1791

RECIBIDO
11:53
19 SEP 2008
Rosa Henríquez
SUPERINTENDENCIA DE PENSIONES

CNSS
CONSEJO NACIONAL DE SEGURIDAD SOCIAL

CONTRALORIA GENERAL

"Año Nacional de la Promoción de la Salud"

CG No. 0961-08
16 de septiembre del 2008

Señora
Licda. Persia Álvarez
Superintendente de Pensiones
Su Despacho.

Distinguida Licda: Álvarez

Después de un cordial saludo, me permito remitirle el informe final de la auditoria que hemos realizado a la Superintendencia de Pensiones (SIPEN) para el periodo comprendido entre el 1ro. de julio del 2005 y el 31 de octubre del 2007.

Nuestro trabajo fue realizado aplicando las Normas Internas de Auditoria Gubernamental (NIAGU), las Normas Internacionales de Auditoria, las Normas Internacionales de Contabilidad (NIC's), así como mejores prácticas para la implementación de sistemas de seguridad de la información y planes de continuidad, como la ISO 27001, ISO 27002 y COBIT.

Este informe contiene las observaciones que identificamos distribuidas por áreas, el criterio en que nos basamos para soportar las observaciones, el impacto que tienen las mismas en la Entidad, las recomendaciones de lugar y las acciones correctivas planteadas por ustedes en su comunicación No. DS-1582 del 30 de junio del 2008.

La dirección de la SIPEN es responsable de la implementación oportuna de las recomendaciones planteadas en este informe.

Atentamente,

Luis Paulino
Contralor General del CNSS

CONTRALORIA CNSS

C.c. Dr. Max Puig / Secretario de Estado de Trabajo y Presidente de CNSS.
Comisión de Presupuesto, Finanzas e Inversiones del CNSS

DESPACHO DEL SECRETARIO
ACUSE DE RECIBO
NOMBRE:
Firma
Fecha
Hora

Av. Tiradentes No. 33, Ensanche Naco, Telf. (809) 472-2064, Fax: (809)472-2909, Santo Domingo, R.D.
RNC: 4-30-01410-9

VICE-PRESIDENCIA

INDICE

I. ASPECTOS GENERALES SOBRE LA SUPERINTENDENCIA DE PENSIONES (SIPEN)

La Ley 87-01 en su Art. 107 Creación de la Superintendencia de Pensiones:

Se crea la Superintendencia de Pensiones como una entidad estatal, autónoma, con personalidad jurídica y patrimonio propio. Su función es velar por el estricto cumplimiento de la presente ley y sus normas complementarias en su área de incumbencia, de proteger los intereses de los afiliados, de vigilar por la solvencia financiera de las administradoras de fondos de pensiones (AFP) y de contribuir a fortalecer el sistema previsional dominicano.

Entre sus funciones principales tenemos:

1. Supervisar la correcta aplicación de la referida ley y sus normas complementarias, así como de las resoluciones del Consejo Nacional de la Seguridad Social (CNSS) y de la propia superintendencia, en lo concerniente al sistema previsional del país.

2. Autorizar la creación y el inicio de las operaciones de las Administradoras de Fondos de Pensiones (AFP) que cumplan con los requisitos establecidos en la Ley 87-01 y el Reglamento de Pensiones; y mantener un registro actualizado de las mismas y de los promotores de pensiones.

3. Supervisar, controlar, monitorear y evaluar las operaciones financieras de las AFP y verificar la existencia de los sistemas de contabilidad independientes.

4. Fiscalizar a las AFP en cuanto a su solvencia financiera y contabilidad; a la constitución, mantenimiento, operación y aplicación de la garantía de rentabilidad, al fondo de reserva de fluctuación de rentabilidad, a las carteras de inversión y al capital mínimo de cada AFP.

5. Requerir de las AFP el envío de las informaciones sobre inversiones, transacciones, valores y otras, con la periodicidad que estime necesaria.

6. Regular, controlar y supervisar los fondos y cajas de pensiones existentes.

7. Cancelar la autorización y efectuar la liquidación de las AFP en los casos establecidos por la presente ley y sus normas complementarias.

8. Velar por el envío a tiempo y veraz de los informes semestrales a los afiliados sobre el estado de situación de su cuenta personal.

9. Supervisar a la Tesorería de la Seguridad Social y al Patronato de Recaudo e Informática de la Seguridad Social (PRISS) en lo relativo a la distribución de las cotizaciones al seguro de vejez, discapacidad y sobrevivencia dentro de los límites, distribución y normas establecidas por la Ley 87-01 y sus normas complementarias.

II. OBJETIVO DE LA AUDITORÍA

Nuestra auditoría fue realizada cumpliendo con lo establecido en la Ley 87-01 en su Art. 25 y en el Reglamento Interno del CNSS en su Art. 32, los cuales dictan lo siguiente:

La Contraloría General de la Seguridad Social tendrá autonomía administrativa y tendrá las funciones de auditar las operaciones, velar por la aplicación correcta de la ley, los reglamentos, acuerdos y resoluciones del CNSS.

Atendiendo a lo que nos requiere la Ley, podemos decir que los objetivos en esta auditoria son los siguientes:

Objetivo General:

Satisfacernos de manera razonable, de que la SIPEN está cumpliendo con las legislaciones correspondientes; que existen controles internos adecuados y que las operaciones se realizan de acuerdo a éstos; así como de la razonabilidad de la información financiera presentada por esta Entidad a la fecha de corte de la auditoria.

Objetivos específicos:

1. Verificar el cumplimiento de la Ley 87-01, reglamentos y resoluciones emitidas por el CNSS.
2. Evaluar la correcta utilización de los recursos recibidos durante el periodo auditado, verificando el cumplimiento de las disposiciones legales reglamentarias.
3. Evaluar los controles internos establecidos por la Entidad para la disminución de riesgos en el desarrollo de sus operaciones.

III. ALCANCE DE LA AUDITORÍA

Esta auditoría comprende el periodo desde el 01/07/2005 hasta el 31/10/2007 e incluye las siguientes áreas:

1. Financiera
2. Operativa
3. Informática
4. Legal

IV. OBSERVACIONES Y RECOMENDACIONES

A continuación presentamos por áreas los principales hallazgos identificados durante la auditoría.

1V.1 RECURSOS HUMANOS

1. Alta rotación de personal

Las mejores prácticas señalan que el reto para cualquier organización es conocer cuan motivadas y satisfechas están las personas vinculadas a la misma, lo que se refleja en el nivel de estabilidad de la fuerza de trabajo y en el grado de compromiso que tienen los empleados con los resultados de la organización a la cual pertenecen.

La rotación de personal de la SIPEN es sumamente alta, tomando en cuenta el resultado de la comparación de las nóminas del 2005 al 2007 y la cantidad de empleados que han salido y entrado de la institución durante el periodo auditado.

Tratadistas del tema señalan que "Generalmente detrás de una excesiva rotación laboral se oculta la desmotivación, el descontento, la insatisfacción laboral y esto a su vez está influenciado por un conjunto de aspectos vinculados en muchos casos por una ineficiente gestión de Recursos Humanos".

También se señala que "Cuando el ambiente laboral donde el trabajador desempeña su labor no es el más adecuado hace que éste se sienta insatisfecho y en casos extremos conduce a la rotación laboral".

IMPACTO

Esta situación incide principalmente en una mayor inversión en entrenamientos y capacitación; de forma indirecta puede desmotivar los planes de carrera del personal en esa institución y crea inconvenientes a una ejecución optima del Plan Estratégico.

RECOMENDACIÓN

Determinar las causas fundamentales que han dado origen a la alta rotación de personal y establecer las acciones que permitan garantizar una mayor estabilidad del personal y mejor ambiente laboral.

ACCION CORRECTIVA

La SIPEN entiende que la alta rotación de su personal se debe principalmente al alto nivel técnico profesional y de especialización de los empleados, conjuntamente con su promedio de edad, hace que los mismos se vean constantemente atraídos por la competencia del mercado y por instituciones de otros sectores de la economía nacional.

Según nos expresaron esta situación plantea un reto permanente en procura de mayores conquistas salariales, por lo que periódicamente realizan programas de motivación y de forma complementaria ejecutan un conjunto de actividades de capacitación con destacados consultores

nacionales e internacionales lo cual ha permitido que el personal de la SIPEN cumpla siempre sus planes estratégicos y cronogramas de trabajo.

2. Evaluación de desempeño

El manual de Administración de Recursos Humanos en su artículo 5.2 Medidas de Controles Internos, punto 4 señala la importancia de evaluar periódicamente el desempeño de las actividades llevadas a cabo de forma individual y colectiva.

En este sentido durante auditoria realizada al área de Gestión Integrar revisamos 26 expedientes de empleados y ex empleados de la SIPEN, determinando que la totalidad de éstos carecían de evaluación de desempeño que evidencie las fortalezas y debilidades en el ejercicio de sus funciones.

Esta práctica además, ayuda a determinar con más objetividad la capacitación que requiere el empleado y sirve de base para promociones y reconocimiento de méritos, entre otros.

RECOMENDACIÓN

Implementar la evaluación de desempeño como herramienta de Gestión Humana para el crecimiento y valoración oportuna y eficiente del personal.

ACCION CORRECTIVA

La SIPEN nos señala que su Plan Estratégico contempla un sistema que actualmente se encuentra en proceso de implementación, el cual establece una metodología de evaluación de desempeño basado en resultados para los empleados de la SIPEN.

3. Inconsistencia expedientes empleados

Basados en el Manual de Administración de Recursos Humanos de la SIPEN y para los 26 expedientes antes señalados, procedimos a verificar el cumplimiento de los requerimientos contentivos en éste manual identificando las observaciones que detallamos a continuación:

- 31% de la muestra seleccionada no presentan contrato de trabajo.
- 69% de la muestra no realizaron pruebas sicológicas.
- 7% de la muestra no presenta copia de los certificados de estudios.

RECOMENDACIÓN

Cumplir con lo que estipula el Manual de Administración de Recursos Humanos e incorporar la información de equipos asignados a los colaboradores y las evaluaciones al personal; entendiendo que las mejores prácticas recomiendan que los documentos relacionados con el personal deben ser incorporados a sus expedientes.

ACCION CORRECTIVA

En su opinión la SIPEN nos indica que todos los empleados tienen sus contratos de trabajo firmados, lo cual se puede verificar a través del departamento de Recursos Humanos y se encuentra en los expedientes individuales de cada uno de ellos.

1V.2 AREA ADMINISTRATIVA

1. Limitación acceso informes de Auditoria Interna

Como parte del proceso de revisión efectuado procedimos a solicitar los informes emitidos por la Dirección de Auditoria Interna de esa entidad, así como los papeles de trabajo por el periodo comprendido entre julio 2005 y octubre 2007. Esto con la finalidad de cumplir con Normas Internacionales, evaluar la calidad de la función de auditoria interna y comprobar la disposición final dada a sus recomendaciones. No obstante nuestros requerimientos, según nos informaron funcionarios de la Entidad, los referidos documentos no fueron encontrados.

IMPACTO

Una de las principales fortalezas de una institución es una buena estructura del sistema de control interno y el área de auditoria interna es uno de esos pilares. La no conformación, seguimiento y compromiso con esta área debilita el control de las actividades administrativas, operativas y financieras de esta entidad.

RECOMENDACIÓN

Cumplir con las funciones descritas en el Manual de Recursos Humanos para la Dirección de Auditoria Interna, así como documentar y dejar evidencia escrita o electrónica de los procesos de revisión llevados a cabo por la unidad responsable de evaluar el cumplimiento y ejecución de control interno de las operaciones de esta entidad.

ACCION CORRECTIVA

La SIPEN señala que en sus procesos de control interno contempla la revisión y el monitoreo permanente de los procedimientos y políticas establecidas, los cuales son efectuados por la Dirección de Auditoria, o en su defecto por la Contraloría de la Entidad, mediante el examen periódico y continuo de las operaciones que ello realizan.

2. Licitación remodelación edificio

La Superintendencia de Pensiones de acuerdo a la Ley de Contrataciones Públicas de Bienes, Servicios, Obras y Concesiones de Estado realizó un proceso de licitación para la remodelación de su edificio. En el proceso fueron precalificadas por el CODIA, la SEOPC y un analista independiente cinco empresas constructoras de las cuales dos (2) obtuvieron las mejores puntuaciones. La empresa seleccionada presentó un presupuesto 7% mayor que la otra empresa, equivalente a RD$3,870,847, donde la decisión para la selección fue la consideración de el factor de evaluación "Menor tiempo de entrega", aún cuando según la opinión del CODIA, en su evaluación sobre el tiempo de ejecución de la firma no seleccionada señala: "El tiempo de

ejecución de la obra está dentro del compromiso de fecha de entrega de la obra". Esta conclusión fue idéntica a la expresada sobre la constructora ganadora de la licitación.

Por otra parte al analizar el Cuadro de Evaluación Final para adjudicar la obra, determinamos subdivisiones en los Criterios de Calificación de las Ofertas (Menor Tiempo y Capacidad de la empresa para ejecutar su propuesta) que no estaban establecidos en la "Base de Licitación para la contratación de Ejecución de Obra remodelación del edificio SIPEN" Las puntuaciones establecidas en este análisis que fue preparado por el Comité de Obras de la SIPEN no se corresponde con la opinión del CODIA, SEOPEC y el analista contratado para tales fines.

IMPACTO

La selección de esta constructora representó para la SIPEN un costo mayor ascendente a RD$3,870,847 con respecto a la compañía que quedó en 2do. lugar, esto sin considerar el addendum al contrato original por un valor de RD$5,070,720. También debemos señalar que aunque el tiempo era un factor preponderante para adjudicar la obra. La ejecución según el contrato se estimó en 105 días, sin embargo se realizó en 154 días; es decir 47% más del tiempo establecido en el contrato de ejecución. No observamos la aplicación de las penalidades establecidas en el contrato.

RECOMENDACIÓN

Entendemos que las puntuaciones asignadas para la adjudicación de las licitaciones propuestas no se corresponden con las opiniones de los expertos consultados para estos fines, por lo que recomendamos cumplir con los criterios establecidos en los Términos de Referencia y transparentar la metodología a ser utilizada para la evaluación final de las firmas precalificadas.

ACCIÓN CORRECTIVA

En su respuesta la SIPEN señala que la selección de la firma adjudicataria para la remodelación del edificio de la SIPEN, fue realizada por el Comité de Licitación y Compras de ésta Entidad, la cual basó su decisión en los requerimientos establecidos en los Términos De Referencia y en los análisis de evaluación con la colaboración de la Secretaría de Estado de Obras Públicas y Comunicaciones y el Colegio Dominicano de Ingenieros y Arquitectos. Asimismo, dicha adjudicación se efectuó considerando las ponderaciones que establecen los Términos de Referencia para la capacidad técnica del contratista para la realización de la obra, tomando en cuenta la experiencia del ingeniero y del equipo técnico asignado al proyecto, así como el compromiso asumido en cuanto al cronograma de trabajo que garantizaba la fecha de entrega.

Nos señalan como justificación de la extensión del periodo de ejecución que durante la realización de la obra, el país estuvo afectado por malas condiciones del clima, con intensas lluvias, situación que afectó e imposibilitó que el personal del contratista pudiese realizar y avanzar en sus trabajos de acuerdo su plan.

1V.3 CONTROL DE OPERACIONES

1. Fiscalizaciones a la TSS y UNIPAGO no realizadas

Según mandato de la Ley 87-01 en su artículo 108 literal "p" se establece que la SIPEN tiene la obligación dentro de sus funciones supervisar a la TSS y UNIPAGO, sin embargo aunque la Dirección de Control Operativo de la SIPEN programó estas auditorias para el año 2007 no las realizó. Es importante destacar que en los últimos 3 años la SIPEN no ha efectuado auditoría presencial en esas entidades.

A parte de lo establecido en la Ley 87-01, el Reglamento Interno de la SIPEN en su artículo 131 señala que ésta debe realizar inspecciones y labores de vigilancia en el ámbito de su competencia a la TSS y UNIPAGO.

IMPACTO

Que ocurran hechos reportables en los procesos y actividades de esas entidades que no se detecten y corrijan oportunamente.

RECOMENDACIÓN

Consideramos que lo mas saludable para el sistema es que la SIPEN efectúe auditorías presénciales a las entidades antes indicadas a la mayor brevedad.

ACCION CORRECTIVA

En su opinión señalan que esta fiscalización, dada su naturaleza, se estableció que fuera fundamentalmente on- line, con uso intensivo de tecnología, considerando los altos volúmenes de información y manejo de base de datos, cruces y validaciones.

Conforme a esa realidad el monitoreo se concentra en el monitoreo de gabinete, sobre la base de que, el mismo sistema automatizado contempla las alertas para efectuar fiscalizaciones in-situ si fuese necesario.

En consonancia con lo planteado el sistema no ha arrojado indicadores de alerta que ameriten una inspección in-situ a dichos entes del Sistema Dominicano de Pensiones. Asimismo, en nuestro plan estratégico 2007-2010 se contempla un proyecto que fortalece aún más tecnológicamente la fiscalización de estas Entidades.

2. Supervisión Administradora Fondo Pensiones

Los informes de supervisión a las AFP emitidos por la Superintendencia de Pensiones aún cuando en muchos casos informan sobre debilidades detectadas no contienen la estructura que requieren éste tipo de reportes técnicos, donde se evidencie la opinión y compromiso del auditado tendente a corregir las debilidades detectadas.

IMPACTO

La carencia de una estructura adecuada en el informe impide conocer la opinión del auditado respecto al hallazgo y el plan de acción a seguir.

RECOMENDACIÓN

Se establezcan los procedimientos para que los informes de supervisión reflejen la opinión y el compromiso del auditado a corregir los hallazgos detectados.

ACCION CORRECTIVA

La SIPEN indica que han desarrollado un modelo de supervisión preventivo, de acuerdo con mejores prácticas internacionales en la materia, donde se promueve la evaluación de riesgos operativos y el uso de herramientas avanzadas de tecnologías.

Cuando se detecta un incumplimiento, se elabora un informe y se desarrolla un plan de acción correctivo con un plazo de ejecución que es supervisado por la SIPEN, el cual contempla las verificaciones e inspecciones para comprobar la efectividad y cumplimiento de dicho plan.

En lo relativo a la estructura de los informes, éstos responden a prácticas internacionales y metodología aplicable a este tipo de fiscalizaciones.

1V. 4 AREA FINANCIERA

El Principio de Contabilidad del Período Contable, establece que las operaciones económicas, así como los efectos de ellas derivados, se contabilizan de forma tal que se correspondan con el periodo económico en que ocurren, para que las informaciones contables muestren con claridad el periodo a que estas corresponden y pueda determinarse el resultado de cada periodo económico.

1. Pólizas de seguro no registradas

El 70% de las pólizas de seguro con vigencia 2007/2008 contratadas con Sol de Seguros, no estaban registradas a la fecha de corte de nuestra auditoría 31 de octubre 2007, a pesar de que fueron pólizas contratadas en fechas que oscilan entre diciembre 2006 y mayo 2007.

PÓLIZAS	DESDE	HASTA	PRIMA
7-821-006870	01-05-07	01-05-08	1,160
2-201-013324	20-12-06	20-12-07	43,657
7-811-006291	01-05-07	01-05-08	73,073
7-712-006260	01-05-07	01-05-08	6,032
7-822-006871	01-05-07	01-05-08	13,560
7-803-006197	01-05-07	01-05-08	191,400
7-813-006290	01-05-07	01-05-08	46,456
Total			**RD$375,338**

IMPACTO

La ausencia de un registro en el periodo en que ocurre, trastorna la comparación real de la información financiera en periodos similares que sirven de base a la toma de decisiones financieras.

RECOMENDACIÓN

Registrar las transacciones en el mes y periodo al que corresponden para una presentación oportuna y no distorsionada de la información financiera.

ACCION CORRECTIVA

En su opinión la SIPEN señala que el registro contable correspondiente a las pólizas de seguro que se indican en el informe, se ejecutaron en el mes de noviembre del 2007.

2. Retención de impuesto a proveedores

El reglamento de aplicación del Titulo II del Código Tributario, Art. 68. Retención en pagos efectuados por el Estado y sus Dependencias, incluyendo los organismos descentralizados y autónomos, deberán efectuar una retención del 5%, sobre los importes de dichos pagos.

En la revisión que realizamos a una muestra de los cheques emitidos por la SIPEN durante el periodo julio 2005 octubre 2007, aproximadamente el 4% de éstos corresponde a pagos efectuados a Verizon, y ninguno de ellos tiene aplicada la retención del 5% de proveedores del Estado. Tal como estipula el Art.68 del Código Tributario, Pág. 208 y sus modificaciones. El monto total pagado a Verizon durante el periodo antes citado asciende a RD$3,494,326.00. y el valor aproximado de las retenciones asciende a RD$174,716.

IMPACTO

Violación de los artículos Nos. 297,309 y 68 del Código Tributario.

RECOMENDACIÓN

Realizar las retenciones de impuestos correspondientes tal como lo señala el Código Tributario y sus modificaciones

ACCION CORRECTIVA

La SIPEN señala que La Dirección General de Impuestos Internos mediante comunicación C. J. NO. 15797 de fecha 23 de abril de 2001, dispuso la no aplicación de la retención sobre pagos efectuados por entidades estatales a empresas que prestan servicios de telecomunicación.

V.5 ÁREA DE TECNOLOGÍA Y SISTEMAS DE INFORMACIÓN

1. Estructura de Sistemas y Tecnologías SIPEN

La Superintendencia de Pensiones no cuenta con una adecuada estructura para la separación de funciones en las áreas de Operaciones, Seguridad y Sistemas.

ISO/IEC 17799:2005. A.10.1.3., Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.

IMPACTO

Que no se puedan reducir las oportunidades de modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización en el área de tecnología de sistema.

RECOMENDACIÓN

Se debe implementar una división de roles y responsabilidades que excluya la posibilidad de que un solo individuo pueda subvertir un proceso crítico. La gerencia debe asegurar que el personal está realizando solamente aquellos deberes permitidos por sus respectivos trabajos y posiciones.

Esta segregación debe cubrir las áreas relacionadas con operaciones, desarrollo, administración de redes, seguridad y bases de datos.

ACCION CORRECTIVA

La SIPEN señala que el 28 de enero del 2008 contrató un Encargado de Seguridad y el 18 de Febrero un Asistente de Seguridad con la finalidad de dar cumplimiento a la Política separación de funciones y Seguridad de la Entidad.

2. Educación en políticas de seguridad

Actualmente la SIPEN no cuenta con un programa formal, coordinado con Recursos Humanos para educar a los empleados sobre las políticas de seguridad.

ISO ISO/IEC 17799:2005. A.8.2.2 Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

IMPACTO

Que ocurran errores humanos por desconocimiento de todos los aspectos relacionados con las políticas y la seguridad de la información, sus responsabilidades, obligaciones y que se amonesten a empleados por violar políticas y medidas que ignoran.

RECOMENDACIÓN

Se debe crear y dar cumplimiento a una política de educación en seguridad de la información que incluya las responsabilidades y obligaciones de los empleados.

Los usuarios deben ser entrenados en procedimientos de seguridad y en el uso correcto de las facilidades de procesamiento de la información para minimizar los riesgos posibles de seguridad.

ACCION CORRECTIVA

La SIPEN señala que desde el mes de enero del 2008 se están desarrollando programas de capacitaciones a todo el personal sobre temas de seguridad utilizando los diferentes medios disponibles en la institución (audiovisual, correo electrónico, etc.). También nos indica que en el Manual de Inducción se le da una introducción sobre la Política se Seguridad de la Entidad.

3. Gestión continuidad de las operaciones

La Superintendencia de Pensiones no cuenta con un Plan de Continuidad para las operaciones criticas, que le permita contrarrestar las interrupciones que puedan ocurrir.

ISO/IEC 17799:2005. A.14.1.1. Incluir seguridad de la información en el proceso de gestión de continuidad comercial. Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesaria para la continuidad comercial de la organización.

RECOMENDACIÓN

Se debe implementar un proceso de administración de la continuidad de las operaciones para reducir la perturbación causada por desastres y fallas de seguridad (las cuales pueden ser el resultado de desastres naturales, accidentes, fallas en equipos y acciones deliberadas) a un nivel aceptable mediante una combinación de controles preventivos y de recuperación.

ACCION CORRECTIVA

La SIPEN indica que ha incluido en su plan de trabajo correspondiente al 2008 una estrategia que va dirigida a la Gestión de un Plan de Continuidad que involucrará todos los procesos de la institución.

4. Políticas y procedimientos para control del código fuente

Actualmente en la SIPEN existen programas fuentes en los equipos de los programadores de sistemas de la Entidad. Estos equipos están en ambiente Windows.

ISO/IEC 17799:2005. A.15.1.5 prevención del mal uso de medios de procesamiento de información.

IMPACTO

Que no se puedan reducir los riesgos de cambio no-autorizados o cambios en el sistema de operación que puedan afectar la continuidad de las operaciones.

RECOMENDACIONES

Deben existir procedimientos documentados para mover los códigos de un ambiente a otro que asegure la separación de medios de desarrollo, prueba y producción.

Se deben eliminar los programas fuentes en los equipos de los programadores y reducir el riesgo de modificación indeseada.

Los accesos a los ambientes de desarrollo y prueba deben ser limitados específicamente al Encargado de Desarrollo o a su superior si solo hay un desarrollador.

ACCION CORRECTIVA

La SIPEN señala que procedieron a mover todos los programas fuentes que residían en los equipos de los programadores a un servidor que habían adquirido en el mes de diciembre del 2007 y que fue destinado para ser el servidor de desarrollo.

5. Ciclo de vida de desarrollo de mantenimiento de Sistemas

La Superintendencia de Pensiones no cuenta con políticas relativas al ciclo de vida de desarrollo y mantenimiento de sistemas. Esto esta motivado porque no se ha establecido una política formal.

IMPACTO

Que no se den seguimiento a Metodología de Desarrollo y Mantenimiento de Sistemas utilizados actualmente.

RECOMENDACIÓN

Se debe crear una política que fortalezca el seguimiento de la metodología de ciclo de vida de desarrollo y mantenimiento de sistemas existente.

ACCION CORRECTIVA

La SIPEN indica que ha elaborado y documentado la Metodología de Desarrollo y Mantenimiento de Sistemas y que esta incluye el ciclo de vida de la misma.

6. Control de cambios a base de datos y sistemas operativos

No se da cumplimiento a la parte de la política establecida para los cambios a la Base de Datos y Sistemas Operativos. En la SIPEN no existe una estructura formal para dar cumplimiento a la misma

AI3.3 Mantenimiento de la Infraestructura Desarrollar una estrategia y un plan de mantenimiento de la infraestructura y garantizar que se controlan los cambios, de acuerdo con el procedimiento de la administración de cambios de la organización. Incluir una revisión periódica contra las necesidades del negocio, administración de parches y estrategias de actualización, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad.

IMPACTO

Que no se pueda controlar los cambios que se estén realizando a la base de datos y las plataformas operativas

RECOMENDACIÓN

La Dirección de Sistemas debe asegurar que se da cumplimiento a una política de control de cambios a la base de datos y los sistemas operativos. El sistema usado para monitorear esos cambios debe ser automático para asegurar el registro de cambios complejos realizados y facilitar su búsqueda.

ACCION CORRECTIVA

La SIPEN señala que ha documentado la política de control de cambios y los procedimientos.

7. Gestión de vulnerabilidades técnicas

Según el reporte de vulnerabilidades técnicas que realizamos con el apoyo de la herramienta Nessus, en la SIPEN existe una situación crítica con el mantenimiento de los sistemas operativos de servidores, que alojan los programas de manejo de los respaldos y la base de datos. Esto esta originado porque no se da mantenimiento formal a los servidores de bases de datos, sistemas y programas operativos que sirven de plataforma al sistema SAS

ISO/IEC 17799:2005. A.12.6.1.- Control de vulnerabilidades técnicas. Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.

IMPACTO

Estas plataformas y bases de datos podrían ser vulnerables a interrupciones por diferentes tipos de amenazas.

RECOMENDACIÓN

Se deben establecer medidas de controles preventivos y correctivos para las vulnerabilidades técnicas en las plataformas operativas y la base de datos.

ACCION CORRECTIVA

La SIPEN señala que ha adquirido una herramienta para realizar análisis de vulnerabilidades técnicas de manera preventiva a su infraestructura de tecnologías y sistemas de manera mensual. La herramienta adquirida ha sido GFI Languard.

8. Conexión a DataReservas vía Dial-up

Las conexiones con DataReservas son hechas vía Dial-up sin pasar por los filtros y controles existentes en el centro de Sistemas y Tecnologías de la SIPEN. Esto se debe la Dirección Administrativa considera que la forma de conexión actual es segura.

ISO/IEC 17799:2005. A.10.4.1.- Controles contra software malicioso. Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.

IMPACTO

Que la red de la entidad pueda se afectada desde el exterior utilizando como canal la conexión Dial-up existente.

RECOMENDACIÓN

El acceso a DataReservas debe ser hecho punto a punto a través del servidor de Firewall. Las conexiones vía firewall son adecuadas para protecciones en contra de ataques como denegación de servicio, accesos no autorizados a las redes internas y controlar cualquier aplicación y el flujo de datos en ambas direcciones.

ACCION CORRECTIVA

La SIPEN señala que procedió a utilizar el servicio de red privada virtual que ofrece Data Reservas eliminando la conexión Dial-up existente.

1V ÁREA DE LEGAL

1. Contratación de asesores

La Superintendencia de Pensiones no cuenta con evidencia de informes que respalden el trabajo realizado por varios asesores contratados por esa entidad y que percibieron durante los años 2005 al 2007 la suma de RD$4,335,000. A continuación detalle:

Asesores y/o Consultores	2005	2006	Acumulado octubre 2007	Total por Asesor
Daysi Montero		330,000	210,000	540,000
Guarionex Rosa	945,000	1,300,000	700,000	2,945,000
Mario Méndez		280,000	270,000	550,000
Pedro A. Suárez		300,000		300,000
Total por año	**RD$945,000**	**RD$2,350,000**	**RD$1,280,000**	**RD$4,335,000**

RECOMENDACIÓN

Es necesario que los asesores soporten con documentos las consultas realizadas, de tal forma que su trabajo sirva de aporte para el desarrollo y memoria histórica de la institución.

ACCION CORRECTIVA

En su opinión indican que los contratos con estos cuatro asesores no requieren la presentación de informes escritos. Además destacan que desde el año 2007 se han venido realizando

addendum a los contratos, que incluyen la presentación de informes periódicos de las asesorías realizadas.

Finalmente, agradecemos el apoyo que recibimos de la Entidad durante el curso de la auditoria.

Lic. Darío Reyes
Encargado Auditoría

Lic. Franklin Inoa
Enc. Auditoria Informática

Licda. Yaquilendis Tejada
Auditora

Licda. Adalgisa Castro
Auditora