RES. 1896/2020

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 23 DE SETIEMBRE DE 2020

(E. E. Nº 2018-17-1-0007007, Ent. INICIADA)

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 Intendencia de Treinta y Tres;

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 Intendencia de Treinta y Tres; y

3) Dar cuenta a la Asamblea General.

bf

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 Intendencia Departamental de Treinta y Tres (en adelante "IDTT"), relevantes para la auditoría financiera, en particular sobre la aplicación que realiza el proceso de liquidación de haberes al 13 de Febrero de 2020.

Opinión

En opinión del Tribunal de Cuentas, la IDTT no ha implementado, al 13 de Febrero de 2020, controles de SI razonablemente efectivos sobre los sistemas de información que soportan la operativa de la aplicación sujeta al objetivo de esta auditoría; existiendo vulnerabilidades que amenazan significativamente a la confidencialidad, integridad y disponibilidad de la información manejada por la misma.

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 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.

[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.

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

La Dirección de la IDTT 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 Señor Intendente 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, 27 de mayo de 2020

bf

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 IDTT, relevantes para la auditoría financiera.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la IDTT al 13 de Febrero de 2020, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera y controles de aplicación en los sistemas que participan en la liquidación de haberes de la Intendencia Departamental de Treinta y Tres.

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 IDTT 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 intendencia no cuenta con una política de seguridad de la información y/o procesos y controles que establezcan claramente los roles, responsables y procedimientos para la gestión de los riesgos asociados a la tecnología de la información.
- No se ha designado o establecido un responsable o área de seguridad de la información.

Posible consecuencia:

- Acceso y uso no autorizado de los sistemas y la información financiera.

Recomendación:

- Diseñar e implementar políticas de seguridad de la información, establecer procedimientos y responsables de la ejecución de las mismas.

Deficiencias relevantes de control:

- No se pudo obtener evidencia de la existencia de contratos que formalicen el alcance de los servicios y acuerden confidencialidad.

Posible consecuencia:

- Negación o incumplimiento del Servicio contratado.

Recomendación:

- Formalizar contratos con terceros, estableciendo claramente acuerdos de niveles de servicio y cláusula de confidencialidad.

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:

- Las cuentas de administrador no son monitoreadas, al igual que las cuentas de terceros (v. gr. empresas contratadas para mantenimiento de los sistemas).

Posible consecuencia:

- Acceso y uso no autorizado de los sistemas y la información financiera.

Recomendación:

- Implementar una política de contraseñas y realizar un monitoreo de las cuentas inactivas y de las cuentas con permisos privilegiados como las de terceros y las de administrador.

Deficiencias relevantes de control:

- El control de acceso a la sala de servidores no es consistente con las prácticas mínimamente aceptables en la materia.

Posible consecuencia:

- Acceso físico no autorizado al equipamiento central e información de la Intendencia.
- Incendio (desastre) que afecte al equipamiento central de la Intendencia.
- Disrupción de la continuidad operativa de la Intendencia.
- Falla de los sistemas y equipamiento.

Recomendación:

- Implementar una sala de servidores adecuada para la sensibilidad de la información y sistemas alojados en los servidores de la Intendencia, que establezca niveles adecuados de seguridad física y ambiental.

Nivel de cumplimiento del objetivo de control: BAJO

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 se cuenta con procedimientos formales de cambios/actualización de aplicaciones e infraestructura.

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.

Deficiencias relevantes de control:

- No se cuenta con procedimientos de cambios de emergencia.

Posible consecuencia:

- Introducción de cambios no aprobados.

Recomendaciones:

- Diseñar procedimientos de cambios de emergencia en las bases de datos y aplicaciones.

Deficiencias relevantes de control:

- Se encuentra instalado software antivirus gratuito. La actualización del mismo en los puestos de trabajo no es centralizada.

Posible consecuencia:

- Integridad, disponibilidad y confidencialidad podrían verse afectadas ante un ingreso a la red no autorizado.

Recomendaciones:

- Verificar la instalación, actualización y mantenimiento de software antivirus o similar, que fortalezca la seguridad lógica tanto en servidores como en puestos de trabajo con accesos a los mismos.

Nivel de cumplimiento del objetivo de control: BAJO

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:

- Se observó una inadecuada segregación de funciones dentro del área informática. Las tareas, excepto algunas específicas, son compartidas por todos los funcionarios de dicha área.

Posible consecuencia:

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

Recomendaciones:

- 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 no planificadas y provee recuperación de operaciones críticas ante fallas o desastres.

Deficiencias relevantes de control:

- No se ha definido por escrito procedimiento de respaldos. Sólo un funcionario que asiste intermitentemente a la intendencia conoce los procedimientos.

Posible consecuencia:

- Errores en la realización/recuperación de respaldos.

Recomendaciones:

- Elaborar políticas y procedimientos de respaldo y recuperación de datos y aplicaciones.
- Realizar periódicamente pruebas de recuperación de respaldos y documentar las mismas.

Deficiencias relevantes de control:

- No ha sido elaborado un plan de contingencia y recuperación de desastres.

Posible consecuencia:

- Interrupción de la continuidad operativa de la Intendencia.

Recomendaciones:

- Elaborar un plan de contingencia y recuperación de desastres.

Deficiencias relevantes de control:

- Inexistencia de seguridad física y ambiental acorde.

Posible consecuencia:

- Acceso físico no autorizado al equipamiento central e información de la Intendencia.
- Ocurrencia de incendio que afecte al equipamiento central de la Intendencia.
- Interrupción de la continuidad operativa de la Intendencia.
- Falla de los sistemas y equipamiento.

Recomendaciones:

- Implementar adecuados controles de acceso físico y ambiental en la sala de servidores.

Nivel de cumplimiento del objetivo de control: BAJO

CONSTATACIONES SOBRE CONTROLES DE APLICACIÓN - MAGIX

Deficiencias relevantes de control:

- No se hallaron deficiencias relevantes.

Nivel de cumplimiento del objetivo de control: ALTO

bf