RES. 3282/19

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 30 DE DICIEMBRE DE 2019

(E. E. Nº 2018-17-1-0006986)

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 Maldonado;

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 la Guía para las normas de Control Interno del sector público (INTOSAI GOV 9100) de la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), habiéndose realizado los procedimientos que se consideraron necesarias en las circunstancias;

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 Maldonado; y

3) Dar cuenta a la Asamblea General.

dc

DICTAMEN AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN (TI)

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 de Maldonado (en adelante "IM"), relevantes para la auditoría financiera, en particular sobre el sistema de liquidación de sueldos SIAP.

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

La Dirección de la IM 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.

Responsabilidad del Auditor

La responsabilidad del Tribunal de Cuentas es expresar una opinión sobre dichos Controles basada en la auditoría realizada.

Esta auditoría fue realizada 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 la Guía para las normas de Control Interno del sector público (INTOSAI GOV 9100) 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

[1] [1] 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.

obtener evidencia suficiente y apropiada, proveyendo una garantía razonable de sustentación para los hallazgos y conclusiones.
Se considera que la evidencia obtenida brinda una base suficiente y apropiada para sustentar la opinión.

Opinión

El diseño y la operación de los Controles de Sistemas de Información evaluados resultan parcialmente inefectivos en términos generales, asimismo se han encontrado carencias de control en el ámbito de los sistemas de aplicación por lo que, se entiende, no ha sido implementada una combinación de controles generales y de aplicación efectiva, afectando la confidencialidad, integridad y disponibilidad de programas y datos lo que amerita la pronta atención y acción de la Administración.

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, diciembre de 2019

dc

INFORME A LA ADMINISTRACIÓN
AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN (TI)
INTENDENCIA DE MALDONADO

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 la IM, relevantes para la auditoría financiera.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la IM al 4 de diciembre de 2019, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera y controles de aplicación en el sistema de liquidación de haberes.

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 IM 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.

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 Políticas de Seguridad de la información.

Posibles consecuencias:

- 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:

- Las cuentas de administrador en las bases de datos son genéricas.

Posible consecuencia:

- Ocurrencia de alteración no autorizada o accidental sin posibilidad de dirimir responsabilidades.

Recomendación:

- Evitar el uso de "usuarios genéricos" y para aquellos que se entienda de estricta necesidad, implementar un protocolo de salvaguarda de sus respectivas contraseñas.

Deficiencias relevantes de control:

- Tanto en el servidor de bases de datos como en el de la aplicación SIAP no se fuerza el cambio de contraseña al primer ingreso ni periódicamente.

Posible consecuencia:

- La ocurrencia de alteración no autorizada o accidental de datos.

Recomendación:

- El sistema debe forzar el cambio periódico de contraseñas y bloquear el usuario ante intentos fallidos. Los accesos fallidos deben ser debidamente reportados e investigados.

Deficiencias relevantes de control:

- No se encuentra implementada una adecuada política de contraseñas.

Posible consecuencia:

- La ocurrencia de alteración no autorizada o accidental de datos.

Recomendación:

- Definir formalmente la Política de contraseñas y diseñar e implantar estándares, normas y procedimientos de control que aseguren el cumplimiento de dichas Políticas.

Deficiencias relevantes de control:

- No se han definido los dueños de los datos y aplicaciones.

Posible consecuencia

- La ocurrencia de alteración no autorizada o accidental de datos.

Recomendación

- Los dueños de los datos y aplicaciones deben controlar la identificación y autorización de los usuarios que los utilizan.

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 hallaron debilidades tales que comprometan el cumplimiento del objetivo de control.

Nivel de cumplimiento del objetivo de control: ALTO

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:

- No se hallaron evidencias de aplicación rutinaria de procedimientos formales de supervisión. No obstante en caso de, por ejemplo, ocurrencia de un incidente se revisan los logs.

Posible consecuencia:

- Ocurrencia de actividades incompatibles.

Recomendación:

- Como medida de detección/prevención controlar periódicamente las actividades mediante procedimientos formales de operación, supervisión y revisión.

Deficiencias relevantes de control:

- Informática cumple tareas de usuario final en las aplicaciones Geotributos y SIAP.

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).

Deficiencias relevantes de control:

- Se ha elaborado un manual de funciones en cómputos, pero no se encuentra aprobado ni ha sido implementado.

Posible consecuencia:

- . Ocurrencia de actividades incompatibles.

Recomendación:

- Elaborar y aprobar un manual de funciones para Dirección de Cómputos, detallando que tareas son competencia de cada puesto en dicha Dirección.

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 realizan periódicamente pruebas de recuperación de respaldos.

Posible consecuencia:

- Pérdida y/o corrupción de la información.

Recomendación:

- Realizar pruebas de recuperación de respaldos periódicamente y documentarlas.

Deficiencias relevantes de control:

- No se ha elaborado un plan de contingencias y recuperación de desastres.

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. Tener en cuenta que el plan de Recuperación de Desastres incluye, en caso de ser necesario, el recuperar la operativa mediante un CPD alternativo.

Nivel de cumplimiento del objetivo de control: BAJO

CONSTATACIONES, POSIBLES CONSECUENCIAS Y RECOMENDACIONES SOBRE CONTROLES DE APLICACIÓN

SISTEMA DE LIQUIDACION DE HABERES (SIAP)

Deficiencias relevantes de control en la ausencia de políticas de contraseñas, a saber:

- No se fuerza el cambio de contraseña en el primer ingreso al sistema.
- No desloguea al usuario por inactividad.
- No fuerza cambio periódico de contraseña.
- No exige mínimo de caracteres, combinación de números y letras, y la existencia de mayúsculas y minúsculas.
- No bloquea al usuario en caso de determinado número de intentos fallidos.

Posible consecuencia:

- La ocurrencia de alteración no autorizada o accidental de datos.

Recomendación:

- Definir formalmente la Política de contraseñas y diseñar e implantar estándares, normas y procedimientos de control que aseguren el cumplimiento de dichas Políticas.

Deficiencias relevantes de control relativas a segregación de funciones:

- Se encuentran 3 funcionarios de cómputos en la lista de usuarios del sistema con perfil de administrador.

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).

Deficiencias relevantes de control en el ingreso de datos:

- Parte de las asistencias ingresan para la liquidación de forma automatizada, el resto es tratado mediante planillas Excel por los sectores Presentismo y Liquidación.

Posible consecuencia:

- El uso de planillas Excel aumenta el riesgo de ingreso y/o modificación errónea o fraudulenta de datos.

Recomendación:

- Automatizar el procedimiento de cálculo y carga de información en los casos donde la información se carga mediante planillas Excel.

Deficiencias relevantes de control relativas a la interfaz entre SIAP y el sistema contable SIFI:

- No se realizan controles internos que verifiquen el correcto funcionamiento de la interfaz pues basan su confianza en los controles automatizados que realiza el SIFI el que, cabe señalar, opera desde setiembre del presente Ejercicio.

Posible consecuencia:

- Que la interfaz pueda no comportarse de acuerdo a los requerimientos.

Recomendación:

- Realizar adecuados controles internos para verificar que la interfaz se comporta de acuerdo a los requerimientos.

Nivel de cumplimiento del objetivo de control: BAJO

dc