Lilliana Rojas Segura
GERENCIA
J.P.S.
01 FEB. 2013

INFORME DE AUDITORÍA INTERNA AI JPS N° 05-2013

ÁREA DE SISTEMAS

TEMA:

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.

PREPARADO POR:

ING. VIVIANA RIVERA BARRANTES
PROFESIONAL III

31 DE ENERO DE 2013

DIRIGIDO A:

GERENCIA

JUNTA DE PROTECCION SOCIAL
INFORMATICA
01 FEB. 2013
11:43am
RECIBIDO

COPIA:

DEPARTAMENTO DE INFORMATICA

INDICE

RESUMEN EJECUTIVO

Informe de Auditoría Interna AI JPS N° 05-2013

Esta Auditoría incluyó dentro del Programa de Trabajo para el Área de Auditoría de Sistemas del año 2012, un estudio sobre el Seguimiento de Recomendaciones Giradas, mediante Informe AI JPS N° 26-2011 denominado *"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"*.

El objetivo general consistió en verificar si los Departamentos que conforman la Administración Activa de la Junta de Protección Social han cumplido con las recomendaciones que fueron 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, a través del informe AI JPS N° 26-2011 denominado *"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"*.

Dentro de los resultados del estudio se estableció:

- De las recomendaciones giradas en los diferentes informes, se comprobó que del 100% de estas recomendaciones, un 8,77% fueron cumplidas, un 33,33% se encuentran parcialmente cumplidas y el 57,89% aún están pendientes.

- La mayoría de las recomendaciones que se encuentran pendientes pertenecen a los Informes AI JPS N° 29-2010 y AI JPS N° 32-2010.

- El informe AI JPS N° 29-2009, incluyó un seguimiento de recomendaciones del Informe AI JPS N° 07-2009 denominado *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*, en relación con este estudio, se comprobó la actualización del sitio Web, donde el Departamento de Informática solicitó por medio de cartel las especificaciones técnicas requeridas para que la nueva página cumpla con la información contenida del sitio Web anterior, además de otra información importante, sin embargo al momento de la revisión los cambios a corregir indicados en las recomendaciones del Anexo N° 1, no se encontraban en producción.

- De cinco advertencias emitidas, se evidenció que cuatro de ellas han sido cumplidas, las cuales fueron giradas mediante oficios AI-105 del 17 de febrero del 2012, AI-167 del 12 de marzo del 2012, AI-229 del 30 de marzo del 2012, AI-788 del 17 de octubre del 2012, sin embargo el oficio AI-901 del 13 de diciembre del 2012 se encuentra pendiente.

Las recomendaciones y advertencias emitidas en las diferentes notas e informes están dirigidas a fortalecer el control interno de la Institución. Es importante que la Administración cumpla con las recomendaciones que se han indicado, del informe 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."*, quedaron pendientes 57 recomendaciones parcialmente cumplidas y pendientes, siendo la base para iniciar el seguimiento de este estudio dando como resultado 52 recomendaciones pendientes de resolver, por lo que durante el año 2012 solamente cinco recomendaciones fueron resueltas por el Departamento de Informática.

1. INTRODUCCIÓN

1.1 Origen de la auditoría

El siguiente estudio corresponde al programa de trabajo del Área de Auditoría de Sistemas del año 2012.

1.2 Objetivo general

Verificar si los Departamentos que conforman la Administración Activa de la Junta de Protección Social han cumplido con las recomendaciones y advertencias que fueron emitidas 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 del informe AI JPS N° 26-2011 denominado *"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"* y advertencias emitidas mediante nota, por lo que el estudio contempló el periodo 2012 y hasta la segunda semana del año 2013.

1.4 Metodología

La metodología utilizada por el Área de Sistemas, fue la siguiente:

1. Realizar entrevistas a las diferentes Secciones del Departamento de Informática sobre las recomendaciones emitidas en los informes.

2. Revisión de la correspondencia recibida en la Auditoría Interna, proveniente de la Administración Activa, con la finalidad de tener referencia sobre el cumplimiento del seguimiento de las recomendaciones giradas.

3. Solicitar de las diferentes Áreas del Departamento de Informática, la información necesaria para la verificación de cada una de las recomendaciones emitidas por la Auditoría de Sistemas.

4. Revisión de la correspondencia recibida del Departamento de Informática, que respalde el cumplimiento de las recomendaciones y advertencias que le fueron giradas.

5. Se efectuaron consultas con los responsables de las funciones y verificación tanto física como de datos, para el cumplimiento de las recomendaciones.

6. Todas las actividades fueron realizadas de acuerdo con la normativa aplicable al ejercicio de la Auditoría.

7. Las actividades fueron realizadas de acuerdo con la normativa aplicable al ejercicio de la Auditoría Interna.

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 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, N° 7428, de 7 de setiembre de 1994."

Artículo 39.- Causales de responsabilidad administrativa

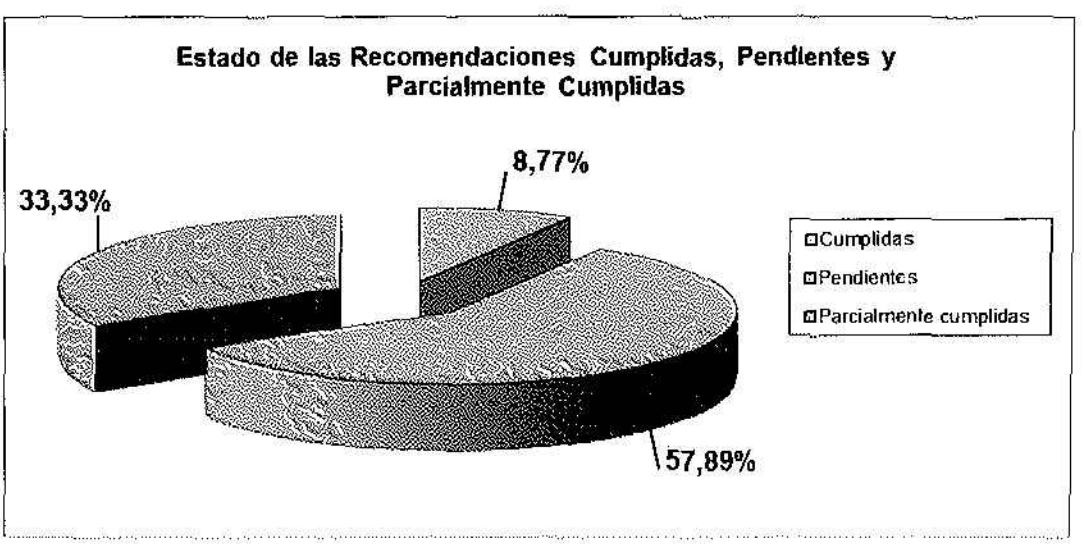
El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios...."

2. RESULTADOS DEL ESTUDIO

A. Al comprobar el cumplimiento de las recomendaciones giradas en los diferentes informes y notas emitidas por el Área de Sistemas de la Auditoría Interna, durante el periodo 2012 y hasta la segunda semana del mes de enero del 2013, se comprobó que del 100% de estas recomendaciones, un 8,77% fueron cumplidas, un 33,33% se encuentran parcialmente cumplidas y el 57,89% aún están pendientes. Cabe mencionar que, todas las recomendaciones fueron emitidas al Departamento de Informática, (Ver Anexo 1). El siguiente cuadro presenta el detalle de lo antes citado:

Status de la recomendación	Cantidad de recomendaciones	% de cumplimiento
Cumplidas	5	8,77
Pendientes	33	57,89
Parcialmente cumplidas	19	33,33
Total de recomendaciones giradas	57	100,00

Adicionalmente presentamos en forma gráfica, el estado de las recomendaciones según el período indicado en el alcance de este informe:



B. Es importante mencionar que como parte de las recomendaciones sin cumplir, se encuentran pendientes, en su mayoría, las recomendaciones giradas en los siguientes Informes AI JPS N° 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", y AI JPS N° 29-2010 denominado *"Seguimiento de Recomendaciones giradas por el Área de Sistemas de la Auditoría Interna"*.

En relación con lo anterior, el señor Ronald Ortiz Méndez, Jefe del Departamento de Informática, indicó en nota I-172-12 del 16 de febrero del 2012, que la solución a algunas de las recomendaciones descritas en los informes mencionados, se encuentran en proceso a finalizar en el año 2012, sin embargo, al momento de la revisión permanecían aún pendientes o parcialmente cumplidas.

C. En el Informe AI JPS N° 29-2009, el cual es parte del alcance de este estudio, se incluyó un seguimiento de recomendaciones del Informe AI JPS N° 07-2009 denominado *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*, en relación con este último, el señor Ortiz Méndez, por medio de la nota I-990 del 17 de octubre del 2012, adjunta las especificaciones técnicas para el *"Cartel para modificaciones al sitio WEB de la Junta de Protección Social"*, a pesar de haberse realizado el cartel los cambios no han sido actualizados en producción, sin embargo, se ha creado un cartel el cual no incluye la totalidad de la información contenida en la página anterior.

En relación con los puntos citados, es importante indicar lo que establece la Ley General de Control Interno Nº 8292 publicada en La Gaceta Nº 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

En el estudio sobre el seguimiento de recomendaciones giradas por el Área de Sistemas de esta Auditoría, se determinó que al 20 de diciembre del 2012, por parte del Departamento de Informática existía un 57,89% de recomendaciones que aún no había cumplido, un 33,33% estaban parcialmente cumplidas y un 8,77% ya

fueron cumplidas, lo anterior, refleja un factor alto de recomendaciones sin cumplir.

Igualmente, del total de las 33 recomendaciones pendientes, 16 pertenecen al Informe AI JPS N° 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"*. Asimismo, 13 recomendaciones corresponden al Informe JPS N° 29-2010 denominado *"Seguimiento de Recomendaciones giradas por el Área de Sistemas de la Auditoría Interna"* y 4 de ellas forman parte del Informe AI JPS N° 31-2010 denominado *"Estudio relacionado con una revisión general de usuarios en los servidores Institucionales"*.

Mediante nota G.117 del 23 de enero del 2012, la Gerencia giró las instrucciones respectivas para que el Departamento de Informática proceda al cumplimiento de las recomendaciones pendientes y a la fecha de este informe únicamente 5 recomendaciones fueron sido cumplidas, dejando un total de 52 recomendaciones pendientes y parcialmente cumplidas.

Además, de acuerdo con el oficio I 264-12, enviado por el señor Ronald Ortiz Méndez, el día 13 de marzo del 2012, indicó en la mayor cantidad de las recomendaciones que se encontraban ya sea parcialmente cumplidas o pendientes las mismas se estarían cumpliendo durante el año 2012, no obstante durante la elaboración de este informe se logró determinar que únicamente 5 recomendaciones fueron sido cumplidas.

Esta Auditoría concluyó la recolección de pruebas y documentación del presente estudio la segunda semana del mes de enero del 2013.

Es importante señalar que, la aplicación de las recomendaciones, permite fortalecer la estructura de control interno inmersa en las diferentes funciones que se llevan a cabo en nuestra Institución. Además, se colabora con la Administración Activa, por cuanto los estudios que lleva a cabo esta Auditoría, son un medio más para el logro de los objetivos y metas Institucionales establecidos en el Plan Anual Operativo así como para la protección del Patrimonio Público.

4. RECOMENDACIONES

Al señor Julio Canales Guillén, Gerente General a.i.

Con base en el presente informe se solicita:

1. Girar instrucciones por escrito al señor Ronald Ortiz Méndez, Jefe del Departamento de Informática, para que proceda al cumplimiento de las recomendaciones y advertencias pendientes de aplicar que se detallan en el Anexo N° 1, conforme lo establece la Ley General de Control Interno.

2. Solicitar al señor Ronald Ortiz Méndez, el cronograma de cumplimiento de las mismas, en un plazo no mayor a diez días hábiles, con copia a esta Auditoría Interna.

Licda. Viviana Rivera Barrantes, MAP
Profesional III

Lic. José Wong Carrion
Jefe Área de Sistemas

JUNTA DE PROTECCION SOCIAL · AUDITORIA INTERNA ·

MBA. Rodrigo Carvajal Mora
Subauditor Interno

ANEXO N° 1

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

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 de Informática **Fecha** 28 de diciembre, 2010

Recomendación	Estado de la recomendación	Seguimiento
A. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO ALTO		
1.Versión de base de datos Sybase desactualizada. Se recomienda diseñar y elaborar un plan para la actualización de la versión del Motor de Base de Datos Sybase, esta mejora debe realizarse bajo un ambiente de pruebas. Asimismo, contar con documentación formal del proceso ejecutado.	Cumplida	El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, mencionó que la recomendación se encuentra: *"Atendido"* De acuerdo con la información extraída de la base de datos por medio de la consulta *"SELECT @@VERSION"*, se detectó que la versión de la base de datos ha sido actualizada a la 15.5. En relación al plan de pruebas y al documento formal ejecutado durante el proceso de cambio de versión, han sido solicitados al Departamento de Informática por medio del oficio AI-822 el 8 de noviembre del 2012, en la cual dieron respuesta con la nota I 1101-12 del 14 de noviembre del 2012, adjuntado el plan de pruebas módulos visual basic 5.0, 6.0 para el cambio de versión de la base de datos sybase 12.5 a 15.5 en el servidor de producción.
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	Parcialmente Cumplida	El pasado 16 de febrero del 2012, el señor Ronald Ortiz jefe del Departamento de Informática por medio del oficio I 172-12, basándose en esta recomendación indicó: *"Se implementará la consola sobre WEB"* De acuerdo a lo anterior, al realizar la verificación de acceso de los usuarios a los sitios web: cajeros BCR – cambio de premios, cajeros bcr – despachar lotería, cementerios, web transaccional, se determinó que es realizada con un único factor de autenticación, a pesar de que la institución posee un certificado de firma digital (llave 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.).		algoritmo: RSA SHA-1 RSA, tamaño de la llave: 2048 bits), emitido por VeriSign. El 19 de diciembre del 2012 se le realizó al señor Ortiz la entrevista N° 1, la cual contenía la siguiente pregunta: *"7) ¿Han facilitado 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 de producto, de acuerdo con la ISO 27002 8.2.2.?"* A lo anterior, respondió: *"No, pero para el próximo año se tienen pensadas sesiones de capacitación sobre el manejo de recurso informático por parte de los usuarios finales, mismo que se encuentra en el Plan de Capacitación Informático remitido al Departamento de Recursos Humanos."* Es importante hacer conciencia a los funcionarios internos y externos sobre el uso de las contraseñas, los riesgos que conlleva una utilización inapropiada, para ello se debe recurrir tal como la indica la recomendación a la ISO 27002 8.2.2. Ante esto, se demuestra que no se le ha facilitado a los funcionarios, información que contenga las ventajas de conocer los riesgos de seguridad, así como tampoco la importancia de mantener los equipos actualizados.
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 encuentra dentro de la red que pueda comprometer los servicios el cual se ofrecen. Desligar la responsabilidad de temas de seguridad de la	Parcialmente Cumplida	El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz en dicha recomendación mencionó: *"Se tiene presupuestado para este asño cumplir este aspecto.* *Se tiene presupuestado para este año sustituir equipos de comunicación antiguos y evaluar los IOS de cada uno.* *Se inició con la definición de la sección y le fue comunicada a la AI mediante oficio I-042-12, el planteamiento de la capacitación fue remitida a la Subgerencia Administrativa según fue indicado en anteriores*

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.		*observaciones sobre la capacitación y en cuanto a la definición de herramientas de monitoreo se están implementando en el actual año."* De acuerdo con la entrevista realizada al señor Ronald Ortiz jefe del Departamento de Informática, en relación a las capas DMZ se determinó que poseen dos niveles de seguridad las cuales son el clúster de Firewalls y el controlador de entrega de aplicaciones Marca F5, no obstante, el señor Ortiz indicó que en efecto poseen un único router para la salida a Internet, y un firewall en clúster uno está pasivo y otro como activo. Por otro lado, mencionó que existe un módulo de IPS activo en el router de internet, y que no se poseen equipos "netscreen" o protección de red, debido a que el mismo se encuentra en proceso. Además, indicó que no se han ofrecido a los usuarios información sobre ventajas de conocer riesgos de seguridad según lo señalado por la ISO 27002, en sus apartados A.10.3.1, A.10.3.2 y A.9.2.4. En lo que respecta a las capacitaciones por parte del oficial de seguridad, se determinó la existencia de una de ellas con respecto al tema de seguridad informática. Con base en la nota I 1227-11 del 23 de noviembre del 2011, el Sr. Ortiz mencionó que el Sr. Bruce Campbell fue designado como Oficial de Seguridad, no obstante esto no representa una Sección de Seguridad con todos los aspectos señalados en la recomendación tales como: herramientas de capacitación, equipos para su gestión, y monitorear los servicios en un modelo de 24/7/365, ya que el Sr. Campbell posee un horario de 8.15 a 3.30, salvo casos de emergencia, por lo que no se estaría monitoreando los servicios en el horario señalado.

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:

DH-DSS-AES256-SHA	Excellent Security	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.
DH-RSA-AES256-SHA	Excellent Security	Similar to the one above, this one uses RSA for authenticationi
DHE-DSS-AES256-SHA	Excellent Security	The next two ciphers are similar to the previous two respectively 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

Parcialmente Cumplida

Con fecha 16 de febrero del 2012, se muestra el oficio I 172-12, emitido por el señor Ronald Ortiz, en la cual se indica:

"Se tiene presupuestado para este año aumentar el nivel de seguridad del certificado actual que si asegura la integridad de la información.

Se implementará la consola sobre WEB"

A la fecha 19-12-2012, se verificó en el sitio Web http://secure.jps.go.cr/jpsvirtual/login.html se observó que es grado A, mediante la herramienta SSLDigger.

Por otro lado, se detectó la utilización requerida de la firma digital, por medio de correo electrónico que lleva de asunto. *"Implementación firma digital en JPS"*, relacionado con la circular I 0187-2012, donde se hace conocimiento que a partir del 10 de abril del 2012, el uso del Certificado de Firma Digital será obligatorio para el acceso a la Consola Corporativa.

En el Informe *"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 la presente recomendación, donde detalla:

"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."

Se determinó que a nivel externo no ha sido implementado una doble validación, únicamente poseen un solo acceso para ingresar a la web institucional, en relación con lo interno la firma digital es utilizada al momento de ingresar a los sistemas institucionales, y al correo

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.		electrónico, con respecto a este último, el uso de la firma digital no es de uso obligatorio.
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 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.	Parcialmente Cumplida	El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, mencionó que dicha recomendación se encuentra: *"Atendido"* En la revisión efectuada se observó que funcionarios internos y consultores del área de informática no lograron ingresar al ambiente de producción, la base de datos en la que se encontraban trabajando ha sido la de pruebas. Sin embargo, en la bitácora *"sybsecurity"* el usuario 'L0206380176' perteneciente al funcionario Jairo Cruz Sibaja, se encontraba haciendo actualizaciones en la tabla *"RH_RolAsistenciasDet"* de la base de datos perdba del ambiente de producción.
6.Analista programadores con acceso al servidor de producción. Eliminar los accesos de los analistas programadores al ambiente de producción.	Parcialmente Cumplida	El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, señaló con respecto a la recomendación actual: *"Eliminados los accesos de personal de informática a los ambientes de producción.* *Por medio servicio al cliente se mantiene acceso solo de consulta"* Se observó que los programadores en las cuentas genéricas (mmasis, fulvio, oviquez, paul, rgutierrezsvillalobos, entre otros) no contaban con acceso al ambiente de producción, no obstante el señor Ronald Ortiz ha indicado que aún mantienen acceso de consulta, lo cual significaría que no ha sido eliminado en su totalidad los accesos según lo señalado en esta recomendación, ya que además hay presencia de actualizaciones realizadas por un funcionario de informática en el ambiente de producción.

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	El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, mencionó: *"En el pasado se trato de implementar pero existió resitencia por parte de usuarios, se estará retomando."* En la información extraída de la base de datos el día 7 de noviembre del 2012, sobre el detalle de los usuarios del área de informática, se verificó sin cumplir lo siguiente: - Usuarios con la longitud mínima de contraseña: 6 (configurada con su valor por defecto). - Expiración del password: 0 (configurado el valor por defecto 0, no permite verificar el vencimiento de contraseñas) - Fecha última de cambio de password: existen fechas que no han sido modificadas desde el 2009. Por otro lado, en la configuración de la base de datos se observó que aún hay parámetros con su valor por defecto: - Minimium password length: Los campos de "valor" y "run" poseen el valor por defecto 6, cuando lo recomiendo es 8. - check password for digit: Los campos de "valor" y "run" poseen el valor por defecto 0, lo cual indica que la complejidad de las contraseñas no está activa. Además, el día 14 de diciembre del 2012 se revisó la Directiva de Seguridad Local en el Active Directory detectándose debilidades, las cuales son:: - Almacenar contraseñas con cifrado reversible: se encuentra deshabilitada. - Exigir historial de contraseñas: actualmente está en 12, cuando lo recomendable es 24 contraseñas. - Longitud mínima de la contraseña: el valor que posee es 7, cuando lo recomendado es 8 caracteres. - Vigencia mínima de la contraseña: posee un valor de 1, y lo recomendable es dos días. - Vigencia máxima de la contraseña: posee un valor de 45, y lo

recomendable es 42 días.

El 7 de noviembre del 2012 se revisó el desglose del comando *"sp_helpserver"* para detectar cual servidor posee la conexión remota activa en la base de datos Sybase, se determinó que existen 4 servidores, de los cuales 3 de ellos (NOD01_XP, NOD02_BS y SYB_BACKUP) no cuentan con un modelo de encriptación segura de acuerdo al modelo "RPC modelo de seguridad A", donde en la sana práctica el modelo a utilizar es "Modelo de seguridad RPC B". En la siguiente tabla se visualiza el estado de cada uno:

Remote Server	Class	Status
NODO1	local	
NODO1_XP	RPCServer	no timeouts, no net password encryption, writable, rpc security model A, enable login redirection
NODO2_BS	ASEnterprise	no timeouts, no net password encryption, writable, rpc security model A, enable login redirection
SYB_BACKUP	[NULL]	timeouts, no net password encryption, writable , rpc security model A, enable login redirection

Por otro lado, por medio del reporte *"Informe de Usuarios por Perfil que contenga 'seguridad'"* con fecha 12 de diciembre del 2012, se evaluó cuáles usuarios se encontraban como administradores de la Web Transaccional, y se determinó que existen usuarios que están definidos como administradores, siendo algunos de estos funcionarios analistas. Entre ellos se encuentran:

Nombre	Puesto
Wen Zhen Wu	Analista Programador
Jairo Cruz Sibaja	Jefe
Ronald Ortiz Méndez	**Jefe de Informática**
Zurika Ruiz Gonzalez	Analista Programador
Lohr Campbell Arguello	Oficial de Seguridad

<table>
<tr>
<td>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".

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>Pendiente</td>
<td>En el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, en referencia a esta recomendación indicó que estaban "Atendidos", no obstante, se determinó que existen colaboradores activos en el syslogins (al 07-11-2011) a pesar de que Recursos Humanos envío correos indicando que algunos funcionarios ya no forman parte de la Institución. Por lo que, se comparó el listado de usuarios de la recomendación #8 del seguimiento de recomendaciones AI JPS 26-2011 con los correos de salida de personal enviados por el Departamento de Recursos Humanos.

Los siguientes usuarios tomados de forma aleatoria se encuentran inactivos, sin embargo en la base de datos institucional, aún permanecen activos:

<table>
<tr><th>suid</th><th>status</th><th>Dbname</th><th>name</th><th>Fullname</th></tr>
<tr><td>1266</td><td>0</td><td>sacdb2003</td><td>L0601820275</td><td>Dunia María Cruz Hernández</td></tr>
<tr><td>1289</td><td>0</td><td>jps_real</td><td>L0301860557</td><td>Mayra Rivas Brenes</td></tr>
<tr><td>1302</td><td>0</td><td>jps_real</td><td>L0601710777</td><td>Juan Villalobos Barquero</td></tr>
<tr><td>1320</td><td>0</td><td>Perdba</td><td>L0301810476</td><td>Daniel Hidalgo Mora</td></tr>
<tr><td>1493</td><td>0</td><td>Perdba</td><td>L0103720132</td><td>Kenneth Barrantes Jimenez</td></tr>
<tr><td>1641</td><td>0</td><td>perdba</td><td>L0900390557</td><td>Gerardo Salazar Mora</td></tr>
<tr><td>1675</td><td>0</td><td>jps_real</td><td>L0106490140</td><td>Jose A. Lizano García</td></tr>
<tr><td>2531</td><td>0</td><td>costos</td><td>L0202540394</td><td>José Joaquín Moreno Perez</td></tr>
<tr><td>2318</td><td>0</td><td>costos</td><td>L0700370958</td><td>John Neil Hamilton</td></tr>
</table>
</td>
</tr>
<tr>
<td>9.Debilidades en la seguridad de la información en los contratos con socios comerciales y canales de distribución.
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>Por medio del oficio I 172-12 el 16 de febrero del 2012, el señor Ronald Ortiz, mencionó:

"Este sistema será sustituido por el nuevo sistema de Lotería Electrónica suministrado por el consorcio Gtech Bold."

En relación a las cédulas jurídicas, se determina por medio de un muestreo de la tabla "syslogins" el día 7 de noviembre del 2012, que existen diferentes números de cédula para un mismo socio comercial,</td>
</tr>
</table>

algunos de ellos son:

Suid	status	Name	fullname
4537	0	L0114760501	Adrian Soto Sanchez
4659	0	TELT51	Adrian Soto Sanchez
3861	0	L030040566010201	Coopeflores Santa Barbara (soc
3862	0	L030040566010202	Coopeflores Santa Barbara (soc
3863	0	L030040566010203	Coopeflores Santa Barbara (soc
3864	0	L030040566010204	Coopeflores Santa Barbara (soc
3865	0	L030040566010301	Coopeflores Santa Barbara (soc
4314	0	L0114470114	Melissa Aleman Hernandez Soci
4304	0	LL0114470114	Melissa Aleman Hernanadez (soc
4034	0	L0112150521	Orlando Gomez Gamboa (socio)
4156	0	L01121505210101	Orlando Gomez Gamboa (socio)
3218	0	L0203390680	Victor Ramirez Rojas
3760	0	L0205650707	Victor Ramirez Rojas (socio)
3907	0	L0205950859	Yanory Aguilar Hernandez (soci
3910	0	L05014914010103	Yanory Aguilar hernandez (soci

No obstante, en virtud de que el nuevo sistema de Lotería Electrónica aún no ha sido implementado, y la información contenida en la base de datos aún refleja más de un registro para un socio comercial, dicha recomendación continúa pendiente.

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

Pendiente

El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, mencionó:

"Se está modificando los accesos para que sea el Sr. Bruce Cambpell el encargado de atender estos menesteres.

Se estarán realizando estudios de penetración para determinar vulnerabilidades

Este sistema no ha recibido mejoras por cuanto será sustituido por el nuevo sistema de Lotería Electrónica suministrado por el consorcio Gtech Bold"

<table>
<tr>
<td>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.</td>
<td></td>
<td>En relación a lo anterior, se determina que el Departamento de Informática aún no ha realizado estudios de costo beneficio, dado que a la fecha 19-12-2012 esta Auditoría no ha recibido copia del resultado obtenido en cuanto al proceso de seguridad local de los equipos y sus puntos de acceso a internet.

Por otro lado, la institución posee el antivirus Karpersky, sin embargo no se encontraron pruebas de vulnerabilidad, la misma muestra estadísticas sobre el estado de las bases de datos, en la cual se indica se las versiones se encuentran actualizadas o no.</td>
</tr>
<tr>
<td><u>12.La opción Allow Remote Access está habilitada.</u>
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.</td>
<td>Pendiente</td>
<td>Se detectó que la opción de "Allow Remote Access" se encuentra con el valor por defecto "1" (habilitado), lo cual indica que permite conexiones remotas con otros servidores.

No obstante, el Señor Ronald Ortiz, Jefe del Departamento de Informática, en el Anexo del oficio I 172-12 del 16 de febrero del 2012 indicó:

"En la actualidad se tienen solamente 25 que son las necesarias para los ambientes de producción. El Allow Remote Access no se puede modificar por cuanto odedece a la necesidad de activar el sistema automático de respaldos."

Sin embargo, no se envió a esta Auditoría ningún estudio técnico que justifique la razón por la cual el parámetro no se puede modificar.</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>Pendiente</td>
<td>De acuerdo con la revisión realizada en la tabla "syssrvroles", se determinó que a la fecha 07 de noviembre del 2012 ningún role contaba con contraseña, los cuales son:

<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>
<tr><td>dtm_tm_role</td><td>keycustodian_role</td></tr>
<tr><td>ha_role</td><td></td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td></td>
<td>No obstante, el Señor Ronald Ortiz por medio del oficio I 172-12 del 16 de febrero del 2012 mencionó:

"Los roles son perfiles que se asignan a los usuarios y por tanto no son componentes que tienen claves, las claves corresponden a los usuarios."

Sin embargo, por medio de correo electrónico del 19 de noviembre 2012 el señor Joaquín Casaw consultor de base datos de la Junta de Protección Social indicó:

"A todos estos roles se les puede asignar un password. Cuando se hace esto los roles quedan por defecto inactivos a la hora de hacer login al motor de bases de datos y para activarlos hay que correr un comando como el siguiente (ejemplo):

set role sa_role with passwd "JPSjpsJPS" on

Una vez que activa el role entonces ya puede hacer todas las tareas que le permite el rol de sa. Tiene que hacer esto cada vez que ingrese a la base de datos y necesite correr una tarea de administrador.

En realidad funciona como una doble seguridad."</td>
</tr>
<tr>
<td><u>14.Debilidades en la asignación de roles sa_role y sso_role.</u>
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.</td>
<td>Pendiente</td>
<td>El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, señaló que esta recomendación se encuentra: "Atendido"

En relación al análisis realizado a los roles sa_role, sso_role y replication_role el día 7 de noviembre del 2012, se determinó que los siguientes usuarios no deberían contar con dicho permiso:

<table>
<tr><th>name</th><th>Fullname</th><th>Name</th></tr>
<tr><td>L0119580306</td><td>Usuario para backup</td><td>sa_role</td></tr>
<tr><td>L0119580306</td><td>Usuario para backup</td><td>sso_role</td></tr>
<tr><td>sc007xdbuser</td><td>Acceso</td><td>sso_role</td></tr>
</table>

De igual manera, se detectó el usuario L0119580306 asignado a varios roles:</td>
</tr>
</table>

		Name / **Fullname** / **Role** L0119580306 / Usuario para backup / sa_role L0119580306 / Usuario para backup / sso_role Se constató que el usuario mmasis, posee permisos de Administrador, además de accesos a diferentes roles: **name** / **fullname** / **name** mmasis / Maynor Masis Castillo / dtm_tm_role mmasis / Maynor Masis Castillo / ha_role mmasis / Maynor Masis Castillo / js_admin_role mmasis / Maynor Masis Castillo / js_client_role mmasis / Maynor Masis Castillo / js_user_role mmasis / Maynor Masis Castillo / keycustodian_role mmasis / Maynor Masis Castillo / messaging_role mmasis / Maynor Masis Castillo / mon_role mmasis / Maynor Masis Castillo / navigator_role mmasis / Maynor Masis Castillo / oper_role mmasis / Maynor Masis Castillo / replication_role mmasis / Maynor Masis Castillo / sa_role mmasis / Maynor Masis Castillo / sso_role mmasis / Maynor Masis Castillo / sybase_ts_role mmasis / Maynor Masis Castillo / webservices_role Al realizar la consulta en el Tribunal Supremo de Elecciones el día 16 de enero del 2013, se comprobó que el usuario L0119580306 pertenece en el Tribunal a la señora LIZZY KAMILA LOPEZ JIMENEZ, sin embargo la señora López no es funcionaria de esta institución.
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.	Pendiente	El 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, mencionó que dicha recomendación se encuentra: *"Atendido"* El 19 de diciembre del 2012 esta Auditoría en conjunto con el señor Ronald Ortiz se extrajo de los servidores la lista de usuarios mediante el comando *"cat/etc/passwd"*. Al hacer la revisión de los mismos se detectó que aún permanecen sin contraseña. Los cuales son:

<table>
<tr>
<td></td>
<td></td>
<td>- Firewall Checkpoint Nombre: fw-nodo0 (10.0.0.5)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp

- Firewall Checkpoint Nombre: fw-nodo1 (10.0.0.4)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp

- Consola Firewall (10.0.0.6)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp

- Servidor Web yire (192.168.1.2)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp, postgres

- Servidor Secure www2 (192.168.1.50)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp

- Servidor BS Jpsquerry (10.0.0.200)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp

- Servidor Aplicaciones (10.0.0.90)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp

- Servidor BD replica (10.0.0.240)
daemon, bin, sys, adm, lp, uucp, nuucp, smmsp, postgres

De acuerdo con lo anterior, se determinó que ninguno de los usuarios mencionados posee contraseña, por lo que esta recomendación aún continúa pendiente.</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>El 7 de noviembre del 2011 se verificó que todavía existen cuentas de usuarios activos en la base de datos "master", a pesar de que por medio del oficio I 172-12 del 16 de febrero del 2012 el señor Ronald Ortiz indicó que estaba "Atendido", por lo tanto se debe recordar que únicamente los usuarios administradores deben tener dicho acceso. Los usuarios que han sido identificados son:

<table>
<tr><th>suid</th><th>status</th><th>dbname</th><th>Name</th><th>fullname</th></tr>
<tr><td>1</td><td>0</td><td>master</td><td>Sa</td><td>[NULL]</td></tr>
</table>
</td>
</tr>
</table>

		955	0	master	SYSSQL	Del Sistema
		3	0	master	Replica	administrador de replicación
		4991	0	master	L0604440444	[NULL]
		4997	0	master	L0113480674	[NULL]
		1435	0	master	L0108950595	Lohr Bruce Campbell Arguello
		1657	0	master	Mmasis	Maynor Masis Castillo
		1707	0	master	L0119580306	Usuario para backup
		4781	0	master	L0402080112	[NULL]
		4797	0	master	L3101424132	[NULL]
		4806	0	master	L0101110111	[NULL]
		4807	0	Master	L0202220222	[NULL]
		4808	0	Master	LUSR_Agregar Login	[NULL]
		5018	0	Master	L0113330240	Katherine Fonseca Montero BCR
		4989	0	Master	master_maint	[NULL]
		4988	0	Master	jps_maint	[NULL]
		4954	0	Master	L0115030621	[NULL]
		4982	0	Master	LL0115140005	[NULL]
		5001	0	Master	L0701520728	[NULL]
		5002	0	Master	L0110080861	[NULL]
		5005	0	Master	L0112250928	[NULL]
		5006	0	Master	L0108700848	[NULL]
		5009	0	Master	L0113700434	[NULL]
		5016	0	Master	L0101630686	[NULL]
		5033	0	Master	L2060900551	[NULL]
		5034	0	Master	L0112070048	Paola Ramírez Zayas BCR
		5035	0	Master	L0205980086	Noemy Alpizar Rojas BCR
		5036	0	Master	L0206090551	Gabriela Alfaro Aviles BCR
17.Existencia de usuarios genéricos y duplicados. 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	Pendiente	El señor Ronald Ortiz por medio del oficio I 172-12 del 16 de febrero del 2012, se refirió a esta recomendación indicando: *"Se eliminarán los duplicados."* A continuación, se detallan los usuarios duplicados y genéricos que fueron detectados al 7 de noviembre del 2012:				

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.

- Usuarios Duplicados

La revisión de los usuarios duplicados se hizo mediante las tablas SG_Usuarios y syslogins.

En la revisión efectuada a la tabla **SG_Usuarios**, se observó que existen usuarios duplicados, los cuales son:

CodigoUsuario	Nombre1	Apellido1	Apellido2	Login	Estado
1078	Andrey	Hernández	Bolaños	L0111840728	A
2355	Andrey	Hernández	Bolaños	L0111840726	A
3135	Angie	Valverde	Morales	L0104830524	A
3231	Angie	Valverde	Morales	L0114830524	A
35	Prueba	Prueba	Prueba	L0109990999	A
3418	Prueba	Prueba	Prueba	L0101110111	A
3420	Prueba	Prueba	Prueba	L0404440444	A
3609	Rafael	Ureña	Quiros	L0101630686	A
3617	Rafael	Ureña	Quiros	L0701630686	A
1445	Sara	Quesada	Garita	L0206110235	A
1628	Sara	Quesada	Garita	L0206110238	A
1520	Susan	Castro	Castro	L0112160527	A
1392	Susana	Castro	Castro	L0112160521	A
2868	Wendy	Madrigal	Diaz	L0102130589	A
2877	Wendy	Madrigal	Diaz	L0112130589	A
1731	Zaida	Sánchez	Abarca	L0503770774	A
1810	Zayda	Sánchez	Abarca	L0503570774	A

En relación con la tabla **syslogins** existen usuarios con cuentas genéricas duplicadas, en donde algunas de ellas poseen estado inactivo (2), lo cual significaría que eventualmente podrían volver a activarse, por lo que se debe valorar la eliminación de las mismas. Entre ellas se encuentran:

suid	status	Dbname	Name	fullname
4537	0	perdba	L0114760501	Adrian Soto Sanchez
4659	0	jps_real	TELT51	Adrian Soto Sanchez
968	2	jps_real	TELT06	ALEJANDRO MUSSIO

1284	0	jps_real	L0108150232	Alejandro Mussio González
1928	2	jps_real	L011119109	Alejandro Bonilla Molina BCR
3264	0	jps_real	L0111190109	Alejandro Bonilla Molina BCR
1773	0	electronicadb	L0107180433	Alexander Lizano Morales
4562	2	electronicadb	aelectronica	Alizano
1220	0	jps_real	brucerh	Bruce Campbell Arguello
1435	0	master	L0108950595	Lohr Bruce Campbell Arguello
3184	0	perdba	L0302200214	Carlos Duran Gonzalez
3327	0	perdba	L0302200124	Carlos Duran Gonzalez
4199	0	jps_real	TELT49	Odice Loria Solano
1278	0	jps_real	L0204210709	Odilce Loría Solano

Por otro lado, se verificó en la misma tabla **syslogins** que algunos usuarios activos fueron creados con una cédula o un nombre que no les corresponde, entre ellos están:

suid	status	dbname	Name	fullname
1942	0	jps_real	L0205110415	Adriana Ledezma Vargas BCR
3299	0	jps_real	L0112660259	Carlos Herrera Araya BCR
3784	0	jps_real	L0111400441	Myrian Chacon Rodriguez BCR
3930	0	jps_real	L0109130062	Ricardo Guzman Saravia (BCR)

Al consultar las cédulas de los usuarios de la lista anterior en el Tribunal Supremo de Elecciones, se determinó que las cédulas se encuentran bajo otro nombre, incumpliéndose el estándar de creación de usuarios (*"El de base de datos es igual al de jurídicos, L0+cédula"*):

Cédulas (según estándar)	Nombre de Base de Datos (fullname)	Nombre en el Registro Civil
L0205110415	Adriana Ledezma Vargas BCR	Angélica Magaña Esquivel
L0112660259	Carlos Herrera Araya BCR	Carlos Vinicio Bellido Ortega
L0111400441	Myrian Chacon Rodriguez BCR	Randall Enrique Hernández Vega
L0109130062	Ricardo Guzman Saravia (BCR)	Karla Vanessa Gamboa Monge

- Existencia de usuarios genéricos activos de la base de datos Sybase.

En la revisión efectuada a la tabla *"syslogins"* se detectó que existen cuentas genéricas activas. Algunas de ellas son:

suid	status	dbname	name	Fullname
2	0	sybsystemdb	probe	[NULL]
4991	0	master	L0604440444	[NULL]
4997	0	master	L0113480674	[NULL]
1484	0	sacdb_pruebas	L03019308822	[NULL]
1945	0	jps_real	L0112650782	[NULL]
3007	0	sc3xdb	dbmon	[NULL]
4781	0	master	L0402080112	[NULL]
4782	0	master	L0113570107	[NULL]
4783	0	master	L0112280440	[NULL]
4784	0	master	L0401970771	[NULL]
4785	0	master	L0204880867	[NULL]
4809	0	master	LL0303330333	[NULL]
4886	0	master	L0155320811	[NULL]
4902	0	master	L105210111	[NULL]
1220	0	jps_real	brucerh	Bruce Campbell

		Arguello
		3393 0 jps_real conectividad7 Conectividad en Sitio Web
		1674 0 jps_real identificaciones Identificaciones Adjudicatario
		1752 0 electronicadb jpsconectividad jpsconectividad
		1657 0 master mmasis Maynor Masis Castillo
		4437 0 jps_real rortiz Ronald Ortiz Mendez Administra
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.	Pendiente	Ante esta recomendación el pasado 16 de febrero del 2012, por medio del oficio I 172-12, el señor Ronald Ortiz, mencionó: *"Se eliminarán los usuarios."* Para verificar lo indicado en el oficio anterior, se procedió a revisar los usuarios activos de los diferentes servidores, dando como resultado usuarios con permisos que nos les corresponde como es el caso de *"ccmona"*, así como también usuarios genéricos que se encuentran activos. El siguiente desglose del 19 de diciembre del 2012 muestra los usuarios que han sido detectados en cada servidor:

Servidor	IP	Usuarios
Firewall Checkpoint Nombre: fw-nodo0	10.0.0.5	- soporte. - monitor.
Firewall Checkpoint Nombre: fw-nodo1	10.0.0.4	- soporte. - monitor.
Consola Firewall	10.0.0.6	- soporte. - monitor.
Servidor Web yire	192.168.1.2	- monitor. - stxwww. - cmona.
Servidor Secure www2	192.168.1.50	- monitor.
Servidor BS Jpsquerry	10.0.0.200	- monitor. - hde

		Servidor Aplicaciones 10.0.0.90 - desa. - monitor. Servidor BD replica 10.0.0.240 - monitor. Por medio de la nota AI-599 del 04 de octubre del 2011 girada al Departamento de Informática, se detectó que existen usuario sin ser removidos a pesar de las instrucciones ya giradas, entre ellos el usuario *"ccmona"* el cual no fue eliminado, pero si modificado paso de ser *"ccmona"* a *"cmona"*. Cabe señalar que el usuario root del servidor 192.168.1.50, está bajo la responsabilidad de los señores Luis Ramírez y Ronald Ortiz.
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.	Pendiente	Se determinó que existen pistas de auditoría para el servidor 10.0.0.135 y están activas. En la entrevista N° 3 el Sr. Ronald Ortiz indicó que llevan bitácoras de las pitas de auditoría, sin embargo, no se realizan formularios internos para la revisión de bitácoras que indiquen la fecha, el nombre y el proceso verificado; por lo tanto el proceso de revisión periódica que incluya la fecha de ejecución, el análisis, el resultado y la firma de autorización de la Jefatura del Departamento de Informática no se está realizando. Según la revisión realizada a la bitácora de la web transaccional el día 19 de diciembre del 2012 en compañía del señor Alexander Lizano del Departamento de Informática, se verificó que sí existe una bitácora en la que se lleva todo el proceso de la transacción, pero no se detectó un control en donde se señale a cual socio comercial se le dio seguimiento, y a qué fecha. Dicha observación en el oficio I 172-12 del 16 de febrero del 2012 el señor Ronald Ortiz mencionó: *"Se asginó al Sr. Alexander Lizano."*. No obstante, la implementación del control no ha sido realizada. Se pudo visualizar en el Active Directory utilizado para la autenticación de usuarios, que no posee configurada las pistas de auditoría. Ante esta situación el señor Ortiz mediante el oficio señalado, hizo mención a lo siguiente: *"Se procederá en activar"*. Lo cual a la fecha 21 de diciembre del 2012, no ha sido ejecutado dicho

		proceso. Las políticas detectadas son: - Auditar el acceso a objetos: Sin auditoría - Auditar el acceso del servicio de directorio: Sin auditoría - Auditar el cambio de directivas: Sin auditoría - Auditar el seguimiento de procesos: Sin auditoría - Auditar el uso de privilegios: Sin auditoría - Auditar eventos de inicio de sesión: Sin auditoría - Auditar eventos de inicio de sesión de cuenta: Sin auditoría - Auditar eventos del sistema: Sin auditoría - Auditar la administración de cuentas: Sin auditoría
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.	Pendiente	En relación a esta recomendación, en nota I 172-12 del 16 de febrero del 2012 el señor Ronald Ortiz, mencionó: *"Atendido"*. Sin embargo, en la revisión efectuada el 12 de diciembre del 2012 esta Auditoría en compañía del Oficial de Seguridad Bruce Campbell del Departamento de Informática quien a su vez es responsable del Active Directory de acuerdo a lo señalado por medio de correo electrónico el señor Ronald Ortiz el día 21 de diciembre del 2012, pudo detectar usuarios que se encuentran como administradores en el servidor Active Directory, los cuales son: ➢ Usuarios del Admins. del dominio o dvillalta o ezromero o ezunigar o KL-AK-2F5D-202X365DB1 o lramireza o mmasis ➢ Usuarios del escritorio remoto. o mmasis o respinozaa ➢ Existencia de un usuario desconocido en el Grupo de replicación de contraseña RODC denegada. o krbtgt

		Existen usuarios creados en el escritorio remoto que no son administradores generando así para la institución un riesgo muy alto, ya que los usuarios que se encuentran como administradores podrían ingresar a los equipos institucionales sin ningún problema, debido a que poseen el control total del dominio, permitiendo además, asignar permisos o derechos a otros usuarios.
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.	Pendiente	El pasado 16 de febrero del 2012, el señor Ronald Ortiz jefe del Departamento de Informática por medio del oficio I 172-12, sobre esta recomendación indicó: *"Se tiene planificado y presupuestado para el año 2012 construir nuestro datacenter en el nivel TIER 2.* *Atendido* *Se procederá en hacer solicitud a Mantenimiento para que sean de concreto.* *Atendido"* Por lo tanto, dado lo anterior, se detectaron las siguientes debilidades: • **Centro de Telecomunicaciones al día 13 de diciembre del 2012:** ✓ Cajas de cartón contenidas en el cuarto de telecomunicaciones. ✓ Puerta sin cerradura. ✓ Mueble determinado sin uso desde el seguimiento de recomendaciones de diciembre 2011. ✓ No se logró observa un extintor. ✓ Paredes de vidrio. • **Sitio Alterno (ubicado en la Uruca) al día 20 de diciembre del 2012:** ✓ No se encontró bitácora de acceso a los servidores, sin embargo en la puerta principal el guarda lleva el control de ingreso al edificio. • **Centro de Datos (ubicado en Informática) al día 20 de diciembre**

<table>
<tr><td></td><td></td><td>del 2012:
✓ Paredes de Vidrio.
✓ Escalera.
✓ Objetos varios (papel en el suelo, escalera, caja de cartón con equipo de cómputo, entre otros).</td></tr>
<tr><td colspan="3">C. HALLAZGOS ENCONTRADOS CON UN NIVEL DE RIESGO BAJO</td></tr>
<tr><td>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.</td><td>Pendiente</td><td>Se determinó por medio de correo electrónico enviado por el Señor Ronald Ortiz el día 15-11-2012, indicó que el estándar para la creación de usuarios de base de datos es:

"El de base de datos es igual al de jurídicos, L0+cédula"

Sin embargo, en la nota I 172-12 del 16 de febrero del 2012 enviada por el Señor Ortiz, mencionó:

"Se procederá en hacer reemplazo de usuarios que no cumplen con el estandar."

En la revisión efectuada el 15 de noviembre del 2012, se determinó que aún continúan usuarios creados sin el debido estándar, aunque algunos se encuentran inactivos podrían activarse en cualquier momento, esto a pesar de que el Señor Ortiz mencionó que procedería a reemplazar usuarios que no cumplían con el estándar. Entre ellos se encuentran:

<table>
<tr><th>suid</th><th>status</th><th>dbname</th><th>Name</th><th>fullname</th></tr>
<tr><td>1498</td><td>2</td><td>seguridad_db</td><td>Segurinternet</td><td>Acceso a la seguridad_internet</td></tr>
<tr><td>4257</td><td>2</td><td>jps_real</td><td>activapremioespecialinternet</td><td>Activa loteria Internet</td></tr>
<tr><td>1697</td><td>2</td><td>actas_pruebas2</td><td>pruebas</td><td>Actualización Actas HDE GROUP</td></tr>
<tr><td>968</td><td>2</td><td>jps_real</td><td>TELT06</td><td>ALEJANDRO MUSSIO</td></tr>
<tr><td>1928</td><td>2</td><td>jps_real</td><td>L011119109</td><td>Alejandro</td></tr>
</table>
</td></tr>
</table>

		4562 2 electronicadb aelectronica Bonilla Molina BCR 3454 2 pruebas_jps_real conectividad7_capacitacion Alizano Capacitacion Comercio Electrón 1665 2 pruebas_loterias L0909990999 Capacitacion y pruebas
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	Por medio del oficio I 172-12 del 16 de febrero del 2012, el Señor Ronald Ortiz indicó: *"No es posible activar el muro de fuego por cuanto hacerlo significaría bloquear servicios requeridos, se comenta que el acceso a este servidor esta controlado por el muro de fuego corporativo quien tiene reglas claras de control de acceso."* Por lo tanto, al hacer la revisión del firewall de Windows se determinó que se encuentra inactivo, aunque en el oficio anterior se haya dado la justificación para no mantenerlo activo, esto no una justificante, ya que se estaría comprometiendo la seguridad de la institución, debido a la misma herramienta permite incorporar aquellos servicios que no requieren ser bloqueados, no obstante, se entiende que existe un muro de fuego corporativo, sin embargo el contar con dos firewall beneficiaría la seguridad institucional, por otro lado la institución no tendría que incurrir en ningún gasto, ya que el negocio cuenta con dicha herramienta.
25.Debilidades en el traslado de respaldo de información fuera de la Institución. Se recomienda fortalecer el control de traslado de respaldos hacia el sitio externo, donde se establezcan personas adicionales a la responsable de ejecutar el control y encargados de verificar que el proceso se ejecute correctamente.	Cumplida	Se determinó por medio del oficio I 172-12 del 16 de febrero del 2012, el Señor Ronald Ortiz el día, indicó: *"Se confeccionó noto al Sr. Luis Ramírez ordenandole proceder según el procedimiento"* Por medio del oficio I 171-12 del 16 de febrero del 2012 se emite oficio para que se incorpore la fecha, la hora, y la firma del que entrega y recibe respaldos de información fuera de la institución. En la revisión efectuada se determinó que la empresa Seguridoc tomó el nombre de Retrievex, por lo que los formularios son distintos, sin embargo en este nuevo formato, se detectó que la documentación

		correspondiente, ya se encuentra con la respectiva fecha, hora y firma.
26.Ausencia de política y/o procedimiento de restauración. 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.	Parcialmente Cumplidas	Por medio del oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, indicó: *"Se procederá en atender lo recomendado"* No obstante, esta Auditoría envío la nota AI-848 el 16 de noviembre del 2012, consultando a Informática sobre la política y/o procedimiento para recuperar la información de la base de datos, el formulario y las bitácoras obtenidas, sin embargo el oficio I 1143-12 del 26 de noviembre 2012 como respuesta al oficio anterior, se hizo entrega de las políticas y procedimientos sobre la realización de respaldos y restauraciones de datos, dejando pendiente el formulario y las bitácoras obtenidas. No obstante, esta Auditoría envío a Informática la nota AI-848 el 16 de noviembre del 2012, consultando sobre la política y/o procedimiento para recuperar la información de la base de datos, el formulario y las bitácoras obtenidas, sin embargo el señor Ronald Ortiz en el oficio I 1143-12 del 26 de noviembre 2012 respondió al oficio anterior haciendo entrega de la siguiente información, "políticas y procedimientos sobre la realización de respaldos y restauraciones de datos", dejando sin entregar el formulario y las bitácoras obtenidas, por lo que no se tiene evidencia de la información antes mencionada.

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

Dirigido a: Departamento de Informática **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 Informática y Recursos Humanos:</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>Para determinar cuáles usuarios se encuentran activos en el Active Directory, se tomaron dos listas:
La tabla RH Empleados emitida por el Departamento de Informática.
El listado de todas las personas activas de la institución, además de las personas inactivas del periodo 2011 y 2012, solicitadas a Recursos Humanos por medio de correo electrónico el día 15 de noviembre del 2012.
De la lista primer lista se tomó una muestra de 20 personas, y se comparó con la segunda lista emitida por Recursos Humanos, una vez determinado que los funcionarios realmente se encontraban inactivos, se comparó con la información obtenida del "Active Directory", dando como resultado lo siguiente:

Lista de Usuarios Inactivos en la Base de Datos, pero Activos en el Directorio Institucional:

<table>
<tr><th>CodigoEmpleado</th><th>NombreEmpleado</th><th>Cedula Empleado</th><th>Estado Puesto</th></tr>
<tr><td>223</td><td>HIDALGO MORA DANIEL</td><td>03-0181-0476</td><td>I</td></tr>
<tr><td>873</td><td>ROLDAN VARGAS MARLON</td><td>01-1263-0433</td><td>I</td></tr>
<tr><td>901</td><td>NAVARRO FERNANDEZ BLANCA EUGENIA</td><td>01-1279-0757</td><td>I</td></tr>
<tr><td>918</td><td>CERDAS MOYA NATALIA LUCIA</td><td>03-0352-0732</td><td>I</td></tr>
<tr><td>941</td><td>MATA SERRANO SONIA</td><td>01-0570-0435</td><td>I</td></tr>
<tr><td>944</td><td>ABARCA MARIN JAVIER MAURICIO</td><td>01-1299-0377</td><td>I</td></tr>
<tr><td>950</td><td>MARIN GOMEZ KATTIA MARIA</td><td>01-0861-0935</td><td>I</td></tr>
<tr><td>965</td><td>CASTRO GONZALEZ MAINOR</td><td>01-1074-0701</td><td>I</td></tr>
<tr><td>967</td><td>VILLALOBOS JIMENEZ EDGARDO</td><td>01-1100-0738</td><td>I</td></tr>
<tr><td>972</td><td>ROJAS CASTRILLO JESSICA</td><td>01-0952-0879</td><td>I</td></tr>
<tr><td>979</td><td>CASTILLO MENDEZ ROSBERLY</td><td>01-0775-0973</td><td>I</td></tr>
<tr><td>995</td><td>CHACON CALVO ROY</td><td>01-0823-0260</td><td>I</td></tr>
</table></td></tr>
</table>

998	CESPEDES PORRAS CARLOS	02-0533-0819	I
1041	SIBAJA NUÑEZ ENRIQUE	02-0360-0898	I
1053	ODIO TRUQUE FEDERICO	01-0952-0029	I
352	SALAZAR MORA GERARDO	09-0039-0557	I

Por otro lado, las siguientes personas se encontraron en el Directorio de la JPS, mas no se encontraron en el oficio RRHH-2090-2012 correspondiente a usuarios activos:

Usuarios Activos en el Directorio de la JPS	
Juliza Hines Cespedez	Maria Ester Zuniga Araya
Alex Yarin Diaz	Maritza Peral Sandi

De acuerdo con el listado anterior, se revisó el Active Directory para verificar si existen usuarios genéricos, lo cual dio como resultado:

Departamento del Active Directory	Usuarios
Seguridad y Vigilancia	Tecnoadmin
Imprenta	Scan
Archivo Central	Administrador, datanet
Loterías	loterías
Informática	desarrollo, ivr_Soporte, rueda
Administradores de TI	SCEAdmin

Tomando de referencia el oficio RRHH-2144-2012 donde se detallan funcionarios inactivos de la institución para los periodos 2011-2012, ha reflejado que las siguientes personas aún permanecen activas en el correo electrónico:

Nombre Empleado	
Daniel Hidalgo Mora	Carlos Cespedes Porras
Gerardo Salazar Mora	Karla Villegas Salas
Natalia Cerdas Moya	Minor Castro Gonzalez
Kembly Guel Zúñiga	Ricardo Hernández Cascante
Sonia Mata Serrano	Rosberly Castillo Mendez
Kattia Marin Gomez	Enrique Sibaja Nuñez
Marlon Roldan Vargas	Roy Mauricio Chacón Calvo
Jessica Rojas Castrillo	Edgardo Villalobos Jimenez

		Aunque estas personas, no laboran para la institución podrían hacer uso del correo, y ver lo que se envía a "todos - junta". El Departamento de Recursos Humanos comunica mediante correo electrónico la salida de funcionarios de la Institución al Departamento de Informática con copia a la Auditoría, siendo este proceso de forma manual, sin embargo, pese a que se comunicó a Informática la salida de los colaboradores por el mismo medio electrónico, este último no actualizó el *"Active Directory"*, razón por la que aún existen personas Activas como el siguiente caso: **Funcionarios** Mainor Castro Gonzalez A pesar de que el Señor Ronald Ortiz, jefe del Departamento de Informática informó mediante correo electrónico: *"proceder de inmediato"* a tres de sus subalternos, la salida del Señor Castro González el mismo continúa activo. Es importante indicar que por medio de la circular DA-10-2012, el señor Jorge Gómez Mc. Carthy Director Administrativo indicó a diferentes áreas administrativas lo siguiente: *"... informar a los Departamentos de Informática y de Recursos Humanos en forma inmediata al movimiento de personal (despido, pensión, permiso sin goce de salario u otros)"*
Al Departamento de Informática:		
2. Efectuar un estudio relacionado con el horario de acceso a los sistemas por parte de los funcionarios y determinar cuales 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 Nº 31-2010 denominado	Parcialmente Cumplida	En la revisión efectuada a los oficios A.S.-0063-2012, A.S.671-2012, DFC-205, A.S. 1583-2012, A.S. 1438-2012, se observó que el oficio DFC-205 con fecha 23 de marzo del 2012, indicaba que se le extendiera dos días el horario a una funcionaria, sin embargo, a pesar de que dicho cambio fue realizado, el mismo se dejó de forma fija, sin dejarlo nuevamente en su estado actual. Se pudo observar que los siguientes funcionarios poseen horario de 24 horas al día 29 de noviembre del 2012: - Administrador - ghidalgoh - mfernandez - oalfaro - hrosales - Tecnoadmin - Slopezch - gcenteno

<table>
<tr>
<td>"Estudio relacionado con una revisión general de usuarios en los servidores Institucionales").</td>
<td></td>
<td>Por otro lado, se determinó que los siguientes funcionarios cuentan con un horario de lunes a domingo de 6 am a 8 pm:

<table>
<tr><td>- ccambronero</td><td>- msalazar</td><td>- Nespinoza</td><td>- fsalas</td></tr>
<tr><td>- mloria</td><td>- fesquivel</td><td>- barrieta</td><td>- lqmena</td></tr>
<tr><td>- apinnock</td><td>- rtapia</td><td>- cortiz</td><td>- aacuna</td></tr>
<tr><td>- caguilar</td><td>- vvega</td><td>- mbarrantes</td><td></td></tr>
</table>

No se entregó por parte de Informática el oficio que justifique el horario extendido de los usuarios anteriores.</td>
</tr>
<tr>
<td>3. 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>Pendiente</td>
<td>En relación con las políticas de contraseña, se verificó por medio de la página web de Microsoft el día 07 de enero del 2013, que la el valor recomendado es 42 días.

<table>
<tr><th>Campo</th><th>Valor Actual</th><th>Recomendado</th></tr>
<tr><td>Vigencia máxima de la contraseña</td><td>45 días</td><td>42 días</td></tr>
</table>

Se verificó en el "Active Directory" los requerimientos mínimos que debe tener la contraseña con respecto a la complejidad, y se observó que se encuentra deshabilitada, se recuerda que la inexistencia de requisitos de complejos debilitaría el control interno, debido a que las claves de acceso son la primera barrera para ingresas a los sistemas.</td>
</tr>
<tr>
<td>4. 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 N° 31-2010 denominado "Estudio relacionado con una revisión general de usuarios en los servidores Institucionales").</td>
<td>Pendiente</td>
<td>En la revisión general efectuada al Active Directory, se verificó que la información de los usuarios no posee los estándares de mantener los datos completos en los campos correspondientes a "Apellidos", "Nombre para mostrar", "Teléfono", detectándose algunos de ellos sin llenar, al día 14 de diciembre del 2012 son:

<table>
<tr><th>Departamento</th><th>Usuario</th><th>Descripción</th><th>Apellidos</th><th>Nombre para mostrar</th></tr>
<tr><td rowspan="4">Sección de Cajas</td><td>Lgarcia</td><td></td><td>X</td><td>X</td></tr>
<tr><td>Kbarquero</td><td>*</td><td></td><td></td></tr>
<tr><td>Dzunigah</td><td>X *</td><td></td><td></td></tr>
<tr><td>Ygonzalez</td><td></td><td>X</td><td>X</td></tr>
<tr><td rowspan="3">Sección de Cheques</td><td>L0601610106 achinchilla</td><td>*</td><td></td><td></td></tr>
<tr><td>Cristian Sanchez</td><td>*</td><td></td><td></td></tr>
</table>
</td>
</tr>
</table>

	Sanchez				
Auditoría	Avmontero				X
Inspectores de Loterías	Vrivera			X	X
	avmunoz	*			
	Ana Isabel Piñero				
Mercadeo	Albertazzi	X *			
	Isanchez			X	X
	Gloria Vega Muñoz	X *			
	Abraham Vargas	*			
	ebadilla	*			
Gerencia	emadriz	*		X	X
	lmoraga	*			
	vcambronero	*			
Administra-dores de TI	lramireza	X *		X	X
	dbadilla	X *		X	X
	gmunoza	*			
	Jorge Madrigal				
	Gonzalez	X *			
Loterías	Vcastro			X	
	Luis Enrrique				
	Villalobos Chacon	X *			
	soviedo	*			
	Julio Garcia Martinez	*			
	acollado	*			
	David Perez				
	Matamoros	X *			
	ezromero	X *			
Informática	ezunigar	*			
	pzamora			X	X
	wzhen			X	X
	Zurika Ruiz				
	Gonzalez	X *			
Jefaturas	obreness			X	X
Junta	Gramirez			X	X

Directiva					
Planificación	Ana Cristina Garro Sanchez (PRAC)	*			
	Laura Vargas Chacón	X *			
	ljimenez		X	X	
	Rmarchena	*			

* Número de Teléfono en blanco

El señor Ronald Ortiz jefe del Departamento de Informática indicó que el formato a utilizar para crear cuentas de usuario es:

"primer letra nombre + apellido, si se tiene otro igual, primer letra nombre + apellido + primer letra segundo apellido. En cuanto a los jurídicos son solo para consumo servicio WEB comercio es L0 más la cédula del responsable".

Sin embargo, en la revisión efectuada al Active Directory se detectó la existencia de algunos usuarios sin el estándar indicado, los mismos serán detallados:

Departamento	Usuarios
Acción Social	Jessica Chaves Perez
	mqvidal
	mrarguedas
Asesoría Legal	Rosibel Alvarado Chacón
Proveeduría	mlarce
Cajeros Tesorería	Ana Gabriela Garro Rojas
	lvmorales
Contabilidad y Presupuesto	fcloaiza
	jfsanchez
	jdramirez
	lscastro
	vcsaenz
	vparce
Revisión y Control	eimora
	Maria Cascante Arias
	Natalia Acuña Ramirez

		Sec. Cheques: L0105590372, Cristian Sanchez Sanchez, L0601610106, Lquiros Mercadeo: avortiz, avmunoz, Ana Isabel Piñero Albertazzi Loterías: Luis Enrique Villalobos Chacón Informática: David Pérez Matamoros, gilquesada, Ronald Gutierrez Chacon, Tatiana Duarte Roldán, Zurika Ruiz Gonzalez, Hugo Brenes, ezromero Administradores de TI: Maynord Masis Castillo IPL: jacerdas Jefaturas: rfcedeño, jjleiton, obreness Planificación: Ana Cristina Garro Sanchez (PRAC), Laura Chacón Vargas
5. Corregir los aspectos descritos en los puntos E, F y G del Apartado II del Informe JPS N° 31-2010 denominado *"Estudio relacionado con una revisión general de usuarios en los servidores Institucionales"*, 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	Se observó que existen 2 usuarios para una misma persona en el "Active Directory" al día 21 de noviembre del 2012, los cuales son:

Departamento	Usuario	Funcionario
Acción Social	mrarguedas mrodrigueza	Mayra Rodríguez Arguedas
Contabilidad y Presupuesto	ksalas ksalasa	Katia Salas Arrollo
	vpadilla vparce	Vinicio Padilla Arce
	jfsanchez jsanchez	Jose Francisco Sanchez Masis

	jdramirez jdiaz	Juan Carlos Díaz Ramírez
Jefaturas	obreness obrenes	Olman Brenes Brenes

En el mismo Directorio se detectó que existen usuarios ubicados en departamentos que no les corresponde, algunos son:

Departamento	Usuario	Referencia
Proveeduría	mrojas	No está en la lista de RH (RRHH-2090-2012)
Salud Ocupacional	mgonzalez	Pertenece al Departamento de Dirección Administrativa, en la unidad de Vigilancia. (RRHH-2090-2012)
Seguros	salvarado	Pertenece a la Dirección Administrativa (RRHH-2090-2012)
Contabilidad y Presupuesto	rmontenegro	No aparece en RRHH-2090-2012 y de acuerdo al correo de RH indican que no pertenece a la Institución.
Acción Social	amejiasc	Aparece como Alonso Mejías Cordero, sin embargo en el TSE se muestra como Eddy Alfonso de Jesús Mejías Cordero.
	mqvida	No se encuentra en Acción Social. (RRHH-2090-2012)
	kvillegas	No labora para la institución. (RRHH-2144-2012)
	rsalazar	Pertenece a Contabilidad. (RRHH-2145-2012)
Agencia de Cartago	bqarrieta fsalas lqmena rsiles vcoto	Pertenecen al Departamento de Dirección Financiera Contable, de la Unidad Financiero Contable (RRHH-2090-2012)
Cementerios	appinnock	No está en la lista de Recursos Humanos, y de acuerdo al correo emitido por ellos el usuario está inactivo.
	fguzman	Pertenece al Departamento de

	lbolanos	Planificación, de la unidad de planificación. (RRHH-2090-2012) No está en el departamento de cementerios. (RRHH-2090-2012)
Recursos Humanos	clizano jarrollo	No está en la lista de RH (RRHH-2090-2012)
Seguridad y Vigilancia	mrizo xmadrigal	No se encuentra dentro de la Unidad de Vigilancia (RRHH-2090-2012)
Servicios Generales	lraraya svillaplana	En la unidad de Servicios Generales de la Dirección Administrativa, no hay un funcionario con el nombre Luis Rodríguez Araya, existe uno similar que es María Lidia Rodríguez Araya. En la unidad de Servicios Generales de la Dirección Administrativa, no hay un funcionario con el nombre indicado.
Dirección Financiero Contable	nbran sbarboza vvega	Pertenece a Gerencia General (RRHH-2090-2012) Pertenece a Tesorería del Departamento Dirección Financiera y Contable (RRHH-2090-2012)
Imprenta	ccespedes	No pertenece a la Institución RRHH-2144-2012
Cajeros Tesorería	hbenavides mjimenezm tcorrales	Pertenece a la Unidad Financiero Contable. (RRHH-2090-2012) Pertenece a Revisión y Control, del Departamento Financiero Contable. (RRHH-2090-2012)
Revisión y Control	rmora rherrera jmorar fugalde aaraya hvargas Natalia Acuña Ramírez	No aparece en la lista de Recursos Humanos (RRHH-2090-2012) Pertenece a la Sucursal de Alajuela (RRHH-2145-2012) Pertenece a la Recursos Humanos

		Sec. Ingresos	amartinezs	Pertenece a Dirección Financiera, unidad Financiero Contable (RRHH-2090-2012)
			vfuentes dnavarroh	Pertenece a Dirección Financiero Contable, unidad Revisión y Control (RRHH-2090-2012)
			gsaenz	En la Dirección Financiera Contable, unidad Tesorería, se encuentra Saenz Calderón, pero no se encontró con ese apellido
			mcastro	Ya no labora en la Institución, de acuerdo con la RRHH-2144-2012
		Sección de Cajas	mherrera	Pertenece a Acción Social
			rgutierrez	Pertenece a Revisión y Control
		Loterías	Julio Garcia Martinez	Pertenece a Financiero Contable
		Cajeros Gerencia	rhernandezc Abraham Vargas Quiros	No se encuentra activo en la Institución. RRHH-2144-2012
6. Para los actuales y futuros contratos con proveedores de servicios de mantenimiento, creación de sistemas y otros, se recomienda cumplir a cabalidad con las políticas establecidas a nivel institucional y con las normas emitidas por la Contraloría General de la República específicamente en todo lo relacionado con las seguridades, debido a que el proveedor de servicios en el momento de la prueba, tenía acceso al ambiente de Desarrollo y Producción. (Punto único del Apartado III del Informe JPS N° 31-2010 denominado *"Estudio relacionado con una revisión general de usuarios en los servidores Institucionales"*).	Cumplida	Se comprobó que los usuarios externos de Informática no poseen acceso a la base de datos de producción, únicamente a la base de datos de Desarrollo.		

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 Informática	**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 6se 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	De acuerdo con la nota I 264-12 el señor Ronald Ortiz jefe del Departamento de Informática, hizo referencia a esta recomendación con la siguiente observación: *"Atendido y cumplido, se evidencia el procedimiento empleado mediante oficio I-151-12"* Según el oficio I 622-11 el señor Ortiz indicó: *"Mediante Oficio I-198-2011 se solicita al Departamento de Proveeduría incorporar la cláusula de confidencialidad."* En correo electrónico fechado al 19 de diciembre del 2012, el Departamento de Proveeduría señaló: *"... de requerirse alguna variación en sus cláusulas el Departamento de Informática debe solicitarlo mediante resolución amparada a lo establecido en el Reglamento a la Ley de Contratación Administrativa en su artículo 200 y así justificarlo ante esta Proveeduría para proceder con el trámite."* Al revisar el oficio I 151-12 del 14 de febrero 2012, el Departamento de Informática emitió a Proveeduría una solicitud para incorporar la cláusula de confidencialidad en los contratos: 2010LA-000019-PROV, 2009LA-000007-PROV, 2010IN-000002-PROV, 2007-LA-000005-PROV, 2008-L000001-PROV, sin embargo no se ha creado el addendum a los mismos.

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.	Parcialmente Cumplida	El oficio I 1622-11 del 14 de junio del 2011, el señor Ronald Ortiz, jefe del Departamento de Informática indicó: *"Cumplida, los nombres que no se ajustan preceden de datos antigos incluso a la actual administración del Departamento de Informática"* Por medio de correo electrónico del 18-12-2012, el señor Ortiz indicó: *"Flechas negras viejas, flechas rojas de sistema.* *Se indica que las rs_*** son de la herramienta de replicación.* *El estándar de creación de las tablas debe ser Sistema (dos o tres caracteres) _ Nombre Claro de Tabla (hasta 30 caracteres)."* No obstante, se determinó que algunas de las tablas de las bases de datos al día 18 de diciembre del 2012 no contaban con el estándar anterior, las siguientes han sido tomadas de forma aleatoria:

Base de Datos	Tabla	# Reg
contabilidad_db	MovimientosTemp	0
Pagos	EnviosADADetalle	0
presupuesto_db	Resultados_JC	1
	Tem_CI_GastosOperativos	73
	TempAux	5302
	TempSaldosK	405
	TemporalCompras	277
	TemporalCuentasBC	204
	TemporalCuentasLL	579
jps_real	L20ARC_Series	98
	C51B01_SeriesManual	88
	L64A15_PAnteriores	122
	L14ARC_Eliminados	118
	L04ARC_Eliminados	1087
	L12ARC_Historico	893
	WebCierreAutomaticoEnc	106343
	WebCierreAutomaticoFallas	5
	WebCierreAutomaticoDet	236729
	WebCierreDesmaterializadosEn	83263

		c WebCierreDesmaterializadosDe t 184458 PadonExtranjero 24445 PadronPaises 235 TablaActualizaFechas 90 ContenidoActa 0 Recomendacion_ES 2293 CorreccionesEstudioBE 236 NumeroDisponible 100 RecomendacionEstudio 72 DescripcionRecomendacion 427 ResumenSituacion 1264 BENE_RecepcionRecibo 2833
16. Realizar un análisis más profundo de la necesidad de migrar el sistema de seguridad actual, de tal modo que la seguridad se administre desde el motor de base de datos, máxime cuando se tenga como base de datos de producción el Oracle, ya que el motor actual no provee las herramientas necesarias para manejar, desde el mismo, dicha seguridad.	Cumplida	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática indicó: *"La seguridad actual implementada desde el año 2008 utiliza esquemas de dos capas, una primer capa administrada por el motor de base de datos y otra independiente administrada por aplicativos combinados con el motor de base de datos. Por otra parte el motor de base de datos actual si ofrece las herramientas de seguridad necesarias aspecto que podría serle aclarado a la Auditoría de Sistemas."* De acuerdo con la nueva versión de base de datos esta recomendación se estaría cumpliendo, a razón de que el motor de base de datos actual ofrece mayor seguridad.
17. Considerar, establecer un proceso de capacitación enfocada al 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.	Pendiente	El oficio I 622-11 del 14 de junio del 2011, el señor Ronald Ortiz M, Jefe del Departamento de Informática indicó: *"Se giró oficio al Departamento de Recursos Humanos en este sentido y se pretende su cumplimiento para el año 2012."* Por medio de la RH-1294-2011 del 9 de diciembre de 2011 se remite a la Auditoría Interna las fechas para recibir capacitación sobre el tema de seguridad informática, la cual fue impartida por la empresa

<table>
<tr><td></td><td></td><td>Deloitte.

De acuerdo con el correo electrónico del 19 de diciembre del 2012 enviado por el señor Ronald Ortiz, se adjuntan los cursos recibidos del Departamento de Informática:

<table><tr><td>Seguridad Informática</td><td>Bruce Campbell Arguello</td></tr><tr><td>Prevención del Lavado de Activos y Delitos</td><td>Ronald Ortiz Mendez</td></tr><tr><td>Ethical Hacking</td><td>Bruce Campbell</td></tr><tr><td>Taller "Firma Digital"</td><td>Jairo Cruz Sibaja</td></tr></table>
Según lo señalado, se puedo observar que el Departamento de Informática recibió cursos técnicos, sin embargo los mismos no se ajustan al programa de capacitaciones enviado por el señor Ortiz al Departamento de Recursos Humanos, por otro lado, dichos cursos recibidos en su mayoría no están relacionados con la seguridad de base de datos.</td></tr>
<tr><td>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.</td><td>Pendiente</td><td>El oficio I 622-11 del 14 de junio del 2011, el señor Ronald Ortiz, jefe del Departamento de Informática indicó:

"Se presupuesto para el año 2012 elaborar esta actividad mediante consultoría externa."

Se determinó que los usuarios creados en la base de datos se encuentran identificados por el número de cédula, sin embargo existe confusión debido a que no hay una diferenciación entre los funcionarios institucionales y los externos de la institución como lo son Socios Comerciales, bancos y usuarios creados como genéricos.

Por otro lado, a pesar de que el Departamento de Informática está trabajando en conjunto con la empresa Deloitte este proceso continúa pendiente, a razón de que aún no ha sido implementado.</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</td><td>Parcialmente Cumplida</td><td>El oficio I 622-11 del 14 de junio del 2011, el señor Ronald Ortiz, jefe del Departamento de Informática indicó:

"Cumplida."</td></tr>
</table>

seguridad, tales como, la firma de contratos de confidencialidad y definición de políticas de seguridad para el acceso a la información institucional.		Se determinó que en las nuevas licitaciones abreviadas ya se está incluyendo la cláusula de confidencialidad, tales carteles son: 2012LA-00009-PROV, 2012LA-00020-PROV, 2011LA-000024-PROV, 2012LA-000020-PROV. Sin embargo, no se encontró evidencia de los addendum realizados a las licitaciones públicas o abreviadas ya existentes.
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 para establecer e implementar las mejores prácticas. Un ejemplo de estándares de seguridad a seguir el ISO-27001.	Pendiente	En el oficio I 622-11 del 14 de junio del 2011, el señor Ronald Ortiz, jefe del Departamento de Informática indicó: *"Se formula el plan para el año 2012."* Se determinó que no existe un programa de capacitación en el tema de seguridad para los funcionarios de Informática, a pesar de que se cuenta con un oficial de seguridad y con sistemas informáticos.

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 Informática **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"*).	Parcialmente cumplida	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática indicó: *"Atendido nuevo sitio"* De acuerdo con la revisión realizada por esta Auditoría a la página institucional, se determinó que la misma no posee el formulario para ingresar denuncias y tampoco posee una guía de cómo presentar una denuncia, a pesar de que el Sr. Ronald indicó que ya estaba atendida. Además en la opción para tramitar una denuncia, se muestra como contacto el funcionario Carlos Luis Artavia Vega, Administrador de la Sucursal de Alajuela, y no el responsable de tramitar las denuncias.
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"*).	Pendiente	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática indicó: *"Atendido"*. Sin embargo, en la revisión efectuada a la nueva página web institucional se determinó que el gráfico no se muestra en la Sección de Acción Social, por lo tanto el requerimiento no ha sido atendido con la nueva página.
9. 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"*).	Pendiente	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática señaló: *"Atendido; no obstante, se eliminó la opción en tanto la administración suministra la información completa"* Según oficio I 1242-12 el señor Ortiz respondió: *"...se eliminó la búsqueda de actas, ya que no se proporcionaron los requerimientos técnicos necesarios para realizar la programación de la misma, y así evitar devolver información que*

		no esté disponible." De acuerdo a la revisión efectuada se determinó que en el nuevo sitio, no se muestra la búsqueda de actas, por otro lado en el nuevo requerimiento planteado al Departamento de Proveeduría en el oficio I 990-12 no se observó dicha solicitud, pese a que se señaló que ya estaba atendido.
10. Revisar y corregir el motor de búsqueda disponible en la página Web de la Junta debido a las siguientes razones : 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")*.	Parcialmente Cumplida	De acuerdo con el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática señaló: *"Se implementará un nuevo motor de búsqueda"* Sin embargo, en la revisión efectuada en distintos apartados de la página web, no se encontró el motor de búsqueda, no obstante se observó el oficio I 990-12 del pasado 17 de octubre del 2012, donde se remite al Departamento de Proveeduría modificaciones al sitio WEB, incluyendo en éste el motor de búsqueda de la página principal, así mismo el oficio DP. 2555 señala como contratación directa N° 2012CD-000660-PROV-01 por "MODIFICACIONES AL SITIO WEB DE LA JPS".
11. 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"*).	Pendiente	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática señaló: *"Se implementará un mapa del sitio"* En la revisión efectuada a la página web, se detectó que la misma no posee un mapa del sitio web, y tampoco considera un motor de búsqueda efectivo en relación a las actas de Junta

		Directiva, a pesar de que el señor Ortiz indicó que se implementaría.
12. Valorar la posibilidad de incorporar en la Sección de Cementerios del sitio Web, la siguiente 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.	Parcialmente Cumplida	En el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática señaló: *"Se implementará"* En la revisión efectuada a la página web, se detectó que la misma no posee una sección de cementerios del sitio web, no obstante el señor Ortiz había indicado que se implementaría. Sin embargo, el oficio I 990-12 del 17 de octubre del 2012, relacionado con las especificaciones técnicas del "Cartel para modificaciones al sitio WEB de la Junta de Protección Social" señala entre sus características: *"2. Incluir una Sección de Cementerios, donde se puedan consultar las propiedades disponibles para su arriendo, así como también sus ubicaciones y sus precios...."*
» 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	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática señaló: *"Se implementará"* En la observación realizada a la página web, se determinó que la misma no posee "número de identificación" y "palabra clave" a los arrendatarios de propiedades, sin embargo el señor Ortiz había indicado que se implementará, no obstante a la fecha 09-01-2013, no ha sido incorporado.
15. Dentro de "Propiedades disponibles para la venta y sus ubicaciones" existe en la parte inferior otra opción de 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*	Pendiente	En el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática señaló: *"Se implementará"* La página institucional no posee ninguna especificación con el nombre "Propiedades disponibles para la venta y sus ubicaciones" , así como tampoco incluye una búsqueda en la que se puedan consultar las propiedades, por lo tanto, al no contarse con una búsqueda no podría realizar el proceso de devolverse a la Página Principal y a la Sección de Cementerios.

San José").		
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"*).	Parcialmente Cumplida	De acuerdo con el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática mencionó: *"Se actualizaron manuales, el motor de busqueda se implementará en el año 2012"* En la revisión efectuada se determinó que el motor de búsqueda no ha sido implementado en el periodo indicado. Otro aspecto a mencionar está relacionado con las opciones del menú: "Metodología y estándares para el Desarrollo de Sistemas de la Junta de Protección Social" ubicado en el área de "Documentos", el cual incluye tres temas: - "Metodología para Desarrollo de Sistemas de Información" - "Guía para la Implementación de un Plan de Pruebas" - "Contenido de los documentos "Manual de usuario" y "Manual Técnico" para un sistema de información" Sin embargo, ninguno de los anteriores funciona, ya que al tratar de ingresar en alguno de ellos, se presentan errores. En relación a la presentación del texto de la página web, la misma se encuentra estandarizada.
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"*).	Pendiente	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, jefe del Departamento de Informática señaló: *"Se recomienda no implementar"* Según oficio I 1242-12 el señor Ortiz respondió: *"... no se implementó el contador de registro de visitantes, ya que se consultaron varias páginas Web nacionales e internacionales y ya ninguna utiliza dicho contador, debido a que el mismo no garantiza la cantidad acertada de visitas a las páginas Web, ya que puede ser que un mismo usuario con IP dinámicas, que esté ingresando a la misma página Web una y otra vez, por lo que el*

		dato no sería correcto y por lo tanto se tendría información falsa de la cantidad de visitantes." A pesar de que en el oficio anterior se indicó de que no se implementó un contador, las justificaciones dadas se rechazan por esta Auditoría, ya que el mantener un contador en la página WEB, ayudaría a la institución a conocer cuánto personal la visita, de esta manera se conoce que tan beneficio está siendo el utilizarla como medio de publicidad.
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"*).	Pendiente	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática señaló: *"Se recomienda no implementar"*
24. Incorporar una sección destinada a la Rueda de la Fortuna, en donde se brinde información sobre ese programa, además los posibles participantes, el premio acumulado que se tiene a una fecha determinada y cualquier otra información de interés para el público. (Punto J.5 del Informe JPS 07-2009 *"Estudio relacionado con la página Web de la Junta de Protección Social de San José"*).	Cumplida	En el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática señaló: *"Se estará implementando"* De acuerdo con la revisión efectuada a la página web se observó que la misma, incluye un apartado de activaciones para participar en la rueda de la fortuna, así como la lista de los participantes al concurso de la rueda de la fortuna.
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"*).	Parcialmente Cumplida	El relación al oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática indicó: *"Atendido"* Esta auditoría efectúo una revisión a la página web y se detectó que la misma posee imágenes nuevas, sin embargo a pesar de haberse incluido un video promocional en la página principal, la misma continua siendo estática.
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	Parcialmente Cumplida	El relación al oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática indicó: *"Atendido"* Según oficio I 1242-12 el señor Ortiz respondió: *"...los requerimientos mencionados están solicitados en el oficio I 990 2012, en un cartel para la Proveeduría desde el 17 de octubre*

ventanas y que éstas contengan la información respectiva. » Que no se concentre excesiva información en la página principal, solo los elementos de referencia.		*2012."* Se verificó la página web institucional y se determinó que la misma es nueva, y posee enlaces a nuevos productos, sin embargo existen recomendaciones pendientes por cumplir relacionados a los aspectos de la página web, se creó un cartel en el cual se solicitaron modificaciones a la página institucional de acuerdo con el oficio I 990-12, sin embargo no ha sido implementado.

En el seguimiento de recomendaciones anterior, se determinaron nuevos errores en la Página Web, tales como:

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.	Parcialmente Cumplida	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática señaló: *"Atendido"* La opción anteriormente la ubicación era en el menú principal "Conozcanos", en "Servicio al cliente" desplegando el nombre de "Donde puede cambiar sus premios" actualmente la ruta es directamente en la pestaña de "Servicio al cliente". En la revisión realizada se observó que la misma, presenta las diferentes provincias, en donde se indica los lugares donde se puede cambiar los premios, así como los respectivos teléfonos, no obstante, no 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.	Pendiente	Con respecto al oficio I 172-12 del 16 de febrero del 2012, referente a esta recomendación el señor Ronald Ortiz, Jefe del Departamento de Informática indicó: "Atendido" Según oficio I 1242-12 el señor Ortiz respondió: *"...los requerimientos mencionados están solicitados en el oficio 1 990 2012, en un cartel para la Proveeduría desde el 17 de octubre 2012."*

		En lo señalado en el oficio I 990-12 relacionado con "Cartel para modificaciones al sitio WEB de la Junta de Protección Social" se solicitó lo siguiente: *"...Incluir en la sección "Quienes Somos" (http://www.jps.go.cr/quienes_somos.cfm), la imagen en formato pdf., del Organigrama autorizado por MidePlan de la JPS."* De acuerdo con lo anterior, se realizó un cartel con la solicitud de la incorporación del organigrama, sin embargo no se ha actualizado la página institucional.

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

Dirigido a: Departamento de Informática **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	De acuerdo con el oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática se refirió a esta recomendación mencionando: *"Se esta actualizando por parte de consultoría externa. En proceso, a finalizar en junio del año 2012"* No obstante, vía correo electrónico el 9 de enero del 2013 el señor Ortiz, mencionó: *"Se actualizará en el 2003"* Por lo tanto, con base en lo anterior, se determina que el Plan Estratégico de Tecnologías de Información no se encuentra actualizado, desde el 2011 que rige el mismo, se indica que el mismo se actualizará en el periodo 2003, sin embargo, el mismo tendría una vigencia hasta el 2014, manteniéndose un periodo aproximado de 3 años desactualizado.
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 administración de bases de datos o la administración de la seguridad de información".*	Parcialmente Cumplida	Existe un Plan Estratégico de TI, que cubre el periodo del 2011 al 2014, sin embargo, a pesar de no estar aprobado, tampoco se encuentra actualizado, ya que el mismo muestra un organigrama en el cual no se refleja el nuevo puesto creado de oficial de seguridad, además de aún mantener un total de 5 funcionarios en el área de sistemas.
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".*	Pendiente	De acuerdo con el correo electrónico enviado por el Señor Ronald Ortiz, el 10 de enero del 2013 indicó: *" modelo de administración de proyectos que esta basado en PMI tropizalizado.* *Gilbert Quesada recibió la capacitación de este modelo por parte de Delloite".* Se detectó que se realizó un cartel con el nombre de "Consultoría técnica especializada para alineamiento e implementación a la normativa N-2-2007-CO-DFOE de la Contraloría General de la República" (N° 2011LA-000024-PROV) con fecha de apertura 10 de junio del 2011, además de otro cartel denominado "Consultoría técnica especializada para seguimiento e implementación a la normativa N-2-2007-CO-DFOE de la Contraloría General de la República" (N° 2012LA-000020-PROV) con fecha 9 de agosto del 2012. En el cartel N° 2011LA-000024-PROV en el apartado 6 se indica: *"... la metodología basada en administración de proyectos, Project Management Institute (PMI)"* Mediante correo electrónico enviado por el señor Ortiz, se determinó que el Departamento de Tecnología de Información se encuentra en proceso de implementar la metodología de administración de proyectos, sin embargo la misma no ha sido

		ejecutada, por lo que no se puede en este momento validar la utilización del estándar en los proyectos, a pesar de que se consultó por medio de correo al sr. Ortiz sobre cuáles contrataciones están utilizando la metodología indicó SIAB, pero no hizo entrega de ninguna información que respaldará lo mencionado. Por otro lado, se indicó en el cartel N° 2011LA-000024-PROV del apartado 1.5.1. lo siguiente *"Documentar la metodología de gestión de proyectos y programas. Capacitar al personal de TI en la aplicación de dicha metodología".* De acuerdo con lo señalado por el sr Ortiz, únicamente un funcionario fue capacitado, incumpliéndose lo citado del cartel ya que los demás funcionarios no fueron capacitados en dicha metodología.
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".*	Pendiente	El oficio I 172-12 del 16 de febrero del 2012, el señor Ronald Ortiz, Jefe del Departamento de Informática se refirió a esta recomendación mencionando: *"Mediante oficio I-1045-2011 se le remite a la Subgerencia Administrativa el cartel correspondiente para contratar la capacitación requerida, mediante oficio I-152-2012 se hace el recordatorio para su trámite y se establece en el mismo sea finalizado en el año 2012. En proceso, a finalizar en junio del año 2012"* El Departamento de Informática elabora un programa de capacitación, sin embargo el mismo no es cumplido. Así mismo, a pesar de haber realizado un Plan Oficial de Capacitaciones para el 2012, este no se realizó.

Advertencias emitidas a través de la Auditoría Interna

N° Nota	Fecha	Advertencia	Estado de la recomendación	Seguimiento
AI-105	17/02/2012	En la Base de datos institucional (pagos) el usuario "paul" perteneciente a Paul Zamora Sanchez, de la empresa Prosoft, S.A., se encuentra dentro del grupo "seguridadinstitucional", con los privilegios de administrador.	Cumplida	Se comprobó en la base de datos "pagos" que el usuario "paul" ya no existe dentro de ésta.
AI-167	12/03/2012	Solicitud al Gerente General del cronograma de cumplimiento de las recomendaciones emitidas en el informe AI JPS N° 26-2011.	Cumplida	Mediante oficio I 264-12 del 13 de marzo del 2012 y el oficio I 172-12del 16 de febrero del 2012.
AI-229	30/03/2012	En el Directorio del Correo Institucional el usuario "gcordero" se encuentra activo, cuando el mismo dejó de laborar desde el 14 de noviembre del 2011.	Cumplida	El usuario "gcordero" no se encuentra en el Directorio del Correo Institucional.
AI-788	17/10/2012	La pantalla principal de la página web institucional muestra el video para promocionar el sorteo de Lotería Nacional conmemorativo al Día de las Culturas, mismo que se celebró el pasado domingo 14 de octubre.	Cumplida	Mediante oficios I 991-12 del 18 de octubre del 2012, I 1084-12 del 8 de noviembre del 2012. El video promocional "Encuentro de las Culturas" ha sido sustituido por el video "Premios Especiales de Chances".
AI-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.	Pendiente	Se respondió mediante oficio I 1242-12 del 18 de diciembre del 2012, sin embargo las recomendaciones continúan igual.