RES. 1788/2020

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 9 DE SETIEMBRE DE 2020

(E. E. Nº 2018-17-1-0007004, 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 Rocha;

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 Rocha, a la Junta Departamental de Rocha; 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 Rocha (en adelante "IDR"), relevantes para la auditoría financiera, con el objetivo de evaluar los Controles de Sistemas de Información (controles generales de TI y de aplicación), en particular sobre el sistema de Liquidación de Haberes (Payroll) y los módulos (Gestión Humana) de desarrollo interno que alimentan dicho sistema.

Opinión

En opinión del Tribunal de Cuentas la IDR ha implementado controles de SI parcialmente inefectivos en términos generales, asimismo, se han encontrado carencias de control en el ámbito de los sistemas de aplicación Payroll y Módulos de Gestión Humana al 27 de enero 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.

[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.

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.

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

La Dirección de IDR 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 la Señora Intendente de la IDR 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, julio 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 IDR, relevantes para la auditoría financiera.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la IDR al 27 de enero de 2020, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera, el sistema de Sueldos (Payroll) y los módulos de Gestión Humana de desarrollo interno que alimentan dicho sistema.

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 IDR 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 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:

- Si bien reciben servicios por parte de empresas, se constató que no poseen contratos con terceros vigentes.

Posible consecuencia:

- Puede afectar la integridad y confidencialidad de la información.

Recomendación:

- La IDR debería regularizar la situación con servicios de terceras partes formalizando contratos de servicio que establezcan claramente el nivel de los mismos y acuerdos de confidencialidad.

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:

- No se han definido los dueños de los datos.

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 lo utilizan.

Deficiencias relevantes de control:

- Servidores y datos, no se encuentran clasificados según su criticidad.

Posible consecuencia:

- La protección dada a los datos puede no ser la adecuada, ya sea por exceso o insuficiencia.

Recomendación:

- Implementar procedimientos que determinen un esquema de clasificación asegurando que el propietario de sistemas de aplicación y datos informe, entre otros aspectos, sobre la sensibilidad de los mismos.

Deficiencias relevantes de control:

- No se realiza una revisión periódica de los permisos de acceso.

Posible consecuencia

- Accesos no autorizados a recursos críticos. Permanencia de usuarios inactivos, que hayan sido dados de baja o que hayan cambiado sus funciones.

Recomendación:

- Los dueños de los recursos deben revisar periódicamente las autorizaciones de los usuarios que tienen acceso a los mismos.

Deficiencias relevantes de control:

- No poseen políticas y procedimientos formalmente diseñados que determinen los pasos a seguir en caso de incidentes. No obstante poseen herramientas de monitoreo con alarmas, las cuales disparan alertas en caso que ocurra algún evento.

Posible consecuencia:

- Un manejo inadecuado de problemas podría favorecer su recurrencia.
- Resoluciones que no ocurran oportunamente y de la manera más eficiente.

Recomendación:

- Se deberían definir e implementar procedimientos e instructivos de administración de problemas que aseguren que todos los eventos operacionales que no formen parte de la operación estándar son registrados, analizados y resueltos oportunamente, generando reportes de incidentes para problemas significativos.

Deficiencias relevantes de control:

- El usuario dbarreriro, correspondiente al Gerente de Informática, en el servidor del sistema sueldos, nunca ha realizado un cambio de la contraseña, ni tiene expiración de la misma.

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: 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 procedimiento para cambios de emergencia documentados.

Posible consecuencia:

- Riesgo de interrupciones no planificadas y pérdida de información sensible.

Recomendación:

- Elaborar políticas, planes y procedimientos de procesamiento de emergencia y verificar que:
  - Las prioridades de recuperación se han desarrollado.
  - La Administración ha aprobado las prioridades.
  - Las prioridades están documentadas.

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

- División Sistemas cumple tareas de usuario final en las aplicaciones Sueldos y Tributos.

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:

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

Posible consecuencia:

- Aumenta la probabilidad que los errores intencionales o involuntarios no sean detectados.

Recomendación:

- Los supervisores deben revisar rutinariamente los logs en busca de actividades incompatibles e investigar cualquier anomalía.

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 existe clasificación formal de criticidad de hardware y software.

Posible consecuencia:

- En caso de contingencia o desastre la información podría no tener un tratamiento diferenciado de acuerdo con su grado de importancia, criticidad y sensibilidad.

Recomendación:

- Elaborar un catálogo en el que se establezcan los servicios informáticos considerados de misión crítica por la Organización y el impacto que tienen en la operativa diaria.

Deficiencias relevantes de control:

- No poseen políticas ni procedimientos de procesamiento de emergencia.

Posible consecuencia:

- Las acciones llevadas a cabo en un procesamiento de emergencia pueden no atender las necesidades del negocio.

Recomendación:

- Diseñar procedimientos de procesamiento de emergencia, que tengan documentadas y aprobadas las prioridades de recuperación.

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.

Deficiencias relevantes de control:

- No poseen un sitio alternativo de procesamiento de datos.

Posible consecuencia:

- Detenimiento de la operación por encima de la máxima tolerancia.

Recomendación:

- 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

De acuerdo con lo solicitado se realizó un relevamiento sobre el procedimiento de otorgamiento de permisos, revisión de logs y seguridad de los controles de aplicación sobre el sistema de sueldos Payroll y los módulos que interactúan con dicho sistema.

INTERFACES:

Deficiencias relevantes de control

- No se observan debilidades de relevancia en el pasaje de la información financiera/asientos desde los sistemas mencionados hacia el sistema contable SISINFO, se verificó la existencia de múltiples controles desde todas las áreas que intervienen que minimizan el riesgo de error en las interfaces relevadas, así como en el procesamiento de la información contable.

Nivel de cumplimiento del objetivo de control: ALTO

SISTEMA DE LIQUIDACION DE SUELDOS (PAYROLL) y MODULOS DE GESTION HUMANA

Los módulos de Gestión Humana son de desarrollo interno de la Intendencia y alimentan de información al sistema de sueldos (Payroll) para que este luego pueda realizar la liquidación.

Deficiencias relevantes de control

- Los funcionarios de la división informática tienen acceso al sistema como usuario final y de administración en la aplicación.

Posible consecuencia:

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

Recomendación:

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

Deficiencias relevantes de control

- Se carece de una adecuada oposición de intereses, dado que informática es la que desarrolla y administra los módulos de Gestión Humana. Estos módulos alimentan de información al sistema de sueldos para poder realizar la liquidación de haberes en el Payroll.

Posible consecuencia:

- Aumenta la probabilidad de que los errores intencionales o involuntarios no sean detectados.

Recomendación:

- Identificar las funciones incompatibles e implementar políticas para mantenerlas separadas.

Deficiencias relevantes de control

- El sistema Payroll no posee ningún tipo de controles automáticos en el ingreso de datos. Por ejemplo, no realiza controles de topes en los campos numéricos, no aplica controles en el ingreso de fechas. Tampoco se requiere de ninguna autorización de un superior de lo ingresado por un usuario como medida de validación final.

Posibles consecuencias

- Imposibilidad de detectar datos erróneos en el ingreso de la información.

Recomendación

- Aplicar controles automáticos en los campos de ingreso de datos al sistema.
- Implementar controles con validaciones de los supervisores de cada área.

Deficiencias relevantes de control

- El sistema Payroll no tiene logs de actividades activado. Cabe agregar que los módulos de Gestión Humana si los poseen y están activados.

Posibles consecuencias

- Imposibilidad de revisar, detectar e investigar, tanto posible actividad inusual como accesos no autorizados.

Recomendación

- Activar los logs de actividades de la aplicación Payroll.

Deficiencias relevantes de control

- La empresa proveedora del sistema Payroll no brinda servicio de mantenimiento a la IDR. El pago mensual que la intendencia realiza a la empresa es solamente por concepto de la licencia del software.

Posibles consecuencias

- Detenimiento de la operativa.

Recomendación

- Revisar y actualizar los acuerdos con terceras partes, verificando las cláusulas de confidencialidad y los niveles de servicio.

Deficiencias relevantes de control

- Tanto en Payroll, como en los módulos que alimentan a este sistema, se realizan cargas de información en forma manual.

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.

Deficiencias relevantes de control

- En Payroll un rol o perfil posee muchas acciones las cuales no pueden ser separadas.

Posibles consecuencias

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

Recomendación

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

Deficiencias relevantes de control

- Las solicitudes de cambio en Payroll se realizan en forma verbal, por lo tanto no cumplen con un procedimiento formalmente registrado.

Posibles consecuencias

- No poder llevar a cabo un adecuado control sobre todo el proceso de cambio.

Recomendación

- Documentar la solicitud, autorización, prueba y la aprobación de los cambios en los sistemas.

Deficiencias relevantes de control

- No se realiza revisión periódica de usuarios y permisos.

Posibles consecuencias

- Accesos no autorizados a recursos críticos. Permanencia de usuarios inactivos, que hayan sido dados de baja o que hayan cambiado sus funciones.

Recomendación:

- Los dueños de los recursos deben revisar periódicamente las autorizaciones de los usuarios que tienen acceso a los mismos.

Deficiencias relevantes de control

- Funcionarios de Informática poseen usuarios del sistema Payroll y de los módulos de Gestión Humana. Dichos usuarios poseen permisos totales.

Posibles consecuencias

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

Recomendación

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

bf