RES. 1879/2020

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 23 DE SETIEMBRE DE 2020

(E. E. Nº 2019-17-1-0004763, Ent. N° 3409/19)

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 Administración Nacional de Correos;

RESULTANDO: que el examen practicado fue realizado de acuerdo con los Principios Fundamentales de Auditoría del Sector Público (ISSAI 100 y 200), las Normas de Auditoría Financiera incluidas en las ISSAI 2315, 2330, 2620 y las Guías sobre Auditoría de Sistemas de información (ISSAI 5100) de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI). Estas normas requieren que se cumpla con requisitos éticos, se planifique y se realice la auditoría para obtener evidencia suficiente y apropiada, proveyendo una garantía razonable de sustentación para los hallazgos y conclusiones;

CONSIDERANDO: que las conclusiones y evidencias obtenidas son las que se expresan en el Informe de Auditoría, que incluye el Dictamen e Informe a la Administración;

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) Expedirse en los términos del Informe de Auditoría que se adjunta;

2) Comunicar a la Administración Nacional de Correos; y

3) Dar cuenta a la Asamblea General.

lm

DICTAMEN

El Tribunal de Cuentas ha examinado los Controles de los Sistemas de Información[1] (en adelante "SI") sobre las aplicaciones en producción de la Administración Nacional de Correos (en adelante "ANC"), relevantes para la auditoría financiera, en particular sobre el sistema de Liquidación de Haberes (Buxis).

Opinión

En opinión del Tribunal de Cuentas la ANC ha implementado controles de SI inefectivos en términos generales, asimismo, se han encontrado carencias de control en el ámbito de los sistemas de aplicación Buxis al 13 de Agosto de 2020 de acuerdo a la Guía para las normas de Control Interno del Sector Público GOV 9100 de la INTOSAI. Por lo que se entiende, no ha sido implementada una combinación de controles generales y de aplicación efectivas afectando la confidencialidad, integridad y disponibilidad de programas y datos lo que amerita la pronta atención y acción de la Administración.

Bases para la opinión

Esta auditoría fue realizada de acuerdo con los Principios Fundamentales de Auditoría del Sector Público (ISSAI 100 y 200), las Normas de Auditoría Financiera incluidas en las ISSAI 2315, 2330, 2620 y las Guías sobre Auditoría de Sistemas de información (ISSAI 5100) de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI). Estas normas requieren que

[11]Los Controles de Sistemas de Información (SI) consisten en aquellos controles internos que dependen del procesamiento electrónico de datos e incluyen: controles generales y controles de aplicación (automáticos y de usuario -efectuados por personal interactuando con sistemas de información-). Los controles generales y de aplicación automáticos son siempre catalogados como Controles de SI. Sin embargo, un control de usuario puede clasificarse como Control de SI sólo si su efectividad depende del procesamiento del sistema de información o de la confiabilidad (exactitud, completitud, validez) de la información procesada por el sistema. En caso contrario, el control se define como manual. Los controles manuales pueden ser necesarios para el cumplimiento de los objetivos de control en combinación con los Controles de SI así como para mitigación de riesgo como consecuencia de debilidades en los Controles de SI.

se cumpla con requisitos éticos, se planifique y se realice la auditoría para obtener evidencia suficiente y apropiada, proveyendo una garantía razonable de sustentación para los hallazgos y conclusiones.

Responsabilidad de la Dirección sobre los controles internos de TI relacionados con el sistema administrativo-contable

La Dirección de ANC es responsable de diseñar, implementar y mantener un sistema de control interno de TI, a efectos de procurar brindar una seguridad razonable sobre el logro de los objetivos de la entidad, la confiabilidad de la información financiera y el cumplimiento de las disposiciones legales y reglamentarias, de acuerdo a las Guías sobre Auditoría de Sistemas de Información ISSAI 5100 de la INTOSAI.

Responsabilidad del Tribunal de Cuentas por la auditoría de los Controles de los Sistemas de Información

El objetivo de la auditoría consiste en expresar una opinión sobre dichos Controles basada en la auditoría realizada.

Como parte de una auditoría de acuerdo con las ISSAI referidas en la sección *Bases para la Opinión*, el Tribunal de Cuentas aplica su juicio profesional y mantiene el escepticismo profesional durante el proceso de auditoría. Se considera que la evidencia obtenida brinda una base suficiente y apropiada para sustentar la opinión.

El Tribunal de Cuentas se comunicó con el Sr. Presidente de la ANC en relación, entre otros asuntos, al alcance y la oportunidad de los procedimientos de auditoría, los hallazgos significativos de auditoría incluidos, en caso de corresponder, y las deficiencias significativas en el control interno que se identificaron en el transcurso de la auditoría.

En el Informe que se agrega se detallan las deficiencias relevantes del control, sus posibles consecuencias asociadas, el nivel de cumplimiento alcanzado en los objetivos de control, así como las recomendaciones correspondientes.

Montevideo, 1 de Setiembre de 2020

lm

INFORME A LA ADMINISTRACIÓN

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 las aplicaciones en producción en ANC, relevantes para la auditoría financiera.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la ANC al 13 de Agosto de 2020, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera y los controles de aplicación del Sistema de Liquidación de Haberes (Buxis).

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.

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 ANC 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.

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.

CONSTATACIONES, POSIBLES CONSECUENCIAS Y RECOMENDACIONES SOBRE CONTROLES GENERALES DE TI

ADMINISTRACIÓN DE LA SEGURIDAD

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.

Deficiencias relevantes de control:

- La estructura Organizacional no contempla la función o grupo de Administración de Seguridad, ni se ha asignado personal a dicha tarea.

  Si bien se ha previsto el funcionamiento de la Unidad "Calidad de Sistemas" de la cual depende la función "Oficial de Seguridad

Informática" no ha podido ser instaurada y a la fecha permanece vacante.

Posibles consecuencias:

- Inadecuada y/o insuficiente protección de los activos de información, comprometiendo la integridad, confidencialidad y disponibilidad de la los datos.

Recomendación:

- Definir y asignar formalmente la función o grupo de Administración de Seguridad de la Institución toda. De ser necesario definir y asignar responsabilidades en seguridad adicionales a nivel de gerencias (v. gr. División Informática) para la resolución de problemas de seguridad relacionados con su cometido específico.

Deficiencias relevantes de control:

- La Institución no cuenta con una metodología mediante la cual se identifiquen y midan los riesgos, que resulte en un plan de acción contra éstos y en una aceptación formal del riesgo residual.

Posible consecuencia:

- Exposición a amenazas que podrían afectar la integridad, confidencialidad y disponibilidad de la información.

Recomendación:

- Se debería establecer un enfoque de avaluación 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 riesgos que, a instancias de un estudio costo-efectividad, requieran la implementación de protecciones y controles.

Deficiencias relevantes de control:

- La institución no cuenta con Políticas de Seguridad de la Información.

Posible consecuencia

- La ausencia de pautas para la seguridad de la información debilitaría ésta, en el entendido que la Política de Seguridad es una condición inicial para lograr una estructura de seguridad efectiva, estableciendo un marco continuo de evaluación de riesgos, implantación de procedimientos de seguridad y el monitoreo y evaluación de la efectividad de dichos procedimientos.

Recomendación:

- Definir formalmente las Políticas de Seguridad de la Información de la Institución y diseñar e implantar estándares, normas y procedimientos de control que aseguren el cumplimiento de dichas Políticas.

Nivel de cumplimiento del objetivo de control: BAJO

CONTROLES DE ACCESO

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.

Deficiencias relevantes de control:

- Se constató la existencia de usuarios en el dominio sin expiración de contraseña para el acceso a la red.

Posible consecuencia:

- El no forzar cambio de contraseña con cierta periodicidad puede comprometer la misma.

Recomendación:

- El sistema debe forzar el cambio periódico de contraseñas.

Nivel de cumplimiento del objetivo de control: MEDIO

GESTIÓN DE LA CONFIGURACIÓN

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.

Deficiencias relevantes de control:

- No poseen procedimientos documentados de desarrollo y mantenimiento de aplicaciones, así como tampoco para cambios de software de base y hardware.

Posible consecuencia:

- Introducción de cambios al software y/o hardware no sería verificable y controlada.

Recomendaciones:

- Diseñar e implementar procedimientos de actualización de los sistemas operativos, aplicaciones y hardware.

Nivel de cumplimiento del objetivo de control: MEDIO

SEGREGACION DE FUNCIONES

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.

Deficiencias relevantes de control

- Si bien existe un documento de tareas por cada una de las áreas de TI, no se han establecido las funciones y responsabilidades de cada uno de los cargos dentro de cada una de ellas.

Posible consecuencia:

- La integridad, confidencialidad y disponibilidad podrían verse afectadas por accesos no supervisados.

Recomendación:

- Implementar una adecuada segregación de funciones a nivel de software de base y de aplicación, en aquellos casos que no sea posible aplicar controles compensatorios (v. gr. supervisión directa, efectiva y continua).

Nivel de cumplimiento del objetivo de control: BAJO

CONTINUIDAD EN EL SERVICIO

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 planificación de contingencia protege los recursos de información, minimiza el riesgo de interrupciones.

Deficiencias relevantes de control:

- No se cuenta con un Plan de Continuidad y/o Contingencia de TI que contemple la recuperación de operaciones ante fallas/desastres bajo diferentes escenarios, y de acuerdo a una ventana de tolerancia establecida con los propietarios de las aplicaciones.

Posible consecuencia:

- Detenimiento de la operación por encima de la máxima tolerancia.
- Aumenta el riesgo de interrupciones no planificadas en la operativa de la institución y pérdida de datos sensibles.

Recomendación:

- Diseñar, probar y mantener actualizados planes de Contingencias y de Recuperación de Desastres.

Nivel de cumplimiento del objetivo de control: BAJO

CONSTATACIONES, POSIBLES CONSECUENCIAS Y RECOMENDACIONES SOBRE CONTROLES DE APLICACIÓN

SISTEMA DE LIQUIDACION DE HABERES (BUXIS)

Deficiencias relevantes de control:

- No existe una interfaz automática entre el sistema de liquidación y el sistema de registro de asistencias. Este pasaje de información se realiza ingresando manualmente los datos de las asistencias en el Sistema de liquidación, lo cual aumenta la probabilidad de cometer errores de digitación. Los controles compensatorios se entienden insuficientes.

Posibles consecuencias

- El ingreso de datos en forma manual aumenta el riesgo de ingreso y/o modificación errónea de datos.

Recomendación

- Automatizar el procedimiento de carga de información en esos casos donde la información se carga manualmente y/o realizar controles compensatorios que mitiguen el riesgo de digitación errónea.

lm