CONTRALORÍA GENERAL DEL ESTADO

DIRECCIÓN DE AUDITORÍAS INTERNAS

DAI-AI-0420-2016

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL IESS

INFORME GENERAL

EXAMEN ESPECIAL A LOS PROCESOS DE GENERACIÓN CONSERVACIÓN Y RECUPERACIÓN DE LAS COPIAS DE RESPALDO DE LOS SISTEMAS DE INFORMACIÓN, EN LA DIRECCIÓN NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN.

TIPO DE EXAMEN : EE **PERIODO DESDE :** 2011/01/01 **HASTA :** 2015/04/30

Nº C.C.:
Nº NIS : 39332
PERIODO : 2015
Nº INGRESO DPECC :

CONTRALORÍA GENERAL DEL ESTADO

DIRECCIÓN DE AUDITORÍAS INTERNAS

DAI-AI-0420-2016

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL IESS

INFORME GENERAL

EXAMEN ESPECIAL A LOS PROCESOS DE GENERACIÓN CONSERVACIÓN Y RECUPERACIÓN DE LAS COPIAS DE RESPALDO DE LOS SISTEMAS DE INFORMACIÓN, EN LA DIRECCIÓN NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN.

TIPO DE EXAMEN : EE **PERIODO DESDE :** 2011/01/01 **HASTA :** 2015/04/30

Orden de Trabajo 12921-13-2015
Fecha O/T 18/05/2015

DIRECCION NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN

"A LOS PROCESOS DE GENERACIÓN, CONSERVACIÓN Y RECUPERACIÓN DE LAS COPIAS DE RESPALDO DE LOS SISTEMAS DE INFORMACIÓN, EN LA DIRECCIÓN NACIONAL DE TECNOLOGÍA DE LA INFORMACIÓN"

Por el período comprendido entre el 1 de enero de 2011 y el 30 de abril de 2015

AUDITORÍA INTERNA DEL IESS

Quito – Ecuador

RELACIÓN DE SIGLAS Y ABREVIATURAS UTILIZADAS

Art.	Artículo
BIA	Por sus siglas en inglés (Business Impact Analysis) – Análisis de impacto del negocio
CD	Consejo Directivo
CI	Comisión Interventora
DDI	Dirección de Desarrollo Institucional
DNTI	Dirección Nacional de Tecnología de la Información
DBA	Por sus siglas en inglés (Database Administrator); Administrador de Base de datos
DPG	Dirección Provincial del Guayas
G.T	Grupo de Trabajo
HL	Historia Laboral
IESS	Instituto Ecuatoriano de Seguridad Social
IESSPRD	Nombre de Base de Datos Oracle, en el ambiente de producción.
Jtrac	Herramienta para registro de Incidentes desarrollada en Java
LOCGE	Ley Orgánica de la Contraloría General del Estado
LOSNCP	Ley Orgánica del Sistema Nacional de Contratación Pública
LSS	Ley de Seguridad Social
LTO	Linear Tape Open
NCI	Norma de Control Interno
PAC	Plan Anual de Contratación
RO	Registro Oficial
RSBSP	Reglamento Sustitutivo de Bienes del Sector Público

ÍNDICE

DIRECCIÓN DE AUDITORÍAS INTERNAS
APROBADO POR:
FECHA: 2016-01-22

Ref. Informe aprobado el

Quito, D.M.

Señores
Presidente y Miembros del Consejo Directivo
Instituto Ecuatoriano de Seguridad Social
Presente

De mi consideración:

La Contraloría General del Estado en uso de sus atribuciones constitucionales y legales, por intermedio de la Unidad de Auditoría Interna del Instituto Ecuatoriano de Seguridad Social, efectuó el examen especial a los procesos de generación, conservación y recuperación de las copias de respaldo de los sistemas información, en la Dirección Nacional de Tecnología de la Información, por el periodo comprendido entre el 1 de enero de 2011 y el 30 de abril de 2015.

Nuestra acción de control se efectuó de acuerdo con las Normas Ecuatorianas de Auditoría Gubernamental emitidas por la Contraloría General del Estado. Estas normas requieren que el examen sea planificado y ejecutado para obtener certeza razonable de que la información y la documentación examinada no contiene exposiciones erróneas de carácter significativo, igualmente que las operaciones a las cuales corresponden, se hayan ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en los comentarios, conclusiones y recomendaciones que constan en el presente informe.

De conformidad con lo dispuesto en el artículo 92 de la Ley Orgánica de la Contraloría General del Estado, las recomendaciones deben ser aplicadas de manera inmediata y con el carácter de obligatorio.

Atentamente,
Dios, Patria y Libertad,

Eco. Vicente Saavedra Alberca

AUDITOR INTERNO DEL IESS

CAPITULO I

INFORMACION INTRODUCTORIA

Motivo del examen

El examen especial en la Direccion Nacional de Tecnología de la información, se realizó con cargo al Plan Operativo de Control del año 2015; y, de conformidad a la Orden de Trabajo 12921-13-2015 de 18 de mayo de 2015, suscrita por el Auditor Interno del IESS.

Objetivos del examen

- Determinar el cumplimiento de las disposiciones, legales, reglamentarias y demás normas vigentes aplicables a la generación de respaldos, conservación, transporte, cadena de custodia, recuperación de la información de los sistemas de información del IESS y los criterios aplicados para garantizar la confidencialidad, integridad y su disponibilidad.

- Verificar la efectividad y grado de confiabilidad de los procedimientos y controles implantados.

Alcance del examen

Se efectúo el examen especial a los procesos de generación, conservación y recuperación de las copias de respaldo de los sistemas de información, por el período comprendido entre el 1 de enero de 2011 y el 30 de abril de 2015.

El análisis comprendió la evaluación de los procedimientos realizados en la Dirección de Desarrollo Institucional y al 30 de abril de 2015, fecha de corte del examen especial denominada Dirección Nacional de Tecnología de la Información, correspondientes a la solicitud, generación, conservación y recuperación de las copias de respaldo de la información de los sistemas informáticos que soportan los procesos Institucionales y la operatividad del IESS.

Base legal

Con Decreto Supremo 9, de 23 de junio de 1970, publicado en el Registro Oficial 6, de 29 de junio de 1970, se suprimió el Instituto Nacional de Previsión, ejerciendo sus atribuciones y funciones el Ministerio de Bienestar Social y Trabajo, los fondos pasaron al Departamento Médico del Seguro Social y los bienes a la Caja Nacional del Seguro Social, hasta que se expida el decreto de restructuración del Seguro Social Ecuatoriano.

Con Decreto 40, de 2 de julio de 1970, publicado en Registro Oficial 15, de 10 julio de 1970, se estipuló que el Régimen del Seguro Social Obligatorio será aplicado por el Instituto Ecuatoriano de Seguridad Social (IESS), organismo que sustituyó a la Caja Nacional de Seguro Social y que continua vigente con la Ley de Seguridad Social, publicada en Suplemento del Registro Oficial 465, de 30 de noviembre de 2001.

El Consejo Directivo del IESS, con Resolución CD 021, aprobó el 13 de octubre de 2003, la nueva estructura orgánica funcional del IESS, en la que se incluyó cinco Unidades de Negocio especializadas, las que fueron la Dirección General, Riesgos de Trabajo, Salud, Seguro Social Campesino y Prestaciones; y, estuvo vigente hasta el 7 de agosto de 2013. En la referida resolución las direcciones especializadas contaron con el apoyo de dependencias responsables en los ámbitos de Reclamación Administrativa, de Nivel Técnico Auxiliar, de Control, de Asistencia Técnica Administrativa, por lo que en ésta última, se ubicó a la Dirección de Desarrollo Institucional (DDI), la que de conformidad a lo dispuesto en el artículo 85, tenía las competencias de administración del sistema informático de la Institución y para su operatividad tuvo bajo su mando a la Subdirección de Servicios Informáticos.

El Consejo Directivo del IESS, con resolución CD 457 de 8 de agosto de 2013, publicada en la edición especial del registro oficial 45 de 30 de agosto de 2013, dividió al IESS en dependencias que desarrollan procesos operativos y de apoyo administrativos; y, renombro a varias dependencias, por lo que la Dirección de Desarrollo Institucional (DDI), se denominó Dirección Nacional de Tecnología de la información (DNTI), a la que se ubicó dentro de los Procesos de Apoyo y está sujeta a la Coordinación General de Gestión Estratégica, la que depende administrativamente de la Dirección General, que estuvo vigente hasta el 30 de abril de 2015, fecha de corte del examen especial.

La DNTI no cuenta en esta estructura con unidades de apoyo y es la responsable de la planificación, coordinación y dirección de las actividades referentes a los procesos de Gestión de Tecnología de Información y Comunicaciones (numeral 2.4.3).

Estructura Orgánica

De conformidad a la estructura orgánica emitida con resolución CD 457 de 8 de agosto de 2013, la Dirección Nacional de Tecnología de la información (DNTI), se encuentra ubicada en los procesos de apoyo, conforme se presenta a continuación:

2. Dirección General

2.4 Coordinación General de Gestión Estratégica

2.4.3 Dirección Nacional de Tecnología de la Información

Objetivo de la entidad

El Instituto Ecuatoriano de Seguridad Social tiene como objetivo proteger a la población urbana y rural, con relación de dependencia laboral o sin ella, contra las contingencias de enfermedad, maternidad, riesgos del trabajo, discapacidad, cesantía, invalidez y muerte; según se especifica en el Art. 17.- Misión Fundamental de la Ley de Seguridad Social.

La DDI y posteriormente DNTI no contaron con objetivos formalmente establecidos y aprobados por el Consejo Directivo de la Entidad, durante el periodo analizado; sin embargo, la primera fue la encargada de la formulación y coordinación de la ejecución de los proyectos y programas de mejoramiento y desarrollo de la institución; en procurar de la eficacia, eficiencia y economía de los procesos del IESS de conformidad con lo establecido en el Plan Estratégico Institucional y las normas y políticas definidas por el Consejo Directivo; y, la segunda fue la responsable de la planificación, coordinación y dirección de las actividades referentes a los procesos de Gestión de Tecnológica de Información y Comunicaciones

Monto de recursos examinados

Los procesos evaluados comprendieron información transaccional, histórica y estratégica de los registros generados por los sistemas de información de propiedad del Instituto Ecuatoriano de Seguridad Social, por lo que su valor no está determinado.

Servidores relacionados

Consta en Anexo 1

CAPITULO II

RESULTADOS DEL EXAMEN

Seguimiento de recomendaciones

La Contraloría General del Estado, ni Auditoría Interna del IESS han realizado exámenes especiales a los procesos de generación, conservación y recuperación de las copias de respaldo de los sistemas de información, en la Dirección Nacional de Tecnología de la Información.

El IESS no estableció los requerimientos de respaldo de la información con base a sus necesidades y objetivos

La Directora General encargada, con memorando IESS-DG-2014-0564-M de 15 de abril de 2014, dispuso a los Directores de los seguros especializados: Seguro de General de Salud Individual y Familiar, Sistema de Pensiones, Seguro Social Campesino, Seguro de Riesgos del Trabajo; y Afiliación y Cobertura; la definición de la información a respaldar; así como, la frecuencia de respaldo en base a las necesidades de negocio; sin embargo, hasta el 30 de abril de 2015, fecha de corte del examen especial, no se evidenciaron requerimientos levantados por parte de los Directores.

Al respecto, la Directora del Sistema de Pensiones, con periodo de gestión entre el 23 de agosto de 2013 y el 30 de abril de 2015; con memorando IESS-DSP-2014-1322-M de 21 de mayo de 2014, informó al Director General:

> *"... se solicitó los detalles de almacenamiento, respaldos y responsables de la información del Sistema de Pensiones a la Dirección Nacional de Tecnología de Información...".*

El Director del Seguro Campesino con periodo de gestión comprendido entre el 7 de septiembre y el 30 de abril de 2015, con Memorando IESS-DSSC-2014-1854-M de 21 de abril de 2014, informó al Director General, sobre el pronunciamiento de la Unidad Informática de esa Dependencia, señaló:

> *"... En ese sentido, y dado que la Unidad de Informática no es propietaria de la información; es responsabilidad de las áreas que utilizan los sistemas mencionados anteriormente, los que deben definir qué información es*

primordial y cuál es la periodicidad con la que se deben realizar los respaldos..."

La Directora de Afiliación y Cobertura encargada, con periodo de gestión comprendido entre el 1 de abril de 2014 y el 30 de abril de 2015, con memorando IESS-DNAC-2015-0787-M de 13 de julio de 2015, adjuntó el memorando IESS-DNAC-2014-0422-M de 28 de abril de 2014, que al respecto señaló:

"... La emisión de acciones realizadas o que se realizaren... corresponden directamente a la actual Direccion Nacional de Tecnología de la Información puesto que la Dirección de Afiliación y Cobertura se encuentra administrando desde agosto de 2012 el aplicativo de seguridades de la plataforma informática de historia laboral en lo relacionado, exclusivamente, a la asignación de roles y claves de usuarios finales y al proceso de entrega de claves a los usuarios externos... "

El Director de Salud Individual y Familiar con periodo de gestión entre el 5 de julio de 2013 y el 30 de abril de 2014, en atención al requerimiento de auditoría realizado con oficio 51000000-RSI-038 de 25 de junio de 2015; en comunicación s/n de 30 de junio de 2015, expresó:

"... Debo informarle que los memos enviado (sic) por la Directora General Encargada, llega a mi dirección, 15 días antes de mi separación de la Dirección General del Seguro de Salud, a mi cargo, por lo que mi acción quedaba reducida..."

La Directora del Seguro General de Salud Individual y Familia con periodo de gestión comprendido entre el 12 de marzo de 2015 y 30 de abril de 2015; no remitió respuesta al requerimiento realizado por auditoría con memorandos IESS-AI-2015-0917-ME y IESS-AI-2015-0993-ME de 17 de julio y 3 de agosto de 2015.

Con memorando IESS-AI-2015-0927-ME de 20 de julio de 2015, auditoría solicitó información al Director del Seguro de Riesgos del Trabajo relación a las gestiones realizadas para el establecimiento de la información a respaldar; quien con memorando IESS-DSGRT-2015-1152-M, de 23 de julio de 2015, remitió información sobre pedidos anteriores efectuados por el equipo de auditoría; sin entregar datos relación a los requerimientos de respaldo de la información.

No se obtuvo evidencia documental sobre las gestiones efectuadas para la definición de la información a respaldar y los requerimientos en cuanto la perdida máxima aceptable de la información para el establecimiento de la frecuencia de la obtención de

respaldos, por parte de los Directores de los Seguros especializados de turno; lo que ocasiono que el IESS no cuente con una estrategia implementada para la obtención, recuperación y conservación de las copias de respaldo de los sistemas de información Institucional, con base en las necesidades del negocio, exponiendo a la Institución a riesgos potenciales, como: la perdida de información a causa de fallas tecnológicas, desastres naturales, sabotaje, inaccesibilidad a sus sitios de procesamiento, entre otros eventos no previstos, en la administración de información bajo su responsabilidad.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales a los funcionarios relacionados con los procesos de generación, recuperación y conservación de las copias de respaldo de los sistemas de información Institucional.

Se obtuvieron las siguientes respuestas:

El Director del Seguro General de Salud Individual y Familiar, con período de gestión entre el 5 de julio de 2013 y el 30 de abril de 2014, en respuesta al oficio 51000000-RSI-DNTI.62 de 12 agosto de 2015, con comunicación de 25 de agosto de 2015; señaló:

> *"... mi función como Director de Seguro de Salud del IESS... inicio el 5 de julio de 2013 y culminó el 30 de abril de 2014, período en el cual y para garantizar los respaldos en los procesos de generación, conservación y recuperación de las copias de respaldo de los sistemas de información, se apoya y se crea mediante la C.D. 457 la creación de la Dirección General de Tecnología de la Información supeditada a la Coordinación General de Tecnología de la Información, entidad responsable de:.- e) Generar lineamientos y directrices para la gestión de infraestructura de la tecnología de la información, bases de datos, redes y sistemas, desarrollo y mantenimiento de aplicaciones y soporte técnico a usuarios.- f)Implementar y administrar seguridades para garantizar la integridad de la información almacenada en las bases de datos de las aplicaciones informáticas de la institución.- En este marco la definición de directrices y procedimientos de seguridad para todas las bases de datos y su correspondiente seguridad correspondían a dicha instancia... "*

La Directora de Afiliación y Cobertura, encargada, con el período de gestión entre el 1 de abril de 2014 y el 30 de abril de 2015, en respuesta al memorando IESS-AI-2015-1060-ME de 12 agosto de 2015, con memorando IESS-DNAC-2015-0985-M de 24 de agosto de 2015, manifestó:

"... se solicitó información acerca de la generación de históricos de los cambios de representantes legales...la liberación de este cambio se la realizó en el mes de noviembre 2013.- Con el fin de mantener un catálogo de las transacciones que guardan en la actualidad pistas de auditoria...se ha elaborado el INFO-3873 dirigido el (sic) área de tecnología con el fin que detalle los campos de los que se está generando los históricos..."

La Directora del Sistema de Pensiones, con periodo de gestión entre el 23 de agosto de 2013 y el 30 de abril de 2015, en respuesta al memorando IESS-AI-2015-1054-ME de 13 de agosto de 2015, con memorando IESS-DSP-2015-2296-M de 24 de agosto de 2015, manifestó:

"... Los aplicativos informáticos del Sistema de Pensiones...se encuentran alojados en los servidores de la Dirección Nacional de Tecnología de la información en los servidores de la... (DNTI), cuyos respaldos se encuentran bajos los estándares que la DNTI.- la DNTI genera y entrega mensualmente a la Dirección del Sistema de Pensiones un DVD, con los resultados del proceso de la ejecución de la nómina... información que se ha venido resguardando desde octubre 2013...la custodia de esta información está a cargo del responsable de nómina y del cual se obtiene una copia adicional de seguridad y que se encuentra bajo la custodia...del responsable informático... la Dirección de Pensiones instrumentará y comunicará las políticas a tomar para el resguardo de la información que se genera mensualmente; a fin de mejorar las condiciones de generación, conservación y recuperación de la información..."

Posterior a la comunicación de resultados efectuada el día 31 de agosto de 2015, con memorando IESS-DNAC-2015-1061-M de 7 de septiembre de 2015, la Directora de Afiliación y Cobertura encargada, señaló:

"... Con memorando Nro.IESS-DNAC-2014-0371-M de 22 de abril de 2014, dispuse a la Dra. (...), servidora de esta Dirección, que respecto a las recomendaciones de la Intendencia Nacional de Seguridad Social... analice e informe las acciones que se implementarán en caso de corresponder a esta Dirección Nacional.- la indicada servidora, generó los incidentes Nro. 16852, 22385 y 29924, constando en el resumen de los mismos: Implementación de procesos para guardar información histórica del afiliado/pensionista y empleador y crear históricos de representante legal de empleadores; con los detalles: "Con el fin de atender la disposición de la Superintendencia de Bancos y Seguros y organismos de control interno y externo.- Los objetivos de estos incidentes eran guardar los históricos de las acciones que: se ejecutan en la página del empleador, desde su registro como tal hasta la generación de novedades, comprobantes, inactivación de la empresa; de los representantes legales en empleadores y la información del afiliado/pensionistas..."

Los Directores de los Seguros Especializados, resaltaron la función de la Dirección Nacional de Tecnología de la Información, respecto de la ejecución de los procedimientos operativos relacionados a la generación, conservación y recuperación

de la información; así también expusieron iniciativas propias de respaldo y los requerimientos realizados a la DNTI, con la finalidad de crear información histórica y pistas de auditoría en la base de datos del IESS; sin embargo, no se evidenciaron requerimientos de respaldo de la información con base en las necesidades institucionales, tales como: políticas institucionales de respaldo, identificación y clasificación de la información a respaldar, su priorización, máximo aceptable de perdida información aceptable (necesidades de disponibilidad), conservación, seguridad de la recuperación, entre otros.

Cabe indicar que dentro de nuestro análisis, existió el informe de la Superintendencia de Bancos y Seguros *"Evaluación tecnológica de los aplicativos que soportan los procesos de la Dirección General de Salud Individual y Familiar con corte a diciembre de 2012"*, comunicado al Director General con oficio INSS-DASS1-2014-0208 de 7 de marzo de 2014, en su recomendación 6, que estableció:

> *"... El Director General del IESS debe disponer: a) los propietarios de información, la definición (SIC) la Información a respaldar así como la frecuencia de respaldo con base en las necesidades del negocio y en el punto objetivo de recuperación de sus procesos (pérdida de datos aceptables en caso de una interrupción de operaciones, sirve para determinar la periodicidad de obtención de los respaldos de información)..."*

Lo que estableció la necesidad de requerimientos originados desde una perspectiva de negocio y levantados desde cada una de las Direcciones de los Seguros Especializados.

Lo mencionado, afectó al proceso de actualización y ajuste de las políticas y procedimientos de respaldo de la información con base en las necesidades institucionales, las que se encuentran establecidas al interior de la Dirección Nacional de Tecnología de la Información.

Conclusión

No se efectuaron las gestiones para la definición de la información a respaldar y los requerimientos en cuanto la perdida máxima aceptable de la información para el establecimiento de la frecuencia de la obtención de respaldos, por parte de los Directores de los Seguros Especializados, lo que ocasiono que el IESS no cuente con una estrategia implementada para la obtención, recuperación y conservación de las copias de respaldo de los sistemas de información; con base en las necesidades y

objetivos institucionales, exponiendo al Instituto Ecuatoriano de Seguridad Social a riesgos potenciales, como: la perdida de información a causa de fallas tecnológicas, desastres naturales, sabotaje, inaccesibilidad a sus sitios de procesamiento, entre otros eventos no previstos.

Recomendación

Al Director General

1. Dispondrá a los Directores de los Seguros Especializados que en conjunto con los responsables de la Coordinación General de Gestión Estratégica y la Dirección Nacional de Tecnología de la Información procedan a definir, clasificar la información y establecer los requerimientos en cuanto a su pérdida máxima aceptable para el establecimiento de la frecuencia de la obtención de respaldos de los procesos y elementos que deban respaldarse, a fin de que las políticas de respaldo implantadas por la Direccion Nacional de Tecnología se ajusten a las necesidades Institucionales para su difusión y cumplimiento en cada una de las dependencias y la información que administran.

Pedidos de generación y recuperación de las copias de respaldo de la información, no reflejan políticas y procedimientos de seguridad para su manejo y gestión

El respaldo lógico consiste en la obtención automática de una copia de un conjunto de información de la base de datos, como por ejemplo: los registros facturación, historial de pagos, entre otros; al respecto de las copias de respaldo lógico, se establecieron a criterio de los analistas informáticos de los sistemas de información del IESS y se configuraron en la Herramienta Tivoli Storage Manager (TSM); las que se ejecutaron, de acuerdo a lo establecido en los requerimientos de *"Solicitud de inscripción de respaldos (Por triplificación)",* los que fueron gestionados a través de correo electrónico por parte del personal de la DNTI, así también, procedimiento similar fue utilizado para la gestión de requerimientos de recuperación de la información de las copias de respaldo, sin que existan lineamientos para el trámite, autorización, responsabilidad y archivo de los sustentos de estos procedimientos.

Sobre las solicitudes para la generación de copias de respaldo lógico, identificamos los siguientes hechos:

El Director de la DDI con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013 y el Director de la DNTI; adjuntaron con oficio PAC-2015-IESS-007 de 17 de junio de 2015; y, con memorandos IESS-DNTI-2015-1191-M de 3 de julio de 2015 y memorando alcance IESS-DNTI-2015-1381-M de 29 de julio de 2015, las políticas y procedimientos establecidos durante sus períodos de gestión respectivamente.

En referencia al formulario de "*Solicitud de Inscripción de respaldos*", se observó lo siguiente:

- Las políticas, directrices y procedimientos internos no describieron lineamientos sobre el contenido, utilización, autorización y trámite del formulario, para los procesos de generación, conservación y recuperación de las copias de respaldos de la información.

- Los pedidos de generación de copias de respaldo, registrados por los servidores de la DDI y DNTI en el formulario de "*Solicitud de Inscripción de respaldos*", no cuentan con firmas de responsabilidad de los servidores que realizaron el pedido; autorizaron y ejecutaron su aplicación, sin que exista un archivo físico o digital de los pedidos realizados y su trámite.

- De los formularios de *"Solicitudes de Inscripción de respaldo"* presentados, se observó que los campos: Frecuencia de Respaldo, Retención de Respaldo en días, Frecuencia de restauración en días; no guardan consistencia con lo establecido en la *"Política Servidores"* emitida en 2012 por la DDI, así como en la *"Política de Respaldos de la base de datos"* aprobada internamente por la DNTI el 18 de marzo de 2014.

Al respecto, la *"Política Servidores"*, estableció respaldos diarios, cuya retención es de 31 días, semanales cuya retención fue de 3 meses, y mensuales de retención ilimitada; mientras que la *"Política de Respaldos de la base de datos"*, aprobada, estableció que las cintas diarias tendrán 31 días de retención, las cintas semanales tendrían 2 meses de retención, las cintas mensuales tendrían 1 año de retención; estas últimas deberán estar guardadas por lo menos 7 años según lo estipula la Ley General de Instituciones del Sistema Financiero; sin embargo, el uso de los campos

referidos en el formulario, induce al establecimiento de nuevos valores en los campos referidos, para la frecuencia de obtención, recuperación y retención de las copias de respaldo.

De lo mencionado, la falta de procedimientos y lineamientos en referencia de los campos que refiere el formulario, su uso, alcance y autorización, se contrapone con lo establecido, en las políticas y procedimientos vigentes, al permitir que los formularios establezcan frecuencias de respaldo, retención y frecuencia de pruebas, sin considerar que estos ya fueron previstos en las políticas y procedimientos internos de la DDI y DNTI.

Acerca de los pedidos de recuperación de las copias de respaldo, las muestras de correo electrónico correspondientes a los años 2013, 2014, remitidas por el personal Administrador de la Base de datos (DBA) de la DDI y DNTI, que solicitaron recuperación de la información de las copias de respaldo lógicos de la base de datos, permanecieron en las cuentas de correo electrónico de cada uno de los servidores inmersos en estas actividades, sin que se conserve un archivo físico y digital que sustente las acciones realizadas sobre el requerimiento, la autorización, ejecución y los resultados del pedido.

El Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015; no definieron, documentaron y difundieron los procedimientos que permitan el cumplimiento de las políticas de respaldo, tampoco conservaron el soporte documental de las operaciones administrativas inherentes a las actividades de solicitud para la generación, conservación y recuperación de las copias de respaldo; ni establecieron lineamientos para el registro de los pedidos de las áreas de gestión institucional y su atención por parte de la unidad de tecnología, así como no actualizaron las políticas de respaldo; lo que originó que parámetros de ejecución de las tareas de respaldo como: la frecuencia, conservación y su recuperación no se ajustaran a las políticas establecidas, tampoco cuenten con el soporte documental de sustento, ni garanticen sus resultados con base en las necesidades y objetivos institucionales; incumpliendo el artículo 77 número 2 de las Autoridades de la unidades administrativas y servidores letra a) de la Ley Orgánica de la Contraloría

General del Estado e inobservaron las Normas de Control Interno 401-03 Supervisión; 405-04 Documentación de respaldo y su archivo; 410-04 Políticas y procedimientos.

La ausencia de procedimientos para la autorización, casos de excepción, contenido de los formularios de requerimientos, archivo y trámite de los requerimientos para la generación, conservación y recuperación de las copias de respaldo; ocasionó que estos, no se ajusten a lo establecido en las políticas de respaldo aprobadas por la DDI y DNTI.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales al Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, sin recibir respuesta.

Conclusión

Los pedidos establecidos en la DDI y DNTI, para la generación y recuperación de las copias de respaldo de la información, no reflejaron las políticas y procedimientos de seguridad para su manejo y gestión, en razón de que el Director de Desarrollo Institucional y el Director Nacional de Tecnología de la Información encargado; no definieron, documentaron y difundieron los procedimientos que permitan el cumplimiento de las políticas de respaldo; así como, al no conservar el soporte documental de las operaciones administrativas inherentes a las actividades de solicitud para la generación, conservación y recuperación de las copias de respaldo; sin que se establezcan lineamientos para el registro de los pedidos de las áreas de gestión institucional y su atención por parte de la unidad de tecnología, considerando los aspectos de: autorización, trámite y su ejecución; lo que originó que parámetros de ejecución de las tareas de respaldo como: la frecuencia, conservación y su recuperación no se ajustaran a las políticas establecidas, tampoco cuenten con el soporte documental de sustento, ni garanticen sus resultados con base en las necesidades y objetivos institucionales.

Recomendaciones

Al Director Nacional de Tecnología de la Información

2. Actualizará las políticas y elaborará los procedimientos a seguir para la generación de las copias de respaldo de la información, considerará entre otros elementos: los formatos diseñados para las solicitudes, contenidos (campos de información) del pedido de respaldo, autorización, flujo del trámite, archivo histórico de estos pedidos y custodia de los formularios que sustentan las actividades, trabajos realizados, los requerimientos de las áreas solicitantes, así como las estrategias de respaldo implementadas por la DNTI. Los formularios a usarse observarán las políticas establecidas por la Dirección Nacional de Tecnología de la Información, con base en las necesidades institucionales.

3. Al interior de las áreas de la Dirección Nacional de Tecnología de la Información, establecerá los procedimientos para las actividades de recuperación y restauración de las copias de respaldo, el flujo de atención de los requerimientos de recuperación, su autorización por parte de las áreas internas de tecnología y de las áreas usuarias, casos de excepción, el archivo documental y su custodia, lineamientos para mantener la documentación de soporte de sus operaciones.

4. Difundirá en el ámbito Institucional las políticas y procedimientos que las diferentes áreas de gestión Institucional deberán seguir al respecto de requerimientos de los procesos de generación y recuperación de la información de copias de respaldo de los sistemas de información.

Procedimientos para la generación, conservación y recuperación de las copias de respaldos de la información, sin descripción de responsabilidades de cada una de las áreas involucradas en su aplicación

El Director de la DDI con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013 y el Director de la DNTI; adjuntaron con oficio PAC-2015-IESS-007 de 17 de junio de 2015; y, con memorandos IESS-DNTI-2015-1191-M de 3 de julio de 2015 y memorando alcance IESS-DNTI-2015-1381-M de 29 de julio de 2015, las

políticas y procedimientos internos establecidos durante sus períodos de gestión respectivamente; sin embargo, en estos documentos no constaron las competencias, las responsabilidades, los flujos de autorización, revisión y ejecución de las actividades realizadas del personal de cada una de las áreas internas de la DDI y la DNTI; y, las que están descritas son generales hacia los niveles de coordinación interna, no fueron notificadas ni con designación formal y corresponden, entre otras, a actividades de: programación de tareas de respaldo, tareas de administración de las herramientas (Oracle y TSM) para su ejecución y monitoreo.

El Director Nacional de Tecnología, con memorando IESS-DNTI-2015-1007-M de 9 de junio de 2015, informó:

> *"... No se cuenta con las funciones y responsabilidades claramente establecidas aprobadas formalmente en la Institución, debido a que no existe una estructura secundaria aprobada..."*

Situación que se ratificó con memorando IESS-DNTI-2015-1606-M de 24 de agosto de 2015, el encargado de la Coordinación de operaciones y producción, quien señaló:

> *"... Cuando se asumió el "encargo" de la coordinación de operaciones y producción por parte del Coordinador saliente y por parte del Director encargado de ese entonces "no se recibió una notificación formal", en el cual se indique esta delegación, o las nuevas responsabilidades, funciones o disposiciones emitidas hasta ese entonces, para el desempeño del encargo; por lo que, la asignación fue realizada de manera verbal por el coordinador saliente de ese entonces... Cabe destacar que este continuo ir y venir de autoridades, directores y personal, provocó una dilatación en los tiempos de ejecución de proyectos y procesos en espera de una nueva revisión y aprobación de cada una de las autoridades entrantes, retardando así el ritmo de avance de lo planificado..."*

La falta de definición de la normativa secundaria, para la gestión y operación del área tecnológica se vio afectada, por los constantes cambios de autoridades, sin embargo, no se identificó propuestas por parte de esas instancias para delinear instrucciones en los ámbitos no legislados, que permitan orientar a la administración y la conducción reglamentada de procesos necesarios en el ámbito informático, hecho que tiene su respuesta en la gestión individual e Institucional así como en el retraso en la implementación, operación, alcance y el ámbito de competencias del personal responsable de labores operativas.

El Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, no establecieron procedimientos que describan las competencias, responsabilidades, roles, y atribuciones de cada uno de los servidores inmersos en los procesos de generación, conservación y recuperación de las copias de respaldo de la información, lo que ocasionó que estas actividades se encuentren potencialmente expuestas a concentración de funciones, duplicidad de tareas, incumplimiento de políticas y procedimientos, desaprovechamiento de los recursos, entre otros factores; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado, e inobservaron las Normas de Control Interno: 410-02 Segregación de funciones, 410 -04 Políticas y procedimientos.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales al Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, sin recibir respuesta.

Conclusión

La falta de descripción de responsabilidades de los servidores de las áreas involucradas en la aplicación de los procedimientos para la generación, conservación y recuperación de las copias de respaldos de la información de la DDI y DNTI, por parte del Director de Desarrollo Institucional y el Director Nacional de Tecnología de la Información encargado, originó que las actividades inmersas en estos procedimientos se encuentren potencialmente expuestas a concentración de funciones, duplicidad de tareas, incumplimiento de políticas y procesos, desaprovechamiento de los recursos, entre otros factores.

Recomendación

Al Director Nacional de Tecnología de la Información

5. En la descripción de los procedimientos a seguir para la generación, conservación y recuperación de las copias de respaldos de la información; incluirá los roles, atribuciones y responsabilidades del personal inmerso en estos procesos, considerará las funciones de la supervisión, ejecutores y servidores con capacidad de autorización de las actividades solicitadas, tareas que serán evaluadas periódicamente y difundidos sus resultados para retroalimentación, lo que permitirá evitar la concentración de funciones, duplicidad de tareas, incumplimiento de políticas y procedimientos, desaprovechamiento de los recursos, entre otros factores.

No se implementaron mecanismos para garantizar la confidencialidad en los procesos de generación y recuperación de las copias de respaldo

En correo electrónico de 30 de julio de 2015, el Administrador de Base de Datos (DBA), informó al equipo de auditoría:

> *"... el factor técnico más crítico es el espacio de almacenamiento puesto que la BDD iessprd actualmente ocupa más de 5 Terabytes.- Actualmente no existen los suficientes recursos de almacenamiento... "*

Lo mencionado, determinó la dificultad técnica existente de replicar un ambiente de pruebas y desarrollo con las mismas características que el ambiente productivo.

Observándose las siguientes circunstancias relacionadas a este hecho:

- Los analistas encargados del mantenimiento y desarrollo de las aplicaciones que efectúan los requerimientos de recuperación de la información, al área de base de datos; cuentan con permisos de consulta, a través de un usuario genérico, en el ambiente de producción para atender los pedidos del área usuaria.

- No se implementó la temporalidad de acceso, sin embargo el Administrador de la Base de Datos (DBA), solicitó que una vez terminado los trabajos se eliminen los objetos, con la finalidad de descartar por no corresponder al ambiente productivo.

En relación a la información recuperada, y el grado de protección contra revelación no autorizada:

- No están implementados mecanismos de encriptación de la información sensible en los procedimientos de generación de las copias de respaldo de los sistemas de información.

Y, en referencia a la autorización de los pedidos de recuperación:

- Los pedidos de recuperación de la información efectuados por el área de desarrollo y mantenimiento, al área de base de datos, a través de correo electrónico, no identificaron el área de negocio y personal autorizado que realizó el requerimiento, no se consideró hacer uso del número de incidente en la herramienta Jtrac, para su registro.

A este respecto, el Administrador de Base de Datos (DBA), en correo electrónico de 28 de julio de 2015, expresó:

> *"... En realidad este tipo de requerimientos es bajo demanda y no son tan frecuentes... los requerimientos de recuperación no tienen que ver necesariamente con los incidentes registrados en jtrac. Actualmente el área de Base de Datos no efectúa un registro adicional y sólo se trabaja en función de correo electrónico..."*

Lo mencionado, por el DBA, ratifica el comentario de auditoria, en razón de que los requerimientos para recuperación de información se realizan vía correo electrónico, sin un registro en la herramienta de incidentes.

La insuficiencia de recursos en relación a la capacidad de almacenamiento y procesamiento de los ambientes de prueba y desarrollo, limita que las peticiones de recuperación de la información, desde las copias de respaldo, ya sea por el mantenimiento de aplicaciones o el desarrollo de procesos nuevos, tengan que efectuarse en el ambiente productivo, lo que consume recursos y degrada potencialmente su desempeño, restringiendo la implementación de controles a fin de precautelar la información de revelación no autorizada, los que variarán según el ambiente de procesamiento y sus usuarios. Esta condición, supone un incremento del

riesgo en cuanto la disponibilidad y confidencialidad de la información del ambiente productivo.

El Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, no emitieron procedimientos ni implementaron mecanismos que precautelen la confidencialidad de la información recuperada y generada desde y hacia las copias de respaldo, las que en el caso de recuperación fueron solicitadas durante las actividades de desarrollo y mantenimiento de sistemas, exponiéndola a revelación no autorizada; incumpliendo lo dispuesto en el artículo; 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; artículo 22.- número 14 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos; e inobservaron las Normas de Control Interno: 410 -04 Políticas y procedimientos, 500-01 Controles sobre sistemas de información.

La DDI y DNTI no contaron con mecanismos implementados para asegurar la confidencialidad de la información en los procedimientos de recuperación y restauración de las copias de respaldo, cuando son utilizadas para las actividades de mantenimiento y desarrollo de los sistemas de información, lo que no garantiza el acceso autorizado a la información Institucional.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales al Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, sin recibir respuesta.

Conclusión

El Director de Desarrollo Institucional y el Director Nacional de Tecnología de la Información encargado, no emitieron procedimientos ni implementaron mecanismos que precautelen la confidencialidad de la información recuperada y generada desde y hacia las copias de respaldo, las que en el caso de recuperación fueron solicitadas durante las actividades de desarrollo y mantenimiento de sistemas, exponiéndola a revelación no autorizada.

Recomendaciones

Al Director Nacional de Tecnología de la Información

6. Elaborará procedimientos sobre la confidencialidad de la información en los procesos de atención de requerimientos de recuperación, restauración de la información de las copias de respaldo y acceso directo a la información de la base de datos, los procedimientos contendrán instrucciones respecto de las autorizaciones de los propietarios de la información y los justificativos del trabajo a realizar, previo su trámite. El documento contendrá además directrices de seguridades e instrucciones relacionadas a:

   - Restricción del acceso directo para consulta o aplicación de cambios a la información de la base de datos y casos de excepción.

   - Documentación de los incidentes relacionados a la recuperación de la información.

   - Los mecanismos para garantizar la integridad, confidencialidad y protección de la información, con base en su clasificación y sensibilidad, para esto considerará instrumentos técnicos como: la encriptación de los campos con información sensible, la encriptación de copias de respaldo de información de sistemas críticos y el fortalecimiento de seguridades en la administración de los usuarios de bases de datos y sus privilegios, caducidad de accesos, entre otros.

7. Evaluará y propondrá soluciones a la Dirección General sobre la capacidad de procesamiento y almacenamiento de los ambientes de desarrollo, pruebas, preproducción y producción e implementará los correctivos necesarios, a fin de reducir los riesgos, el efecto y su impacto en el desempeño, confidencialidad e integridad de la información de los ambientes antes referidos.

No se implementaron mecanismos para generar copias de respaldos de la información crítica en el Centro de Cómputo Alterno

En el Centro de Cómputo Alterno, ubicado en la ciudad de Guayaquil, no se mantuvieron copias de respaldos de la información replicada en los servidores de contingencia, de los sistemas críticos del IESS, a pesar de estar equipado con una Librería de cartuchos IBM System Storage TS3500 Tipo 3584 Modelo L53, con número de serie 7825963, que se encontró sin utilizar, lo que expuso a la Institución, a interrupciones en su operación, ocasionados por potenciales eventos que provoquen la falta de disponibilidad de la información crítica que se procesa y almacena en los diferentes centros de cómputo del Edificio de Riesgos del Trabajo, Cintoteca Bóveda Matriz IESS ubicados en la ciudad de Quito.

También se comprobó la existencia de cartuchos que corresponden a: limpieza (8 unidades), de prueba (2 unidades), y de datos (3 unidades), lo que demostró que no se mantuvo la cantidad de cartuchos necesarios para la ejecución de tareas de respaldo en el Centro de Computo Alterno.

El Director de la DDI con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013, con oficio PAC-2015-IESS-007 de 17 de junio de 2015, informó:

> *"... Lo que se logró durante mi período de gestión fue: .- 3. Implementar un sitio de contingencia en la ciudad de Guayaquil, que contiene otra base de datos Stand by y equipamiento que permitiría levantar los servicios más importantes en caso de un desastre en la ciudad de Quito.- 4. Se implementó una solución de respaldo, que incluye una Virtual Tape Library (VTL), en la que se obtienen los respaldos mediante un sistema que se llama Tivoli Storage Manager(TSM), y posteriormente estos respaldos son grabados en cintas física mediante una Librería de Respaldos..."*

El Analista informático, a cargo del soporte y monitoreo del referido Centro de Cómputo Alterno, en los numerales 2) y 6) de su Oficio IESS-DNTI-2015-0125-OF de 29 de julio de 2015, expresó:

> *"... No realizo actividad alguna que esté relacionada con la generación, conservación y recuperación de copias de respaldo de los sistema de información de la DNTI.- A continuación listo los cartuchos que se hallan almacenados en el centro de datos GYE: IBM Total Storage LTO Ultrium 1.5 TB Data Cartridge (3 unidades).- IBM Total Storage LTO Ultrium Test Tape (2 unidades).- IBM Total Storage LTO Ultrium Universal Cleaning Cartridge (8 unidades).-Cabe mencionar que no existe acta de entrega recepción de los mismos..."*

El Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, no implementaron procedimientos de supervisión para la generación y conservación de las copias de respaldo en el Centro de Cómputo Alterno ubicado en la ciudad de Guayaquil, equipado con una Librería de cartuchos IBM System Storage TS3500 Tipo 3584 Modelo L53, con número de serie 7825963, que se encontró sin utilizar; lo ocasionó la subutilización de recursos y expuso a la Institución, a potenciales eventos de interrupción en su operación, en el escenario de una falta de disponibilidad y/o acceso a la información crítica procesada y almacenada en los diferentes centros de cómputo y cintotecas ubicados en la ciudad de Quito, al no contar con las copias respaldo de la información crítica fuera de la ciudad para levantar sus servicios; incumplieron lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; articulo 4.- número 4.3.2.4 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos; e inobservaron las Normas de Control Interno: 100-04 Rendición de cuentas, 401-03 Supervisión, 410-08 Adquisiciones de infraestructura tecnológica, 410-10 Seguridad de tecnología de información.

En la DDI y DNTI no se implementaron los mecanismos necesarios para generar copias de respaldos de la información crítica replicada en los servidores de su Centro de Computo Alterno ubicado en la ciudad de Guayaquil, a pesar de contar con el equipamiento IBM System Storage TS3500 Tipo 3584 Modelo L53, con número de

serie 7825963, para la generación de las copias de respaldo y la gestión de la librería de estos medios físicos, sin que este componente sea utilizado; situación que provocó la subutilización de recursos y el incremento del riesgo de interrupción de las operaciones en caso de contingencia en los servicios de tecnología de la oficina principal en Quito, al no contar con las copias respaldo de la información crítica fuera de la ciudad para levantar sus servicios.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales al Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, sin recibir respuesta.

Conclusión

El Director de Desarrollo Institucional y el Director Nacional de Tecnología de la Información encargado no implementaron procedimientos de supervisión para la generación y conservación de las copias de respaldo en el Centro de Cómputo Alterno ubicado en la ciudad de Guayaquil, equipado con una Librería de cartuchos IBM System Storage TS3500 Tipo 3584 Modelo L53, con número de serie 7825963, que se encontró sin utilizar; lo ocasionó la subutilización de recursos y expuso a la Institución, a potenciales eventos de interrupción en su operación, en el escenario de una falta de disponibilidad y/o acceso a la información crítica procesada y almacenada en los diferentes centros de cómputo y cintotecas ubicados en la ciudad de Quito, al no contar con las copias respaldo de la información crítica fuera de la ciudad para levantar sus servicios.

Recomendaciones

Al Director Nacional de Tecnología de la Información

8. Dispondrá el uso de los recursos adquiridos por el Instituto, como el caso de la Librería de Medios IBM System Storage TS3500 Tipo 3584 Modelo L53, con número de serie 7825963, para la administración y generación de las copias de respaldo de la información con base en las definiciones institucionales, minimizando la exposición de riesgos de la información de los sistemas críticos, ante eventos adversos, desastres naturales, sabotaje, entre otros.

9. Presentará a la Dirección General un plan de fortalecimiento de las estratégicas implementadas en el Centro de Computo Alterno de la ciudad de Guayaquil, así como en todos los sitios de procesamiento o almacenamiento externos al sitio principal, donde consten las alternativas, cobertura del plan (escenarios), análisis de riesgos, basados en costo beneficio, para mitigar los riesgos de interrupción en la operación de los sistemas e infraestructura tecnológica.

Administración de usuarios de la herramienta Tivoli Storage Manager (TSM), sin características de seguridad

A partir de los registros exportados en hoja electrónica, desde la herramienta Tivoli Storage Manager (TSM), en donde se almacena la configuración de las políticas de las copias de respaldo de la información, se verificó que en la implementación efectuada a mediados de 2010, sus registros constaban grabados únicamente con el usuario TSMADMIN, sin garantizar una configuración de usuarios que permita identificar los autores de las actividades como: creación, modificación, eliminación o actualización de las operaciones que registra la herramienta TSM.

La Norma de Control Interno 401-03 Supervisión, dispone:

> *"... Los directivos de la entidad, establecerán procedimientos de supervisión de los procesos y operaciones.- La supervisión de los procesos y operaciones se los realizará constantemente para asegurar que se desarrollen de acuerdo con lo establecido en las políticas, regulaciones y procedimientos..."*

La Norma de Control Interno 410-12 Administración de soporte de tecnología de información, establece:

> *"... La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen.- 2. Seguridad de los sistemas bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad..."*

Lo observado muestra la falta de directrices y lineamientos sobre aspectos de seguridad de las herramientas que soportan la operación de los servicios de tecnología, como: restricción en el uso de usuarios genéricos, cambio periódico de contraseñas, caducidad de claves, complejidad de contraseña, entre otras características de seguridad para la gestión de los usuarios privilegiados y genéricos; aspectos que deben formar parte de las políticas y procedimientos de tecnología aprobados, a fin de precautelar la confiabilidad de las actividades técnicas efectuadas y los servicios.

Desde la adquisición e implementación, a mediados del año 2010, de la herramienta de respaldos, Tivoli Storage Manager (TSM), las operaciones realizadas, se registraron con el usuario TSMADMIN, condición que no permitió establecer quien efectuó las actividades de administración y configuración de las políticas de respaldo automático registradas en esta herramienta.

Comunicados los resultados a los funcionarios relacionados con el informe, conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se obtuvieron las siguientes respuestas:

Al oficio 51000000-RSI-DNTI.59 de 12 agosto de 2015, el Director Nacional de Tecnología de la Información encargado, con período de gestión desde el 16 de diciembre de 2013 hasta el 28 de enero de 2014, señaló:

> *"... mientras ejercía mi encargo como Director Nacional de Tecnología de la información (Encargado), ejerció simultáneamente mi cargo titular como Coordinador General de Territorio .- En el período de mi encargo, la institución se encontraba en el cierre del ejercicio fiscal 2013 y apertura del ejercicio*

2014, por lo que la prioridad se encontraba en la aprobación del Plan Anual de Contrataciones.- Adicionalmente, en el período de mi encargo respecto a las políticas que reglamentan las actividades relacionadas con tecnologías de información con el fin de regular y asegurar la calidad de los servicios de tecnologías de información que presta la institución, se remitió al Subdirector General de la época con el propósito de gestionar ante la máxima autoridad el conocimiento, la formalización y la comunicación de las Políticas y Procedimientos inherentes al área de Tecnología de la Información conforme consta en el Memorando No. IESS-DNTI-2014-0123-M, fechado el 29 de enero de 2014..."

El criterio expuesto señala la prioridad concedida a la aprobación del PAC, en tanto que, la reglamentación de las políticas y actividades relacionadas con la tecnología de la información fueron direccionadas hacia instancias con menor capacidad de decisión y regulación, limitando de esta manera su accionar a propuestas que no pasaron de su propio conocimiento y de su inmediato jerárquico.

Al oficio 51000000-RSI-DNTI.61 de 12 agosto de 2015, el Director Nacional de Tecnología encargado del IESS, con período de gestión desde el 17 de octubre al 16 de Diciembre de 2013, señaló:

"... Mi período de gestión en el Instituto Ecuatoriano de Seguridad Social (IESS) como Director Nacional de Tecnología de información encargado del 17 de Octubre de 2013 al 16 de Diciembre de 2013, es decir 60 días... tiempo en el cual inicié el proceso de conocimiento del cargo así como del análisis situacional general de la DNTI, proceso que no pudo ser concluido en totalidad debido al muy corto tiempo de mi permanencia en el cargo y al tamaño y complejidad de la institución... el muy corto tiempo de mi permanencia... no me permitió que se revisen a detalle y peor aún se propongan nuevas políticas, directrices y procedimientos...pues para hacerlo se debería realizar en primer lugar un análisis técnico muy detallado y posteriormente se debería realizar una propuesta que debería ser revisada por varias instancias ..."

Lo manifestado, al respecto de la limitación, debido al corto periodo de gestión del Director Nacional de Tecnología de la Información, no permitió una propuesta de políticas y procedimientos ajustada a los objetivos institucionales.

Al respecto, dada la exposición de los Directores Nacionales de Tecnología de la información encargado y titular respectivamente, se observó que en ambos casos, se presentaron cortos periodos de gestión, lo que limito el accionar de la gestión de los referidos servidores, al respecto de la elaboración, revisión y aprobación de políticas y procedimientos de la unidad a su cargo; en razón de que se requería una revisión

detallada de los procesos, actividades y practicas implantados para la generación, conservación y recuperación de las copias de respaldo.

Con oficio 51000000-RSI.EX-DDI.52 de 12 de agosto de 2015, se comunicaron los resultados; al Director de Desarrollo Institucional con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013, así también se comunicó con oficio 51000000-RSI.DNTI.51, al Director Nacional de Tecnología de la información con periodo de gestión comprendido desde el 10 de abril de 2014 al 24 de junio de 2014; con oficios 51000000-RSI.DNTI.55; 57 y 58 a los Directores Nacionales de Tecnología de la Información encargados en sus correspondientes periodos de gestión comprendidos del 25 de junio de 2014 al 7 de enero de 2015; desde el 8 de enero de 2015 al 21 de abril de 2015; desde el 9 de enero de 2014 al 31 de marzo de 2014 respectivamente; sin que tengamos respuesta o comentario sobre estos temas.

Posterior a la comunicación de resultados realizada el día 31 de agosto de 2015, con oficio 009-RCH-IESS-2015 de 3 de septiembre de 2015, el Director Nacional de Tecnología de la Información con periodo de gestión comprendido entre el 17 de octubre al 16 de diciembre de 2013, en referencia a la comunicación de resultados se ratifica en lo expresado en contestación al oficio 51000000-RSI-DNTI.61 de 12 agosto de 2015, señalando que su accionar fue limitado durante su corto período de gestión; criterio aceptado por el equipo de auditoría.

El Director Nacional de Tecnología de la Información encargado, cuyo periodo de gestión comprendió del 8 de enero de 2015 al 21 de abril de 2015, con oficio AGBB-AI-005-2015 de 25 de septiembre de 2015, en respuesta al oficio 51000000-RSI.DNTI.57 de 12 de agosto de 2015, manifestó:

> *"... La carencia de un Gobierno de Tecnologías de Información, basado en procesos de gestión tecnológica muy bien establecidos (desde la planificación, diseño, implementación, mantenimiento y control de los servicios informáticos y los componentes tecnológicos que los soportan), impiden que se dispongan de políticas y procedimientos completos y con un sustento adecuado que esté acorde a las necesidades institucionales y exigencias de los entes de control. Durante el período de mi gestión, no existían procesos de gestión tecnológica formalmente aprobados, esto conlleva a tener políticas de diferente índole, las cuales en muchas ocasiones, se encuentran desactualizadas, o no obedecen a las necesidades actuales, esto es una de las consecuencias de la no tenencia de una Gobernanza de TI implementada.- Es por ello... que durante mi período de gestión me centre en estructura un proyecto... se denominaba "Consultoría*

para la implementación del Modelo de TI del IESS", enviado a Coordinación General Estratégica mediante memorando IESS-DNTI-2015-0511-M de fecha 30 de Marzo de 2015... respecto de las propuestas del proyecto para la implementación del Gobierno de TI y la aprobación de la organización interna para la DNTI, hasta el 21 de Abril de 2015, fecha fin de mi gestión, ambas propuestas se encontraban en trámite... a mi salida... desconozco el estado de cada una... "

Lo manifestado por el Director Nacional de Tecnología de la Información, ratifica la opinión del equipo de auditoría, sobre la ausencia de políticas y procedimientos de tecnología que permitan entre otros regular la seguridad en la administración de las herramientas para la operación de los servicios de respaldo de la información, sin embargo las iniciativas expuestas por el referido servidor, no se concretaron, constituyéndose el corto de periodo de gestión en una limitante, tal como ya fue expuesto en párrafos anteriores por otros Directores de la DNTI.

Conclusión

No fueron implementados los mecanismos para asegurar la confiabilidad de las tareas de administración y operación de la Herramienta Tivoli Storage Manager (TSM), que desde su implementación a mediados de 2010, mantuvo la administración de cuentas usuarios, sin identificar el personal responsable de políticas de respaldo automático configuradas; las que fueron creadas, modificadas, eliminadas, o actualizadas por el usuario genérico TSMADMIN, sin que se evidencie la implantación de procedimientos de seguridad para la gestión de usuarios privilegiados, lo que no permitió determinar el personal responsable de las operaciones efectuadas en la referida herramienta.

Recomendación

Al Director Nacional de Tecnología de la Información

10. Dictará lineamientos para la administración segura de las herramientas tecnológicas que soportan los servicios de tecnología (bases de datos, Librería de medios (respaldos), sistemas operativos, entre otros); entre los criterios se considerará en la configuración de los parámetros para la gestión de usuarios, las prácticas de seguridad como: restricción en el uso de usuarios genéricos, cambio periódico de contraseñas, caducidad de claves, complejidad de contraseña, y otras características de seguridad.

Períodos de retención implementados en las copias de los respaldos de la información, no consideraron disposiciones legales, para su conservación

Los períodos de retención establecidos en las políticas configuradas para la generación de las copias de respaldo de información del sistema Host y de los sistemas cuya información se mantiene en la base de datos Oracle de la Subdirección de Servicios Informáticos, DDI y DNTI respectivamente, no cumplen con las disposiciones de conservación de la información, legalmente aplicables al Instituto Ecuatoriano de Seguridad Social; así a partir de los registros exportados en hoja electrónica, con base de las políticas configuradas en la herramienta Tivoli Storage Manager (TSM); y, del análisis de los datos de la biblioteca para la administración de cartuchos de cintas de las copias de respaldo físico del sistema Host (transacción TCI1), se observó lo siguiente:

- Los cartuchos de copias de respaldo anual del sistema Host administrados en Quito y Guayaquil tuvieron un período máximo de retención de la información de 3 años.

- La política mensual configurada PD_AIX_MENSUAL, en la herramienta Tivoli Storage Manager, para los respaldos lógicos de la base de datos Oracle y la configuración del sistema operativo AIX, fue implementada el 7 de octubre de 2010, donde se definió una retención ilimitada de las copias de respaldo

- La política mensual configurada PD_BDD_MENSUAL, en la herramienta Tivoli Storage Manager, para los respaldos lógicos de la base de datos Oracle, implementada el 19 de mayo de 2014, tiene definido una retención de la información de un año.

- Las políticas diaria, semanal y mensual configuradas (PD_BDD_DIARIO, PD_BDD_SEMANAL, PD_BDD_MENSUAL) en la herramienta Tivoli Storage Manager (TSM), implementadas el 19 de mayo de 2014, para el respaldo lógico de bases de la datos denominada IESSPRD; no corresponden con lo establecido en la Política de Respaldos de Bases de Datos DNTI-OSI-O03, aprobada, el 18 de marzo de 2014.

Con correo de 27 de julio de 2015, el servidor coordinador del Grupo de Soporte y Plataforma Z10 del sistema Host, ratificó, el modelo de versiones que se emplea para la obtención de las copias de respaldos es: diario, mensual, semanal y anual, como sigue:

> *"... DIARIO: Librerías en cartucho físico (3 versiones) y datos en disco.-SEMANAL : 4 versiones librerías y datos duraría 5 semanas (se cruza el mensual).- Mensual : 3 versiones librerías y datos duraría 3 meses.- Anual: 3 versiones librería y datos duraría 3 años..."*

El Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015; y el Subdirector de Servicios Informáticos con periodo de gestión comprendido entre el 1 de enero de 2011 y el 31 de marzo de 2013; no establecieron lineamientos sobre los procedimientos de conservación de las copias de respaldo de la información que se ajusten con las disposiciones aplicables al IESS, lo que ocasionó que los períodos de retención de la información establecidos en las políticas configuradas para la generación de las copias de respaldo del sistema Host y los mantenidos para las copias de respaldo de la base de datos Oracle no cumplan las disposiciones legales con relación a la retención de la información y su conservación; y, que no se satisfaga las necesidades institucionales sobre la disponibilidad de la información; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; 80.- de la Ley General de Instituciones del Sistema Financiero; 225 del Código Monetario, Registro Oficial 332; e inobservaron las Normas de Control Interno: 401-03 Supervisión.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales a los funcionarios de los cuales, se obtuvieron las siguientes respuestas:

El Subdirector de Servicios Informáticos del IESS, con periodo de gestión comprendido entre el 1 de enero de 2011 y el 31 de marzo de 2013; con oficio FAOF-04-2015 de 21 de agosto de 2015, en respuesta al oficio 51000000-RSI-EX DDI.53 de 12 agosto de 2015, señaló:

"... Anexo al presente una muestra de los medios pasivos obtenidos, en el período de mi gestión, en el que se puede constatar la existencia de cartuchos con los backups de los archivos VSAM de la plataforma Host, con vigencia de más de 7 años, como lo que exige la norma de control interno..."

De lo mencionado, si bien es cierto, se mantiene un inventario de medios pasivos (información que ya no se encuentra en línea, sino únicamente almacenada en cartuchos), la observación efectuada por auditoria, compete a las copias de respaldo de la información transaccional del sistema Host, entre los cuales, las copias de respaldo que se obtienen con periodicidad anual, mantienen un período de retención de 3 años; motivo por el cual se ratifica el comentario de auditoria.

Con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, se comunicaron los resultados provisionales; al Director de Desarrollo Institucional con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013, y al Director Nacional de Tecnología de la Información encargado con periodo de gestión comprendido entre el 25 de junio de 2014 y el 7 de enero de 2015, sin obtener respuesta.

Conclusión

La falta de lineamientos en los procedimientos de conservación de las copias de respaldo de la información que se ajusten a las disposiciones aplicables al IESS, por parte del Director de Desarrollo Institucional; el Director Nacional de Tecnología de la Información encargado; y, el Subdirector de Servicios Informáticos, ocasionó que los períodos de retención de la información establecidos en las políticas configuradas para la generación de las copias de respaldo del sistema Host y los mantenidos para las copias de respaldo de la base de datos Oracle no cumplan las disposiciones legales exigidas al IESS, con relación a la retención de la información y su conservación, y; que no se satisfagan las necesidades institucionales sobre su disponibilidad.

Recomendación

Al Director Nacional del Tecnología de la información

11. Dictará procedimientos acerca de la conservación de la información de las copias de respaldo, incorporando los períodos de retención con base en las definiciones y

necesidades institucionales, asegurando el cumplimiento de las disposiciones legales aplicables al Instituto Ecuatoriano de Seguridad Social. Difundirá y monitoreará, su implementación en todas las áreas de gestión informática que realicen actividades de respaldo.

Deficiencias en la administración, manejo y el control de inventarios de los medios físicos de las copias de respaldo de la información

Las copias de respaldo de la información de los sistemas informáticos que manejan la DDI, DNTI y G.T Servicios Informáticos de la Dirección Provincial del Guayas; se encuentran alojados en cartuchos, los que están ubicados en la Cintoteca local y Librería de Medios TS3500 Tipo 3584 Modelo L53 del Centro de Cómputo del Edificio de Riesgos del Trabajo de la ciudad de Quito; en la Bóveda de la Tesorería del Edificio Matriz en Quito, en el Centro de Cómputo Alterno de la DNTI en Guayaquil y en la oficina de la Auditoría Interna de esa ciudad; en estas instalaciones se observó lo siguiente:

- No se nombró formalmente al custodio de los medios físicos de almacenamiento (inventario de cartuchos) y responsable de su control y ubicación.

- Se identificó la ausencia de lineamientos para la secuencia en el etiquetado de los cartuchos de cintas, en las adquisiciones efectuadas con procesos de compra IESS-PG-2014-260-C, 021-SBSG-2012.

- La administración de los medios físicos de almacenamiento (control de inventario), elaboración y control de las guías de remisión y transportación son realizados por una misma persona, sin que se muestren niveles de autorización y supervisión periódica.

- Los formatos utilizados en las guías de remisión no fue pre numerado, ni pre impreso.

- En las actas de inventario de cintas en la DNTI, con corte al 4 de agosto de 2015, se constató un total de 839 cintas, inicialmente no fueron ubicados 7 cartuchos con información de configuración, posteriormente fueron presentadas sin que exista soporte documental de su movimiento o salida del lugar de ubicación.

- Ausencia de un registro completo de los movimientos de los cartuchos y los responsables de su utilización, desde y hacia localizaciones como: cintotecas, la librería de medios, sitios alternos, u otras instalaciones.

- No se hicieron constataciones periódicas de los medios físicos de almacenamiento (cartuchos de cintas) del Sistema Host administrados en Quito y Guayaquil, en las instalaciones de la Matriz en Quito (Bóveda y Cintoteca) de la DDI y DNTI y en la Cintoteca del G.T Servicios Informáticos de la Dirección Provincial del Guayas.

- No fueron ejecutadas conciliaciones físicas periódicas de los inventarios de las copias de respaldo de la información y los registros de Librería de medios en la herramienta Tivoli Storage Manager (TSM), administrada por la DDI y DNTI.

- No se definieron procedimientos para la gestión de los medios físicos de almacenamiento dañados, así como instrucciones de baja del inventario.

- Los procesos de entrega recepción de cintas no tienen definidos procedimientos de actuación, en este caso se encuentra lo informado por el Coordinador de G.T Servicios Informáticos (IESS DPG) quien con memorando IESS-DPGSAGE-2015-1854-M de 22 de julio de 2015, no evidenció la realización de un proceso de verificación y confirmación de la recepción, que compruebe las condiciones en que fueron recibidos por el personal destinatario, (Subdirección de Servicios Informáticos), para el respectivo descargo.

- No se emitieron como parte de los procedimientos de conservación de las copias de respaldos, los lineamientos acerca del correcto y adecuado manejo físico de las cintas y cartuchos de las copias de respaldo.

- Ausencia de directrices acerca de los parámetros de reusó y vida útil de los cartuchos de las copias de respaldo de la información.

De las prácticas sobre el manejo, organización y condiciones en las que se encontraron almacenados los cartuchos, en las diferentes instalaciones destinadas para su conservación, se determinó:

- Los cartuchos remitidos a la matriz por parte de la DDI y DNTI fueron enviados, con guía de remisión y notificación mediante correo electrónico al servidor encargado, estos no están organizados en el sitio para su fácil ubicación, permaneciendo en cartones, en una gaveta elevada destinada para este propósito.

- A raíz del traslado de la oficina del G.T Servicios Informáticos, en el mes de septiembre de 2014, se reubicaron en cartones, los inventarios de cartuchos de información histórica y backup del sistema Host Guayaquil; en la bodega del área de auditoría interna en el sexto piso de la Dirección Provincial del Guayas y en las inmediaciones del centro de cómputo alterno de la DNTI ubicado en el primer piso del mismo edificio, donde las condiciones físicas y organización de los cartuchos fueron deficientes, los cuales estuvieron en cajas apiladas, sin respaldo de acta entrega recepción o un registro del inventario recibido en el caso de los cartuchos ubicados en el centro de cómputo alterno.

El encargado del grupo de Soporte y Plataforma Z10 (Host), con correo electrónico de 28 de julio de 2015, señaló:

> *"... haciendo un poco de histórico (SIC) lo últimos cartuchos fueron adquiridos alrededor del 2010, cuando éramos SSI, la persona encargada de la Bodega ya está jubilada...".*

El encargado del soporte del Centro de Cómputo Alterno, mediante Memorando IESS-DNTI-2015-0125-OF de 29 de julio de 2015, dijo:

> *"... No se firmó acta de entrega recepción alguna de los cartuchos de respaldo del sistema Host. Se solicitó un inventario pero este no fue facilitado por el G.T. Servicios Informáticos GYE..."*

Lo descrito, confirma la ausencia de lineamientos adoptados, para el manejo, control y uso de los cartuchos de las copias de respaldo de la información, no permite mantener estándares aplicables a todas las áreas de gestión de tecnología, la que está sujeta al criterio del servidor responsable de estas tareas.

El Director de Desarrollo Institucional con período de actuación comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; el Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015; no establecieron lineamientos para la secuencia e identificación en el

etiquetado de los cartuchos, organización y ubicación, registro de los movimientos del inventario, soporte y supervisión de las actividades de transporte, preservación de la cadena de custodia; sin efectuar conciliaciones y constataciones físicas periódicas del inventario de activos de información de los sistemas que generan su información en la base de datos institucional, ni definir lineamientos para su manejo, cuidado y gestión de medios físicos dañados; situación que expuso a la entidad a pérdida y daños de las copias de respaldo (en cartuchos) afectando la disponibilidad e integridad de la información en ellos almacenada; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; articulo 4.- número 4.3.2.4 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos; los artículos 5.- Responsabilidad del Servidor, 6.-Control de los Bienes, 7.-Registros para el control, 8.-Entrega recepción de Bienes, 9.- Constatación física y 10.-Reposición por pérdida de bienes del Reglamento para el control administrativo de los bienes no considerados activos fijos publicado en Registro Oficial 26 de 16 de septiembre de 1996 e inobservaron las Normas de Control Interno: 100-04 Rendición de cuentas, 401-01 Separación de funciones y rotación de labores, 401-03 Supervisión, 410-08 Adquisiciones de infraestructura tecnológica, 410-10 Seguridad de tecnología de información; el numeral 8 del artículo 86.- Responsabilidades, del orgánico funcional emitido con Resolución CD 21 de 13 de octubre de 2013 y el literal b) del numeral 2.4.3 del Orgánico Funcional emitido con Resolución CD 457 de 8 de agosto de 2013.

El numeral 8) del artículo 86.-Responsabilidades de la Dirección de Desarrollo Institucional, del Orgánico Funcional del IESS, emitido con Resolución CD 21 de 13 de octubre de 2013 dice:

> *"... La administración del sistema informático del Instituto Ecuatoriano de Seguridad Social, que incluye el desarrollo, mantenimiento y actualización de su plataforma, de conformidad con el Plan Estratégico...".*

El literal b) del numeral 2.4.3 Dirección Nacional de Tecnología de la Información, del Orgánico Funcional del IESS, emitido con Resolución CD 457 de 8 de agosto de 2013 que establece:

"... Administrar, desarrollar, operar y mantener los sistemas informáticos, redes y sistemas, infraestructura de comunicaciones, equipos y/o centros de cómputo del IESS..."

Los Subdirectores de Servicios Informáticos con períodos de actuación comprendidos entre el 1 de enero de 2011 y el 31 de marzo de 2013; y entre el 1 de abril de 2013 al 30 de julio de 2013 respectivamente, no establecieron procedimientos para efectuar conciliaciones y constataciones físicas del inventario, no definieron lineamientos para su manejo, cuidado y gestión de medios (cartuchos) dañados; no documentaron los procedimientos de recepción y verificación de los cartuchos procedentes de la Coordinación de G.T Servicios Informáticos de la Dirección Provincial del Guayas; no supervisaron la recepción; lo que expuso a la Entidad al riesgo de pérdidas y daños de las copias de respaldo del sistema Host; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; articulo 4.- número 4.3.2.4 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos; los artículos 5, Responsabilidad del Servidor; 8, Entrega recepción de Bienes; 9, Constatación física y 10,Reposición por pérdida de bienes del Reglamento para el control administrativo de los bienes no considerados activos fijos publicado en Registro Oficial 26 de 16 de septiembre de 1996 e inobservaron las Normas de Control Interno: 401-03 Supervisión, 410-08 Adquisiciones de infraestructura tecnológica.

El Coordinador del G.T Servicios Informáticos con periodo de gestión comprendido entre el 16 de noviembre de 2012 y el 30 de abril de 2015, no precauteló la conservación de la información de las copias de respaldo, sin mantener condiciones físicas de los cartuchos que almacenan el respaldo del sistema Host administrado en Guayaquil, no conto con un levantamiento de los inventarios de los cartuchos en las nuevas localidades y no realizó el acta entrega recepción del mismo al encargado del monitoreo del Centro de Cómputo Alterno de la DNTI; hechos que expusieron a la entidad a perdida y daño de los medios físicos (cartuchos), afectando la disponibilidad e integridad de la información de las copias de respaldo de los sistemas informáticos; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; articulo 4.- número

4.3.2.4 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos; los artículos 5.- Responsabilidad del Servidor, 8.-Entrega recepción de Bienes, 9.- Constatación física y 10.-Reposición por pérdida de bienes del Reglamento para el control administrativo de los bienes no considerados activos fijos publicado en el Registro Oficial 26 de 16 de septiembre de 1996 e inobservaron las Normas de Control Interno: 401-03 Supervisión.

Por lo antes indicado, no se establecieron procedimientos para el manejo, control y uso de los cartuchos, ni se designaron los responsables de la custodia de los medios de almacenamiento, tampoco existió supervisión de su administración; lo que ha ocasionado que la información de las copias de respaldo esté expuesta a eventos adversos: como daño, pérdida, robo, fuga de la información, circunstancias que afectaron su disponibilidad e integridad.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales a los funcionarios de los cuales, se obtuvieron las siguientes respuestas:

El Subdirector de Servicios Informáticos del IESS con periodo de gestión entre el 1 de enero de 2011 y el 31 de marzo de 2013; con oficio FAOF-04-2015 de 21 de agosto de 2015, en respuesta al oficio 51000000-RSI-EX DDI.53 de 12 agosto de 2015, con respecto al manejo de cartuchos y los sustentos entre los movimientos de cintras entre el Host Guayaquil y Quito, informó:

> *"... 1) Si bien es cierto, no se disponía de una política escrita, que permita por un lado llevar el control del número de veces que un cartucho magnético era utilizado para realizar los backups, y por otro lado, obligar a la persona responsable de administrar la Cintoteca o a su vez al operador de turno para que los cartuchos que cumplieron su vida útil sean etiquetados para darlos de baja.- 3) En junio de 2011, se gestionó la comisión de servicios a la ciudad de Quito, de la señora... responsable de la administración de la Cintoteca del G.T Servicios Informáticos de Guayas para que junto con el (...) operador responsable de la administración de la Cintoteca del Host Quito, realicen al entrega recepción formal de los cartuchos magnéticos con los backups de información generada en el computador del Guayas, así como las respectivas pruebas de recuperación de información de dichos cartuchos a la partición administrada por el personal G.T de Servicios Informáticos de Guayas en el computador IBM Z/10. Mediante oficio N° 63100000-088-2011 de fecha de 1 de junio de 2011.- 4)... la ex Subdirección de Servicios informáticos, mantenía en*

Veinte y ocho

canceles son espacios individuales que permitían una adecuada identificación y garantizaba su preservación en el tiempo... A partir del año 2009 la totalidad de las cintas magnéticas fueron reemplazadas por cartuchos... Estos eran ubicados verticalmente en casilleros de madera, con lo cual se garantizaban que no se apilen, precautelando posibles daños en la parte física de la cinta magnética... 6) Por políticas implementadas antes del año 2000, todo medio magnético... que presentaba daño físico se etiquetaba como dañado y se guardaba en la Cintoteca, en una estantería específica para este tipo de medios magnéticos... En el año 2009, fue el único año en que se realizó una baja masiva..."

Lo expuesto ratifica el comentario enunciado, en relación a las prácticas de manejo, reusó, optimización de la vida útil y cuidado de los cartuchos de cintas; al respecto de la documentación soporte de la verificación de la recepción de los cartuchos de Host Guayaquil y su traslado a Quito, no documentaron la gestión de los hechos relatados.

El Coordinador del G.T Servicios Informáticos de la Dirección Provincial del Guayas, con memorando IESS-DPGSAGE-2015-2184-M de 26 de agosto de 2015, en respuesta al oficio 51000000-RSI-EX DDI.56 de 12 de agosto de 2015, informó:

- Respecto de la ubicación temporal de los cartuchos y acta entrega recepción:

"... No se realizó Acta de entrega recepción, porque no ha existido cambio de custodio, los cartuchos siguen en el área de Servicios Informáticos y la otra en la Auditoría, lugar donde nos encontramos temporalmente... Ambas áreas, en las que se encuentran los cartuchos cuentan con condiciones ambientales...y de seguridad... "

Lo expuesto, no justifica la inexistencia del inventario ubicado temporalmente en las inmediaciones del Centro de Cómputo Alterno de la DNTI en Guayaquil, pese a encontrarse dentro del área destinada para el G.T Servicios Informáticos, sin que el personal responsable de su custodia, realice la coordinación con el servidor de la DNTI, encargado del Centro de Cómputo Alterno.

Sobre los cartuchos enviados a la Dirección Provincial de Pichincha, manifestó:

"... Si existen los archivos físicos con los que se entregó los cartuchos a la Subdirección de Servicios informáticos y se encuentra registrado en el sistema de Control de Cartuchos, los cartuchos que fueron trasladados a Quito, el mismo permite en cualquier momento obtener un archivo, con todos los cartuchos que fueron trasladados a Quito..."

Lo mencionado, ratifica el comentario de auditoria, pese a la identificación del inventario de Host Guayaquil en el sistema de Control de cartuchos administrado en Quito; sin embargo no se evidenció la verificación efectuada por parte de la Subdirección de Servicios Informáticos y las condiciones de recepción de los cartuchos.

- Del manejo físico y procedimientos para la gestión de cartuchos dañados, mencionó:

  "... El Sr... conoce el correcto y adecuado tratamiento físico de las cintas y cartuchos que aún se tienen en esta Dirección Provincial.- los cartuchos no están contemplados como bienes de larga duración, son considerados fungibles y los cartuchos dañados son muy pocos, por lo que la norma...no aplica..."

Lo indicado, ratifica el contenido de este comentario, en razón de que, el catalogar los cartuchos como bienes consumibles, no observa el criterio técnico que señala que estos son objetos de registro administrativo por contener información de carácter Institucional para su uso y manejo; por lo que su descarte requiere contar con procedimientos específicos para precautelar los criterios de integridad, confidencialidad y disponibilidad de la información alojada en ellos.

Con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, se comunicaron los resultados provisionales; al Director de Desarrollo Institucional con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013 y al Director Nacional de Tecnología de la Información encargado con periodo de gestión comprendido entre el 25 de junio de 2014 y el 7 de enero de 2015, sin obtener respuesta.

Conclusiones

- El Director de Desarrollo Institucional y el Director Nacional de Tecnología de la Información encargado, no establecieron lineamientos para la secuencia e identificación en el etiquetado de los cartuchos, organización y ubicación, registro de los movimientos del inventario, soporte y supervisión de las actividades de transporte, preservación de la cadena de custodia; sin efectuar conciliaciones y constataciones físicas periódicas del inventario de activos de información de los

sistemas que generan su información en la base de datos institucional, ni definir lineamientos para su manejo, cuidado y gestión de medios físicos dañados; situación que expuso a la entidad a pérdida y daños de las copias de respaldo (en cartuchos) afectando la disponibilidad e integridad de la información en ellos almacenada.

- Los Subdirectores de Servicios Informáticos, no establecieron procedimientos para efectuar conciliaciones y constataciones físicas del inventario, no definieron lineamientos para su manejo, cuidado y gestión de medios (cartuchos) dañados; no documentaron los procedimientos de recepción y verificación de los cartuchos procedentes de la Coordinación de G.T Servicios Informáticos de la Dirección Provincial del Guayas; no supervisaron la recepción; lo que expuso a la Entidad al riesgo de pérdidas y daños de las copias de respaldo del sistema Host.

- El Coordinador de G.T Servicios Informáticos Dirección Provincial del Guayas, no precauteló la conservación de la información de las copias de respaldo, sin mantener condiciones físicas de los cartuchos que almacenan el respaldo del sistema Host administrado en Guayaquil, no conto con un levantamiento de los inventarios de los cartuchos en las nuevas localidades y no realizó el acta entrega recepción del mismo al encargado del monitoreo del Centro de Cómputo Alterno de la DNTI; hechos que expusieron a la entidad a perdida y daño de los medios físicos (cartuchos), afectando la disponibilidad e integridad de la información de las copias de respaldo de los sistemas informáticos.

Recomendación

Al Director Nacional del Tecnología de la información

12. Dictará lineamientos y procedimientos para la administración, registro, custodia, transporte y manejo de los medios de almacenamiento físico (cartuchos), considerará, entre otros, los siguientes aspectos:

    - Etiquetado, organización y ubicación.
    - Procesos de custodia, responsabilidades.
    - Registro, entrega – recepción.

- Manejo y uso de medios de almacenamiento físico.
- Reutilización.
- Procedimientos de baja
- Procedimientos de constatación física periódica

Copias de respaldo de la información, sin procedimientos de verificación periódica

En la Dirección de Desarrollo Institucional se efectuó una verificación de las copias de respaldo, por iniciativa del área de Plataforma en coordinación con el área de Control de Calidad, este proceso se efectuó el 18 de enero de 2012, a través del *"Plan de pruebas para aseguramiento de calidad de restauración y respaldos de servicios"*, en este documento constó un formulario de pruebas; sin embargo, no se evidenció documentación de los procedimientos efectuados para esta verificación; actividad que no fue realizada de manera periódica. Cabe indicar que se efectuaron recuperaciones y restauraciones de las copias de respaldo lógico de la base de datos, las que se ejecutaron bajo demanda, para actividades de análisis y mantenimiento de los sistemas.

No se evidenció la ejecución de pruebas periódicas, de las copias de respaldo físico, alojados en cartuchos, de la base de datos Oracle: denominada IESSPRD.

En relación a las tareas de recuperación, el Administrador de bases de datos, mediante correo electrónico de 28 de julio de 2015, sobre la recuperación de respaldos lógicos, dijo:

> *"... En realidad este tipo de requerimientos es bajo demanda y no son tan frecuentes..."*

Al respecto de los respaldos lógicos, estos se componen de un conjunto de información de la base de datos, cuyo objetivo entre otros, es contar con la información para análisis, consulta y resolución de problemas presentados en los sistemas de información del IESS.

El personal de Administración de la base de datos, mediante correo electrónico de 30 de julio de 2015, acerca las pruebas de las copias de respaldo físico, informó:

"... Para este tipo de prueba, el factor técnico más crítico es el espacio de almacenamiento puesto que la BDD iesprd actualmente ocupa más de 5 Terabytes. Por otro lado estamos hablando que para recuperar ese tipo de información de cinta a disco, el tiempo aproximado sería entre 1 y 2 días".

Agregó:

"... 1. No existe un procedimiento establecido actualmente pero estimo no sería tan fácil hacer uno en razón de la gama de posibles escenarios de daños que se pueden dar.- 2. Actualmente no existen los suficientes recursos de almacenamiento donde se pueda efectuar este tipo de ejercicio.- 3. Efectuar este tipo de recuperación implica un daño masivo a nivel de la Base de Datos, ventajosamente no se ha dado esta situación, no obstante los backups respectivos si se han utilizado durante el año 2012 para la implementación de las Bases de datos Standby físicas tanto la que está localizada en Quito (iesslsby) como de la que está localizada en Guayaquil (iessrsby). Dichas bases están operativas actualmente y constituyen por si mismas pruebas del trabajo efectuado.- 4.Sería factible siempre y cuando se dispongan al menos 6 Terabytes de almacenamiento y estimo que entre el tiempo del restore, recovery y configuración de la base de pruebas tomaría entre 3 y 4 días."

Al respecto del respaldo físico, este aborda una copia de toda la base de datos y archivos que permiten una recuperación completa de la base de datos, hasta el punto donde se produjo la pérdida de datos, lo que en caso de contingencia es garantía para la recuperación de toda la información, tarea que resulta costosa en términos de almacenamiento, procesamiento y tiempo, como lo refirió en el párrafo anterior el Administrador de la Base de Datos denominada IESSPRD.

De otra parte, el procedimiento *"Política de Respaldos de base de datos DNTI-OSI-003"*, aprobado por el Director de la DNTI encargado, el 18 de marzo de 2014, estableció:

"... 15. Es necesario probar la confiabilidad del sistema de respaldo no solo para respaldar, sino que también para recuperar. Por lo que se efectuaran pruebas de recuperación de las copias de respaldo cada 120 días. Estas pruebas servirán para comprobar que se pueden obtener correctamente los datos grabados en la cinta al momento de ser necesarios."

El servidor coordinador del equipo de Soporte y Plataforma Z10 del Host en la Matriz del IESS, con memorando IESS-DNTI-2015-1323-M de 17 de julio de 2015, y correo de 5 de agosto de 2015, en relación de la necesidad de personal especializado para

realizar las tareas de recuperación de información de las copias de respaldo, manifestó:

> *"... Se conoce que existe un proceso de recuperación, el cual fue probado con el personal que tenía el conocimiento (system programmers) que ya no labora en la institución, alrededor de 5 años atrás.- En el año 2010, con la solución del Host, donde se adquirió el IBM Z10, entiendo que como una prueba de la migración de la antigua plataforma (multiprice 2000) al Z10, realizaron esa prueba, las persona encargadas de este proceso, ya no laboran en la institución..."*

Al respecto, en oficio FAOF-04-2015 de 20 de julio de 2015, del Subdirector de Servicios Informáticos, identificó la necesidad de personal especializado para los procesos de verificación periódica de respaldo de la información.

Las necesidades de personal especializado, constaron en correo electrónico dirigido a los Directores de la DNTI encargados, de 16 de julio y 13 de octubre de 2014; de 21 de enero y 28 de abril de 2015, donde hicieron conocer la situación actual, y necesidades de personal para la Plataforma que soporta las operaciones del sistema Host.

El Coordinador del G.T Servicios Informáticos de la Dirección Provincial del Guayas, en memorando IESS-DPGSAGE- 2015-1854-M de 22 de julio de 2015, informó sobre el último requerimiento de recuperación de las copias de respaldo atendido en el sistema Host Guayaquil, expresó:

> *"... Adjunto el archivo que ha sido preparado, producto del análisis de las estructuras de archivos y la unificación de los 320 cartuchos existentes de las pensiones de jubilación Patronal desde el año 199605 al 201106, cumpliendo en forma conjunta con el Tec, las actividades que se detallaron en el cronograma de trabajo presentado en días anteriores. Cabe indicar que el Téc. , avanzó el día Sábado 5 de julio con la parte del trabajo, así como también durante esta semana hemos dedicado exclusivamente a este trabajo más de 10 horas de trabajo, para poder concluir con el mismo..."*

La importancia de realizar pruebas periódicas, radica en garantizar la efectividad de los procedimientos de generación de las copias de respaldo, estas verificaciones toman mayor relevancia, a medida que las copias de respaldo tienen un mayor tiempo de retención.

CUARENTA Y CUATRO

El Director de Desarrollo Institucional con periodo de gestión comprendido entre el 1 de enero de 2011 y 5 de junio de 2013; el Director Nacional de Tecnología de la Información encargado con periodo de gestión desde el 25 de junio de 2014 hasta el 7 de enero de 2015; el Subdirector de Servicios Informáticos con periodo de gestión desde el 1 de enero de 2011 y 31 de marzo de 2013 y el Coordinador del G.T Servicios Informáticos con periodo de gestión comprendido entre el 16 de noviembre de 2012 y el 30 de abril de 2015, no implementaron mecanismos de prueba periódicos para la verificación de la efectividad de las copias de respaldos en medios físicos de la información de la base de datos y tampoco de las copias de respaldos en cartuchos del sistema Host de Quito y Guayaquil, por lo que no comprobaron la obtención correcta de los datos grabados en los medios de almacenamiento físico (cartuchos), lo que afectó potencialmente la disponibilidad de la información e incrementó el riesgo de interrupción de las operaciones del Instituto; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; articulo 4.- número 4.3.2.4 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos; e inobservaron la Norma de Control Interno: 401-03 Supervisión.

La falta de incorporación de procedimientos de verificación y su frecuencia, que cuente con un plan, con personal independiente a los procesos de generación y recuperación de las copias de información, incidió en la ausencia de esta práctica de control.

No se implementaron mecanismos de prueba periódicas de las copias de respaldo tanto de las base de datos Oracle, tampoco de la información del sistema Host administrado en Quito y Guayaquil, ni se encontraron documentados los planes de prueba aplicables para diferentes escenarios de recuperación de la información de las copias de respaldo.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales a los funcionarios de los cuales, se obtuvieron las siguientes respuestas:

El Subdirector de Servicios Informáticos del IESS con periodo de gestión entre el 1 de enero de 2011 y el 31 de marzo de 2013; con oficio FAOF-04-2015 de 21 de agosto de 2015, en respuesta al oficio 51000000-RSI-EX DDI.53 de 12 agosto de 2015, señaló:

> *"... el personal técnico requerido para realizar las funciones de operación y/o Programación del Sistema Host era limitado, efectivamente no se priorizo las actividades de prueba para verificar la efectividad de los backups contenidos en cartuchos, puesto que la prioridad de la ex Subdirección de Servicios informáticos se centró en el "proyecto de conversión y respaldo de archivos Históricos de los computadores IBM/390 de UIO y GYE ", cuyo propósito era, realizar un análisis minucioso de los archivos vigentes e históricos de los Host...para realizar la migración a la plataforma de Historia Laboral... Para el efecto, mediante oficio N° 630000000-503-2012 de fecha 7 de febrero de 2012, la Subdirección a mi cargo a través de la Ex DDI, solicito... a fin de contratar una consultoría especializada... Por razones externas al IESS, no se lleva a cabo la referida contratación... "*

Lo expuesto, ratificó el comentario de auditoria, en razón de que se expone la limitación de personal especializado para las tareas de recuperación de la información de copias de respaldo, así también la ausencia de pruebas de verificación de las copias de respaldo y la priorización de los esfuerzos para concretar la migración de la información, sin que estos se materialicen.

El Coordinador del G.T Servicios Informáticos de la Dirección Provincial del Guayas, con memorando IESS-DPGSAGE-2015-2184-M de 26 de agosto de 2015, en respuesta al oficio 51000000-RSI-EX DDI.56 de 12 de agosto de 2015, señaló:

> "... La unidad de cartuchos no se encuentra en esta Dirección Provincial..."

Lo mencionado, no cambia el criterio de auditoría, por cuanto la administración de la librería de cartuchos, independientemente de su ubicación física; sigue realizándose por el personal del Grupo de Trabajo de la ciudad de Guayaquil, en coordinación para los trabajos de respaldo con los operadores del grupo de Soporte de la Plataforma Z10 en Quito.

Con oficios 51000000-RSI.EX-DDI.52 y 51000000-RSI.DNTI.55 de 12 de agosto de 2015, se comunicaron los resultados; al Director de Desarrollo Institucional con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; y, al Director Nacional de Tecnología de la Información encargado con periodo de

CUARENTA Y SEIS

gestión comprendido entre el 25 de junio de 2014 y el 7 de enero de 2015, sin obtener respuesta.

Conclusión

El Director de Desarrollo Institucional, el Director Nacional de Tecnología de la Información encargado, el Subdirector de Servicios Informáticos y el Coordinador del G.T Servicios Informáticos, no implementaron mecanismos de prueba periódicos para la verificación de la efectividad de las copias de respaldos en medios físicos de la información de la base de datos y tampoco de las copias de respaldos en cartuchos del sistema Host de Quito y Guayaquil, por lo que no comprobaron la obtención correcta de los datos grabados en los medios de almacenamiento físico (cartuchos), lo que afectó potencialmente la disponibilidad de la información e incrementó el riesgo de interrupción de las operaciones del Instituto.

Recomendación

Al Director Nacional de Tecnología de la información

13. Dictará y establecerá los mecanismos de comprobación periódica de la efectividad de los procedimientos de generación, conservación y recuperación de los respaldos, los que serán documentados. La muestra de cartuchos considerada para estas pruebas, incluirá aquellos de mayor antigüedad y otros de diferentes períodos de retención. La comprobación permitirá medir la integridad de la información recuperada del respaldo, el tiempo de recuperación de la información, reporte de novedades, entre otros aspectos.

Condiciones para la operación de la Plataforma Z10 y equipamiento para el respaldo e impresión, sin mantenimiento

Se constató que en el Centro de Cómputo que contiene la Plataforma Z10, ubicado en el edificio Matriz del IESS no se efectuó el mantenimiento preventivo ni correctivo, al sistema de aire acondicionado ni a la red de suministro eléctrico durante los años 2014 y 2015, similar situación; sucedió con las unidades de cartucho e impresoras (equipos periféricos del sistema Host), durante los años 2013, 2014, 2015.

- Sobre las condiciones ambientales y de suministro del Centro de Cómputo que contiene la Plataforma Z10, se efectuaron las siguientes gestiones:

El servidor a cargo de la coordinación del grupo de Soporte y Plataforma Z10, mediante correo electrónico de 16 de julio de 2014, comunicaron al Director de la DNTI encargado, y señalaron:

> *"... Aire acondicionado para el Data Center del Edificio Matriz: se adjunta el informe técnico y las ofertas enviadas a infraestructura.- No se cuenta con contrato de mantenimiento"*

El técnico informático a cargo de grupo de Soporte y Plataforma Z10, con memorando IESS-DNTI-2014-1253-M de 27 de agosto de 2014, informó al Director Nacional de Tecnología de la Información encargado:

> *"... me permito informar a usted, que se han suscitado problemas a nivel de sistema de la red eléctrica en el Data Center de la Plataforma Z10 del edificio Matriz, producto de lo cual los equipos llegaron a apagarse bruscamente..."*

Con correo electrónico de 21 de enero de 2015, el Coordinador del área de Soporte y Plataforma Z10, informó al Director de la DNTI encargado con periodo de gestión comprendido entre el 8 de enero de 2015 y el 21 de abril de 2015, respecto de las necesidades de personal, licenciamiento, mantenimiento de la plataforma Z10 y equipos periféricos (unidades de cartuchos e impresoras de Quito y Guayaquil) y equipos de acondicionamiento (aire), suministro de energía, contingencia y estabilización, advirtiendo acerca del potencial efecto adverso.

Mediante correo electrónico de 28 de abril de 2015, del Coordinador del grupo de Soporte y Plataforma Z10, al Director de la DNTI encargado, se recordó el informe y pedido de 21 de enero de 2015.

Al respecto, el Director Nacional de Tecnología de la Información con periodo de gestión comprendido entre el 8 de enero de 2015 y 21 de abril de 2015, en respuesta al requerimiento de información de auditoria realizado con oficio 51000000. RSI.DNTI.049 de agosto de 4 de 2015, con oficio AGBB-AI-003-2015 de 18 de agosto de 2015, señaló:

"... En el inicio del período de mi gestión desde el 10 de enero de 2015, la plataforma Z10 no disponía de un contrato de mantenimiento y soporte técnico vigente, lo cual se confirma en el informe adjunto emitido por el Ing..., aspecto que demuestra que este evento se venía arrastrando desde el año 2014.- a mi llegada a la Institución en la fecha expuesta, existía un PAC 2015 establecido por la DNTI en el año 2014, el cual sufrió recortes presupuestarios a inicios de año, dejando muchos proyectos incompletos para poder ejecutarlos.- existían inconvenientes con los presupuestos establecidos en el PAC 2015, así como inconvenientes de no inclusión de ciertos procesos de contratación requeridos para la operación de los servicios tecnológicos de la DNTI.- En función de lo expuesto, una vez revisado el PAC 2015, corregidos los inconvenientes presupuestarios, se generó el memorando IESS-DNTI-2015-467-M del 23 de marzo de 2015... donde se solicita y justifica al Coordinador General de Gestión Estratégica, realizar una reforma al PAC 2015, tomando en cuenta los antecedentes expuestos... uno de estos informes que se adjunta es el emitido por el Coordinador del área de TIC, donde se en(sic) el ítem 5, se menciona que existieron ciertos procesos de contratación que no fueron incluidos en el PAC 2015, y que en la presente propuesta de reforma se los debe incluir. Uno de esto procesos es el relacionado al aire acondicionado requerido para la plataforma Z10.- Dentro de este PAC, se disponía los siguientes procesos de contratación relacionados a la Plataforma Z10: Renovación de licencias de uso ZVSE y ZVM; Mantenimiento y Soporte de Equipos IBM Mainframe; Adquisición de Aire acondicionado de la Matriz (A espere de asignación presupuestaria producto de la reforma al PAC 2015 solicitada).- es importante reiterar que en el inicio de mi gestión, no existían desarrollados estudios técnicos, términos de referencia, y la información requerida para el inicio de los procesos de contratación... aspecto que retrasa de manera considerable la ejecución del PAC 2015.- Los procesos de contratación mencionados venían a solventar las necesidades expresadas en el informe del Ing, relacionado con... ausencia de mantenimiento de la plataforma Z10, con este mantenimiento vigente, solventar el problema de la fuente alarmada, así como disponer de un aire acondicionado para mejorar la climatización existente, y con ello poder disponer del UPS desconectado operativo.- Respecto de la reforma al PAC 2015, hasta el fin de mis funciones (21 de abril de 2015), desconozco si se dio la aprobación y reforma solicitados... "

Lo manifestado, demostró la gestión efectuada por el Director Nacional de Tecnología de la Información, sin embargo no se concretaron finalmente los mantenimientos requeridos. Por lo que el equipamiento tecnológico para el procesamiento, almacenamiento y demás que soportan la operación del Sistema Host, se encuentro expuesto a un inminente riesgo, debido a que trabajaron en condiciones que sobre exponen la capacidad permitida por el equipamiento, sin los estándares recomendados, para su óptimo funcionamiento. Así también al respecto del sistema de suministro eléctrico, el cual debe de ser estabilizado y continuo de manera de evitar fallos en los discos y equipos.

- En relación al mantenimiento de los equipos periféricos de la Plataforma Z10 del Host: unidades de cartuchos e impresoras, se desprendieron los siguientes hechos:

El Subdirector de Servicios Informáticos, con periodo de gestión comprendido entre el 1 de enero de 2011 y 31 de marzo de 2013, con oficio FAOF-04-2015 de 20 de julio de 2015, informó:

> *"... por políticas de la empresa IBM, a partir del año 2012 los equipos periféricos del Host ya no constaban con servicio de mantenimiento preventivo-correctivo debido a que se consideraban como obsoletos, sin embargo, por necesidad Institucional, la Subdirección de Servicios informáticos gestionó el servicio de mantenimiento con proveedores especializados a través de contratos complementarios, que se pagaban con un fondo rotativo que manejaba la Subdirección y cuyo monto ascendía a USD 3.000,00 por cada reposición.- los equipos obsoletos eran básicamente la unidad de cartuchos (3490), y la impresora matricial de alta velocidad(6400).- Como se explicó..., la Subdirección de Servicios Informáticos, garantizó el mantenimiento de los dispositivos descritos a través de servicios per call a las empresas especializadas en esta línea, y cuyos costos se cancelaban con el fondo rotativo hasta el año 2011 y por medio de caja chica a partir del año 2012..."*

Con memorando de 6 de agosto de 2013, el encargado del área de Soporte de la Subdirección de Servicios Informáticos, solicitó al Director de Desarrollo Institucional encargado, la autorización para realizar un contrato de mantenimiento preventivo, correctivo y de soporte técnico de las unidades de cartucho e impresoras del Centro de Cómputo de la Plataforma Z10, al que se adjuntó la siguiente documentación:

- La Subdirección de Bienes y Servicios Generales, junto oficio de pedido No. 63000000-247 de 29 de enero de 2013, presentó la certificación PAC No: CPAC-50-SBSG-2013, el 22 de febrero de 2013.

- De los términos de referencia, elaborado por el personal técnico del grupo de Soporte y Plataforma Z10, se desprende lo siguiente:

> *"... **Problema existente:** Los dispositivos periféricos, unidades de cartuchos e impresoras tienen un nivel de funcionamiento constante, permitiendo dar continuidad a las actividades de operación del sistema, dispositivos que están expuestos por el tiempo de fabricación y uso a daños los cuales impedirían el normal funcionamiento de la plataforma, provocando la no atención de requerimientos a nivel nacional y soporte de respaldos de la información del Host tanto de UIO y GYE."*

Con memorando DDI-OP-363-2013 de 6 de septiembre de 2013, el Coordinador de Producción y Operaciones encargado, señaló, respecto del pedido efectuado por el servidor de la Subdirección de Servicios Informáticos, lo siguiente:

> *"... me permito informar que basado en el informe técnico se recomienda replantear los TDR tomando en cuenta uno solo mantenimiento por el período 2013, y realizar un estudio de factibilidad para determinar la continuidad de los sistemas de respaldo e impresión y en caso de afirmar la continuidad contemplar un rubro en el PAC 2014 para mantenimiento y repotenciación del stock de cartuchos"*

El informe técnico correspondiente al mantenimiento preventivo, correctivo y soporte técnico de las unidades de cartuchos e impresoras del Data Center de la Plataforma Z10, presentado el 4 de septiembre de 2013, por el Coordinador de Infraestructura Tecnológica, expuso lo siguiente:

En el numeral 2. Desarrollo

> *"... Los equipos utilizados para estos servicios actualmente no disponen de ningún contrato de mantenimiento ni garantía técnica desde la caducidad de la misma, por lo que el personal de esta unidad requirente ha dado soporte a problemas menores, pero por su uso y tiempo de operación es necesario disponer de un contrato de mantenimiento que garantice la reposición de repuestos en caso de requerirlos sin generar costos adicionales al IESS"*

En el numeral 3. Conclusiones

> *"... Los equipos por su estructura, tiempo de fabricación y uso presenta problemas de funcionamiento que han sido soportados por la subdirección de servicios informáticos en la parte básica, pero al momento que se requieran repuestos o el daño sea critico no estamos en la capacidad de responder a estos eventos, por lo que es necesario y urgente iniciar con el proceso de contratación.- Los equipos desde la finalización de la garantía técnica hasta la fecha no han tenido un contrato de mantenimiento ni soporte técnico.- La disponibilidad de la plataforma es necesario para brindar servicio de backup e impresión a los sistemas Host.- Los documentos, estudios técnicos (TDR) y presupuesto referencial a la fecha se encuentra en el área de contratación pública de la DDI desde julio de 2013. Con un presupuesto referencial (más alto) de $ 4.862,32, proceso asignado por el Ing(...).- Existe disponibilidad de partida presupuestaria No. 53040202 correspondiente a mantenimiento de maquinaria y equipo.- Las unidades de cartuchos e impresoras están descontinuadas por el fabricante, por tal razón el servicio es ofrecido por otras empresas..."*

CINCUENTA Y UNO

En el numeral 4. Recomendaciones

> *"... Dada la fecha es necesario replantear, el tipo de servicio requerido para los equipos y solicitar nuevas proformas contemplando un mantenimiento.- Por el tiempo de uso y magnitud de respaldo es necesario realizar un estudio de factibilidad para repotenciar el stock de cartuchos que se dispone para este sistema, así como, la continuidad o no de la utilización de backups e impresoras..."*

De lo expuesto, los estudios técnicos (TDR) y proformas para el establecimiento del valor referencial del servicio requerido, se encontraban en el área de contratación pública de la DDI desde julio 2013; sin embargo, los informes técnicos remitidos por los Coordinadores de Producción y Operaciones e Infraestructura, se elaboraron y remitieron al Director Nacional de Tecnologías de la Información encargado, en el mes de septiembre de 2013, con lo que su gestión fue extemporánea, debido a las fechas en que las proformas de los proveedores de servicio fueron emitidas (15 y 17 de julio de 2013 respectivamente), en consecuencia las proformas inmersas en el proceso perdieron su validez, hecho que se ratifica en el numeral 4 Recomendaciones, donde sugiere, al considerar la fecha, replantear el tipo de servicio requerido para los equipos y solicitar nuevas proformas contemplando un mantenimiento.

Sobre este tema, con memorando IESS-DNTI-2015-1606-M de 24 de agosto de 2015, el informático especialista, Coordinador de Producción, informó:

> *"... este continuo ir y venir de autoridades, directores y personal, provoco una dilatación de los tiempos de ejecución de proyectos y procesos en espera de una nueva revisión y aprobación de cada una de las autoridades entrantes, retardando así el ritmo de avance de lo planificado... A partir del año 2014, se mantiene las prioridades en el manejo de los procesos antes indicados, evidencia de esto es el archivo consolidado PAC2014 de proyectos a ser ejecutados en producción..."*

De lo informado, se desprende que el mantenimiento de Unidades de cartucho e impresoras periféricos de la plataforma Z10, fue considerado en la planificación del PAC2014, remitida por el Coordinador de Producción, sin que finalmente esta se considere en el PAC aprobado.

Con memorando IESS-DNTI-2015-1370-M de 27 de julio de 2015, el Director Nacional de Tecnología de la Información del IESS, hizo entrega de: *"Copias del POA y PAC aprobado y ejecutado correspondientemente a los años 2011-2012-2013-2014"*, de

donde se desprende que no se concretaron las gestiones acerca del mantenimiento y soporte de los equipos periféricos de la plataforma Z10 (Host).

Durante el segundo semestre de 2013, no se atendieron los requerimientos realizados de mantenimiento preventivo y correctivo y soporte técnico de los dispositivos periféricos unidades de cartucho e impresoras de la Plataforma Z10 del Host, sin que de seguimiento al análisis al respecto de la continuidad de los servicios (generación y recuperación de respaldo e impresión de órdenes de trabajo del Sistema Host) que hacen uso de los referidos periféricos, incrementando el riesgo de daños los cuales impedirían el normal funcionamiento de la plataforma, provocando la falta de atención de requerimientos a nivel nacional y soporte.

El Director Nacional de Tecnología de la Información encargado con periodo de gestión desde el 25 de junio de 2014 hasta el 7 de enero de 2015, no precauteló la ejecución de procedimientos de mantenimiento del equipamiento del Centro de Cómputo de la Plataforma Z10, situación que no garantizó la seguridad de las operaciones, la protección de las instalaciones físicas, el óptimo estado de funcionamiento de los equipos que procesan, almacena, y respaldan la información del sistema Host Quito y Guayaquil, sobre exponiendo la capacidad permitida del equipamiento e incrementado el riesgo a fallas de los equipos obsoletos y sin soporte; incumpliendo lo dispuesto en el artículo 77.- Máximas autoridades, titulares y responsables, número 2 Autoridades de las unidades administrativas y servidores, letra a), de la Ley Orgánica de la Contraloría General del Estado; los artículos 95.- Plan de mantenimiento y 99.- Clases de Mantenimiento del Reglamento general sustitutivo para el manejo y administración de bienes del sector público; e inobservaron las Normas de Control Interno: 401-03 Supervisión, 406-13 Mantenimiento de bienes de larga duración, 410-09, Mantenimiento y control de la infraestructura tecnológica, 410-10 Seguridad de tecnología de información.

No se efectúo el mantenimiento preventivo y correctivo de componentes de la infraestructura (aire acondicionado, unidades de cartucho e impresoras) y suministro del Centro de Cómputo de la Plataforma Z10 del sistema Host ubicada en el edificio Matriz de la ciudad de Quito, sin que se garantice la continuidad de los servicios y la protección de los equipos que procesan, almacenan, y respaldan la información del sistema Host administrado en Quito y Guayaquil.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales al Director Nacional de Tecnología de la Información encargado con período de actuación desde el 25 de junio de 2014 y 7 de enero de 2015, con oficio 51000000-RSI.DNTI.55 de 12 de agosto de 2015, sin recibir respuesta.

Posterior a la comunicación de resultados realizada el día 31 de agosto de 2015, con comunicación, de 25 de septiembre de 2015, en atención a las comunicaciones 51000000.RSI.DNTI.57 y 80; el Director Nacional de Tecnología encargado, con período de gestión comprendido entre el 10 de Enero y el 21 de abril de 2015, ratifica su posición comunicada con oficio AGBB-AI-003-2015 de 18 de agosto de 2015, la cual ratifica los comentarios de auditoria, documentado su afirmación de la gestión realizada, punto de vista aceptado por el equipo de auditoría.

Conclusión

El Director Nacional de Tecnología de la Información encargado no precauteló la ejecución de procedimientos de mantenimiento del equipamiento del Centro de Cómputo de la Plataforma Z10, situación que no garantizó la seguridad de las operaciones, la protección de las instalaciones físicas, el óptimo estado de funcionamiento de los equipos que procesan, almacena, y respaldan la información del sistema Host Quito y Guayaquil, sobre exponiendo la capacidad permitida del equipamiento e incrementado el riesgo a fallas de los equipos obsoletos y sin soporte.

Recomendación

Al Director Nacional de Tecnología de la información

14. Gestionará el mantenimiento del aire acondicionado, del suministro de energía eléctrica del Centro de Cómputo, de las unidades de cartuchos (IBM 3490) e impresoras (6400) de la plataforma Z10, los cuales soportan las operaciones del sistema Host, precautelando su óptimo funcionamiento mientras se mantengan sus operaciones y demás sistemas.

Pruebas de efectividad de los procedimientos de recuperación de las copias de respaldo

Los procesos de recuperación de las copias de respaldo lógico son ejecutados en el ambiente productivo, con el uso de nombres nuevos para la creación de las estructuras de datos recuperados, estos procesos están sujetos a la eliminación de los datos recuperados una vez concluida la prueba. De una muestra de 3 pruebas realizadas se observó, lo siguiente:

1. La información proporcionada por la Directora del Sistema de Pensiones con Memorando IESS–DSP–2015 – 2026 - M de 27 de julio de 2015, del mes de febrero de 2015, registra el monto de USD 41 066 782,47, correspondiente al pago de nómina situada en la Dirección Provincial de Pichincha, correspondiente al mes de junio de 2012, en tanto que, la información consultada en la base de datos en línea, el valor fue de USD 41 070 439,98 y en la recuperada de la copia de respaldo, ascendió a USD 42 125 149,47; lo que determinó diferencias tanto en valores como en número de registros.

2. No fue posible obtener la información respaldada en cartuchos de cintas, sobre Glosas por Mora y Responsabilidad Patronal de la Dirección Provincial de Napo del mes de junio de 2013, a pesar de que existe la información de la base de datos en línea.

La Norma de Control Interno 401-03 Supervisión, dice:

> *"... Los directivos de la entidad, establecerán procedimientos de supervisión de los procesos y operaciones.- La supervisión de los procesos y operaciones se los realizará constantemente para asegurar que se desarrollen de acuerdo con lo establecido en las políticas, regulaciones y procedimientos..."*

La Norma de Control Interno 410-12 Administración de soporte de tecnología de información, establece:

> *"... La Unidad de Tecnología de Información definirá, aprobará y difundirá procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen. 10. Administración adecuada de la información, librerías de software, respaldos y recuperación de datos..."*

Las políticas configuradas en la herramienta TSM, que fueron implementadas para la obtención de los respaldos analizados en la prueba, corresponden al período comprendido entre el 7 de octubre de 2010 hasta el 19 de mayo de 2014.

Con memorando IESS-AI-2015-1019-ME de 6 de agosto de 2015, solicitamos información sobre el hecho comentado al Director Nacional de Tecnología de Información, sin recibir respuesta; así como también con Memorando IESS-AI-2015-1103-ME de 21 de agosto de 2015, a la Directora del Sistema de Pensiones, al respecto la Directora de Pensiones, se ratificó con memorando IESS-DSP-2015-2298-M de 25 de agosto de 2015:

> *"... debo informar que la Dirección del Sistema de Pensiones se ratifica en la información entregada, ya que no existen errores en relación a los datos proporcionados de manera física..."*

El Coordinador de Infraestructura, mediante correo electrónico de 30 de julio de 2015, señaló:

> *"... existe un problema a nivel de TSM no me despliega la información del 2013, no tengo ningún mensaje de error, estoy solicitando al vendedor de los driver del año anterior si me pueden dar una mano, el tema es que el técnico no está en la ciudad de Quito..."*

Lo señalado por el Coordinador de Infraestructura, evidenció la imposibilidad de recuperación de la información de las copias de respaldo sobre Glosas por Mora y Responsabilidad Patronal de la Dirección Provincial de Napo del mes de junio de 2013, en el momento que se solicitó.

Sobre las diferencias establecidas en el ejercicio de recuperación practicado, desde la copias de respaldo que correspondieron al pago de nómina situada en la Dirección Provincial de Pichincha, correspondiente al mes de junio de 2012, no se establecieron las razones de la novedad presentada. El personal de tecnología que brindo apoyo a las pruebas desconocía si se disponía de pistas de auditoria (fecha de creación, usuario que lo creo, última modificación y usuario que lo modificó) y tablas históricas que permitirían realizar verificaciones adicionales a la información de la base de datos denominada IESSPRD.

Podemos también afirmar que, del número de pruebas efectuadas (3) dos de ellas no fueron efectivas y confiables durante los períodos 2012 y 2013, lo que demuestra que la efectividad de los procedimientos de generación y recuperación corresponde al 33%.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales al Director de Desarrollo Institucional con periodo de gestión comprendido entre el 1 de enero de 2011 y el 5 de junio de 2013; con oficio 51000000-RSI.DNTI.52 de 12 de agosto de 2015, sin recibir respuesta.

Posterior a la comunicación de resultados realizada el día 31 de agosto de 2015, en comunicación de 7 de septiembre de 2015, el Director Nacional de Tecnología de la Información encargado, en referencia a las diferencias de la cantidad de los registros y valores recuperados en la Nómina de pensiones de la Dirección de Provincial de Pichincha situada en junio de 2012, dijo:

> *"... se volvió a realizar la prueba de restauración de la información y se obtuvieron los siguientes resultados.- Consulta de Datos en Línea (DNTI) USD 41, 066,782.47.- Reporte cortado al 13 de junio de 2012(SP) USD 41, 066,782.47.- El resultado permite indicar que no hay diferencias entre lo guardado en respaldos y la información en línea, la diferencia se presentó debido a la utilización de una consulta incorrecta la ocasión que se realizó la prueba, para evidencia se adjunta documento de sustento..."*

De lo dicho, aunque efectivamente, los nuevos resultados coinciden; sin embargo la documentación adjunta al memorando remitido, muestra lo siguiente:

- La consulta a la base de datos y su respaldo, tiene fecha 25 de agosto de 2015, es decir, 29 días posteriores a la validación inicialmente preparada con fecha de 24 de julio de 2015

- La consulta efectuada en el mes de julio tuvo como medida de validación, una tabla, en tanto que la realizada en el mes de agosto hace relación a tres tablas de la base de datos.

- En el reporte con fecha de 25 de agosto de 2015, se presentaron campos de información adicional, que permitirían realizar una análisis con mayor detalle de los

CONTINUA Y 82.12

registros obtenidos, para cada una de las estructuras consideradas en la consulta preparada en julio (históricos y pistas de auditoria).

Lo descrito y a pesar que la DNTI demostró, en una segunda instancia, la consistencia entre los datos (base de datos en línea, el reporte entregado por la Directora de Pensiones de la Nómina a junio de 2012 de la Dirección Provincial de Pichincha y la información recuperada de la copia de respaldo); expuso la falta de confiabilidad en sus procedimientos y criterios de consulta empleados para la extracción de la información requerida de las bases de datos, a falta de la automatización de un reporte para el efecto. Por lo tanto se mantiene el criterio de auditoria en cuanto la efectividad de las pruebas de recuperación de las copias de respaldo.

Conclusión

Las políticas configuradas en la herramienta TSM para la generación automática de copias de respaldo en medios de almacenamiento físico del período comprendido entre: 7 de octubre de 2010 hasta el 19 de mayo de 2014, no garantizaron la efectividad de recuperación de la información, en razón de que 2 de las 3 pruebas efectuadas a los procesos de recuperación dentro del referido periodo, presentaron novedades en sus resultados, lo que evidenció la ausencia de pruebas periódicas efectuadas a las copias de respaldo y de procedimientos para la comprobación de la integridad de información recuperada, así como la necesidad de automatización de reportes de la nómina y estándares de consulta probados. Determinando un 33% de efectividad de los procedimientos de recuperación, circunstancia que incrementó el riesgo en la disponibilidad y confiabilidad de la información recuperada de las copias de respaldo.

Recomendaciones

Al(a) Directora(a) del Sistema de Pensiones

15. Identificará con apoyo de la Dirección de Procesos y la Dirección Nacional de Tecnología de la Información, las necesidades de automatización correspondientes a los reportes transaccionales e históricos del Pago de nómina, generando los requerimientos funcionales necesarios para su implementación por parte de la

Dirección Nacional de Tecnología de la Información, a fin de contar con mecanismos de consulta fiable, probados y aceptados por la unidad propietaria de la información.

Al Director Nacional de Tecnología de la Información

16. Dictará y establecerá mecanismos que permitan realizar pruebas de efectividad de recuperación de las copias de respaldo de la información, contando con un plan de prueba que contemple la información actualizada del modelo de datos, los scripts (sentencias de consulta a la base de datos), documentados y probados para la evaluación de la consistencia (integridad) de la información, contando con el aval de las áreas usuarias acerca del resultado de consultas y reportes de la información alojada en la base de datos y/u otro medio físico o digital de almacenamiento.

Recuperación de copias de respaldos del Sistema Host en riesgo

Las copias de respaldo del sistema Host se generan en el Centro de Cómputo ubicado en el Edificio Matriz del IESS ubicado en la ciudad de Quito y son obtenidas a través de las unidades de cartuchos Modelo IBM 3490, las cuales se encuentran obsoletas, sin contar con personal especializado suficiente para el soporte de las operaciones de generación y recuperación de estos respaldos, poniendo en riesgo su disponibilidad.

El sistema Host y su plataforma se encuentran operativos, constituyéndose en el Sistema Histórico de la historia laboral del Instituto Ecuatoriano de Seguridad Social.

Lo dispuesto en el anexo 2, numeral 6, Políticas Presupuestarias, 6.1 Generales en la Resolución C.D 461 de 26 de diciembre de 2013, donde señaló:

> *"... Desde el 1 de enero la Dirección Nacional de Afiliación mantendrá una sola base de datos en la que conste la historia laboral y prestacional de todos los afiliados y pensionistas del IESS, hasta el 31 de marzo se darán de baja los sistemas Host y Micros y su información será migrada al sistema único de historia laboral"*

Estableció la necesidad Institucional de contar con una única base de datos para la historia laboral.

La plataforma Z10 del sistema Host (Quito y Guayaquil) y su información, a la fecha de ejecución de nuestra acción de control, fue insumo para algunos procesos efectuados por la nueva plataforma de Historia Laboral, como por ejemplo señalamos:

- Host Guayaquil, en el período 2011 – 2015, colaboró en:

    - La carga Cuenta Individual de Fondos de Reserva en Historia Labora (HL)
    - Envió de información para bloqueo de aportes en HL

- Host Quito

    - Para completar determinados trabajos por Ej. para entregar una prestación de Cesantía de afiliado fallecido, en HL, calificación a los derecho habientes (familiares), así como la repartición de valores.

    - Certificados de deuda, fondos de reserva, montepíos, cobro de préstamos en mora registrados en el sistema Host, y otros.

    - Envío de Archivos a HL.-*"SEMANAL: QRM11 (MORA EN PRESTAMOS Host para control den Prestaciones y servicios).- POR DEMANDA: AIM01, FRM03, FRM06 (cuando faltan aportes o fondos de reserva).- MENSUAL: PAM04 (para emisión de estadísticas)."*

Sobre el personal especializado, necesario para recuperación de información de las copias de respaldos del Sistema Host, durante los años 2014 y 2015, se emitieron informes remitidos a los diferentes Directores de la DNTI de turno, con referencia a la Situación actual de esta Plataforma, el encargado, informó:

> *"... no se cuenta con system programmers y operadores.- que se requieren para el proyecto de cierre de la plataforma, mantener en línea el servicio y para el apoyo en visión de utilización del IBM /Z10 en el core de la DNTI..."*

A través de correos de 9 y 23 de enero de 2014, el coordinador a cargo del grupo de Soporte y Plataforma Z10, insistió en dar a conocer la situación de las necesidades de personal, y señaló:

"... analice con estos eventos y al no tener un especialista en Sistema operativo (System Programmer) mantener el criterio de soporte técnico que apoye al proceso del proyecto.- vamos a necesitar un soporte externo que sea especialista en el sistema operativo y System Programmer del ZVSE (host)..."

Sobre los comunicados, efectuados por el coordinador a cargo del grupo de Soporte y Plataforma Z10, no se presentó documentación de gestión por parte de los Directores de la DNTI.

Con oficio FAOF-04-2015 de 20 de julio de 2015, respecto de las gestiones efectuadas acerca la migración de la Plataforma Host, el Subdirector de Servicios Informáticos, con periodo de gestión entre el 1 de enero de 2011 y 31 de marzo de 2013, dijo:

"... los equipos obsoletos eran básicamente la unidad de cartuchos (3490), y la impresora matricial de alta velocidad(6400).- previo el apagado de la Plataforma Host, se requería que en la plataforma de Historia Laboral administrada por al Ex DDI, se desarrollen los aplicativos que permiten a las Áreas usuarias llevar a cabo sus procesos de actualización y consulta de información que estaba en el ambiente de producción del Host, así como la consulta de información histórica almacenada en medios magnéticos pasivos (8000 cartuchos aproximadamente). Situación que no se llevó a cabo..."

Los Proyectos *"Conversión y respaldo de archivos Históricos de los computadores IBM/390 de UIO y GYE"* y *"Migración de información del computador IBM Z/SERIES (HOST) a la nueva plataforma"*, en donde entre otros fueron identificaron los siguientes riesgos, calificados como *"ALTOS"*:

"... Problema 1.- Información histórica en cintas, no disponible; Causa: Unidad de cinta dañada; Problema 5.- Salida de Servicio los Host de UIO y GYE; Causa: Daño irreparable de los equipos; Problema 8.- Estructura de archivos no identificadas; Causa: No existe documentación y/o programas con dichas estructuras...Problema 1.- Información histórica en cartuchos no disponible.- Causa: Unidad de Cartuchos dañada; Problema 3.- Salida de servicio del Host.- Causa: Daño irreparable de los equipos; Problema 6.- Estructuras de archivos no identificadas.- Causa: No existe documentación y/o programas con dichas estructuras.- Problema 8.- Insuficiente personal calificado en el uso de herramientas del Host.- Causa: Renuncia del personal ..."

Así también, el mencionado proyecto de migración señaló:

"... Existen aproximadamente 8500 cartuchos magnéticos con información histórica, un porcentaje significativo no se encuentra en los discos que están en el ambiente de producción y que luego del aval de las Áreas Usuarias debería ser migrada a la nueva plataforma para consulta en caso de juicios o demandas contra la Institución..."

SESENTA Y CINCO

Con memorando IESS-DNTI-2015-1370-M de 27 de julio de 2015, el Director Nacional de Tecnología de la Información, informó acerca el Proyecto de Cierre Host y Micros, donde señaló que el proyecto de migración, considera las etapas de análisis, diseño, casos de uso para el desarrollo de las nuevas funcionalidades así como la migración de la información en línea, respaldada e histórica a través de la presentación de una propuesta para el desarrollo interno y la propuesta de externalizar el desarrollo, existiendo procesos de contratación los cuales han resultado desiertos por el riesgo y complejidad del proyecto, consideró además, lo siguiente:

> *"... El proyecto de cierre host y micros ha sido implementado parcialmente, es así que se ha completado la migración de estructuras e información desde los sistemas host y micros hacia la plataforma historia laboral, entendiéndose por historia laboral a la migración a arquitectura web, con bases de datos relacionales. Sin embargo era y es necesario replicar y desarrollar la nueva arquitectura ciertas funcionalidades aun usadas en Host y micros. Por lo que se realizó el análisis respectivo para la generación de casos de uso y el mapeo de las estructuras de datos antiguas a las nuevas"*

De lo expuesto, el Sistema Host y su plataforma, al 30 de abril de 2015, fecha de corte del examen especial, se encontraron operativos y utilizados a nivel nacional (a pesar de considerarse histórica); la necesidad de migración establecida a fin de contar con una única base de datos, se suma al factor de obsolescencia de la tecnología inherente a este sistema, lo que ocasiona que los procedimientos de recuperación en casos de fallo del sistema; se vuelven críticos, ya que dependen de la disponibilidad de los cartuchos pasivos y de respaldo del sistema Host con información administrada por Quito y Guayaquil, y del personal especializado disponible, volviéndose en sí mismas tareas costosas, en razón de los tiempos que toman y el conocimiento especializado requerido.

La Norma de Control Interno 100-03 Responsables del control interno, manifiesta:

> *"... Las servidoras y servidores de la entidad, son responsables de realizar las acciones y atender los requerimientos para el diseño, implantación, operación y fortalecimiento de los componentes del control interno de manera oportuna, sustentados en la normativa legal y técnica vigente y con el apoyo de la auditoría interna como ente asesor y de consulta..."*

La Norma de Control Interno 401-03 Supervisión, dispone:

> *"... Los directivos de la entidad, establecerán procedimientos de supervisión de los procesos y operaciones.- La supervisión de los procesos y operaciones se los realizará constantemente para asegurar que se desarrollen de acuerdo con lo establecido en las políticas, regulaciones y procedimientos;"*

La Norma de Control Interno 410-03 Plan informático estratégico de tecnología, señala:

> *"... La Unidad de Tecnología de Información elaborará planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, estos planes incluirán los portafolios de proyectos y de servicios, la arquitectura y dirección tecnológicas, las estrategias de migración, los aspectos de contingencia de los componentes de la infraestructura y consideraciones relacionadas con la incorporación de nuevas tecnologías de información vigentes a fin de evitar la obsolescencia..."*

El numeral 4.3.3.9 del Capítulo V.- De la Gestión de Riesgo Operativo del Libro I.- Normas Generales para las instituciones del Sistema Financiero Titulo X.- De la Gestión y Administración de Riesgos, señala:

> *"... Con el objeto de garantizar que el proceso de adquisición, desarrollo, implementación y mantenimiento de las aplicaciones satisfagan los objetivos del negocio, las instituciones controladas deben contar al menos con lo siguiente.- 4.3.3.9 Procedimientos de migración de la información, que incluyan controles para garantizar las características de integridad, disponibilidad y confidencialidad..."*

Las copias de respaldo del sistema Host, se encuentran en riesgo debido al factor de obsolescencia de los equipos para la generación de copias de respaldo, así como la limitación del personal especializado, y las tareas de migración que se encuentran en proceso y sin concluir.

Conforme a lo establecido en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado, se comunicó los resultados provisionales a los funcionarios de los cuales, se obtuvieron las siguientes respuestas:

Se obtuvo la siguiente respuesta:

El Director Nacional de Tecnología de la Información encargado, con período de gestión desde el 16 de diciembre de 2013 hasta el 28 de enero de 2014, en respuesta al oficio 51000000-RSI-DNTI.59 de 12 agosto de 2015, señaló:

> *"...Mi encargo como Director Nacional de Tecnología de la Información (encargado) inicio el 16 de diciembre de 2013 y finalizo el 29 de enero de 2014, es decir, un total de 30 días laborables...En el período de mi encargo respecto a las políticas que reglamentan las actividades relacionadas con tecnología de la información con el fin de regular y asegurar la calidad de los servicios de tecnologías de información que presta la institución, se remitió al Subdirector General de la época con el propósito de gestionar ante la máxima autoridad el conocimiento, la formalización y la comunicación de las Políticas y Procedimientos inherentes al área de tecnologías de la información..."*

El criterio expuesto señala la prioridad concedida a la aprobación del PAC, en tanto que, la reglamentación de las políticas y actividades relacionadas con la tecnología de la información fueron direccionadas hacia instancias con menor capacidad de decisión y regulación, limitando de esta manera su accionar a propuestas que no pasaron de su propio conocimiento y de su inmediato inferior jerárquico.

Con oficios 51000000-RSI.DNTI.55, 57 y 58 de 12 de agosto de 2015, se comunicaron los resultados provisionales a los Directores Nacionales de Tecnología de la Información encargados en sus correspondientes periodos de gestión comprendidos desde el 9 de enero de 2014 al 31 de marzo de 2014; desde el 25 de junio de 2014 al 7 de enero de 2015 y desde el 8 de enero de 2015 al 21 de abril de 2015; y respectivamente; sin recibir respuesta.

Posterior a la comunicación de resultados realizada el día 31 de agosto de 2015, con oficio No. 009-RCH-IESS-2015 de 3 de septiembre de 2015, el Director Nacional de Tecnología de la Información con periodo de gestión comprendido entre el 17 de octubre al 16 de diciembre de 2013, en referencia a la comunicación de resultados se ratifica en lo expresado en contestación al oficio 51000000-RSI-DNTI.61 de 12 agosto de 2015, señalando que su accionar fue limitado durante su corto período de gestión; criterio aceptado por el equipo de auditoría.

> *"... Respecto al proceso de cierre de Host, este proyecto se ha venido arrastrando desde años anteriores, a mi llegada a la Dirección de la DNTI, tuve conocimiento al respecto y de su poco avance que se ha tenido, es por ello que se decidió asignar un nuevo gerente de proyecto, hacer una análisis detallado de la situación actual, así como determinar las necesidades para avanzar lo*

más pronto posible, es así que se pudo determinar que el cuello de botella era la necesidad de personal para el desarrollo de los módulos existentes, así como la formalización de los casos de uso por parte de las unidades de negocio responsables funcionales, de esto se decidió conformar el proyecto para contratación de fábrica de desarrollo, así como hacer un trabajo conjunto con las unidades de negocio para la formalización de los caso de uso faltantes, insumo fundamental para los procesos de desarrollo... "

Lo mencionado, ratifica los comentarios de auditoria, sin embargo la alta rotación de los Directivos de la DNTI, afectó los planes, ejecución y su implementación, manteniéndose las circunstancias descritas, sin variación significativa sobre los planes de migración hacia la base de historia laboral y el desarrollo de las aplicaciones necesarias para el cierre del sistema host.

Sobre este tema, es importante señalar que las circunstancias descritas, se han visto afectadas por los continuos cambios en el nivel jerárquico, de estructura y de procesos que está atravesando el Instituto, lo cual ha producido suspensión o cambios de los planes trazados, los cuales, también requieren la coordinación e involucramiento de las áreas usuarias, al respeto del cierre de la plataforma Z10 y migración del sistema Host; sin embargo lo dispuesto en el anexo 2, numeral 6, Políticas Presupuestarias, 6.1 Generales en la Resolución C.D 461 de 26 de diciembre de 2013, estableció como plazo máximo el 31 de marzo de 2014, únicamente 3 meses para su consecución, proyecto que a criterio de la auditoria es de alta complejidad, en razón de las necesidades de recursos, plazos, compromisos y experiencias requeridos a nivel Institucional.

Conclusión

Las copias de respaldo del sistema Host se generan en el Centro de Cómputo ubicado en el Edificio Matriz del IESS ubicado en la ciudad de Quito y son obtenidas a través de las unidades de cartuchos Modelo IBM 3490, las cuales se encuentran obsoletas, sin contar con personal suficiente para el soporte de las operaciones de generación y recuperación de estos respaldos; la alta rotación de autoridades del Instituto y en especial de la Dirección Nacional de Tecnología del Información durante los años 2014 y 2015, afectó los planes con relación al proyecto de la migración de la información del Sistema Host y sus copias de respaldo, el mismo que se consideró de un alto nivel de complejidad; circunstancia que expuso al Instituto a un riesgo potencialmente alto de

pérdida de su información histórica y la imposibilidad de la recuperación de las copias de respaldo.

Recomendaciones

Al Director Nacional de Tecnología de la Información

17. Presentará a la Dirección General, el proyecto para migración de la información y cierre de la Plataforma Host y Micros, y demás servicios soportados por el grupo de Soporte y Plataforma Z10, donde considerará la situación actual, los riesgos, alcance y factores claves de éxito, especificando las necesidades de recursos humanos, capacidades y competencias requeridos, adquisiciones, y contrataciones de ser el caso; planteando un cronograma y presupuesto tentativo para ejecutar el proyecto. Socializará las alternativas contempladas, y las presentará en términos de costo beneficio y con enfoque de riesgos, para la migración y cierre exitoso del Sistema Host y su plataforma, así como sus copias de respaldo.

Al Director General

18. Dispondrá a las Direcciones de los Seguros Especializados, que nombren un delegado que gestione la generación de los requerimientos funcionales en los aplicativos necesarios durante el proceso de migración del Sistema Host y cierre de su plataforma, las pruebas funcionales y conformidad de la implementación efectuada por la DNTI, para cumplir con el cronograma de cierre, una vez aprobado.

Eco. Vicente Saavedra Alberca
AUDITOR INTERNO DEL IESS