		
12.La opción Allow Remote Access está habilitada. En un ambiente de pruebas, desactivar el parámetro de conexiones remotas y evaluar el impacto que este genera en la plataforma. Documentar el resultado de la prueba en el ambiente de pruebas y determinar si el mismo procede para su aplicación en producción.	Cumplida	A través del oficio GG.1847-2014 del 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el Departamento de Tecnologías de la Información"*, y se mencionó: • *"Control implementado"* *"1. Se configuró el parámetro de la opción Allow Remote Access en 1.* *Este parámetro se configuro en dicho valor ya que se requiere para la*

		realización de respaldos diarios de la organización, caso contrario no se podrían ejecutar los respaldos. ..." • *"Comentarios/Observaciones"* *"Se realizó la consulta adicional los consultores especializados en el manejo de la Base de Datos Sybase, y los mismos indicaron que si la opción Allow Remote Access no se configura en 1, imposibilitaría realizar los respaldos o copias de seguridad de la Base de Datos."* Dada la necesidad expresada por mantener habilitado el parámetro, esta Unidad da como Cumplida dicha recomendación, haciendo el recordatorio que el manejo de la seguridad de los servidores se encuentra bajo responsabilidad del Departamento de Tecnología de la Información.
15.Usuarios por defecto activos y sin contraseña. Se recomienda configurar una contraseña para todos los usuarios por defecto e incluir en el procedimiento de instalación, la modificación de contraseñas por defecto.	Cumplida	En el oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1.Se implementó el cifrado correspondiente a cada uno de los usuarios que se detectaron no estaban con el cifrado correspondiente en cada uno de los servidores mencionados en el informe AI-05-2013:* *Servidor 10.0.0.240 : Se cifraron los usuarios daemon, bin, sys, adm, lp, uucp, nuucp,smmsp, postgres* *Servidor 10.0.0.90 : daemon, bin, sys, adm, lp, uucp, nuucp, smmsp* *Servidor 10.0.0.200 : daemon, bin , sys, adm, lp, uucp, nuucp, smmsp* *Servidor 192.166.1.50 : daemon, bin, sys, adm,lp, uucp,nuucp,smmsp* *Servidor 192.168.1.2 (Servidor Web Yire) este servidor dejo de estar en producción.* *Servidor 192.168.1.102: daemon, bin, sys, adm, lp, uucp,nuucp,smmsp* *Servidor 10.0.0.246 : daemon, bin,adm,lp, uucp* *Servidor Desarmllo-v490 : bin, sys, adm,lp, uucp, nuucp,smmsp* *Los equipos 10.0.0.4, 10.0.0.5, 10.0.0.6 son equipos alojados en el sistema que aloja el firewall institucional Checkpoint.* *Únicamente cuenta con los usuarios administradores autorizados."* Al hacer la revisión se observó que los usuarios fueron bloqueados de

		acuerdo al parámetro adecuado *LK*. No obstante, se indica que se acoge lo señalado mediante oficio GG.1847-2014 donde cita: *"Únicamente cuenta con los usuarios administradores autorizados"*, haciendo mención que los usuarios creados como administradores es responsabilidad del Departamento de Tecnologías de la Información.
18.Debilidades en la configuración de usuarios en los servidores Sun Solaris. Realizar un análisis de los usuarios mencionados en el punto N° 18 de Resultados del Informe 32-2010 denominado *"Estudio sobre la verificación de la seguridad en la Comunicación de Datos entre los entes externos y la Institución, relacionada con los Productos que comercializa la Junta de Protección Social"* con el fin de remover los usuarios que no son requeridos. Documentar cuales son los usuarios permitidos y quién es el encargado de éstos. Comunicar a la Auditoría Interna sobre resultado de ese análisis.	Cumplida	El pasado 8 de agosto del 2014 por medio del oficio GG.1847-2014, se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, en el cual respondieron: *"1. Se eliminaron los usuarios genéricos (cmona, desa) que se encuentra en los servidores institucionales Sun Solaris y que se determinó justificación alguna su permanencia en el servidor.* *Adicionalmente en la consola de administración del firewall se eliminó de los usuarios administradores a: Sefisa, Soporte."* Además, indicaron: *"El usuario monitor no fue removido debido a que el mismo es utilizado como porte del monitoreo a los equipos Sun Solaris y por lo tanto es indispensable su habilitación.* *El usuario hde no fue eliminado porque pertenece al sistema institucional de actas y en caso de deshabilitarlo afectaría el servicio de gestión del aplicativo. No obstante se procede a cifrar.* *Se hace hincapié en este documento en que no se deben crear usuarios en los servidores institucionales sin la debida justificación del caso. El área de Producción es responsable de la administración de usuarios dentro de los equipos servidores institucionales."* Se acoge lo señalado en esta recomendación, no obstante se recuerda que es responsabilidad del Departamento de Tecnologías de las Información el uso y la seguridad que se les dé a los usuarios creados en los servidores Sun Solaris.
F. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO BAJO		
26.Ausencia de política y/o procedimiento de restauración.	Cumplida	En el oficio GG.1847-2014 del 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría*

Diseñar y elaborar un procedimiento para la ejecución de pruebas de legibilidad de la información, donde quede evidencia de la frecuencia de ejecución, formulario de la solicitud del proceso y una bitácora del resultado obtenido. El formulario de solicitud al menos debe contar: • Departamento que solicita. • Persona que solicita. • Información que solicita. • Fecha de solicitud. • Autorización de la Jefatura del Departamento de Informática. Bitácora de resultado: • Fecha de ejecución. • Información restaurada. • Resultado de la restauración. • Persona que ejecuta. • Firma de la jefatura del Departamento de Informática.		*Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se actualizó y ajusto el procedimiento institucional "PR-GRR-2013 Procedimiento Generación de respaldos" y se comunicó al responsable de la generación y utilización de dicha normativa, seguir de acuerdo al procedimiento institucional la documentación o registro de la "BITACORA DE RESPALDOS Y RESTAURACIONEES DE BASES DE DATOS Y COMUNICACIONES" y del formulario de solicitud de respaldo y recuperación tal y como se anexa en dicho procedimiento.* *Este procedimiento se observa en el anexo 08 – PR-GRR-2013 Procedimiento Generación de respaldos."* Se comprobó el procedimiento *"Generación de respaldos"*, el cual incluye el formulario para los respaldos de bitácoras, cumpliéndose con lo citado en dicha recomendación.

Informe AI JPS N° 31-2010 Estudio relacionado con una revisión general de usuarios en los servidores Institucionales.

Dirigido a: Departamento de Tecnologías de la Información **Fecha** 27 de diciembre de 2010

<table>
<tr><th>Recomendación</th><th>Estado de la recomendación</th><th>Seguimiento</th></tr>
<tr><td colspan="3">A los Departamentos de Tecnologías de la Información y Desarrollo del Talento Humano:</td></tr>
<tr><td colspan="3">Al Departamento de Tecnologías de la Información:</td></tr>
<tr><td>5. Establecer requerimientos mínimos que deben contener las claves de acceso a la red e incorporarlos al "Active Directory", deben considerarse aspectos tales como: la longitud de la clave, combinación de números y letras, caracteres especiales y otros aspectos a considerar por el Departamento de Informática. (Punto C. del Apartado II del Informe JPS N° 31-2010 denominado "Estudio relacionado con una revisión general de usuarios en los servidores Institucionales").</td><td>Cumplida</td><td>De acuerdo con la circular I 334-2013 el Departamento de Tecnologías de la Información, emitió un enunciado sobre las políticas de contraseña para accesar Windows indicando:

"...plazo de vigencia máxima 42 días y la nueva clave debe tener los siguientes requerimientos: longitud mínima de 8 caracteres, debe incluir mayúsculas, minúsculas, números y caracteres especiales..."

No obstante, en oficio GG.1847-2014 del 8 de agosto del 2014 se adjuntó el Informe "Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información", donde se respondió:

"1. Se configuró en la directiva de contraseña del active directory los siguientes parámetros de acuerdo al manual de buenas prácticas de configuración de active directory y políticas de seguridad institucionales:

<table><tr><td>Exigir historial de contraseñas</td><td>24</td></tr><tr><td>Las contraseñas deben cumplir los requisitos de complejidad</td><td>Habilitado</td></tr><tr><td>Longitud mínima de la contraseña</td><td>9</td></tr><tr><td>Vigencia máxima de la contraseña</td><td>90 d</td></tr><tr><td>Duración del bloqueo de cuenta</td><td>15 mm</td></tr><tr><td>Restablecer recuentos de bloqueo de cuenta tras</td><td>15 mm</td></tr><tr><td>Almacenar contraseña usando cifrado reversible</td><td>Deshabilitado</td></tr><tr><td>Vigencia mínima de la contraseña</td><td>1</td></tr><tr><td>Umbral de bloqueo de la cuenta</td><td>5</td></tr></table>
"

En la revisión del reporte de resultados de directivas de grupo, se comprobó que las directivas de contraseñas citadas mediante oficio GG.1847-2014 se encuentran aún vigentes en el "active directory".</td></tr>
</table>

Estudio: 29-2010 "Seguimiento de recomendaciones giradas por el área de sistemas de la Auditoría Interna"
Este informe incluye los Informes N° 06-2008, N° 07-2009 y N° 10-2009, según el siguiente detalle:

Informe AI JPS N° 06-2008 Estudio sobre la verificación de la seguridad en el manejo de las transferencias electrónicas de fondos y la seguridad, integridad y consistencia de la información contenida en las bases de datos institucionales referentes al manejo de las loterías.

Dirigido a: Departamento de Tecnologías de la Información **Fecha** 19 de junio, 2008

Recomendación	Estado de la recomendación	Seguimiento
14. La documentación que explica los estándares que se deben utilizar para la creación de objetos en la base de datos, no son acatados en su totalidad, debido a que aún existen tablas con nombres no estandarizados, por lo tanto se recomienda seguir los estándares en las tablas que conforman las bases de datos.	Cumplida	De acuerdo con el oficio GG.1847-2014 del 8 de agosto del 2014, en la referencia al hallazgo número 2 denominado "Estándares para la creación de objetos en la base de datos", se citó: *"Nota: Los nombres de tablas que no cumplen el estándar de creación no se procedieron a eliminar debido a lo siguiente. Se realizó el análisis en conjunto con el consultor especializado de la BD y personeros del área de Producción de TI, y es un tema que podría afectar los registros o datos de la base de datos, puesto que el cambio del nombre de la tabla podría desencadenar algunos problemas de conectividad entre el motor de BD y aplicaciones. El riesgo puede ser crítico para la organización y la recomendación es no realizar el cambio .Se hace hincapié a los funcionarios del área de Producción de TI que a partir de la fecha actual la creación de objetos o tablas en la Base de Datos debe cumplir estrictamente con el estándar de creación asignado."* **(El subrayado no es del original)** Con base en la justificación planteada por dicha unidad, se toma la recomendación como cumplida.

Informe 07-2009 Seguimiento de recomendaciones giradas por la Auditoría Interna al Departamento de Informática en el Informe N° 08-2006 referente a "Estudio relacionado con la página Web de la Junta de Protección Social de San José"

Dirigido a: Departamento de Tecnologías de la Información **Fecha:** 20 de abril, 2009

Recomendación	Estado de la recomendación	Seguimiento
2. Corregir el error que presenta el gráfico en la Sección de Acción Social al ingresar a *"Distribución de utilidades de lotería a organizaciones de bienestar social período 2005 según leyes establecidas"*, por cuanto las cifras del gráfico no corresponden al cuadro que da su origen. (Punto B.1 del informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	Según la revisión efectuada a la página web institucional se comprobó que el gráfico no está en la Sección de Acción Social, por lo que no se detectó la *opción "Distribución de utilidades de lotería a organizaciones de bienestar social periodo 2005 según leyes establecidas"*. Así mismo, a través del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, respondiéndose: *"... en el sitio web web www.jps.go.cr esta opción no se encuentra habilitada. ..."*
10. Incorporar una guía clara para el usuario en la "Sección de búsqueda de actas" así como indicar que actas están disponibles dentro de la base de datos, de esta forma el usuario puede llevar a cabo una búsqueda más acertada y no crearse expectativas sobre información que no esté disponible. (Punto D.1. del informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"... no se evidenció en ninguna sección el ítem de búsqueda de actas esto debido al cambio del sitio web anterior. El sitio web fue rediseñado en el año 2012 por lo tanto dicha sección fue removida. ..."* Al hacer la revisión en la página web se comprobó que dicha sección de búsqueda no fue incluida en el nuevo sitio web.
11. Revisar y corregir el motor de búsqueda disponible en la página Web de la Junta debido a las siguientes razones :	Cumplida	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de*

Los rangos de búsquedas que se listan a continuación no producen ningún resultado: (Punto D.2. del informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*). Del 01 de enero al 31 de diciembre 2006 Del 01 de enero al 31 de diciembre 2005 Del 01 de enero al 31 de diciembre 2002 Del 01 de enero al 31 de diciembre 2001 Del 01 de enero al 31 de diciembre 2000 Del 01 de enero al 31 de diciembre 1999 Del 01 de enero al 31 de diciembre 1998 El rango de búsqueda que va del 1° de enero al 31 de diciembre del 2003 y del 1° de enero al 31 de diciembre del 2004, presenta solamente un acta que dice "acta de prueba 5000". Asimismo, el rango entre el 1° de enero al 31 de diciembre de 1964, proyecta los resultados que van del 14 de octubre de 1963 al 26 de julio de 1965. (Puntos D.3 y D.4 del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).		*Tecnologías de Información"*, donde se respondió: *"Se implementó un motor de búsqueda personalizado para el sitio web el cuál cumple a cabalidad con las búsquedas que sean seleccionadas."* En la revisión efectuada al sitio web el día 23 de setiembre del 2014, se observó la existencia de un motor de búsqueda a nivel general, el cual despliega las diferentes opciones sobre el tema requerido.
12. Establecer un índice para las actas de Junta de Directiva, de tal forma que, si a través de una búsqueda el usuario no ubica la información deseada, entonces que lo pueda hacer a través del índice. (Punto D.5. del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se implementó un motor de búsqueda personalizado para el sitio web.* *..."* En la revisión efectuada se determinó que la sección de actas no se encuentra en dicha página, ya que la misma ha sido eliminada. Con respecto a la búsqueda de diferentes documentos estos efectivamente se pueden realizar.
15. Dentro de "Propiedades disponibles para la venta y sus ubicaciones" existe en la parte inferior otra opción de	Cumplida	La página web de la institución no posee un titulo idéntico al señalado en esta recomendación *"Propiedades disponibles para la*

búsqueda, la cual también debe ser ajustada por cuanto la misma presenta un error. En este mismo bloque deben corregirse los enlaces que posee para devolverse a la Página Principal y a la Sección de Cementerios. (Se debe indicar que el texto "Propiedades disponibles para la venta y sus ubicaciones" no es una sección específica del menú, sino el resultado de una búsqueda realizada con la palabra *propiedades...* (Punto F.2. del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*) .		*venta y sus ubicaciones"*, sin embargo, se creó el siguiente *"Lista de Propiedades de cementerios disponibles"*, en relación a las opciones para devolverse a la página principal y a la sección cementerios la misma se encuentra en funcionamiento.
17. Agregar en las Subsecciones de: "Metodología y estándares para el Desarrollo de Sistemas de la Junta de Protección Social de San José" y de "Manuales de Procedimientos", un índice con enlaces entre éste y su contenido, así como un motor de búsqueda. En estas mismas secciones se recomienda estandarizar la presentación del texto tal como se presenta en secciones como Legislación y Acción Social entre otras. (Puntos G.2. y G.3 del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	Al verificar la página web se comprobó que la sección *"Metodología y estándares para el Desarrollo de Sistemas de la Junta de Protección Social"*, y *"Procedimientos"* se encuentran dentro de la opción *"Transparencia Institucional"*, se verificó el uso del motor de búsqueda, las secciones Legislación y Acción Social en el nuevo diseño, no fue posible localizarlos.
21. Establecer como estándar que, cada vez que se ingrese a una sección del menú "Conózcanos", dicha sección, en tanto el usuario permanezca dentro de ésta, quede marcada, ya sea por cambio de color o tamaño del texto, esto ayudará al usuario a saber en todo momento cual parte está visitando. (Punto J.2. del informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	Al revisar la página web se observó que la misma es llamativa, a pesar de que el menú *"Conózcanos"* no se encuentra, existe un menú denominado *"¿Quiénes somos?"*, no obstante el sitio actual fue diseñado.
22. Valorar si es conveniente establecer en forma visual dentro de la página Web un registro del número de visitantes a la misma. (Punto J.3. del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	Se da por cumplida en el entendido de que la recomendación iba en función de que Informática valorara si era necesaria su implementación.
25. Analizar la posibilidad de dar movimiento y cambios graduales a las fotos que aparecen, tanto en la parte superior como en la parte inferior de la página Web. (Punto K.1. del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	El oficio GG.1847-2014 del 8 de agosto del 2014 posee adjunto el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"... la página principal presenta una variación pues se presenta*

		en video algunas de las últimas actividades que la JPS ha venido realizando e implementando, por lo que se evidencia en cierto modo movimiento, audio en el sitio web. … " A pesar de que la recomendación indica que las fotos deben mostrar movimientos y cambios graduales en la parte superior o inferior de la página, esto se ve reflejado en el centro de la página al visualizar el video con información de la institución.
27. Finalmente se recomienda un rediseño total del sitio Web de la Institución, que además de tomar en consideración las anteriores recomendaciones, contemple al menos las siguientes características: » Que contenga una página principal que sirva de punto de referencia hacia la información pertinente. » Que la página principal posea enlaces hacia otras ventanas y que éstas contengan la información respectiva. » Que no se concentre excesiva información en la página principal, solo los elementos de referencia.	Cumplida	Actualmente, se hizo un rediseño en la página web, y se encuentra en producción. En donde se comprueba que dicha página posee enlaces hacia otras ventanas, además de mostrarle al usuario, información relativa a los distintos sorteos y tipos de lotería.

Recomendación	Estado de la recomendación	Seguimiento
a. En el menú principal "Conózcanos", en "Servicio al cliente" al ingresar a esta opción, despliega el título "Donde puede cambiar sus premios", los números de teléfono de contacto, se encuentran desactualizados.	Cumplida	Los números de teléno que presenta la página web en la ruta www.jps.go.cr en la Sección "Contáctenos" se encuentran actualizados.
c. En el Organigrama Institucional en cual se encuentra bajo el título de "Organización" en el menú principal, no se hace diferencia entre las dos subgerencias.	Cumplida	El organigrama que presenta actualmente la página web corresponde al de la nueva estructura institucional, mismo que está ubicado en la ruta *"www.jps.go.cr"*, en la sección *"¿Quiénes somos?"*, por medio del oficio AL 0671 del pasado 28 de mayo del 2013 emitido por la señora Marcela Sánchez de la Asesoría Legal, indica: *"... las plazas a reestructurar para la implementación nueva estructura, suman un total de 5 plazas, ... "* Por lo que la página web, muestra el nuevo organigrama en la ruta *"http://www.jps.go.cr/quienes_somos.cfm"* bajo el título *"Organigrama de la nueva estructura de la JPS"*

Informe 10-2009 Seguimiento de recomendaciones giradas por los despachos de auditores externos Carvajal y Colegiados y Castillo-Dávila, Asociados

Dirigido a: Departamento de Tecnologías de la Información **Fecha:** 30 de junio 2009

Recomendación	Estado de la recomendación	Seguimiento
VI. Metodología de administración de proyectos. **Recomendación para el hallazgo N° 1:** *"Se recomienda utilizar un proyecto como plan piloto para validar si la utilización del estándar de administración de proyectos puede ser lograda a cabalidad con una relación costo beneficio positiva para la organización y suministrar capacitación al personal de cómputo para que conozcan la forma de administrar proyectos siguiendo dicho modelo".*	Cumplida	Por medio del oficio GG.1847-2014 del pasado 8 de agosto del 2014 se adjuntó el Informe *"Respuesta y solución a los hallazgos identificados por la Auditoría Interna en el departamento de Tecnologías de Información"*, donde se respondió: *"1. Se aplicó el uso de la metodología de administración de proyectos para el Sistema de Administración de Beneficiados SIAB y para el proyecto Migración de beneficiados a .NET y desarrollo de requerimientos en Beneficiados, Ayudas técnicas y giros directos. Ambos proyectos cuentan con su respectiva documentación de la metodología de proyectos aprobada con el fin de utilizados como proyectos piloto en la aplicación de la metodología de administración de proyectos.."* En los anexos adjuntos al oficio citado, se observó el plan de Recursos Humanos de TI, del período 2014-2017, donde se muestra la capacitación en Administración de Proyectos por un monto de $1.000, así como el plan de capacitación.

Informe AI JPS N° 22-2012 Estudio sobre la verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la junta de protección social por medio de los socios comerciales

Dirigido a: Departamento de Tecnologías de la Información, Gerencia Administrativa Financiera **Fecha** 20 de diciembre, 2012

Recomendación	Estado de la recomendación	Seguimiento
3- Se recomienda que los funcionarios del Departamento de Informática, porten el carné de identificación y la tarjeta magnética utilizada para el ingreso a dicho Departamento, en lugares separados, con el fin de evitar de que en caso de que la tarjeta magnética sea extraviada, el tercero que la encuentre desconozca el lugar donde pertenece.	Cumplida	En la revisión realizada a los señores Jairo Cruz y Ronald Ortiz ambos del Departamento de Tecnologías de la Información, se logró comprobar que tanto el carnet de identificación como la tarjeta magnética se encuentran separadas.
4- Se recomienda proteger las paredes de la sala de cómputo y comunicaciones con un material no vulnerable a agresiones externas o rompimiento por accidente.	Cumplida	El Centro de Datos se trasladó contiguo al Edificio Principal, y sus paredes se encuentran con material contra agresiones externas. Con respecto a las paredes de la sala de cómputo y comunicaciones están recubiertas con una película protectora, lo cual ayudaría a evitar algún daño externo.
5- Se recomienda la utilización de bitácoras de acceso para controlar el ingreso a las salas de cómputo y comunicaciones.	Cumplida	Se encuentra en uso al ingresar al Departamento de Informática.
6- Se recomienda utilizar detectores de humedad dentro de la sala de servidores, así como monitorearlos periódicamente.	Cumplida	El día 26 de agosto, en compañía con el señor Jairo Cruz al centro de datos de la JPS, se comprobó que existen detectores de humedad. Sin embargo, no se logró comprobar que dichos detectores sean revisados de forma periódica.
7- Se recomienda trasladar el mueble ubicado en las salas de cómputo y comunicaciones y su contenido (papelería), en un lugar distinto a dichas salas, donde no exista la posibilidad de incendio.	Cumplida	Al hacer la revisión el día 26 de agosto del 2014 al centro de datos, se observó que en dicho lugar no se encontraba ningún mueble con papelería.
10- Se recomienda que en la aplicación para realizar apuestas deportivas, se definan controles para el cumplimiento de los requerimientos de complejidad de las contraseñas, impidiendo al usuario definir contraseñas de fácil deducción como por ejemplo el mismo nombre de la cuenta, números consecutivos, números de	Cumplida	De acuerdo con lo señalado verbalmente por el señor Ronald Ortiz, citó: *"Actualmente la administración de apuestas deportivas no le corresponde a la Junta de Protección Social."*

cédula de identidad, entre otros. Se recomienda el uso de combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales. Previo a la implantación de este control, se recomienda la concientización hacia los usuarios.		No obstante, a través de correo electrónico el señor Jairo Cruz emitió la *"política sobre el uso de las contraseñas"*, asimismo se logró verificar la codificación de base de datos referente a los requerimientos de contraseñas.
11- Se recomienda la definición dentro del sistema de apuestas de Progol, de un control que obligue al usuario (socios comerciales) a cambiar la contraseña al menos cada 90 días acorde a las mejores prácticas de seguridad.	Cumplida	De acuerdo con la política PL-SUC-2013 sobre el uso de las contraseñas, entregada por el Departamento de Tecnologías de la Información se señala: *"...El password de los usuarios administradores de la Base de Datos debe cambiarse cada 30 días. ..."* Con respecto al procedimiento *"MSG_TraerRegistrcUsuario"* generado a través de la base de datos se comprobó que en la programación del mismo se encuentra lo siguiente: *"...* *Select* *@FechaCambioClave =* *DATEADD(Day,90,CONVERT(DATETIME,* *CONVERT(VARCHAR,* *ISNULL(MAX(FechaCambio),'2014/03/12'), 112))), ..."* Como se pudo observar dicha restricción se aplica a los sistemas de la consola corporativa, dado que el sistema de apuestas deportivas Progol no está siendo utilizado.
13- Se recomienda el uso de protocolos de comunicación seguros como SSH, el cual cifra las credenciales de acceso antes de ser enviadas a la red.	Cumplida	Al consultar la ruta 10.0.0.215 de la aplicación Putty, se comprobó que el tipo de conexión que se está utilizando es SSH y que no posee acceso directo al telnet. Con respecto al ftp este permite el acceso al mismo, no obstante no acepta el ingreso de comandos, es importante eliminarlo por completo dicho acceso, a no ser que sea estrictamente necesario.
14- Se recomienda remover cualquier servicio RPC (Remote procedure call) que no sea estrictamente necesario para las	Cumplida	Por medio de correo electrónico el día 28 de agosto el señor Bruce Campbell mencionó:

funciones de la organización.		*"No se puede deshabilitar totalmente el RPC dado a que en esos equipos esta activo los servicios de CLUSTER que requieren del algunas ramificaciones del RPC para funcionar y por ello no se puede apagar dado a que dejaría sin funcionar la redundancia que existe entre los 2 servidores que brindan los servicios que tienen la IP 10.0.0.215"* En reunión con el señor Hugo Brenes de la empresa CESA se comprobó que algunos servicios localizados en el RPC fueron desactivados, sin embargo otros no, dado que éstos son necesarios para las labores propias del Departamento de Tecnología de la Información.
15- Se recomienda filtrar el puerto *portmapper* (puerto 111) a través de un firewall o cerrar los puertos mencionados en el punto N° 15 de este estudio, que no sean estrictamente necesarios para las funciones de la organización.	Cumplida	De acuerdo con la revisión efectuada en compañía del señor Ronald Ortiz, se comprobó que el servidor "obrenes1" no está disponible. En relación con el puesto 21 correspondiente al telnet, este no está siendo utilizado, asimismo, se indica que en referencia al puerto 111 (RPC) no se pudo desactivar la totalidad del puerto dado que algunos servicios son necesarios para el funcionamiento de algunas aplicaciones del Departamento de Tecnología de la Información.
16- Se recomienda deshabilitar el método de comunicación HTTP TRACE en caso de no ser requerido. De lo contrario, solo habilitarlo temporalmente en el momento en que se requiera, ya que con este método de comunicación eventualmente se pueden detectar contraseñas e información sensible que viaje a través de la red.	Cumplida	El servidor "obrenes1" no se encuentra habilitado, asimismo al efectuar la revisión en los servidores 192.68.1.102 y 192.168.1.106, se comprobó que la opción del trace se encuentra desactivada con el comando #Service method="TRACE" fn="service=trace"
17- Se recomienda deshabilitar el atributo *AutoComplete* para el campo de texto correspondiente a la contraseña en el servidor Web y en el equipo "obrenes1". Del mismo modo, se recomienda deshabilitar este atributo para el campo de texto correspondiente al Cumplida nombre del usuario.	Cumplida	Actualmente en lo que se refiere al servidor Web, no se está utilizando, por lo que el atributo *AutoComplete* tampoco está siendo utilizado.
18- En cumplimiento a la Norma 1.4.4 Seguridad en las operaciones	Cumplida	En la revisión efectuada el día 14 de agosto del 2014 en

y comunicaciones de las Normas técnicas para la gestión y el control de las tecnologías de información emitido por la Contraloría General de la República se recomienda el uso de software no obsoleto.		compañía del señor Ronald Ortiz, se comprobó que la versión del sistema operativo SunOS del servidor 10.0.0.215 es 5.10.
19- Se recomienda restringir el *Zone Transfer* únicamente a servidores DNS del mismo dominio. Si se usa un solo servidor de DNS, se recomienda deshabilitar el *Zone Transfer*.	Cumplida	Al verificar la Zone Transfer del active directory se observó que dicha opción se encontraba deshabilitada.
20- Se recomienda actualizar la aplicación Adobe ColdFusion con los parches liberados por el proveedor.	Cumplida	El día 14 de agosto 2014 el señor Ronald Ortiz por medio del correo electrónico indicó: *"En primer instancia te comento que ya no vendemos lotería por Cold Fusion u otro medio a socios comerciales (venta por internet) en cuando a las aplicaciones de cambios de premios y entrega de lotería se hace por la nube usando .net, gracias"* Con base en lo anterior, se determina que efectivamente la herramienta Cold Fusion no se encuentra en uso por dicha Institución.
26- Recomendar a los Socios Comerciales no compartir las cuentas y contraseñas y asignar por parte de Informática una cuenta y contraseña por usuario.	Cumplida	No se mostró recomendaciones sobre no compartir contraseñas, no obstante a través del oficio I 54-13 del pasado 22 de enero del 2013, la cláusula Vigésima Sétima del convenio vigente que se suscribe con los socios comerciales, señala: *"... el uso de esa clave personal y secreta y del dispositivo de acceso, la responsabilidad será absolutamente del SOCIO COMERCIAL."*

Informe AI JPS N° 04-2013 Manejo del fondo y la bolsa para el pago de premios de la Lotería Pega Millones en la determinación de utilidades

Dirigido a: Gerencia General, Gerencia Administrativa Financiera, Departamento de Contable Presupuestario y Departamento de Administración de Loterías **Fecha** 23 de enero, 2013

Recomendación	Estado de la recomendación	Seguimiento
1. Se modifique la metodología de registro contable utilizada en la acumulación de la Bolsa para el Pago de Premios, de tal manera que la misma incluya únicamente el monto de los premios no acertados, los cuales se conocen desde el momento en que se realiza el sorteo, permitiendo reflejar a una fecha dada el saldo exacto que se tiene acumulado (Resultado 2.1.1).	Cumplida	A través del Oficio G.0664-2013 del pasado 21 de marzo del 2013, en el cronograma de implementación de las recomendaciones, en lo que se refiere a la columna de observaciones para la recomendación número uno, se señaló: *"El reglamento de lotería electrónica indica en el artículo 11 " la Junta Directiva de la junta establecerá el porcentaje de pago de premios que corresponde al juego de pega millones y lo dará por informado en un periódico de circulación nacional.* *La bolsa de premios a repartir entre los ganadores, la cual se distribuye entre los ganadores de cuatro, cinco y seis aciertos, se determina al aplicar el porcentaje de pago de premios al total de los ingresos recibidos por concepto de ventas.* *Desde el punto de vista contable se aplica lo que dicta el reglamento, para cumplir dicha recomendación se requiere que la administración reforme el reglamento."* En respuesta a lo anterior, esta Auditoría por medio del oficio AI-417 del 21 de junio del 2013, citó: *"... la recomendación corresponde a modificar la metodología de registro contable utilizada en la acumulación de la Bolsa para el Pago de Premios.* ... *Con esta mecánica, por efecto neto se están obteniendo los premios no acertados de la siguiente manera:* *Premios No Acertados = Plan de premios - Premios Pagados - Premios no Cambiados*

Sin embargo, estos eventos no son simultáneos, ya que el registro de los planes de premios se realizan al cierre del mes y por la totalidad de los sorteos, los premios pagados en el día que se efectúa su cancelación, y los premios caducados al cierre del mes en donde se cumple su periodo para reclamo.

Es decir, esta mecánica ocasiona que no se pueda reflejar el saldo exacto de la Bolsa a una fecha dada, siendo el procedimiento más conveniente que se incluya en esta cuenta únicamente el monto de los premios no acertados, los cuales se conocen al momento de ejecutar el sorteo. El control de los premios acertados por pagar puede ser manejado en otra cuenta contable.
..."

Ante lo citado, el señor Rafael Angel Oviedo Chacón, jefe ai del Departamento de Contabilidad y Presupuesto, en oficio DCP-1597 del 27 de agosto del 2013, señaló:

"Con la finalización del juego "Pega Millones"; y la liquidación del mismo en julio 2013, esta recomendación no es procedente.

Por lo anterior, se hará de aplicación a las liquidaciones del juego denominado Lotto.

Se realizarán los ajustes necesarios, así como la creación de las sub partidas correspondientes"

1. Por medio del Reporte *"Resumen Liquidación de Lotería"* del juego correspondiente a Lotto, se comprobó que:

   a) A partir del sorteo número 1321, se realizó el siguiente cambio:

      a. El 55% del total de las ventas, forman parte de los premios por pagar.
      b. Los premios ganados están compuestos por los premios efectivamente pagados más los premios no

cobrados.

b) Con base en el 55% de los premios por pagar, se creó un asiento contable el cual contempla:

   a. Cuenta de débito:
      5.3.1.01.02.99.9.12 *"Costo Pago Premios Efectivos – Lotería Electrónica (Lotto)"*

   b. Cuenta de crédito:
      2.1.4.01.99.99.9.20 *"Bolsa Lotto 54%"*
      2.1.4.01.99.99.9.22 *"Reserva Lotto 1%"*

c) Con respecto, a los premios efectivamente pagados y a los premios no cobrados se generó el registro en las cuentas:

   a. Cuenta de débito:
      2.1.4.01.99.99.9.11 *"Premios por pagar – Lotería Electrónica (Lotto)"*

   b. Cuenta de crédito:
      5.3.1.01.02.99.9.12 *"Costo Pago Premios Efectivos – Lotería Electrónica (Lotto)"*

Se solicitó al Departamento Contable Presupuestario los reportes de las liquidaciones de los juegos de Lotto No. 1396 y 1397, así como copia de los comprobantes de registro que generaron dichas liquidaciones. Además se extrajo del Sistema de Contabilidad el mayor general de la cuenta 2.1.4.01.99.99.9.20 Bolsa Lotto 54%, con el propósito de observar la aplicación de estos comprobantes de registro.

En cuanto al sorteo de Lotto No. 1396 se recibió copia de los comprobantes de diario No. 13191 y 13192 de fecha 30 de abril de 2014, en donde para el caso del comprobante No. 13191 se evidencia el registro de la Bolsa para el pago de premios por la suma de ¢25,894,728, calculado como un 54% de las ventas

		brutas para ese juego, así como la disminución mediante comprobante 13192 de la Bolsa por los premios acertados por ¢12,003,600. De la mecánica de registro anterior, si se tiene la posibilidad de reflejarse a una fecha dada el saldo exacto que se tiene acumulado para la Bolsa.
2. Ajustar contablemente el saldo de la Bolsa para el Pago de Premios, dado que el dato de los premios acertados utilizado por el Departamento de Contabilidad y Presupuesto para determinar los premios caducados no es exacto, lo cual implica que se arrastren inconsistencias en el saldo de este pasivo (Resultado 2.1.1).	Cumplida	En referencia al Oficio G.0664-2013 del pasado 21 de marzo del 2013, en el cronograma de implementación de las recomendaciones, en lo que se refiere a la columna de observaciones para la recomendación número dos, se señaló: *"Se consultará al Departamento de Informática la modificación al reporte Lo anterior debido a que por efectos de redondeo en el pago de premios éste se da por 2 decimales y el sistema está por 4.* *Es importante indicar que el monto a ajustar de ¢1,046.88 es inmaterial en comparación con el monto que representa los premios de la lotería electrónica de cada juego."* Esta Auditoría por medio del oficio AI-417 del 21 de junio del 2013, mencionó: *"... la suma indicada de ¢1,046.88, tal como se mencionó en la página N° 7 del Informe, corresponde solo a los sorteos del mes de julio 2012, le corresponde al Departamento de Contabilidad y Presupuesto, determinar las diferencias por los demás sorteos a la fecha.* *..."* No obstante, el señor Rafael Angel Oviedo Chacón, jefe ai del Departamento de Contabilidad y Presupuesto, en oficio DCP-1597 del 27 de agosto del 2013, citó: *"A partir de diciembre de 2009 se muestra un total de ¢62,445.91, correspondiente a los redondeos en los cambios de premios por los diferentes sorteos de pega millones.*

		Se procedió a realizar el comprobante no.28223 del 31 de julio del 2013, en el cual se ajusta con un cargo al resultado acumulado del periodo anterior por la suma de ¢15,078.28 y resultado del periodo actual por ¢47,367.63 y un crédito a otros ingresos por estas diferencias. *..."* Se aportó por parte del Departamento Contable Presupuestario el *"Comprobante de Diario"* No. 28223 del 31 de julio de 2013, mediante el cual se ajusta por parte de esa Dependencia los registros de los premios acertados, según lo recomendado por esta Auditoria Interna.
4. Que la estructura para el cálculo de las utilidades en las Liquidaciones de la Lotería Pega Millones se ajuste a lo establecido por la normativa en cuanto a los premios, es decir que el rubro a incluir sean los premios efectivamente pagados y los premios no acertados, ya que si bien es cierto con la estructura actual del plan de premios y los premios caducados se lograría por efecto neto el mismo resultado, se tiene que la Liquidación en sí misma deja de aportar información que resultaría de mucho interés, tal como el monto de premios no acertados que se acumula a la Bolsa por modalidad de acierto en ese sorteo y la cuantía de los premios efectivamente pagados (Resultado 2.1.1).	Cumplida	En el Oficio G.0664-2013 del 21 de marzo del 2013, en el cronograma de implementación de las recomendaciones, en la columna de observaciones para la recomendación número cuatro, se detalló: *"Para dar cumplimiento a esta recomendación debe de reformarse el reglamento de lotería electrónica en el artículo 11, es importante indicar que además el registro contable del plan de premios de la lotería electrónica cumple con el artículo 14 de la ley 8718 y el artículo 11 del reglamento de ese tipo de lotería.* *Con la Puesta en práctica de la aplicación de las NIIF a partir de enero del 2014 se aplicará la Contabilidad por segmentos por lo que la Distribución de Utilidades se realizará con base al Resultado Financiero Mensual, en donde la liquidación por sorteo cumplirá una herramienta de información administrativa, no así para soporte de registro contable"* En el oficio AI-417 del 21 de junio del 2013 esta Auditoría, mencionó: *"Se puede observar que la recomendación se refiere a que la estructura para el cálculo de las utilidades en las Liquidaciones de la Lotería Pega Millones se ajuste a lo establecido por la normativa en cuanto a los premios, es decir que el rubro a incluir sean los premios efectivamente pagados y los premios no*

acertados, información que no está siendo incorporada en las liquidaciones…

Sobre los premios no acertados, la Asesoría Legal indicó mediante oficio AL-0436 del 8 de mayo del 2012, lo siguiente:

"…los premios acumulados no acertados en la Lotería Electrónica, tienen el mismo efecto que los "premios efectivamente pagados",… "

… el tema es del manejo en las Liquidaciones (confeccionadas por el Departamento de Loterías) y no en el registro contable, no obstante, se aclara que no se requiere reformar el Reglamento de Lotería Electrónica tal como es indicado por el Departamento de Contabilidad y Presupuesto. El artículo N° 11 de este Reglamento, citado por dicho departamento, menciona el establecimiento del pago de premios, calculado como un porcentaje sobre los ingresos por venta, este monto se reparte entre las modalidades de acierto, y en el caso que no se produzca el mismo, la suma se acumula por cada modalidad; como se observa, este tema no tiene relación directa con la estructura financiera para la determinación de las utilidades, que es el punto en análisis. "

En oficio DCP-1597 del 27 de agosto del 2013, el señor Rafael Angel Oviedo Chacón, jefe ai del Departamento Contable Presupuestario, mencionó:

"Con la finalización del juego "Pega Millones en mayo del 2013, esta recomendación no procede por lo que será aplicada al juego lotto.

A partir de Junio del 2013, se aplican los cambios en las liquidaciones."

Se observa que las liquidaciones mantienen el rebajo del plan de premios y el aumento de los premios no acertados para el cálculo de la utilidad, no obstante, las mismas ya ofrecen la información de los premios ganados, los premios

		efectivamente pagados, los premios no cobrados y la reserva, incluso se refleja la acumulación de la bolsa y la reserva dentro de la liquidación, a manera de documentación se aprecia la liquidación del sorteo de Lotto No. 1391 del 12 de febrero del 2014.
5. Se aplique producto de la estructura utilizada en las Liquidaciones de la Lotería Pega Millones, un incremento en la determinación de utilidades por la suma correspondiente a los premios caducados no incorporados al cálculo de la renta, cuyo monto al menos entre el sorteo No. 527 y No. 530 asciende a ¢1,356,180.00 (un millón trescientos cincuenta y seis mil ciento ochenta colones con 00/100) (Resultado 2.1.1).	Cumplida	Por medio del oficio G.0664-2013 del pasado 21 de marzo del 2013, en la columna observaciones de la recomendación número cinco en el cronograma de implementación de las recomendaciones, se citó: *"El Departamento de Loterías incluyó para el proceso de la distribución de diciembre del 2012, correspondientes a los sorteos de octubre del 2012 la cantidad indicada. Se adjunta reporte de ajuste de utilidades."* Esta Auditoría a través del oficio AI-417 del 21 de junio del 2013, mencionó: *"... se señaló que la suma de ¢1,356,180.00 (un millón trescientos cincuenta y seis mil ciento ochenta colones con 00/100), es la detectada al menos entre el sorteo N° 527 y N° 530.* *Corresponde a la Administración Activa verificar la existencia de sumas adicionales para otros sorteos."* El señor Rafael Angel Oviedo Chacón, jefe ai del Departamento Contable Presupuestario, por medio del oficio DCP-1597 del 27 de agosto del 2013, señaló: *"Se realizó la verificación de los sorteos anteriores al No.519, arrojando un saldo de ¢3,205,610.00 el cual se ajustó con la distribución de utilidades de julio 2013.* *El saldo lo conforman los sorteos del No.359 al 518 ya que cuando se realizó el ajuste por ¢170,956.00* *Se adjunta copia de los reportes soportes."*

		Con base en lo anterior, se determina que se realizó un ajuste por ¢1,356,180.00 de incremento en las utilidades de octubre de 2012, adicionalmente, tal como fue indicado por esta Auditoría Interna, se debía verificar la necesidad de ajustes adicionales por este concepto. El Departamento Contable Presupuestario determinó un monto adicional de ¢3,205,610 que se incluyó en el cálculo de utilidades de julio 2013.
6. Incluir en la determinación de utilidades la suma de premios no acertados entre los sorteos No. 519 y No. 526, los cuales no fueron rebajados del cálculo de la renta y por tanto no se cuenta con la acumulación real de la Bolsa para ese periodo, cuyo monto asciende a ¢22,956,555.50 (veintidós millones novecientos cincuenta y seis mil quinientos cincuenta y cinco colones con 50/100) (Resultado 2.1.1).	Cumplida	Por medio del oficio G.0664-2013 del pasado 21 de marzo del 2013, en la columna observaciones de la recomendación número seis en el cronograma de implementación de las recomendaciones, se citó: *"Dicha recomendación no aplica ya que la cantidad de ¢22,959,555.50 para los sorteos 519 al 526 por premios no acertados fue considerada en la Distribución de Utilidades de Loterías y otros Productos de Azar, asi como en las liquidaciones oficiales de dichos sorteos.* *El Departamento de Loterías realizó el ajuste a la Distribución de Utilidades de octubre del 2012 por el monto de ¢170,956.00, según detalle adjunto suministrado por el Departamento de Informática."* Esta Auditoría a través del oficio AI-417 del 21 de junio del 2013, mencionó: *"Las liquidaciones obtenidas por esta Auditoría en el Sistema de Liquidaciones con fecha 15 de noviembre de 2012, no reflejan en su estructura la incorporación de los premios no acertados...* *No obstante, en las liquidaciones para los mismos sorteos suministradas por el Departamento de Contabilidad y Presupuesto el pasado día 10 de mayo de 2013, si se reflejan los mismos ...* *En virtud de lo anterior, se tienen como incorporados los premios no acertados en el cálculo de las utilidades, señalados para los*

		sorteos del N° 519 al N° 526. *Se desconoce el origen de la suma de ¢170,956.00 señalada por el Departamento de Contabilidad y Presupuesto, por lo cual es responsabilidad de la Administración Activa analizar que dicho ajuste corresponda."* El 27 de agosto del 2013 el señor Olman Brenes Brenes Gerente Administrativo Financiero, por medio del oficio DCP-1597, señaló: *"Esta recomendación se aplicará al nuevo juego Lotto."* Tal como se indicó y documentó en la nota AI-417 del 21 de junio de 2013, las liquidaciones obtenidas para el estudio por esta Auditoria Interna en el Sistema de Liquidaciones con fecha 15 de noviembre del 2012 no contenían los premios no acertados, no obstante las liquidaciones suministradas por el Departamento Contable Presupuestario el día 10 de mayo del 2013 sí reflejan los mismos. En virtud de lo anterior, se tienen como incorporados los premios no acertados en el cálculo de las utilidades.
7. Se efectúe un ajuste contable con el propósito de reintegrar al Fondo de Premios Adicionales los recursos tomados para crear el "Fondo de Electrónica" por ¢10,000,000.00 (Diez millones de colones con 00/100) cuenta 2.2.4.01.99.99.01.04 y el "Fondo para Premios de Pega Millones" por ¢25,000,000.00 (Veinticinco millones de colones con 00/100) registrados en la cuenta 2.2.4.01.99.99.01.06 denominada Bolsa Pega Millones. Este reintegro debe reflejarse adicionalmente en el saldo del Fondo de Premios Adicionales que muestra el Departamento de Loterías en las Liquidaciones de la Lotería Nacional (Resultado 2.1.2).	Cumplida	Se observó que a través del comprobante de diario No. 24892 del 30 de junio del 2013, se reintegra al fondo de premios adicionales la suma de ¢10,000,000 tomados para el fondo de electrónica. Así como el comprobante de diario No. 9286 del 28 de febrero del 2013 donde se reintegra la suma de ¢25,000,000 al fondo de premios extra. El Departamento Contable Presupuestario aportó la liquidación del sorteo de nacional 4247 del 4 de agosto de 2013 en la que se incluye un incremento de ¢60 millones (es decir 25,0 millones más 25,0 millones más 10,0 millones) dentro del ajuste realizado a dicho fondo.

8. Mostrar mediante notas a los Estados Financieros el compromiso de utilizar recursos del Fondo de Premios Adicionales hasta por un monto de ¢25,000,000.00 (veinticinco millones de colones con 00/100) para garantizar un premio por esa cuantía en caso de que se produzcan los seis aciertos y la Bolsa acumulada presente una suma inferior (Resultado 2.1.2).	Cumplida	Esta recomendación se fundamentaba en el manejo y caracteristicas propias del juego Pega Millones, el cual presentaba una acumulación en la bolsa que debía ser por un monto mínimo de premios de ¢25,0 millones, tomados del fondo de premios adicionales. No obstante, en la actualidad el juego Pega Millones no existe, por lo que el Departamento Contable Presupuestario estableció en el oficio DCP-1597 del 27 de agosto del 2013 que su aplicación sería en el juego Lotto. Por lo tanto, en virtud de que el juego Lotto presenta variaciones en su procedimiento respecto a lo que se manejaba en el juego Pega Millones, tales como: la cuantía del monto mínimo (actualmente 20 millones) y el origen del financiamiento de ese premio mínimo (el reglamento no hace referencia a que se tome del fondo de premios adicionales), la recomendación inicial presenta la necesidad de adaptarse a la mecánica del nuevo juego Lotto. Se da por cumplida, dado que en el Estado Financiero del mes de noviembre de 2014, momento a partir del cual indica esa dependencia procederá a incorporar la obligación del premio mínimo de ¢20.0 millones como parte de la nota 15 denominada *"Provisiones y Reservas Técnicas"*, dicha nota se encontraba debidamente incorporada.
9. Devolver al saldo del Fondo de Premios Adicionales los ¢25,000,000.00 (veinticinco millones de colones con 00/100) utilizados para financiar parcialmente el premio por los seis aciertos, y proceder con la afectación de esa suma dentro de la estructura para el cálculo de las utilidades (Resultado 2.2.1).	Cumplida	El señor Rafael Angel Oviedo Chacón, jefe ai del Departamento de Contable Presupuestario, por medio del oficio DCP-1597 del 27 de agosto del 2013, mencionó: *"Se procedió a realizar el comprobante de diario 28247 del 31 de julio del 2013 por la cantidad ¢25,000,000.00. en el que se ajusta con un cargo al costo de pago de premios lotería electrónica y un crédito en el fondo de premios extra, además se incorporó dentro de la estructura de la liquidación de pega millones del sorteo 1320.* *..."*

		A través de correo electrónico enviado el día 12 de diciembre del 2014, por el Departamento de Contabilidad, se mencionó: *"... En la línea "Ajuste Premios Efectivos", el monto indicado se compone de los ¢25, 000,000.00 menos ¢2,552,967.50 en cumplimiento a las recomendaciones 10-11 y 12 del Informe AI-04-2013."* Además, se logró apreciar el comprobante contable No. 28247 del 31 de julio de 2013, donde se refleja el reintegro al fondo de premios adicionales de la suma de ¢25,000,000 que fueron utilizados para financiar parcialmente el premio de los seis aciertos del juego Pega Millones, lográndose además, observarse en la liquidación del juego Pega Millones No. 1320 la afectación al cálculo de las utilidades. En la revisión efectuada por esta Auditoría, se comprobó que efectivamente los 25.0 millones se encuentran neteados junto con los 2,552.967.50 (mencionado en la recomendación No. 12)

Informe AI JPS N° 17-2013 Estudio sobre las Compras de Equipos de Cómputo realizadas a Componentes El Orbe S.A., Comprendidas entre los períodos 2009, 2010 Y 2011 inclusive

Dirigido a: Departamento de Tecnologías de la Información, Departamento de Recursos Materiales **Fecha** 20 de noviembre, 2013

Recomendación	Estado de la recomendación	Seguimiento
Recursos Materiales		
1. Remitir invitaciones de participación a procesos de contratación únicamente a proveedores debidamente inscritos en el Registro de Proveedores (Ver punto N° 3.2 del apartado Resultados del Estudio).	Cumplida	Por medio del oficio AI-666 del pasado 5 de setiembre del 2014, se solicitó ampliar la circular N° 007 del 11 de diciembre del 2012 de la siguiente manera: *"1. Solicitar a los funcionarios que dejen evidencia en el expediente de la contratación, del uso del Registro de la Dirección General de Administración de Bienes y Contratación Administrativa, o bien del que se utilice en determinado momento.* *2. Fijar un mecanismo para la selección de los proveedores del Registro de la Dirección General de Administración de Bienes y Contratación Administrativa (o del que se utilice en ese momento) que serán invitados."* A través del oficio GG-2430-2014 del pasado 29 de setiembre del 2014 se adjuntó la Circular N° 07-2014, en la cual se indica: *"...* *El uso del registro del Sistema CompraRed se utilizará única y exclusivamente si en el registro de proveedores Institucional no se encuentran proveedores inscritos o si la cantidad es interior a tres. (La selección de los proveedores en este sistema debe realizarse de manera aleatoria) y en la medida de lo posible que garantice una rotación de los mismos. (Se debe dejar constancia en el expediente de los proveedores invitados de ese sistema.)"*
2. Comprobar que los proveedores ofertantes presenten correctamente los requisitos fijados en el cartel de la contratación, principalmente en aspectos como las garantías de participación y cumplimiento, de esta manera la Institución se mantendría respaldada en caso de ser necesario (Ver puntos N° 3.3.1 y 3.3.2 del	Cumplida	El pasado 05 de setiembre de 2014 por medio del oficio AI-666 dirigido al señor Milton Vargas Mora, Gerente General, citó: *"... Se tiene clara la posibilidad del subsane por parte del oferente, sin embargo, debe comprobarse que el mismo se produzca. Sobre el*

apartado Resultados del Estudio).		*plazo de la garantía de cumplimiento no se aportó criterio por parte del Departamento de Recursos Materiales.* *El interés de esta Auditoría Interna es que se fortalezcan los controles para comprobar que los proveedores ofertantes presenten correctamente los requisitos fijados en el cartel de la contratación, lo cual puede ser recordado a los funcionarios responsables del proceso."* En el Anexo 1 *"GG-2224-2014"* del oficio GG-2430-2014 del pasado 29 de setiembre de 2014, se mencionó: *"... 2- En cuanto a la comprobación de la presentación correcta de los requisitos fijados en el cartel de la contratación, en aspectos como las garantías de participación y cumplimiento; los aspectos que pueden ser considerados como subsanables y por ende otorgarse una prevención; debe comprobarse que el subsane se produzca."* Por lo tanto se da como cumplida dicha recomendación.
4. Efectuar por lo menos una vez al año en el Periódico La Gaceta y en dos diarios de circulación nacional, la publicación correspondiente a la invitación para formar parte del Registro de Proveedores Institucional (Ver punto N° 3.4.2 del apartado Resultados del Estudio).	Cumplida	A través del oficio AI-666-2014 del 5 de setiembre del 2014, se mencionó: *"Se solicita aportar la instrucción efectuada al encargado del registro para que las publicaciones se lleven a cabo entre los meses de julio y agosto de cada año."* El señor Milton Vargas Gerente General, por medio del oficio GG-2430-2014 del pasado 29 de setiembre de 2014, adjuntó el Anexo 1 *"GG-2224-2014"* del 16 de setiembre del 2014, emitiendo la siguiente instrucción: *"5- Efectuar en los meses de julio y agosto de cada año la publicación de la invitación a formar parte del Registro de Proveedores Institucional, en el periódico La Gaceta."* Asimismo, por medio del oficio RM. 1413-2014 del anexo 2 del oficio citado GG-2430-2014, se señaló:

		"Ejecutado, ver publicaciones adjuntas." Con base en lo adjunto, logró apreciar las dos publicaciones tanto en el diario extra como en la nación, así como en La Gaceta, además de la instrucción en dicho oficio.
9. Garantizar que al Departamento de Proveeduría le corresponda, determinar y establecer los incumplimientos por parte del proveedor y las posibles sanciones, empleando la información proporcionada por el Almacén General y la Unidad solicitante del bien (Ver punto N° 3.4.3.1 del apartado Resultados del Estudio).	Cumplida	A través del acta 29-30 Julio, sobre la siguiente recomendación se indicó: *"Ésta recomendación fue atendida con el oficio GG-1290-2014 que se adjunta como ANEXO 06."* Por lo que en el oficio GG.1290-2014 del pasado 11 de junio de 2014, se mencionó: *"... esta Gerencia a dispuesto asignar al Departamento de Recursos Materiales la instrucción de este tipo de procedimientos referidos a la aplicación de multas y de la clausula penal ..."* Asimismo, el procedimiento *"Recepción de Mercadería"*, código *"ALM-RM"*, que lleva como objetivo *"Ejecutar el debido proceso, que conlleva la recepción de mercadería a las instalaciones del Almacén General de la Junta de Protección Social con el fin de mejorar el control, disminuir el error, aumentar la coordinación, y asegurar el cumplimiento por parte del proveedor."*, posee como políticas internas del Departamento de Recursos Materiales lo siguiente: *"1. El jefe de Almacén será el responsable ante el jefe del departamento de Recursos Materiales del eficiente desempeño de su unidad, para lo cual deberá cumplir adecuadamente las disposiciones reglamentarias existentes y mediante el uso de los adecuados procedimientos administrativos."* Dado lo anterior, se acoge la instrucción girada por la Gerencia al Departamento de Recursos Materiales, dándose como cumplida dicha recomendación.

Tecnologías de la Información		
1. Que se realice un estudio técnico que fundamente los casos donde se realizan modificaciones a las especificaciones técnicas establecidas en el cartel, el mismo debe ser remitido al Departamento de Proveeduría, junto con el criterio de aceptación o rechazo de la modificación al cartel, para que sea incorporado por el Departamento de Proveeduría al expediente de la contratación (Ver punto N° 3.1.1 del apartado Resultados del Estudio).	Cumplida	A través del oficio AI-666 del 5 de setiembre del 2014 esta Unidad mencionó: *"... **se solicita aportar una copia del documento u otro mediante el cual se giró dicha instrucción**. Esta instrucción, para atender adecuadamente la recomendación, **debe contener la indicación de que la emisión del rechazo o aceptación debe estar debidamente fundamentado** en el respectivo oficio, así como que **debe presentarse un estudio técnico** al Departamento de Recursos Materiales en las modificaciones que no son mejoras."* El señor Milton Vargas Gerente General, a través del oficio GG-2430-2014 del pasado 29 de setiembre de 2014, adjuntó el Anexo 1 *"GG-2224-2014"* del 16 de setiembre del 2014, emitiendo la siguiente instrucción: *"Tecnologías de la Información:* *1- Acreditar debidamente el título "Propuesta de Mejora" en los oficios emitidos como propuestas de mejora en los expedientes de las contrataciones.* *2- La propuesta de mejora del proveedor, deberá ser analizada y aprobada por la Jefatura pertinente, (aprobación o rechazo debidamente fundamentados) quién dará el aval del criterio técnico para la recepción del bien.* *3- Por consecuente queda claro que la "Propuesta de Mejora del proveedor", es el estudio técnico necesario para determinar la procedencia de la condición que se presente y será responsabilidad única del competente del área1 avalarla o rechazarla.* *4- Para las modificaciones que no se tratan de mejoras, debe presentarse en el expediente un estudio técnico al Departamento de Recursos Materiales.* *..." (El subrayado no es del Original)* Dada la instrucción emitida por el señor Milton Vargas al Departamento de Tecnología de la Información, esta Dependencia da como cumplida la misma.

ANEXO N° 3

Detalle de las advertencias emitidas por el Área de Sistemas de la Auditoría Interna (Pendientes y Parcialmente Cumplidas)

N° Nota	Fecha	Advertencia	Estado de la recomendación	Seguimiento
27	18/01/2013	Sitio Alterno de Informática cedido al Consorcio GTECH-Boldt Gaming	Parcialmente Cumplida	En la revisión efectuada el día 10 de diciembre del 2014 al centro de datos ubicado en el edificio de Contabilidad se comprobó lo siguiente: 1. El espacio físico cedido a Gtech-Bold Gaming fue separado del equipo de comunicaciones (enlace entre el Edificio Principal y el Anexo) perteneciente a la Institución, es decir, se trasladó a la sala contigua a Gtech. 2. El área destinada para equipo de Tecnologías de la Información (Rack, UPS) se encuentra en el mismo sitio donde el Departamento Contable Presupuestario almacena los archivos (expedientes). 3. No hay control de acceso para el área de Tecnologías de la Información. 4. No hay cámaras de seguridad que sean monitoreadas por el departamento de Tecnologías de la Información. 5. El Departamento de Tecnología de la Información no posee llave para ingresar a dicha área. Por lo tanto, pese a que el Gtech y el equipo de comunicaciones de la Junta de Protección Social fueron separados, este no posee controles de seguridad.
101	06/03/2013	Acta de Entrega de lotería devuelta al señor Olivier Zamora Matamoros	Pendiente	No se observó respuesta por parte de la Administración Activa, donde señalen que se acogen al cumplimiento de dicha advertencia.
102	08/03/2013	Instalación del cableado estructurado en la Auditoría Interna	Parcialmente Cumplida	Mediante oficio I 360-13 del pasado 21 de marzo del 2013, el señor Ronald Ortiz mencionó:

				"En atención al oficio en referencia, se informa que todos los puntos fueron atendidos..." En la observación realizada el día 20 de mayo del año en curso, se comprobó que algunos puntos citados en oficio AI-102 del 8 de marzo aún continúan pendientes, entre ellos se encuentran: *"...* *2. Al cruzar la tubería de aluminio por el entrepiso, que baja del piso cuarto al tercero, por el área de secretarias, dejaron orificios visibles en el cielo raso de estereofon. En esa misma área desprendieron canaletas de cable eléctrico, las cuales no fueron colocadas de nuevo...* *3. Una de las ventilas de salida del aire acondicionado ubicada al fondo de esta dependencia, fue removida por dicha empresa para realizar sus labores, sin embargo, no fue instalada correctamente..."*
124	15/03/2013	Mensaje de texto enviado a los suscriptores del servicio gratuito de envió de resultados de los sorteos de las loterías de la JPS el 14/03 (dato erróneo)	Pendiente	Por medio del oficio I 364-13 del pasado 22 de marzo del 2013 mencionó: *"... ya esta jefatura había ordenado con anterioridad la implementación de un aplicativo que los envía de forma automática por el mismo digitalizador del Departamento de Loterías y esperamos que esté implementada en el mes de abril del 2013. "* A través del oficio TI 445-2014 del 30 de mayo del 2014 el señor Ronald Ortiz jefe del Departamento de Tecnologías de Información, señaló que el desarrollo del servicio gratuito de envió de resultados de los sorteos de las loterías de la Junta de Protección Social por mensajes de texto a los teléfonos celulares se encuentra en periodo de pruebas, siendo desarrollado a nivel interno. No obstante, la fecha que inicialmente citó el señor Ortiz fue en el mes de abril del 2013, sin embargo al día 30 de mayo del 2014 se encuentra en proceso de implementar dicha herramienta en producción.
320	16/05/2013	Demostración de los sistemas desarrollados por el Consorcio GTECH-Bold Gaming (pruebas de	Pendiente	En dicha advertencia se requirió la siguiente documentación:

		aceptación y puesta en marcha de las apuestas electrónicas)		" *a.Los manuales de procedimientos para la realización de apuestas, pago de premios, sorteos y contabilización de las transacciones.* *b. Planes de contingencias definidos en la comercialización de la Lotería Electrónica, ante la presencia de situaciones que puedan afectar el normal desarrollo de la actividad.* *c.Los diagramas de comunicación, procesamiento y seguridad en la comunicación entre los sistemas del Consorcio GTECH-Bold Gaming y los sistemas de la Junta de Protección Social.* *d. Los accesos a los sistemas que van a ser proporcionados a esta Auditoría Interna para la verificación y seguimiento de las operaciones de apuestas, pago de premios, liquidación de sorteos, recursos a ser trasladados a la institución y definición de los premios prescritos de cada uno de los juegos que se comercialicen, entre otros requisitos."* A pesar de que el señor Abraham Vargas Gerente General a.i. por medio del oficio G.1162-2013 del 23 de mayo del 2013, solicitó en su momento a los responsables de Dirección de Producción y Ventas, Departamento de Mercadeo, y al Departamento de Informática atender los requerimientos de Auditoría Interna, la información que se pidió a través del oficio AI-320 no fue remitida completa a esta Dependencia.
419	21/06/2013	Estructura de las tablas utilizadas para la carga de información de las apuestas efectuadas por el Consorcio Gtech	Pendiente	Con base en el oficio TI 741-13 fechado el 28 de junio del 2013, el señor Ronald Ortiz, mencionó: *"... los sistemas suplidos por el Consorcio no están diseñados y conceptualizados para capturar el número de identificación de los compradores y ganadores de los diferentes juegos de manera individual para cada transacción de venta y pago de premios de Lotería Electrónica. ... si la Administración Superior de la Institución determina y gestione ante el Consorcio, que dicha información debe ser capturada y suministrada por, procederíamos de inmediato a realizar los ajustes pertinentes en nuestra estructura de datos."*

				Lo anterior, refleja que la inclusión del campo correspondiente a la cédula de identidad en las respectivas tablas citadas en el oficio AI-419, no ha sido realizado.
501	17/07/2013	Resultado en ventas de los sorteos de Nuevos Tiempos *** En referencia al AI - 704 del 16/10/2013	Pendiente	En la respuesta emitida a través del oficio G.2909-2013 del pasado 31 de octubre del 2013, no se observó el estudio de valoración de riesgo del producto "Nuevos Tiempos", así como tampoco se logró visualizar las responsabilidades de los funcionarios encargados del control de esos juegos donde informen periódicamente los resultados obtenidos de ese producto, así como además no se indica si fue necesario el estudio de costo beneficios sustentados para garantizar que dichas medidas no afectarán la generación de utilidades de los acreedores de las rentas.
549	16/08/2013	Revisión efectuada a los reportes "Informe Gerencial – Detalle de Premios Pagados – Plan de Premios Emisión" y "Liquidación de Lotería"	Pendiente	Por medio del oficio TI 927-13 del 3 de setiembre del 2013 el señor Ronald Ortiz, solicitó a los Departamentos de Tesorería, Contabilidad y Presupuesto, y Loterías, lo siguiente: *"... se le solicita que nos informen el nombre y la ruta de acceso de los reportes que consideren necesario, esto con el propósito de realizar una revisión a los cuales posean relación con el Plan de Premios u otros reportes que sean considerandos esenciales."* Como respuesta a lo anterior, se emitieron los oficios: • T 570 del 10 de setiembre 2013, Departamento de Tesorería. • DCP-1863 del 22 de octubre del 2013, Departamento de Contabilidad y Presupuesto. El día 9 de diciembre del 2014 el señor Rodrigo Fernandez Cedeño, jefe del Departamento de Tesorería, mencionó: *"... el inconveniente se da con los premios de la Caja Seca (premios mayores tramitados por medio del Banco de Costa Rica), los cuales no se cargan automáticamente en la información de los reportes, sino que se tiene que estar solicitando la actualización de los datos, pero cada vez que se genera un nuevo sorteo y se le van cargando premios, estos no se visualizan automáticamente."*

				Por otro lado, el día 11 de diciembre del 2014, la señora Elena Morales del departamento Contable Presupuestario, señaló las diferencias entre el reporte *"Auxiliar de pago de premios sorteos"* y la *"liquidación oficial"*. Con base en lo anterior, se determina que al continuar diferencias en los reportes y no haberse corregido aún el problema de la información emitida a través de los reportes, esta advertencia aún se mantiene pendiente.
615	16/09/2013	Errores detectados en la página Web (Marco Jurídico de la JPS)	Pendiente	Según oficio TI 983-13 del 19 de setiembre del 2013 el señor Ronald Ortiz Méndez mencionó: *"...* • *En lo que respecta a la actualización de la normativa institucional y otros aspectos de carácter legal como el que nos informan en el citado oficio AI-615, salvo mejor criterio, correspondería a nuestra Asesoría Legal el velar porque dicha información esté vigente y actualizada, comunicándonos de cualquier actualización que debe realizarse para proceder de conformidad.* *2) En atención de lo comunicado y solicitado por su Unidad, procedemos de manera inmediata a realizar la actualización del Reglamento Orgánico de la Junta de Protección Social según decreto No 33436-MP-MTSS.* *...* *"* El día 9 de mayo del 2014, esta Unidad procedió a verificar el *"MARCO JURIDICO DE LA JUNTA DE PROTECCION SOCIAL DE SAN JOSE"*, en la página web http://www.jps.go.cr/legislacion.cfm, observándose que el mismo se encuentra desactualizado, es decir, dicha situación no ha sido corregida, a pesar de que mediante referencia AI-615 del 16 de setiembre del 2013 fue señalado, por lo que lo citado por el señor Ortiz *"procedemos de manera inmediata a realizar la actualización del Reglamento Orgánico de la Junta de Protección Social"* no pudo ser comprobado.

<table>
<tr><td>631</td><td>19/09/2013</td><td>Pozo acumulativo del juego Pitazo</td><td>Pendiente</td><td>En la advertencia girada se solicitó informar a esta Auditoría sobre las acciones tomadas a fin de ajustar el monto del pozo acumulativo que se estaba anunciando al público, como además implementar una política de acumulación para ese pozo, no obstante esta Dependencia no ha recibido ningún oficio señalando la forma en como fue resuelta la advertencia.</td></tr>
<tr><td>656</td><td>27/09/2013</td><td>Operaciones económicas no incorporadas en la ejecución presupuestaria 2012 (cuentas "Equipo de Transporte" y "Alquiler de Edificios, Locales y Terrenos")</td><td>Pendiente</td><td>Mediante oficio GAF-716-2013 del 17 de octubre del 2013 el señor Olman Brenes Gerente Administrativo Financiero, citó:

"Se acoge para su atención inmediata la advertencia de la Auditoría Interna dada en el oficio AI-656 del 27 de setiembre, asimismo, implementar puntos de control de la información presupuestaria y contable, para que situaciones como la que nos ocupa no vuelvan a presentarse."

Al hacer la revisión al reporte "Control de Presupuesto, Versión 1 Periodo: 2013 Programa: 1 Unidad: 507 Nombre: MEJORAMIENTO EDIF. CENTRAL 2013 Cuenta: 10101Subcuenta: 0 Nombre: ALQUILERES DE EDIF., LOCALES Y TERRENOS", se detectaron las siguientes cuentas, a continuación se transcribe lo que interesa:

"
<table><tr><th>Fecha</th><th>Descripción</th></tr><tr><td>...</td><td></td></tr><tr><td>01/10/2013</td><td>VIENE DEL AÑO 2012. REGISTRO DEL ALQUILER TERRENO CONCEDIDO POR LA CCSS DE OCTU 2012 A SET.2013. MONTO TOTAL ¢1.380.000,00,. R DE ENERO A SET.2013 ¢1.035.000. NOTA GAF-RE 039-2013 DEL 30-09-2013. CANCELADO POR REL PAGO EL 15/11/12.DCP-1704</td></tr><tr><td>...</td><td></td></tr><tr><td>07/10/2013</td><td>ALQUILER DE TERRENO EN PRECA CORRESPONDIENTE A LOS MESES DE OCTUBR NOVIEMBRE, 2013</td></tr><tr><td>...</td><td></td></tr><tr><td>11/12/2013</td><td>ALQUILER DE TERRENO EN PRECA CORRESPONDIENTE A DICIEMBRE 2013. CUEI CORRIENTE 179395-5 BNCR.</td></tr></table></td></tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>"

Por otro lado, en referencia al reporte "Control de Presupuesto, Versión 1 Periodo: 2014 Programa: 1 Unidad: 212 Nombre: MEJORAMIENTO EDIFICIO CENTRAL 2014 Cuenta: 10101Subcuenta: 0 Nombre: ALQUILERES DE EDIF., LOCALES Y TERRENOS", se observó la cuenta mencionada:

"
<table>
<tr><td>Fecha</td><td>Descripción</td></tr>
<tr><td>...</td><td></td></tr>
<tr><td>24-01-2014</td><td>PAGO POR EL USO DE TERRENO EN PRECA PARA PARQUEO INSTITUCIONAL PROVISIONAL</td></tr>
</table>
"

Con base en lo anterior, se observa que el Departamento de Contable Presupuestario no informó a esta Unidad sobre las acciones que tomaría en cuenta de esta situación, así como además no acogió la instrucción emitida por el señor Brenes, razón por la que en el periodo 2014, se reflejó un gasto por 1,380,000.00, el cual corresponde al monto total por alquiler. Sin detectar que los meses octubre, noviembre y diciembre todos del 2013, ya fueron detallados en ese periodo por un total de ¢345,000.00.</td>
</tr>
<tr>
<td>840</td>
<td>04/12/2013</td>
<td>Cambio en la contraseña del correo electrónico Zimbra</td>
<td>Pendiente</td>
<td>Con base en el oficio TI 138-13 del pasado 12 de diciembre del 2013 el señor Ronald Ortiz Méndez mencionó:

"...luego de una investigación por medio de Internet y un sondeo a nivel de instituciones estatales como la Contraloría General de la República que ya utilizan exitosamente el software Zimbra como su motor de correo electrónico, lo cual nos alentó a tomar la decisión del utilizar esta herramienta como nuestro motor de email.
...
En lo que respecta al aspecto señalado de los requisitos de cambio de contraseña, se procederá de inmediato a realizar la valoración y ajustes correspondientes a fin de verificar la seguridad que utilizad dicho software y evitar en la medida de lo posible que situaciones similares vuelvan a suceder."</td>
</tr>
</table>

				Se debe indicar que el correo Zimbra permitió el uso de dos contraseñas sin embargo este problema ya fue resuelto, no obstante, en lo que respecta a la solicitud de información que justifique el porqué de la escogencia del motor de correo Zimbra y las minutas del proceso de implementación, dicha documentación aún no ha sido enviada.
841	04/12/2013	Publicación errónea de resultado Nuevos Tiempos en Facebook, perfil de *"Loterito"*	Pendiente	En el oficio AI-841 se solicitaron los controles para verificar si la información está siendo veraz y oportuna, y quién es el responsable de verificar los "logs" de las publicaciones realizadas a través de redes sociales.

ANEXO N° 4

Detalle de las advertencias emitidas por el Área de Sistemas de la Auditoría Interna (Cumplidas)

N° Nota	Fecha	Advertencia	Estado de la recomendación	Seguimiento
901	13/12/2012	Advertencia girado en torno a que no se dio respuesta en el tiempo indicado al oficio AI-874 del 03/12/2012, sobre las Inconsistencia entre las recomendaciones N° 9, 22, 27 del Informe AI JPS N° 26-2011 "Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante informes AI JPS N° 29-2010, AI JPS N° 31-2010 y AI JPS N° 32-2010", con las respuestas brindadas en el oficio I 172-12 del 16 de febrero del 2012.	Cumplida	Mediante oficio I 1242-12 del pasado 18 de diciembre del 2012, se dio respuesta a la referencia AI-874.
135	20/03/2013	Problemas en la nueva plataforma de correo electrónico	Cumplida	Por medio del oficio TI 814-13 del pasado 23 de julio del 2013; el señor Ronald Ortiz mencionó: *"Luego de revisarse y analizarse cuidadosamente la nómina de cuentas del correo institucional se realizaron las modificaciones en el directorio de la nueva plataforma del correo electrónico institucional, donde efectivamente existían cuentas en cuyo campo "nombre" no aparecía el nombre, sino el nombre de la cuenta usuario.* *... se procedió a eliminar la cuenta cesa@ps.go.cr, la cual se utilizó en su debido momento para realizar las pruebas de migración del correo antiguo al correo actual."* Con base en la referencia citada, se observa que el en el directorio de correo electrónico al día 13 de mayo del 2014 está corregida las

				cuentas del directorio en cuyos casos, en vez del nombre se mostraba la cuenta de usuario; por otro lado en lo que respecta a la cuenta cesa@jps.go.cr esta ya fue eliminada.
348	28/05/2013	Participación en la exposición de los sistemas desarrollados por el Consorcio GTECH-Bold Gaming	Cumplida	A través del oficio TI-754-13 del pasado 3 de julio 2013 se adjuntaron los documentos solicitados por esta Auditoría, el cual incluía los procesos desarrollados por el consorcio Gtech-Bold, así como los diagramas de comunicación, procesamiento y seguridad de comunicaciones.
350	28/05/2013	Contrato para Implementación de Modificaciones y Requerimientos al Sitio WEB Transaccional y en los módulos web institucionales (Sin respuesta de nota AI-324).	Cumplida	Mediante oficio I 579-13 del 29 de mayo del 2013, el señor Ronald Ortiz da respuesta a las consultas realizadas a través del oficio AI-350.
446	01/07/2013	Diferencia detectada entre lo emitido en el reporte del sistema ICS y los sistemas del consorcio GTECH	Cumplida	Al verificar los reportes institucionales y los de GTECH, los datos concuerdan correctamente.
649	24/09/2013	Documentos sin foliar (expediente N° 2012LA-000020-PROV, Licitación Abreviada "consultoría técnica especializada para seguimiento e implementación a la normativa N-2-2007-CO-DFOE de la Contraloría General de la República)	Cumplida	En la revisión efectuada el día 4 de junio del 2014 al expediente N° 2012LA-000020-PROV se encontraron los documentos debidamente foliados.
730	28/10/2013	Comportamiento de las utilidades obtenidas para los meses de agosto y setiembre de 2013 (Loterías tradicionales y electrónica)	Cumplida	A través del oficio G.3189-2013 del 3 de diciembre del 2013 se incluyeron las aclaraciones y las acciones llevadas a cabo, donde el señor Francisco Ibarra Gerente de Producción y Comercialización señala: *"Al respecto me permito remitir el oficio MER-632-2013 de fecha 29 de noviembre de 2013 en el cual se brindan las aclaraciones respectivas y acciones tomadas, en donde la reserva del producto juega*

				un papel muy importante, se establecieron topes a los números de la Lotería Nuevos Tiempos y se ha reforzado el plan de comunicación (medios) para el juego Pitazo." Con base en las acciones tomadas para mitigar el riesgo y en las acciones estratégicas, esta Dependencia da por Cumplida dicha recomendación.
746	04/11/2013	Diferencia detectadas en las fiscalizaciones del juego Pitazo N° 19 y 20	Cumplida	A través del oficio TI 1255-13 del 20 de noviembre del 2013, el señor Ronald Ortiz jefe del Departamento de Tecnologías de la Información, señaló las causas, por las que se dieron las diferencias de transacciones, y la diferencia presentada en la consulta general de productos electrónicos, mismas que fueron comprobadas mediante reportes corregidos.
769	08/11/2013	Incumplimiento en la hora de inicio de la fiscalización del Juego Nuevos Tiempos N° 13425	Cumplida	Mediante oficio TI 1245-13 del 19 de noviembre 2013, el señor Ronald Ortiz procedió a responder las consultas planteadas por esta Auditoría.
865	20/12/2013	Reporte de escrutinio del juego Pitazo (datos que no aparecen impresos)	Cumplida	Al realizar la revisión entre los reportes se comprobó que el reporte *"Informe de Resultados de Escrutinio JPS Lotería Pitazo – Sorteo No. ..."*, ya se encuentra corregido.
401	10/06/2014	Recomendación pendiente de solucionar (referente a informe 31-2010) (Correos electrónicos activos de personal que no pertenece a la institución)	Cumplida	Por medio del oficio GG.1302-2014 del 12 de junio del 2014 el Gerente General, le solicita al Departamento de Tecnologías de la Información para que realicen la corrección de los funcionarios que se mostraron activos. Ante esto, a través del oficio TI 498-14 del 16 de junio del 2014, el señor Ronald Ortiz comunica cuales usuarios han sido eliminados, y cuales fueron bloqueados.
418	16/06/2014	Referente fiscalización del escrutinio del Juego Pitazo realizado el 09 de junio 2014	Cumplida	En cumplimiento a esta advertencia, por medio del oficio TI 512-14 del 18 de junio del 2014, el señor Ronald Ortiz jefe del Departamento de Tecnologías de la Información citó: *"... Para corregir el mensaje se cambió mediante la solicitud de servicio 2003-2014 ejecutada el día 17 de Junio del 2014, la leyenda*

				de "No se insertaron los ganadores del escrutinio" por "No hay ganadores para este juego", cuando en el proceso de escrutinio no se genera ganadores."
440	20/06/2014	Referente a la no presencia en la compra de excedentes del representante de la Gerencia el 13 de junio de 2014, en la Sucursal de Puntarenas	Cumplida	A través del oficio GO-673 del 26 de junio del 2014, se le mencionó al Administrador de la Sucursal de Puntarenas, que tomara en consideración estas situaciones para que no vuelvan a repetirse. Se les recordó además, a los administradores de las diferentes Sucursales, que en la compra de excedentes debían estar los tres funcionarios responsables para la fiscalización, así como las respectivas firmas.

ANEXO N° 5

Detalle de recomendaciones cumplidas, parcialmente cumplidas y pendientes por informe, así como los informes incluidos en los anteriores seguimientos

Informes				Recursos Materiales			Informática			Contabilidad			Total
				PC	C	P	PC	C	P	PC	C	P	
22-2012	Verificación de la seguridad de los sistemas informáticos relacionados con las apuestas deportivas que comercializa la junta de protección social por medio de los socios comerciales.						3	16	7				26
4-2013	Manejo del fondo y la bolsa para el pago de premios de la lotería pega millones en la determinación de utilidades.									2	8	3	13
05-2013	Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante Informes AI JPS N° 26-2011 y advertencias emitidas mediante notas.						17	22	13				52
	26-2011	Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna, mediante informes AI JPS N° 29-2010, AI JPS N° 31-2010 y AI JPS N° 32-2010.											
		29-2010	Seguimiento de recomendaciones giradas por el Área de Sistemas de la Auditoría Interna.				8	14	3				
			06-2008	Estudio sobre la verificación de la seguridad en el manejo de las transferencias electrónicas de fondos, y la seguridad, integridad y consistencia de la información contenida en las bases de datos institucionales referentes al manejo de las loterías.			4	1	1				
			07-2009	Seguimiento de recomendaciones giradas por la Auditoría Interna al Departamento de Informática en el informe 8-2006 referente a "Estudio relacionado con la página web de la Junta de Protección Social de San José".			1	12	2				
			10-2009	Seguimiento de recomendaciones giradas por los despachos de auditores externos Carvajal y colegiados y Castillo-Dávila, asociados.			3	1					
		31-2010		Estudio relacionado con una revisión general de usuarios en los servidores institucionales.			1	1	3				
		32-2010		Estudio sobre la verificación de la seguridad en la comunicación de datos entre los entes externos y la Institución, relacionada con los productos que comercializa la junta de Protección Social.			8	7	7				
17-2013	Estudio sobre las compras de equipos de cómputo realizadas a Componentes El Orbe S.A, comprendidas entre los periodos 2009, 2010 y 2011 inclusive.			1	4	4	1	1	1				12
			Total :	1	4	4	21	39	21	2	8	3	103

Nota: El informe 05-2013 es un seguimiento del informe 26-2011 que a su vez es un seguimiento de los informes 29-2010, 31-2010 y 32-2010, asimismo el informe 29-2010 incluye un seguimiento de los informes 06-2008, 07-2009 y 10-2009