

RES. 2579/19

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 23 DE OCTUBRE DE 2019

(E. E. N° 2019-17-1-0000888)

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 Caja de Jubilaciones y Pensiones Bancarias;

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 necesarios 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 Caja de Jubilaciones y Pensiones Bancarias; y
- 3)** Dar cuenta a la Asamblea General.

CLC

DICTAMEN

El Tribunal de Cuentas ha examinado los Controles de los Sistemas de Información¹¹ (en adelante “SI”) sobre las aplicaciones en producción de la Caja de Jubilaciones y Pensiones Bancarias (en adelante “CJPB”), relevantes para la auditoría financiera.

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

La Dirección de la CJPB 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

¹¹Los 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

En opinión del Tribunal de Cuentas, la Caja de Pensiones y Jubilaciones Bancarias ha implementado, al 27 de setiembre de 2019, controles de SI razonablemente efectivos sobre los sistemas sujetos al objetivo de esta auditoría; no existiendo vulnerabilidades que amenacen significativamente a la confidencialidad, integridad y disponibilidad de la información manejada por estas aplicaciones. Sin perjuicio de lo anterior, amerita la pronta atención y acción de la Administración el hecho de mitigar o corregir las deficiencias referidas a “Control de Acceso” y “Continuidad del Servicio”.

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, setiembre de 2019

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 CJPB, relevantes para la auditoría financiera.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la CJPB al 27 de setiembre de 2019, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera de la Caja de Jubilaciones y Pensiones Bancarias.

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 CJPB, 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.

CONSTATAIONES, 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:

- No se hallaron debilidades tales que amenacen significativamente al cumplimiento del objetivo de control.

Nivel de cumplimiento del objetivo de control: ALTO

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 se encuentran nominadas y su actividad no es monitoreada.

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

- No poseen políticas y procedimientos que determinen los pasos a seguir en caso de incidentes. No obstante, poseen identificada la debilidad y la documentación al respecto se encuentra pendiente de aprobación.

Posible consecuencia:

- Un manejo inadecuado de problemas podría favorecer su recurrencia.

- Resoluciones que no ocurran oportunamente y de la manera más eficiente.

Recomendación:

- Se debería continuar con el proceso tendiente a tener procedimientos formales y aprobados en lo que respecta a la 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

- La configuración de los parámetros QPWDLMTAJC, QPWDPOSDF, QPWDLMTREP, y QPWDLMTCHR no está acorde con las mejores prácticas. No obstante los parámetros de estos comandos, que refieren a las políticas de sesión de usuarios y sus contraseñas, se encuentran configurados y alineados con lo aprobado por el Consejo Honorario de la Caja.

Posible consecuencia:

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

Recomendación:

- Estudiar la posibilidad de reever la política de contraseñas a efecto del fortalecimiento de las mismas.

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	Confiability
√		√	√		

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 amenacen significativamente al 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	Confiablez
✓					

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:

- Las actividades de los administradores y usuarios no son monitoreadas. No obstante ello, poseen registro de actividades de los usuarios, por lo cual es auditable.

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: ALTO

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 a 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 vigente y aprobado por la institución. No obstante ese documento se encuentra en fase de aprobación.

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:

- Si bien poseen un plan de contingencias y recuperación de desastres, no se encuentra aprobado y está en fase de acuerdo entre TI y Seguridad.

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: MEDIO