CG No.0296

CNSS
CONTRALORÍA
GENERAL

"Año Nacional de la Generación de Empleo"

Santo Domingo, D.N.
Martes 17 de enero del 2006

Señora
Lic. Persia Álvarez
Superintendente de Pensiones
SIPEN
Su Despacho.-

Estimada Licenciada:

A continuación le remito el informe de la auditoria operativa, financiera y de sistemas de esa Institución, por el periodo revisado *30.06.2005* el mismo tiene ***calidad de Informe Definitivo***, dados los comentarios y acciones correctivas por ustedes a esta Contraloría General de la Seguridad Social, luego de las dos discusiones del presente informe.

2996

RECIBIDO
SUPERINTENDENCIA DE PENSIONES
18 ENE 2006
Por: KG. 10:40AM

Sin otro particular me despido,

Muy atentamente,

CONSEJO NACIONAL DE SEGURIDAD SOCIAL
CNSS
Contraloría
Santo Domingo, R.D.

Lic. Luis Paulino
Contralor General del CNSS

Dr. José Ramón Fadul, Secretario de Estado de Trabajo y Presidente del CNSS
Ing. Eduardo De Castro, Presidente Comisión PF e I.
Miembros de la Comisión de PF e I

INFORME DE AUDITORIA
NO. 1

Superintendencia de Pensiones

Auditoria Operativa y Financiera
Al 30.06.2005

CNSS
CONSEJO NACIONAL DE SEGURIDAD SOCIAL

Contraloría General del CNSS
Santo Domingo, Rep. Dom.

INFORME DE AUDITORIA

De: Contraloría General del CNSS
A la: Superintendencia de Pensiones

Con el fin de ordenar y facilitar la lectura del presente informe, se expone a continuación la clasificación temática del mismo:

1. Objetivos de la auditoria
2. Alcance y metodología de trabajo
3. Procedimientos aplicados
4. Principales observaciones, consecuencias y recomendaciones
5. Tecnología y Sistemas
6. Opinión del auditado
7. Opinión del auditor.

1. OBJETIVOS DE LA AUDITORIA

- Asegurarnos de que la información contable posea los atributos de confiabilidad, integridad y oportunidad y que la misma esté basada de acuerdo a las normas internacionales de contabilidad (NIC'S).

- Confirmar que la totalidad de los ingresos y egresos de fondos se encuentren registrados contablemente y estén respaldados por la documentación que la da origen.

- Verificar que la Entidad funcione de acuerdo a sus procedimientos internos y que los mismos vayan acorde a lo establecido en la Ley 87-01.

- Evidenciar las debilidades significativas de control para establecer los riesgos de auditoria asociados.

- Formular las debidas recomendaciones de lugar.

2. ALCANCE Y METODOLOGÍA DE TRABAJO

A continuación se informan, para cada una de las pruebas realizadas, los periodos y criterios de selección utilizadas:

Áreas auditadas	Periodo de Revisión	Criterio de Selección	Alcance
Efectivo	31.12.2004 y 30.06.2005	Importes más significativos y más vulnerables.	75%
Cuentas por Cobrar	31.12.2004 y 30.06.2005	Importes más significativos	60%
Inventario Materiales de oficina	31.12.2004 y 30.06.2005	Importes más significativos	50%
Otros Activos	31.12.2004 y 30.06.2005	Importes más significativos	70%
Activos Fijos	31.12.2004 y 30.06.2005	Importes más significativos	70%
Pasivos	31.12.2004 y 30.06.2005	Importes más significativos	70%
Ingresos	31.12.2004 y 30.06.2005	Importes más significativos	80%
Gastos	31.12.2004 y 30.06.2005	Importes más significativos. Diferentes conceptos	75%
Áreas técnicas		Aleatoria	50%

Para el área de Sistema y TI, esta revisión no incluyó pruebas a códigos de programación y bases de datos. Tampoco incluyo la revisión de cada uno de los módulos del sistema PAGOSS.

3. PROCEDIMIENTOS APLICADOS

Realizamos la planeación del trabajo que consistió en determinar las áreas en las cuales existan posibles riesgos de errores e irregularidades y determinar las pruebas y procedimientos a aplicar.

Aplicamos pruebas de cumplimientos para la evaluación del control interno.

Realizamos un análisis al funcionamiento de algunas áreas técnicas de la Entidad como lo son: Estudios Estratégicos, Beneficios, Control de Inversiones, Sistemas y Tecnología y Control Operativo.

Realizamos las pruebas sustantivas para la verificación de los saldos.

Nuestra mayor atención estaba dirigida hacía los procedimientos y prácticas contables utilizadas, e hicimos énfasis en los siguientes renglones financieros:

- Efectivo.
- Activos fijos.
- Inversiones Activos Fijos en Proceso

- Fondos de Contrapartida
- Ingresos.
- Gastos.

También hicimos énfasis en lo siguiente:

- El uso de procedimientos de revisión analítica y pruebas predicativas en la medida en que sea posible, para comprobar la efectividad operacional de la Entidad, los controles internos y disminuir o aumentar la naturaleza de las pruebas sustantivas.

- Se utilizaron enfoques modernos en la ejecución de las pruebas sustantivas y las pruebas de controles, la razonabilidad de los balances se enfocaron principalmente en la confirmación de los saldos con terceros lo que disminuirá nuestro tiempo en la ejecución de dichas pruebas.

Un resumen de las pruebas que realizamos es el siguiente:

- *Pruebas de cumplimiento.*

  -Pruebas de desembolsos
  -Pruebas de conciliación bancaria
  -Prueba de depreciación
  -Prueba de nómina

- *Pruebas sustantivas.*

Estas pruebas las realizamos para detectar errores materiales en los balances y transacciones específicas de las cuentas, entre ellas realizamos las siguientes:

- Confirmaciones
- Análisis de movimientos de cuentas
- Análisis de ingresos.
- Análisis de gastos.
- Otros, según se consideramos necesarios.

4. PRINCIPALES OBSERVACIONES, CONSECUENCIAS Y RECOMENDACIONES

Los principales hallazgos detectados son los siguientes:

Observaciones y Consecuencias	Recomendaciones
1. Adquisición y Remodelación Edificio	
▪ Durante nuestra revisión pudimos notar que la Entidad incurrió en la compra y remodelación de un edificio donde se alojarán las oficinas de la SIPEN. El monto de lo mismo es de US$900,000 para la adquisición y RD$67,736,221.14 para la remodelación. Si bien es cierto que para la adquisición y remodelación de este inmueble la Entidad realizó una reserva lo cual se presenta dentro de sus estados financieros al 30.06.2005 por valor de RD$37,113,315.90 para la adquisición del bien y RD$40,200,000 para la remodelación y equipamiento de la Entidad, también es cierto que esta partida no fue contemplado dentro del presupuesto del año 2005 y tampoco fue aprobada por el CNSS su adquisición. ***Acción Correctiva*** Si bien corresponde a la Superintendencia someter al CNSS el presupuesto anual de la institución en base a la política de ingresos y gastos establecidas por éste, no es sino mediante Resoluciones 123-04 de febrero de 2005 para el presupuesto del 2006 cuando se establecen dichas políticas, las cuales en algunos aspectos contradicen la autonomía que confiere el articulo 107 de la Ley 87-01 a la Superintendencia, difiriendo que ha sido sometido por la SIPEN a la Cámara de Cuentas de la Republica Dominicana en funciones de Tribunal Contencioso Administrativo para fines de solución definitiva. Según ellos expresan que la decisión de adquirir este inmueble no fue con mal intención y los mismos entendían que como el mismo fue conocido por el CNSS, era sobrentendido que esto estaba aprobado.	Consideramos que todas las adquisiciones deben ser contempladas dentro del presupuesto de un determinado año y dicho presupuesto debe ser sometido ante el CNSS para su aprobación y seguimiento del mismo, según se contempla en el art. 110 acápite e, de la Ley 87-01.

2. Tecnología y Sistemas	
A. Políticas de Seguridad	
Pudimos notar que las políticas de información de la Entidad no poseen o no contienen: • Una declaración escrita que exprese la intención de la Alta Gerencia en cuanto al apoyo de lograr metas y principios en materia de seguridad de la información. • Una definición de seguridad de información. ***Acción Correctiva*** El apoyo de la Alta Gerencia está expresado en el Manual de Políticas y Controles internos de la SIPEN, específicamente en los numerales 12 y 13 del Capítulo V. Asimismo, en los objetivos estratégicos, en las capacitaciones en materia de seguridad de la información y auditoria de la Tecnología de la Información que han sido aprobadas el Plan de Trabajo del 2006 , donde se establece un proyecto de implementación del Sistema de Gestión de información BS-7799. No obstante, a SIPEN acoge la recomendación de agregar una declaración en el manual de políticas de la información reiterando el apoyo por parte de la Alta Gerencia en lo relativo a la seguridad de la información. La Entidad también acoge la recomendación para agregar una definición conceptual en lo relativo a seguridad de información.	Recomendamos que el manual de políticas de información contenga: • Una declaración escrita que exprese la intención de la alta gerencia en cuanto al apoyo de lograr metas y principios en materia de seguridad. • Una (varias) definición(es) de seguridad de información.
B. Organización y Seguridad	
i) Notamos que en cuanto a aspectos físicos y lógicos se refieren los controles de accesos de las AFP y UNIPAGO no incluyen contratos que especifiquen las condiciones de seguridad, los métodos de accesos, usuarios autorizados, responsabilidades legales y otros aspectos. Pudimos notar que en el capitulo II, art. 133 del Reglamento interno de la SIPEN no se les exige a las AFP deber de confidencialidad, sino más bien el mismo hace sus exigencias a la Superintendencia y a sus funcionarios.	Recomendamos también en cuanto a aspectos físicos y lógicos se refiere que los controles de accesos incluyan contratos con las partes externas que requieren accesos a la SIPEN y que especifiquen las condiciones de seguridad, los métodos de accesos, usuarios autorizados, responsabilidades legales y otros aspectos.

ii) No existe un comité de seguridad de la información para dirigir, administrar y coordinar las medidas de seguridad Notamos que si existe un comité ejecutivo pero lo que se refiere a un comité específicamente de seguridad de la información, a la fecha de nuestra revisión no existía. ***Acción Correctiva*** Existe el comité ejecutivo responsable de emitir, dirigir, administrar y coordinar todas las estrategias y políticas de la SIPEN, incluyendo aquellas políticas referentes a la seguridad de la información. Considerando que en su cronograma de trabajo del 2006 se contempla la implementación del BS-7799, se tiene programado la creación de un subcomité de Seguridad de la Información que se encargará de administrar y coordinar las estrategias y políticas de seguridad de la información.	Recomendamos al más alto nivel de la entidad la creación de un comité de seguridad de la información para dirigir, administrar y coordinar las medidas de seguridad. Los entes de este comité deberían ser responsables en distintos grados de la seguridad de la entidad. El comité de seguridad informática debería estar compuesto por los representantes de las Gerencias de la entidad (Recursos Humanos, Auditoria, Seguridad, Operaciones, Contabilidad, etc.), así como también del gerente de Informática. Este comité estaría encargado de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad informática y comunicaciones. También seria responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres, entre otros. Durante sus reuniones el comité efectuaría la evaluación y revisión de la situación de la entidad en cuanto a seguridad informática incluyendo el análisis de incidentes ocurridos y que afectaron la seguridad.
C. Seguridad Física y del Medio Ambiente	
i. Notamos que no existe una política de control de entrada y salida para memorias flash y diskettes El uso de memorias Flash y Diskettes está deshabilitado en las Computadoras que están fuera del Centro de Operaciones de la entidad, pero no está formalmente regulado dentro del Centro de cómputos. Según el Director de Sistemas existe un procedimiento verbal en este sentido, pero el mismo no está escrito.	Recomendamos que la existencia de una política de control de entrada y salida para: • Los empleados de informática, así como de otras áreas que tienen Memorias Flash.
ii. Los formularios de control de traslado de activos fijos no demuestran que los empleado que tienen Laptops deban llenar el mismo y especificar en el los datos que están sacando. Estos formularios solo expresan que se llenan para viajes y cuando se va a enviar a reparar.	Recomendamos que la existencia de una política de control de entrada y salida para: • Los empleados que tienen laptops asignadas y que están autorizados a sacarlas de la entidad.
iii. No notamos la existencia de señales que expresen la prohibición de no comer,	Recomendamos la existencia de estas señalizaciones.

	fumar o beber a lo interno del centro de cómputos principal, así como la existencia de gráficos de instalaciones de Red, Ups y eléctricas debidamente colocadas dentro o próximas a los paneles o Backbones principales y servidores.	

5. OPINION DEL AUDITADO

Uno de los procedimientos que consideramos en la fase del proceso de auditoria, consiste en considerar la opinión del Ente auditado; para lo mismo nos reunimos en una ocasión para recibir las acciones correctivas de la Entidad. Procedimos a verificar dichas acciones correctivas para luego proceder a la emisión de un 2do. *Informe en calidad de 2do. Borrador.*

Los descargos de este 2do. borrador pueden ser efectuados dentro del termino de los 7 días hábiles de recibido el informe de auditoria.

6. OPINIÓN DEL AUDITOR

Los hallazgos y recomendaciones que se presentan en este informe están contenidos en la sección de Principales observaciones, consecuencias y recomendaciones y los mismos tienen como fin específico fortalecer los controles y hacer más efectiva la gerencia de la Superintendencia de Pensiones

Cabe aclarar que hemos presentado nuestras recomendaciones por puntos específicos, a la vez queremos resaltar que es importante implementarlos de manera integral para llegar a los resultados deseados.