



TRIBUNAL DE CUENTAS

RES. 2421/2021

RESOLUCION ADOPTADA POR EL

TRIBUNAL DE CUENTAS

EN SESION DE FECHA 27 DE OCTUBRE DE 2021

(E. E. N° 2020-17-1-0004858, Ent. Iniciada)

VISTO: que este Tribunal de Cuentas procedió a la evaluación y prueba de efectividad de los controles de sistemas de información, relevantes para la Auditoría Financiera del BPS;

RESULTANDO: que el examen fue realizado de acuerdo con los Principios Fundamentales de Auditoría (ISSAI 100 y 200) y las Normas 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 Dictamen e Informe a la Administración;

ATENTO: a lo dispuesto por los Artículos 211 literales C) y E) de la Constitución de la República, 111 del TOCAF y Ordenanza N° 89 de este Tribunal;

EL TRIBUNAL ACUERDA

1) Aprobar el Informe de Auditoría que se adjunta y expedirse en los siguientes términos;

1.1) que conforme a lo establecido en el Dictamen, el Banco de Previsión Social ha implementado, al 18 de Agosto de 2021, controles de SI razonablemente efectivos sobre los sistemas de información que soportan la



TRIBUNAL DE CUENTAS

operativa de la aplicación sujeta al objetivo de esta auditoría; no existiendo vulnerabilidades que amenacen significativamente la confidencialidad, integridad y disponibilidad de la información manejada por la misma;

1.2) que el Organismo deberá tener en cuenta las recomendaciones efectuadas en el Informe a la Administración incluidas en el capítulo 5 en las categorías, Controles de Acceso y Continuidad en el Servicio;

2) Dar cuenta a la Asamblea General;

3) Devuélvase.

ar



Dr. Matias Consonni De León
Adscripto a la Secretaría General



TRIBUNAL DE CUENTAS

DICTAMEN AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN (TI)

El Tribunal de Cuentas ha examinado los Controles de los Sistemas de Información¹ (en adelante "SI") sobre las aplicaciones en producción del Banco de Previsión Social (en adelante "BPS"), relevantes para la auditoría financiera, en particular sobre el sistema de GRP.

Opinión

En opinión del Tribunal de Cuentas, el BPS ha implementado, al 18 de Agosto de 2021, controles de SI razonablemente efectivos sobre los sistemas de información que soportan la operativa de la aplicación sujeta al objetivo de esta auditoría; no existiendo vulnerabilidades que amenacen significativamente 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.



TRIBUNAL DE CUENTAS

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

La Dirección del BPS 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

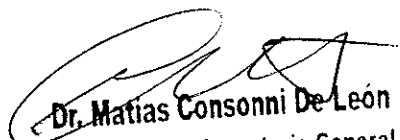
El objetivo de la auditoría consiste en expresar una opinión sobre dichos Controles basada en la auditoría realizada.

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 del BPS 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, 13 de setiembre de 2021


Dr. Matias Consonni De León
Adscripto a la Secretaría General



TRIBUNAL DE CUENTAS

INFORME A LA ADMINISTRACIÓN
AUDITORÍA TECNOLOGÍA DE LA INFORMACIÓN (TI)
BANCO DE PREVISIÓN SOCIAL

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 BPS, relevantes para la auditoría financiera.

3. ALCANCE

La revisión se circunscribió a los Controles de SI vigentes en la BPS al 18 de Agosto de 2021, a saber: controles generales de TI en el contexto relevante para los objetivos de auditoría financiera y sistema integrado de gestión (GRP).

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



TRIBUNAL DE CUENTAS

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 del BPS 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.



TRIBUNAL DE CUENTAS

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



TRIBUNAL DE CUENTAS

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 cuentan con una revisión periódica de los accesos asignados y revocados. En la política de seguridad de la información se establece que debería realizarse con una frecuencia anual para las cuentas comunes y de forma más frecuente para las cuentas privilegiadas, documentando el resultado e informarlo a las gerencias, a los propietarios de los activos y a cada uno de los usuarios involucrados.

Posible consecuencia:

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

Recomendación:

- Realizar revisiones periódicas sobre los accesos asignados y revocados, documentar e informar los resultados a las partes establecidas en la política.



TRIBUNAL DE CUENTAS

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 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	Confiabilidad
√					



TRIBUNAL DE CUENTAS

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 debilidades tales que amenacen significativamente al cumplimiento del objetivo de control.

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 se han elaborado procedimientos 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.



TRIBUNAL DE CUENTAS

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

CONSTATAIONES SOBRE CONTROLES DE APLICACIÓN - GRP

Deficiencias relevantes de control:

- No se hallaron deficiencias relevantes.

Nivel de cumplimiento del objetivo de control: ALTO


Dr. Matías Consonni De León
Adscripto a la Secretaría General