TRIBUNAL DE CUENTAS

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 26 DE NOVIEMBRE DE 2014

(E. E. Nº 2014-17-1-0008244)

VISTO: que se procedió a la evaluación y prueba de efectividad de los controles de sistemas de información relevantes para la auditoría financiera de la Contaduría General de la Nación, en particular sobre el Sistema Integrado de Información Financiera módulo Ejecución Presupuestal de Gastos;

RESULTANDO: que el examen practicado fue realizado de acuerdo con los Principios Fundamentales de Auditoría (ISSAI 100 y 200), las Directrices de Auditoría Financiera incluidas en las ISSAI 1315, 1330 y 1620, y particularmente, con las Directrices de la Auditoría TI (ISSAI 5310) de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), habiéndose realizado los procedimientos que se consideraron necesarios en las circunstancias;

CONSIDERANDO: que las conclusiones y evidencias obtenidas son las que se expresan en el Informe que se adjunta, las cuales están suficientemente probadas y documentadas;

ATENTO: a lo dispuesto por el Artículo 228 de la Constitución de la República y por el Artículo 111 del TOCAF;

EL TRIBUNAL ACUERDA

1) Aprobar el Informe referido;

2) Remitir dicho Informe a la Contaduría General de la Nación;

3) Remitir dicho informe al Ministerio de Economía y Finanzas; y

4) Dar cuenta a la Asamblea General.

ag

Cra. Lic. [illegible]inelli Taubner
[illegible] General

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

INFORME DE AUDITORÍA DE SISTEMAS DE INFORMACIÓN

CONTADURÍA GENERAL DE LA NACIÓN

1. ANTECEDENTES

Se realiza la presente evaluación en el marco de las Auditorías que realiza el Tribunal de Cuentas de conformidad con lo dispuesto por el Artículo 228 de la Constitución de la República y por el Artículo 111 del TOCAF.

2. OBJETIVO

El objetivo consistió en evaluar y probar la efectividad de los Controles de SI sobre el SIIF en producción en la Contaduría General de la Nación relevante para la Auditoría Financiera, en particular sobre el SEG.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la Contaduría General de la Nación al 31 de octubre de 2014, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera y los controles de aplicación sobre el subsistema SEG del SIIF.

Se deja constancia que el estudio no constituye en forma alguna auditoría, revisión u otra forma de dictamen sobre estados financieros-contables o declaración sobre el objetivo básico de razonabilidad de la información financiera.

A su vez, este informe no emite opinión sobre el nivel de eficacia y eficiencia operacional de las aplicaciones bajo revisión. Sin embargo, este informe sí emite opinión sobre la efectividad y confiabilidad de los controles de SI significativos para los objetivos de auditoría financiera.

ApiaDocumentum Folio n° 41

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

4. METODOLOGÍA

Fase I: Evaluación de Controles Generales de TI

Los Controles Generales de TI son estructuras, políticas y procedimientos con el objetivo primario de proporcionar un marco de protección para los recursos computacionales, aplicaciones y datos relacionados en este caso con información financiera. Dichos controles incluyen actividades para prevenir, detectar o corregir errores y/o irregularidades significativas en los reportes financieros o divulgaciones inapropiadas.

Fase II: Evaluación de Controles de Aplicaciones

Los Controles de Aplicación son diseñados para prevenir o detectar transacciones contables no autorizadas y dar soporte a objetivos financieros tales como completitud, exactitud, existencia y debida autorización de transacciones a través del sistema de información financiera, asegurando la integridad de los registros contables.

Fase III: Evaluación de combinación de Controles

El diseño e implementación adecuada de los controles generales y de aplicación son esenciales para proteger los recursos computacionales, aplicaciones y datos de la Contaduría General de la Nación del riesgo de acceso y/o divulgación no autorizada y/o modificación inapropiada (fraude o error) de información financiera; daño o pérdida de recursos e interrupción de las operaciones, entre otros factores de vulnerabilidad. En términos generales, debe configurarse una combinación efectiva de los controles generales y de aplicación para asegurar la confiabilidad, apropiada confidencialidad y disponibilidad de la información financiera.

La efectividad de los controles generales es un factor significativo para establecer confianza en los controles de aplicación, en el entendido que estos últimos pueden volverse inefectivos por modificación o burla (entre otros), ante la presencia de controles generales débiles.

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

No obstante, los procedimientos íntegramente manuales ejercidos por los usuarios pueden proporcionar control efectivo -aunque en general limitado- a nivel de la aplicación.
Por todo lo expuesto, los controles generales deben ser documentados con anterioridad a los de aplicaciones específicas.

5. PROCEDIMIENTOS APLICADOS

Se han llevado a cabo los procedimientos considerados necesarios en las circunstancias (indagación, observación, análisis de documentación, prueba de controles y sustantivas), en consistencia con los Principios, Directrices y Guías señaladas.

6. CONSTATACIONES, POSIBLES CONSECUENCIAS Y RECOMENDACIONES SOBRE CONTROLES GENERALES DE TI

6.1. ADMINISTRACIÓN DE LA SEGURIDAD [2]

El objetivo de control impacta directamente sobre los siguientes criterios de información:

Efectividad	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
√	√	√	√		

Objetivo: El control debe proveer seguridad razonable que la administración de seguridad es efectiva, incluyendo: i) diseño y operación de políticas, procedimientos y prácticas de seguridad; ii) evaluaciones periódicas de riesgos mitigando o corrigiendo las vulnerabilidades detectadas y iii) control sobre las actividades ejecutadas por terceras partes.

[2] Mapeo con los procesos del modelo COBIT v. 4.1 (Objetivos de Control para la Información y Tecnologías afines): PO9 "Evaluar y administrar riesgos de TI", DS2 "Administrar servicios de terceros", DS5 "Garantizar la seguridad de los sistemas".

ApiaDocumentum **Folio n° 43**

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

Fortalezas relevantes	Deficiencias relevantes de control		
	Constatación	Posibles riesgos	Recomendaciones
Políticas de Seguridad de la Información aprobadas por Resolución del 19 de octubre de 2011, que toman como base "La Política de Seguridad de la Información para Organismos de la Administración Pública" establecida por AGESIC.	No se han documentado los procedimientos y controles de seguridad de la información.	La ausencia del logro de una estructura de seguridad efectiva, expone a amenazas que podrían afectar la integridad, confidencialidad y disponibilidad de la información.	Diseñar y documentar los procedimientos y controles de seguridad de la información.
	En Resolución del 19 de octubre de 2011, se designó un comité responsable de la seguridad de la información. Sin embargo, no se han constatado recomendaciones del mismo a la División Sistemas. A su vez, dicha División no cuenta con función o grupo de administración de la seguridad de la información. Sin perjuicio de lo expuesto, cabe señalar que se ha constatado la voluntad proactiva de la Administración en materia de Seguridad (v. gr. Contratación de consultores y profesional especialista en materia de seguridad).	Inadecuada y/o insuficiente protección de los activos de información, comprometiendo la integridad, confidencialidad y disponibilidad de los datos.	Definir y asignar formalmente la función o grupo de administración de seguridad de la información que tenga la responsabilidad de administrar los riesgos y la seguridad de TI.

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

	No se ha elaborado una metodología mediante la cual, con periodicidad, se identifiquèn y midan los riesgos, que resulte en un plan de acción contra éstos y en una aceptación formal del riesgo residual. Cabe señalar que la Administración, a efectos de minimizar esta carencia, contrató en el año 2013 una consultoría y en base a sus resultados elaboró un plan de trabajo a mediano y largo plazo. La Administración informa que la implementación del Sistema de Gestión de Seguridad de la Información (que contemple los procesos críticos de seguridad como ser análisis de riesgo, continuidad del negocio y gestión del personal), está prevista para el mediano plazo.	Exposición a amenazas que podrían afectar la integridad, confidencialidad y disponibilidad de la información.	Se debería establecer un enfoque de evaluación de riesgos de TI mediante el cual se identifiquen y midan los riesgos y que proporcione la definición de un plan de acción contra aquellos que, a instancias de un estudio costo-efectividad, requieran la implementación de protecciones y controles.
Nivel de riesgo: ALTO			

ApiaDocumentum **Folio n° 45**

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

6.2.- CONTROL DE ACCESO [3]

El objetivo de control impacta directamente sobre los siguientes criterios de información:

Efectividad	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
	√	√	√		

Objetivo: El control debe proveer seguridad razonable que el acceso a los recursos computacionales (datos, equipamiento, instalaciones) es adecuado y restringido a personal autorizado, incluyendo efectividad en i) protección de la información y recursos sensibles; ii) mecanismos de identificación, autenticación y autorización; iii) capacidad de monitoreo y auditabilidad.

Fortalezas relevantes	Deficiencias relevantes de control		
	Constatación	Posibles riesgos	Recomendaciones
El acceso lógico se encuentra restringido mediante mecanismos de autorización, identificación y autenticación en la base de datos Oracle.	En la base de datos Oracle donde se han implementado todos los controles del sistema, entre ellos los de acceso lógico, no se han configurado parámetros de contraseña.	Contraseñas sencillas de descifrar permitirían accesos no autorizados.	Implementar en la base de datos Oracle la política institucional de contraseña aprobada mediante Resolución del 23 de enero de 2014.

[3] Mapeo con los procesos del modelo COBIT v. 4.1 (Objetivos de Control para la Información y Tecnologías afines): DS5 "Garantizar la seguridad de los sistemas", DS12 "Administrar el ambiente físico".

ApiaDocumentum Folio n° 46

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

Las salas de equipamiento central cuentan con adecuados controles de acceso físico.	Se encontraron al menos 11 usuarios genéricos en la base de datos Oracle, de los cuales 3 son usuarios poderosos: SYS, SYSTEM y REPADMIN. Si bien se guardan logs de auditoría, éstos sólo se revisan a demanda. La Administración ha informado que se están tomando las medidas necesarias para estar en condiciones de implementar un adecuado proceso de auditoría en el mediano plazo.	Dificultad para delimitar responsabilidades ante acciones no autorizadas, ya sean éstas por error o maliciosas.	Implementar que todos los usuarios y sus actividades sean identificadas de manera unívoca. En caso de requerirse, para situaciones especiales, conservar usuarios genéricos implementar controles compensatorios. Las actividades de los usuarios con derechos equivalentes a administrador deben ser supervisadas.
Nivel de riesgo: MEDIO			

6.3.- GESTIÓN DE LA CONFIGURACIÓN[4]

El objetivo de control impacta directamente sobre los siguientes criterios de información:

Efectividad	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
√		√	√		

Objetivo: El control debe proveer seguridad razonable que los cambios a los recursos de sistemas de información son autorizados y que los sistemas (software de base y de aplicación) están siendo configurados y operados en forma segura, incluyendo efectividad en i) políticas y procedimientos de administración de configuración; ii) autorización, prueba, aprobación y seguimiento de los cambios; iii) oportunas actualizaciones de software para su protección contra vulnerabilidades conocidas; iv) aprobación y documentación de cambios de emergencia.

[4] Mapeo con los procesos del modelo COBIT v. 4.1 (Objetivos de Control para la Información y Tecnologías afines): AI6 "Administrar cambios", DS9 "Administrar la configuración".

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

Fortalezas relevantes	Deficiencias relevantes de control		
	Constatación	Posibles riesgos	Recomendaciones
Se ha configurado protección contra los accesos desde el exterior mediante firewalls y zona desmilitarizada.	No se cuenta con inventario de software de base y hardware actualizados.	El no mantener actualizada la identificación de la configuración, podría incidir negativamente en la gestión de la misma, además de ser imprescindible para situaciones de contingencia.	Realizar y documentar un inventario del software de base y el hardware, manteniéndolo actualizado.
	No se han definido formalmente los procesos de gestión de cambio. No se ha definido ni se aplica una práctica uniforme para el mantenimiento del SIIF y del software de base y hardware que le da soporte, mediante la cual se verifique que todo cambio ha sido autorizado, genera documentación técnica, es registrado, probado y aprobado. La Administración informa sobre la inminencia de aprobación e implementación de los procesos de gestión de cambios.	La introducción de un cambio sin el adecuado control puede acarrear modificaciones y/o pérdida de información.	Documentar el proceso de gestión del cambio a la configuración. La aplicación de dicho proceso deberá asegurar que todos los cambios son apropiadamente controlados (autorizados, probados, aprobados y registrados).
Nivel de riesgo: ALTO			

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

6.4.- SEGREGACIÓN DE FUNCIONES [5]

El objetivo de control impacta directamente sobre los siguientes criterios de información:

Efectividad	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
√					

Objetivo: El control debe proveer seguridad razonable que las funciones y responsabilidades incompatibles se encuentran efectivamente segregadas y que las actividades del personal son supervisadas y revisadas.

Fortalezas relevantes	Deficiencias relevantes de control		
	Constatación	Posibles riesgos	Recomendaciones
La estructura funcional de la División Sistemas provee una adecuada segregación de funciones.	Si bien se guardan logs de auditoría, éstos no son periódicamente revisados en busca de actividades incompatibles. Al respecto la Administración informa que está prevista su implementación a mediano plazo.	Ocurrencia de modificación no autorizada y/o uso inadecuado de activos.	Ejercer una adecuada revisión de las bitácoras.
Nivel de riesgo: BAJO			

6.5.- CONTINUIDAD DEL SERVICIO [6]

El objetivo de control impacta directamente sobre los siguientes criterios de información:

Efectividad	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad
√		√	√		

[5] Mapeo con los procesos del modelo COBIT v. 4.1 (Objetivos de Control para la Información y Tecnologías afines): PO4 "Definir procesos, organización y relaciones de TI".

[6] Mapeo con los procesos del modelo COBIT v. 4.1 (Objetivos de Control para la Información y Tecnologías afines): DS4 "Garantizar la continuidad del servicio", DS10 "Administrar los problemas", DS12 "Administrar el ambiente físico".

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

Objetivo: El control debe proveer seguridad razonable que la planificación de contingencia protege los recursos de información, minimiza el riesgo de interrupciones no planificadas y provee recuperación de operaciones críticas ante fallas o desastres.

Fortalezas relevantes	Deficiencias relevantes de control		
	Constatación	Posibles riesgos	Recomendaciones
Para el servidor de base de datos se ha implementado un cluster de AIX (dos servidores espejados) con software de monitoreo asociado. Se realizan respaldos diarios a cinta y su recuperación es probada a diario. La custodia de los mismos es consistente con las buenas prácticas en la materia.	No se cuenta con sitio de procesamiento alternativo, propio o de terceros, y no ha sido diseñado un plan de contingencias y recuperación de desastres. La Administración informa que se están tomando medidas tendientes a subsanar dichas carencias.	Detenimiento de la operación por encima de la máxima tolerancia. Pérdida y/o corrupción de la información.	Elaborar, probar y mantener un plan de contingencias y recuperación de desastres.
	Los sensores de humo están conectados a un equipo de monitoreo especializado, cuya alarma es audible sólo en el centro de procesamiento.	No poder actuar oportunamente en caso de incendio fuera del horario laboral.	Conectar el equipo a una central de alarmas general o externa.
Nivel de riesgo: MEDIO			

Expediente N°: 2014-17-1-0008244

TRIBUNAL DE CUENTAS

7. CONSTATACIONES, POSIBLES CONSECUENCIAS Y RECOMENDACIONES SOBRE CONTROLES DE APLICACIÓN

7.1.- SISTEMA SIIF SUBSISTEMA SEG

Fortalezas relevantes	Deficiencias relevantes de control		
	Constatación	Posibles riesgos	Recomendaciones
Controles de Ingreso: Se minimizan errores de digitación mediante listas de selección y carga de información de forma automatizada. El sistema cuenta con controles automáticos de existencia, de disponibilidad, de correspondencia, de etapa anterior cumplida (de lo contrario no permite continuar), de autorización, de correctitud y de montos.	No se hallaron debilidades tales que amenacen significativamente al cumplimiento del objetivo de control.	N/A	N/A
Controles de Procesamiento: El procesamiento interno asegura razonablemente la completitud, exactitud y la integridad de las transacciones.			
Controles de Salida: El acceso a reportes, consultas e información se encuentra en el marco del proceso de otorgamiento de permisos sobre la aplicación, es decir que los usuarios para consultar información se encuentran debidamente autorizados por los propietarios de la aplicación y datos.			
Nivel de riesgo: BAJO			

Cra. Lic. Olga Santinelli Taubner
Secretaria General