GUID 5259

Sistemas de Información Sobre Deudas Públicas

Las Guías INTOSAI (GUID) son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) como parte del Marco INTOSAI de Pronunciamientos Profesionales. Para más información visite www.issai.org

INTOSAI

Documento pre-IFPP – este documento fue desarrollado antes de la creación del Marco INTOSAI para Pronunciamientos Profesionales (IFPP) en 2016. Por ende, es posible que difiera en su motivo formal de Directrices para Auditorías de la INTOSAI más recientes.

INTOSAI

INTOSAI, 2019

1. Ratificado como ISSAI 5450: Directrices en la Auditoría de Sistemas de Información de la Gestión de Deudas Públicas en el 2016.
2. Con la institución del Marco INTOSAI de Pronunciamientos Profesionales (IFPP, por sus siglas en inglés), retitulado y catalogado como GUID 5259: Sistemas de Información sobre Deudas Públicas, con cambios editoriales en el 2019.

GUID 5259 está disponible en todas las lenguas oficiales INTOSAI: árabe, inglés, francés, alemán y español

TABLA DE CONTENIDOS

PREFACIO 5

LISTA DE ABREVIATURAS 7

INTRODUCCIÓN 8

1. PLANEACIÓN 9

2. CONTROLES GENERALES 13

Controles Organizacionales 14

Controles de Acceso Físico 14

Controles de Acceso Lógico 15

Controles Ambientales 15

Controles de Cambios a Programas 15

Plan de la Continuidad del Negocio y Recuperación ante Desastres 16

3. CONTROLES DE APLICACIÓN 16

3.1. NORMAS DE DOCUMENTACIÓN 17

3.2. CONTROLES DE ENTRADA 19

Pantallas de Captura de Datos 20

Rutinas de Preparación de Datos 20

Autorización de Captura de Datos 20

Retención de Documentos de Entrada 21

Validación de Entrada de Datos 21

Errores de Captura De Datos 22

Mecanismos de Apoyo a la Captura de Datos 23

3.3. CONTROLES DE PROCESAMIENTO **23**

Integralidad 23

3.4. CONTROLES DE SALIDA **25**

3.5. COMPROBACIÓN DE CONTROLES DE APLICACIÓN **26**

3.6. ELABORACIÓN DE INFORMES SOBRE LOS RESULTADOS DE AUDITORÍA **28**

APÉNDICE I: Tabla de Planeación **29**

APÉNDICE II: Matriz de Pruebas para Controles Generales **35**

APÉNDICE III: Matriz de Pruebas para Controles de Aplicación **42**

Figura 1: Auditorías a la Deuda Pública por EFS: El caso de Brasil **61**

Figura 2: Auditorías de Deuda Pública por EFS: El caso de Moldavia **66**

BIBLIOGRAFÍA **68**

PREFACIO

1) La deuda pública está en el centro de cualquier discusión sobre la gestión de finanzas públicas. En la búsqueda por expandir sus economías y mejorar los servicios sociales en sus respectivos países, la mayoría de los gobiernos enfrentan grandes necesidades financieras. En teoría, la deuda pública es una herramienta eficaz para el crecimiento económico y para distribuir equitativamente la carga fiscal entre las generaciones actuales y futuras de contribuyentes. Sin embargo, debido a su importancia para el equilibrio económico, es esencial dimensionar y administrar la deuda pública con mucha cautela.

2) El objetivo principal de la gestión de la deuda es la obtención de un financiamiento estable, al menor costo posible y en niveles prudenciales de riesgo, para sostener las actividades del gobierno. La *Revisión de las Directrices para Gestión de la Deuda Pública* del Banco Mundial y el Fondo Monetario Internacional (FMI) brindan un conjunto sólido de prácticas relacionadas con los controles internos de gestión de la deuda. Entre ellas se encuentra la determinación de que "las actividades de gestión de la deuda deben estar apoyadas por un sistema de información para la gestión exacto e integral con salvaguardas adecuadas". Los países interesados en asegurar una gestión eficaz de la deuda pública deben dar alta prioridad al desarrollo de sistemas confiables para registrar y reportar información de deuda. Esto es necesario no sólo para desarrollar datos de deuda y garantizar el pago oportuno de la deuda, sino también para mejorar la calidad de los informes de presupuesto y transparencia de las cuentas públicas, lo que permite a las autoridades y los administradores de la deuda pública alcanzar las metas en esta materia.

3) La auditoría de Sistemas de Información para la Gestión de la Deuda Pública pretende garantizar la eficiencia, eficacia y efectividad de la gestión de la deuda pública. Por esta razón, cualquiera de este tipo de auditorías debe clasificarse como una auditoría de desempeño. Sin embargo, este trabajo puede ser también de gran relevancia en el contexto de auditorías financieras, las cuales se centran en determinar si la información financiera del gobierno es presentada de conformidad con el marco regulatorio aplicable a la presentación de informes financieros y si la información es confiable y libre de fraude o error. En este contexto, este trabajo adquiere gran importancia, ya que contribuye a lograr un sistema de información que recopila y produce información precisa y confiable sobre uno de los elementos financieros gubernamentales más significativos: la deuda pública.

4) Esta GUID pretende proporcionar a los auditores una directriz descriptiva sobre la Auditoría de los Sistemas de Información para la Gestión de la Deuda Pública. Teniendo en cuenta que la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI) cuenta ya con algunos documentos relacionados con auditorias de Tecnologías de la Información (TI), desarrollados por el grupo de trabajo sobre auditoría de TI (WGITA), el enfoque de esta GUID se centra en los controles de las aplicaciones, que deben ser específicos para el Sistema de Información para la Gestión de la Deuda Pública.

LISTA DE ABREVIATURAS

BCP – Plan de Continuidad del Negocio (Business Continuity Planning)

CAAT – Técnicas de Auditoría Asistida por Computadora

CS-DRMS – Secretaría de la Commonwealth – Sistema de Registro y Gestión de la Deuda

DMO – Oficina de Gestión de la Deuda

DRP – Plan de Recuperación ante Desastres

EFS – Entidad Fiscalizadora Superior

FMI – Fondo Monetario Internacional

FMIS – Sistema de Información para la Gestión Financiera (Financial Management Information System)

INTOSAI – Organización Internacional de Entidades Fiscalizadoras Superiores

MF – Ministerio de Finanzas

PDMIS – Sistema de Información para la Gestión de la Deuda Pública

SID– Sistema de Deuda Integrada del Gobierno Federal de Brasil (Integrated Debt System of the Federal Goverment of Brazil)

SIGADE – Sistema de Gestión y Análisis Financiero de la Deuda (DMFAS, por sus siglas en inglés)

TI – Tecnologías de la Información

UNCTAD – Conferencia de las Naciones Unidas sobre Comercio y Desarrollo

WGITA – Grupo de Trabajo sobre Auditoría de las TI

WGPD – Grupo de Trabajo sobre Deuda Pública

INTRODUCCIÓN

Bajo los términos de referencia establecidos por el Consejo Directivo de la INTOSAI, el Grupo de Trabajo sobre Deuda Pública (WGPD) recibió la tarea de publicar directrices y otros materiales informativos para ser utilizados por las Entidades Fiscalizadoras Superiores (EFS) para fomentar una divulgación adecuada de la deuda pública y una sólida gestión de la misma.

Esta GUID pretende aumentar la capacidad del WGPD al proporcionar un marco general que pueda ser utilizado en las auditorías de las EFS para evaluar controles generales y de aplicación de los Sistemas de Información para la Gestión de la Deuda Pública (PDMIS). Es importante considerar que, en las referencias, PDMIS abarca uno o más sistemas de información utilizados en la gestión de la deuda pública.

Con el avance de las Tecnologías de la Información, las organizaciones gubernamentales se han vuelto cada vez más dependientes del uso de las TI para llevar a cabo sus operaciones de negocios y servicios de entrega, así como para procesar, mantener y reportar información esencial. Según un Documento de Trabajo del FMI, “un FMIS (Sistema de Información para la Gestión Financiera) generalmente se refiere a la informatización del proceso de gestión del gasto público, incluyendo la formulación del presupuesto, el ejercicio presupuestario y la contabilidad, con la ayuda de un sistema totalmente integrado para la gestión financiera en los ministerios competentes y otros organismos que efectúen gastos.”

La norma del Instituto de Ingenieros en Electricidad y Electrónica (IEEE, por sus siglas en inglés) define los sistemas como “una colección de componentes organizados para cumplir una función específica o un conjunto de funciones”. En particular, la actividad principal de un sistema en una oficina de deuda es mantener la base

de datos de préstamos para operaciones del sector público, utilizando un software adecuado tanto para registro como para la ejecución de funciones analíticas por parte de la Oficina de Gestión de la Deuda (DMO).

La auditoría a las TI puede clasificarse, con respecto a los enfoques predominantes, como se indica a continuación:

- Gobernanza de las TI;
- Auditoría de Datos;
- Auditoría a los Sistemas de Información;
- Contratación de las TI, y
- Seguridad de la Información.

En general, un auditor de las TI trabaja con más de un enfoque, sin embargo, el auditor puede elegir el enfoque predominante. En esta directriz, el enfoque predominante es la *Auditoría a los Sistemas de Información.*

Esta GUID está estructurada en planeación, evaluación de controles generales y evaluación de controles de aplicación.

1. PLANEACIÓN

El Sistema de Información para la Gestión de la Deuda Pública (PDMIS, por sus siglas en inglés) puede considerarse como un conjunto de partes interdependientes (estructuras físicas, personal, herramientas tecnológicas) que interactúan con el fin de registrar, controlar, evaluar y administrar las transacciones que se generan al adquirir, mantener y solventar la deuda pública.

Esta fase ayuda al auditor en la comprensión de las operaciones y controles relacionados al sistema, así como de los riesgos relacionados en vista de los riesgos de flujo de operación inherentes a la deuda pública. Con base en este entendimiento, el auditor evalúa el entorno general de control, identifica los sistemas utilizados en la gestión de la deuda pública, mide toda la documentación relativa a estos sistemas

y hace una evaluación preliminar del riesgo. El resultado de la evaluación guiará el alcance de los procedimientos a ser empleados en la fase de prueba.

La EFS también examina todas las estructuras relacionadas con la Oficina de Deuda Pública, tales como personal, proceso, tipos de deudas, seguridad de datos, herramientas tecnológicas y otros.

En esta fase el auditor debe incluir una evaluación preliminar de la estructura de la oficina de deuda pública y de los flujos de operación de la deuda pública, cubriendo lo siguiente:

- ¿cómo está organizado el PDMIS: cuáles son los sistemas utilizados para registro, procesamiento, informe, control y gestión de deuda pública y cuáles son los principales procesos y funciones que realiza cada sistema?;
- el funcionamiento de la auditoría interna;
- los resultados de auditorías previas (internas o externas) respecto al PDMIS;
- el almacenamiento físico de los documentos de operaciones;
- el uso del hardware y software y la responsabilidad de su mantenimiento;
- las operaciones procesadas por sistemas de información y su importancia relativa;
- cómo ocurre la relación entre los componentes de información de deuda pública;
- métodos y procedimientos establecidos para la implementación de nuevas operaciones o las revisiones de operaciones existentes, y
- evaluación previa de los controles internos de la Oficina de Gestión de la Deuda (DMO, por sus siglas en inglés). Si los controles internos de la DMO no fueron evaluados previamente, la EFS debe hacer esta valoración. Este procedimiento es muy importante para evaluar el grado de los riesgos existentes y, de ese modo, determinar las pruebas de auditoría que sean necesarias.

El nivel de refinamiento del sistema no afecta en la evaluación de controles generales, la cual siempre debe ser llevada a cabo. Sin embargo, determina los procedimientos de auditoría a ser llevados a cabo e indica cuántos especialistas de TI son necesarios para realizar el trabajo de auditoría. Se sugiere por lo menos un especialista en TI como parte del equipo que realiza todos los trabajos que involucran sistemas. Es importante, para los auditores en el equipo que son nuevos en la auditoría a las TI, adquirir conocimientos sobre los términos generalmente empleados. En este caso, un buen diccionario técnico de TI representa una inversión importante para una EFS. El documento *Auditoría a los Sistemas de Información – Glosario de Términos*, del Grupo de Trabajo de la INTOSAI sobre Auditoría a las TI (WGITA, por sus siglas en inglés), es muy útil para este propósito.[1]

Los auditores que ya estén familiarizados con la terminología de las TI deben conocer también la terminología utilizada en la DMO, especialmente siglas y abreviaturas (tipos de encabezados, sectores de la DMO, acreedores, nombres de los sistemas, software utilizado por la DMO, etc.). Se considera esencial contar con este conocimiento antes de realizar las entrevistas. Un glosario muy útil, desarrollado por la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD), puede encontrarse en los siguientes enlaces:

» http://unctad.org/en/docs/pogiddmfasm3r3.en.pdf – Debt and DMFAS Glossary (versión en inglés)

» https://unctad.org/es/docs/pogiddmfasm3r3.sp.pdf – Glosario de la deuda y del SIGADE (versión en español)

Entender a detalle un PDMIS significa conocer los flujos inherentes de información y de datos. Por lo tanto, es muy importante, en la fase de planeación, mapear los procesos clave de la deuda pública (registro, procesamiento, control, seguridad, informes y análisis) y comprender cómo se llevan a cabo estos procesos a través del sistema de información. Después de eso, es necesario realizar una evaluación del riesgo para identificar los riesgos mayores asociados a procesos clave de operación y de gestión de la deuda pública, teniendo en cuenta su impacto y probabilidad de incidencia. La evaluación del riesgo es fundamental para determinar el alcance de los procedimientos necesarios para administrar los niveles de riesgo asociados.

1 Algunos glosarios en línea, que pueden ser muy útiles, son: http://www.webopedia.com o http://whatis.techtarget.com.

La antigua *ISSAI 5410: Directrices para la Planeación y Conducción de Auditorías de Controles Internos de la Deuda Publica* podría ser considerada, cuando desempeñada, como la evaluación de riesgo. Adicionalmente, podría establecerse la evaluación de riesgos en el contexto de auditorías financieras.

Los flujos de un PDMIS casi siempre son determinados en la DMO. Otras oficinas pueden ser igualmente responsables de la captura de datos de deuda, por ejemplo, en el caso de deuda contractual. Cuando la DMO se divide en oficina interna (back-office), intermedia (middle-office) y frontal (front-office), cada función clave tiene sus propios flujos de datos y de información. La oficina frontal es comúnmente responsable de ejecutar transacciones en los mercados financieros, incluyendo la gestión de subastas y otras formas de préstamos, así como todas las otras operaciones de financiamiento. La oficina interna se encarga de la liquidación de las transacciones y del mantenimiento de los registros financieros. Una oficina intermedia, o de gestión de riesgos, independiente generalmente lleva a cabo el análisis de riesgos y monitorea e informa sobre riesgos de cartera y evalúa el desempeño de los administradores de deuda contra objetivos o referencias estratégicas. La mayoría de los flujos de datos relacionados con la deuda pública, incluyendo los datos externos, se encuentran en la oficina interna, encargada del registro y control de la captura de datos.

Dado que muchos países utilizan un sistema comercial desarrollado y actualizado por organizaciones internacionales a cargo de terceros (por ejemplo, SIGADE, CS-DRMS) para la gestión de la deuda pública, es muy importante el uso de informes relacionados con el desempeño, tales como evoluciones acontecidas, solicitudes de mantenimiento al sistema y registros de incidentes.

El programa SIGADE, desarrollado por la UNCTAD, se centra en actividades “descendentes”. Estas incluyen mantenimiento de bases de datos, validación de datos, operaciones de deuda, informes de deuda interna y externa, estadísticas y análisis básico de deuda, así como establecer vínculos informáticos entre gestión de la deuda y otros softwares financieros. Complementan otras actividades más “ascendentes”, como análisis de sostenibilidad de la deuda suministrado por otros proveedores como el Banco Mundial. Adicionalmente, el programa ayuda cada vez más a los países a establecer vínculos entre el sistema SIGADE y otros softwares gubernamentales (por ejemplo, los utilizados para la elaboración de presupuestos, administración de tesorería, gestión de ayuda) o al interior de complejos sistemas

financieros integrados como parte de los esfuerzos globales de los países en materia de gestión financiera pública.[2]

La aplicación del CS-DRMS, que es brindado por el Secretariado del Commonwealth, ayuda a las EFS en el registro, administración y análisis de su deuda desde una perspectiva integral. Esto brinda un repositorio central para varias categorías de deuda garantizada pública y privada, externa e interna, incluyendo deuda a corto plazo. El sistema también maneja becas, préstamos de gobierno y re-préstamos.[3]

En el caso de países que utilizan SIGADE o CS-DRMS parala gestión de la deuda pública, los informes de auditoría del PDMIS llevados a cabo por otros países (EFS) podrían ser de gran utilidad para la identificación de las deficiencias más frecuentes, de aquellas que tienen el mayor impacto, o ambas.

En el Anexo I, se incluye una tabla sobre la información, los procedimientos y las preguntas requeridas que la EFS debe responder, mismas que pueden ser utilizadas por el equipo de auditoría durante la fase de planeación del trabajo de auditoría a los sistemas de deuda pública.

2. CONTROLES GENERALES

Los controles generales brindan el marco de controles globales para funciones de las TI[4].Esos controles están diseñados para abordar temas de desarrollo, operación y mantenimiento del entorno. Los objetivos de los controles generales son salvaguardar los datos, proteger los programas de aplicación y garantizar el funcionamiento continuo de las operaciones de cómputo en caso de interrupciones inesperadas.

Aunque una auditoría del sistema de deuda pública requiere la verificación de los controles generales de TI, este documento no abordará estos controles a fondo dado que la INTOSAI ha emitido documentos sobre auditoría de TI que atienden en detalle esos controles generales.

2 Para mayor información, visite: http://unctad.org/dmfas.
3 Para mayor información, visite: http://www.csdrms.org.
4 IDI – Curso Virtual sobre Auditoría a la Gestión de la Deuda Pública, Sesión 6: Auditoría al Sistema de Información para la Gestión de la Deuda Pública.

Se sugiere que, al realizar una auditoría de sistema, el equipo de auditoría podría considerar el uso del contenido de la antigua ISSAI 5310 : Directrices sobre Auditorías de Seguridad en Sistemas de Información (ISec), una guía para la revisión de la seguridad de los sistemas de información en las organizaciones gubernamentales.

Otro documento que puede ser útil para la planeación de controles generales es el Manual sobre Auditoría de TI para Entidades Superiores *(Handbook on IT Audit For Supreme Institutions)* del WGITA - IDI, que proporciona a los usuarios información esencial y preguntas clave para una planeación efectiva de auditorías de TI.

El Apéndice II presenta una matriz de pruebas, con algunos controles generales y sugerencias de procedimientos que pueden ayudar al auditor para realizar pruebas generales a los controles.

Un conjunto completo de las distintas categorías de controles generales incluye los puntos que se describen a continuación:

» CONTROLES ORGANIZACIONALES

Controles organizacionales son las políticas, procedimientos y marco organizativo establecidos para asegurar políticas de recursos humanos y prácticas de gestión sólidas, segregación de funciones, y políticas de seguridad de la información, además de brindar métodos para determinar la eficacia y garantizar controles operacionales y eficiencia.

» CONTROLES DE ACCESO FÍSICO

Los controles de acceso físico incluyen normas y prácticas para prevenir el acceso no autorizado y la interferencia con los servicios de TI, incluyendo procedimientos administrativos, tales como requerimiento de gafetes de identificación de personal y control de visitantes, y medidas físicas tales como cerraduras mecánicas y cerraduras electrónicas, cámaras y otros medios para limitar el acceso físico a servidores y a toda infraestructura crítica.

» CONTROLES DE ACCESO LÓGICO

Los controles de acceso lógico utilizan seguridad integrada en los sistemas informáticos para impedir el acceso no autorizado a datos y archivos confidenciales y para asegurar que todos los usuarios tengan derechos de acceso limitados a las exigencias de sus funciones. Estos controles incluyen firewall, software antivirus, y detección de intrusos y de malware.

En sistemas modernos, estos controles se obtienen de muchas y variadas maneras. Se implementan a través de software de aplicación, sistema operativo, sistema de gestión de base de datos, software de control de acceso, monitores de procesamiento de transacciones en línea, servidores, la red, la red del área local (LAN) y posiblemente otro software.[5]

» CONTROLES AMBIENTALES

Los controles ambientales son reglas, prácticas y condiciones intrínsecas para evitar daños por inestabilidad eléctrica, fuego, polvo, agua, alimentos, temperaturas o humedad extremas, o electricidad estática, entre otros.

Aunque el enfoque de estos controles es el centro de datos (o espacio dedicado al equipo de TI, que requiere un entorno específico o al menos protección contra el robo), también son aplicables a todos los entornos de oficina.

» CONTROLES DE CAMBIOS A PROGRAMAS

Los controles de cambios a programas incluyen reglas para asegurar que todos los cambios en la configuración del sistema se manejen con precisión, de manera completa y oportuna.

Las actualizaciones y modificaciones deben tener un proceso formal para asegurar el registro de todos los cambios y para proporcionar la capacidad de dar marcha atrás en caso de problemas con la nueva versión.

5 Xenia Ley Parker, Auditorías de Tecnologías de la Información (Information Technology Audits), CCH Incorporated, USA 2006.

Una aprobación formal debe ser requerida antes de que los programas sean transferidos de ambientes de pruebas a bibliotecas de producción, y toda la documentación de sistema, operaciones y programas debe mantenerse completa; actualizada, y conforme a las normas, políticas y procedimientos.

» PLAN DE LA CONTINUIDAD DEL NEGOCIO Y RECUPERACIÓN ANTE DESASTRES

El plan de continuidad del negocio (BCP, por sus siglas en inglés) y el plan relacionado de recuperación ante desastres (DRP, por sus siglas en inglés) están diseñados para atender el objetivo de disponibilidad. La planeación de contingencia y de recuperación ante desastres, viabilidad de los planes, pruebas, monitoreo, y la necesidad de actualización continua de los planes son factores críticos.[6]

ElBCP es un enfoque general para proveer vías alternativas de soporte a los procesos críticos del negocio en caso de emergencia, desastre u otra disrupción. El enfoque está en la supervivencia total del negocio y no sólo de las TI. Sin embargo, el plan general debe incluir la consideración de requerimientos de sistemas de información y de red de telecomunicaciones. Esta parte del BCP es un DRP.

Los planes DRP y los planes relacionados BCP pueden desarrollarse al mismo tiempo, de tal manera que todos los aspectos sean considerados simultáneamente. Como mínimo, el plan debe incluir procedimientos y criterios para determinar cuándo una situación es un desastre, quién es la persona encargada de tomar tal determinación, y cómo declarar formalmente un evento como desastre y poner el plan en marcha.

3. CONTROLES DE APLICACIÓN

Los controles de aplicaciones están automatizados en las aplicaciones de los sistemas de información para ayudar a asegurar la autorización, integridad, exactitud y validez de las transacciones. Están integrados en la programación de una aplicación y son frecuentes en las operaciones de entrada, procesamiento y salida de la aplicación. Su objetivo es garantizar la integridad, fiabilidad y exactitud del procesamiento de datos.

6 Xenia Ley Parker, Auditorías de Tecnologías de la Información, (Information Technology Audits), CCH Incorporated, USA 2006.

Ejemplos de controles de aplicación incluyen verificaciones realizadas por la aplicación en el formato de los datos introducidos con el fin de evitar la entrada de datos no válidos, controles de proceso que impiden el registro de transacciones no autorizadas, y generación de informes detallados y controles sobre transacciones totales para asegurar que todas las transacciones sean registradas completa y precisamente.

Los controles de aplicación pueden clasificarse como sigue:

» de entrada;

» de procesamiento; y

» de salida.

3.1. NORMAS DE DOCUMENTACIÓN

Las normas de documentación aseguran que se mantenga la documentación de la aplicación de manera adecuada y vigente. También es importante su cuidados a actualización.[7]

Una documentación adecuada es importante para mejorar la comprensión sobre los controles que estén implementados o que deban estarlo.

Una buena documentación de las aplicaciones reduce asimismo el riesgo de que los usuarios no sigan los procedimientos de control previstos por la administración. La revisión de una documentación completa y actualizada ayuda al auditor a adquirir la comprensión del funcionamiento de cada aplicación y puede ayudar a identificar los riesgos particulares de auditoría.

» La documentación de aplicación: ayuda a los programadores de mantenimiento a comprender la aplicación, corregir los problemas y realizar mejoras. La documentación se incrementa en cada fase del proceso de desarrollo y puede ser elaborada en distintos formatos tales como diagramas, gráficos, tablas o texto. La documentación puede incluir detalles

7 Oficina del Contralor y Auditor General de la India, Information Technology Audit - General Principles. (IT Audit Monograph Series # 1)

sobre fuente de datos, atributos de datos, pantallas de entrada, validaciones de datos, procedimientos de seguridad, descripción de cálculos, diseño del programa, interfaces a otras aplicaciones, procedimientos de control, manejo de errores, instrucciones de operación, archivo, respaldo, así como procedimientos de almacenamiento y recuperación. La documentación de la aplicación debe actualizarse a medida que se modifique la aplicación. User documentation: Includes descriptions of both automated and manual workflows to aid in initial training on the application and for ongoing reference.

» Documentación de usuario: Incluye descripciones tanto de los flujos de trabajo automatizados como de los flujos manuales para ayudar en la capacitación inicial sobre la aplicación y como referencia continua. En ambos casos, la documentación de la aplicación debe actualizarse a medida que se modifique la aplicación.

La documentación debe incluir:

» un resumen de la aplicación;

» especificación de requisitos de usuario;

» descripción y listado de los programas;

» descripción de entradas y salidas;

» descripción de contenido de archivos;

» manuales de usuario;

» instrucciones de escritorio;

» descripción de controles de seguridad de la aplicación;

» resumen reciente de las evaluaciones de seguridad;

» decisiones recientes de seguridad y acciones recomendadas; y

» estado de las acciones recomendadas.

3.2. CONTROLES DE ENTRADA

Los controles de entrada son muy importantes para disminuir el riesgo de error o de fraude en aplicaciones de cómputo. Los controles sobre las entradas son vitales para la integridad de los datos.

Los controles de entrada aseguran la autorización, exactitud, integridad y oportunidad de los datos introducidos en una aplicación. La autorización se garantiza al requerir aprobaciones secundarias de transacciones que rebasen un umbral definido. La exactitud es asegurada por controles de edición que validan los datos introducidos antes de aceptar una transacción para su procesamiento. La integridad está garantizada a través de procedimientos de manejo de errores que proporcionan su registro, informe y corrección. La oportunidad está garantizada mediante el monitoreo deflujo y registro de transacciones y presentación de informes de excepciones.

Los controles de entrada pueden estar presentes en:

- pantallas de captura de datos;
- rutinas de preparación de datos;
- autorización de captura de datos;
- conservación de documentos de captura;
- validación de captura de datos;
- procedimientos para errores en captura de datos; y
- mecanismos de apoyo a la captura de datos.

Los controles mencionados anteriormente pueden eludirse si existe la posibilidad de introducir o modificar datos desde fuera de la aplicación. Debe haber comprobaciones automáticas de integridad en la aplicación que detecten e informen cualquier cambio externo a los datos. Por ejemplo, debe existir una verificación que detecte e informe modificaciones no autorizadas a la base de datos de transacciones subyacente.

» PANTALLAS DE CAPTURA DE DATOS

Las pantallas de captura de datos estandarizadas pueden garantizar la consistencia de los datos.

El PDMIS puede incluir las siguientes funcionalidades:

- » pantallas de entrada estructuradas en un formato y diseño estandarizado;
- » campos de entrada que restrinjan lo que los usuarios puedan capturar;
- » entrada obligatoria para ciertos campos; y
- » función de ayuda (por ejemplo, F1) para ayudar a los usuarios a llenar los campos.

» RUTINAS DE PREPARACIÓN DE DATOS

El objetivo de las rutinas de preparación de datos es evitar fallas durante los procedimientos de entrada.

El PDMIS puede incluir entornos integrados para procedimientos de compartir datos para transferir estos a otras aplicaciones.

» AUTORIZACIÓN DE CAPTURA DE DATOS

Autorización de captura de datos tiene por objeto garantizar que toda captura de datos haya sido registrada y autorizada por la persona apropiada.

El PDMIS puede incluir las siguientes funcionalidades:

- » contraseña de acceso requerida;
- » registro en bitácora de acceso cuando existe una captura manual de datos, y
- » requisito de dos aprobaciones para ciertas operaciones sensibles (por ejemplo, activación de contratos, modificación de tasas de interés, y modificaciones de valores de contratos).

» RETENCIÓN DE DOCUMENTOS DE ENTRADA

Esta dimensión de controles de entrada de datos se refiere al mantenimiento y control de los documentos originales que respaldan los registros de datos de deuda. En el caso de transferencia automática de archivos entre aplicaciones, el PDMIS debe mantener los datos originales, recibidos de la otra aplicación, por un período preestablecido por la DMO.

» VALIDACIÓN DE ENTRADA DE DATOS

Los controles de validación de datos están diseñados para asegurar que los datos de entrada son válidos y precisos.

El PDMIS puede incluir las siguientes funcionalidades:

- Listas de comprobación automática para verificar ausencia de valores (por ejemplo, al descargar una serie histórica de índices, el PDMIS comprueba si falta un valor diario, mensual o anual).

- Todas las pantallas de captura de datos identifican claramente los campos obligatorios y la aplicación permite la confirmación de la operación sólo si se ha introducido toda la información obligatoria.

- Cada tabla de base de datos debe contener, en los campos, una regla específica que no permita la duplicación de datos.

- Si la aplicación considera que se introducen datos duplicados, rechazará la entrada hasta que la duplicación se haya resuelto.

- La aplicación no permite la modificación de algunos datos después de su registro (por ejemplo, el tipo de cambio del día de la operación). Con respecto a otros datos, la aplicación podría permitir alteraciones si se cumplen ciertas condiciones (por ejemplo, cuando el estado de un contrato sea “Bloqueado” o “Concluido”, ningún dato podrá ser modificado).

- Algunos campos, al ser llenados, requieren que otros sean llenados (por ejemplo, si el usuario captura la comisión de compromiso de un contrato, debe introducir también el impuesto de compromiso).

- Los campos de "fecha" son esenciales para el control general de un contrato de deuda. Son particularmente útiles en los cálculos de parcialidades, para evitar retrasos de pagos, cobro de multas, etc. Por lo tanto, la aplicación debe tener reglas básicas para la inserción de "fecha".

- Con la excepción de operaciones simuladas, la aplicación del sistema no permite el registro de datos, para una fecha futura, por ejemplo: desembolso, reversión de pago, cancelación de contrato, o adición de éste.

ERRORES DE CAPTURA DE DATOS

Un registro o bitácora de auditoría es un registro cronológico, un conjunto de registros o bien registros de origen y destino, relativos a la seguridad, que proporcionan evidencia documental de la secuencia de actividades que han afectado en cualquier momento una operación, procedimiento o evento específico. Los rastros de auditoría o archivos de bitácora deben restringirse al personal apropiado.

El PDMIS puede incluir las siguientes funcionalidades:

- la DMO debe definir responsables de los expedientes pendientes;

- la aplicación debe contar con programas para registrar las incidencias de errores, reportar errores pendientes, y registrar las correcciones éstos;

- en un proceso de descarga automática de datos, cuando la aplicación identifica disparidades en las series, un correo electrónico automático debe ser enviado a los usuarios apropiados para su seguimiento, y

- la aplicación debe enviar informes periódicos de errores no resueltos – incluyendo el tiempo que los errores han permanecido sin resolverse y su prioridad- al personal apropiado.

» MECANISMOS DE APOYO A LA CAPTURA DE DATOS

Estos controles están relacionados con los procedimientos de apoyo en la DMO que ayudan a los usuarios a introducir datos en la aplicación informática, reinicializar aplicaciones y monitorear las actividades de usuario para evitar posibles desviaciones de las reglas establecidas.

Estos mecanismos están a menudo incluidos en los controles generales.

3.3. CONTROLES DE PROCESAMIENTO

Los controles de procesamiento garantizan la exactitud, integridad y oportunidad de los datos durante el procesamiento por lotes o en línea. Estos controles ayudan a asegurar que los datos sean procesados con precisión a lo largo de la aplicación y que ningún dato sea añadido, extraviado o alterado durante el procesamiento.[8]

» INTEGRALIDAD

La Integralidad puede ser asegurada, en el procesamiento por lotes, balanceando las transacciones recibidas por un sistema con las transacciones enviadas por un sistema subsidiario.

El balanceo debe ocurrir entre aplicaciones que comparten datos comunes, mediante la creación de un informe de conciliación que presente los datos de ambas aplicaciones e informe las posibles diferencias en un grupo de usuarios.[9]

Los totales de balanceo deben incluir, una cuenta de transacción y los totales para todos los campos de monto, para cada tipo de transacción, así como el cruce de los totales para los campos de detalle a los campos totales.[10]

En los archivos donde no haya totales significativos, pueden crearse cifras de control que sumen todos los datos en una columna para verificar que la misma cifra es

8 Frederick Gallegos, Sandra Senft, Daniel P. Manson, y Carol Gonzales, Information Technology Control and Audit– Second Edition, Auerbach Publications, EUA 2004.
9 Ídem.
10 Ídem.

aceptada por el siguiente proceso. Por ejemplo, la suma de las cantidades del acuerdo de deuda no es significativo, pero esta cifra se puede utilizar para verificar que todas las cantidades del acuerdo hayan sido incluidas correctamente en el proceso.[11]

El PDMIS puede incluir las siguientes funcionalidades:

» En la interfaz con aplicaciones de otros sistemas, si hay un error al procesar un archivo, se genera un archivo de errores que queda registrado en la aplicación del sistema. Los usuarios deben desarrollar un enfoque de interoperabilidad más profundo para los perfiles técnicos y en la capacitación dentro de la entidad.

» La aplicación cuenta con un gran número de tareas programadas por lotes, como, por ejemplo: actualización del capital accionario, planeación financiera, índices, y pagos futuros. Los usuarios deben evaluar las salidas de sistemas de tiempo real suave, enfocándose en las bitácoras de procesos por lotes, así como en las capacidades de "tiempo real duro" para medir una información de procesamiento actualizada.

» En caso de error en trabajos por lotes, la aplicación envía un mensaje al usuario con información sobre el error. El usuario puede verificar las capacidades de consolidación dentro del sistema para cumplir con las políticas de corrección de errores y configurar procedimientos de control.

» Después de concluida una operación, la aplicación muestra un mensaje confirmando que el proceso ha sido exitoso, incluyendo un resumen de los datos introducidos.

» Después de una modificación a datos previamente registrados, la aplicación muestra un mensaje informando del éxito de la modificación y presenta un resumen de los datos modificados.

» Después de una eliminación de datos previamente registrados, la aplicación muestra un mensaje informando del éxito de la eliminación y presenta un resumen de los datos eliminados

11 Ídem.

» Si la eliminación de un registro afecta la integridad relacional de la base de datos, la aplicación no permite la eliminación y muestra un mensaje informando que no es posible eliminar el registro. Por ejemplo, los datos de un banco acreedor no pueden ser eliminados de la tabla de acreedores si este acreedor tiene contratos vigentes en la aplicación.

» La aplicación realiza algunas comprobaciones entre los datos de la oficina frontal y la oficina interna, como, por ejemplo, requiriere que la oficina interna valide la entrada de datos de subastas. Los usuarios pueden verificar, en las comunicaciones, las interrelaciones de arquitectura de datos entre componentes y sistemas para comprobar los flujos de datos conforme al esquema de interoperabilidad.

3.4. CONTROLES DE SALIDA

Los controles de salida aseguran la integridad y la distribución correcta y oportuna de las salidas generadas. Las debilidades en el proceso a veces pueden ser compensadas por controles sólidos en la salida.[12] Una aplicación bien controlada en la entrada y el procesamiento será probablemente socavada totalmente si la salida no es controlada.[13]

La integralidad e integridad de los informes de salida dependen de restringir la capacidad de modificar las salidas y de incorporar controles de integridad tales como números de página y sumas de verificación.[14]

Los archivos de salida deben ser protegidos para reducir el riesgo de modificaciones no autorizados. Posibles motivaciones para modificar la salida de la computadora incluyen el encubrimiento de procesamientos no autorizados o la manipulación de resultados financieros no deseados.[15]

La salida de una aplicación puede conformar la entrada a otra aplicación. En este

12 Frederick Gallegos, Sandra Senft, Daniel P. Manson, y Carol Gonzales, Information Technology Control and Audit– Second Edition, Auerbach Publications, EUA 2004.
13 Organización de Entidades Fiscalizadoras Superiores de Asia. IT Audit Guidelines– 6th Edition, Septiembre de 2003.
14 Oficina del Contralor y Auditor General de la India, Information Technology Audit - (General Principles, IT Audit Monograph Series
15 Ídem.

caso, el auditor debe buscar controles para asegurar que las salidas se transfieran con precisión de una etapa de procesamiento a la siguiente.[16]

En el PDMIS, los controles de salida pueden programarse para identificar la información crítica que requiera de acciones prioritarias por parte de la gestión de la deuda pública. Por ejemplo, para los contratos con vencimiento en el mes en curso, la aplicación puede mostrar alertas diarias, en la primera pantalla del sistema, cuyas fechas de pago expirarán en los siguientes cinco días.

La aplicación también puede permitir que ciertos perfiles de usuario generen informes, en modo prioritario, de modo que la aplicación pueda asignar prioridades a los informes que a ser generados.

La aplicación brinda:

» comparación automática de la suma de los datos de origen contra la suma de los datos procesados;

» la aplicación debe informar a los usuarios sobre el estado de las solicitudes de generación de informes, por ejemplo, “no iniciado”, “en proceso” y “concluido”, y

» al final de un proceso de generación de informes, la aplicación envía un mensaje al usuario que hizo la solicitud informándole que esa tarea concluyó.

3.5. COMPROBACIÓN DE CONTROLES DE APLICACIÓN

Una vez que los controles han sido identificados, el siguiente paso en una auditoría es verificar su eficacia.

Esto puede lograrse mediante:

» presentación de un conjunto de datos de prueba que producirán resultados conocidos, si la aplicación funciona correctamente;

16 Ídem.

» desarrollo de programas independientes para volver a ejecutar la lógica de la aplicación, y

» evaluación de los resultados de la aplicación.

Los procedimientos anteriores comprueban la integridad de un programa incorporado en el PDMIS y no la integridad de los datos.

Si la aplicación cuenta con un ambiente de pruebas, este puede usarse para probar los controles, siempre y cuando el ambiente de pruebas sea una copia confirmada del ambiente de producción.

Para probar las reglas de cálculo, como las que se refieren a la actualización del capital accionario o al servicio de la deuda, el auditor necesitaría emplear Técnicas de Auditoría Asistida por Computadora (CAAT, por sus siglas en inglés), las cuales incluyen numerosos tipos de herramientas y técnicas tales como software generalizado de auditoría, software de utilidad, datos de prueba, rastreo y mapeo de software de aplicación y aplicaciones expertas de auditoría. Podrían incluir herramientas que analicen la lógica de la hoja de cálculo y los estimados para precisión. Podría utilizarse asimismo herramientas para analizar aplicaciones de base de datos y generar un diagrama lógico de flujo. El software generalizado de auditoría puede ser utilizado para analizar los datos producidos por la mayoría de las aplicaciones.

El auditor debe evaluar la necesidad de utilizar las CAAT. Debe basarse en la sofisticación de la aplicación de gestión de deuda pública.

Este documento incluye una matriz sugerida de pruebas (Ver Apéndice III), que puede ser utilizada por el equipo auditor como referencia para realizar pruebas de controles de las aplicaciones. Esta matriz identifica algunos requisitos y funcionalidades que los sistemas de deuda pública deben brindar y las consultas que deben ser capaces de realizar, así como los requisitos mínimos para las capacidades de tales sistemas.

Es importante tener en cuenta que, así como la deuda de cada país tiene diferente composición y características, los sistemas de gestión de la deuda presentan igualmente características diferentes. Por lo tanto, es responsabilidad del equipo de auditoría identificar, ajustar si es necesario y utilizar los elementos aplicables a los sistemas de deuda de su país.

3.6. ELABORACIÓN DE INFORMES SOBRE LOS RESULTADOS DE AUDITORÍA

Además, como cumplir con la *INTOSAI-P 1: La Declaración de Lima,* cuando corresponda, los informes de auditorías de los PDMIS pueden considerar el contenido de la antigua ISSAI 5440 , *Guía para la Realización de una Auditoría de Deuda Pública - La Utilización de Pruebas Sustantivas en las Auditorías Financieras*, sección 2.6 Elaboración de informes sobre los resultados de auditoría.

Como se informó previamente, una auditoría al PDMIS, es una auditoría de desempeño, por lo que es importante que el informe siga las normas de los informes de auditoría de desempeño, como se indica en la *ISSAI 3000: Norma para la Auditoría de Desempeño*, basada en las Normas de Auditoría y experiencia práctica de la INTOSAI, *ISSAI 300: Principios de la Auditoría de Desempeño.*

APÉNDICE I: TABLA DE PLANEACIÓN

Información, Documentos, e Informes Requeridos

- Inventario de los sistemas de información utilizados por la DMO y documentación de sistemas relacionada

- Inventario de sistemas operativos tanto de computadoras y como de red utilizados por la DMO

- Mapas actualizados de los flujos de procesos de la DMO

- Informes de auditoría previos de la DMO

- Informes de auditoría previos relacionados con los sistemas de TI de la deuda

- Leyes y reglamentos relacionados con el marco de la DMO y la gestión de la deuda pública

- Lista de gerentes de la DMO y administración de TI, gestión de continuidad del negocio, gestión de recursos humanos, gestión de riesgos, auditoría interna, y otros, así como sus labores, direcciones, correos electrónicos y números de teléfono

- Documentos que muestren el funcionamiento de la DMO y/o sus sistemas, así como manuales escritos de políticas y procedimientos de la DMO o del Ministerio de Finanzas, como se muestra a continuación:

• Administración de personal

- Administración de Cambio
- Acceso Físico
- Requerimientos de entorno/ubicación de las TI
- Acceso lógico
- Planeación de Continuidad del Negocio (BCP)
- Plan de Recuperación ante Desastres (DRP)
- Plan de contingencia
- Servicios de terceros (Servicios de TI)
- Informes previos de evaluación de riesgos
- Resumen reciente de evaluaciones de seguridad;
- Decisiones recientes de seguridad y acciones recomendadas
- Estado de las acciones recomendadas.
- Aprobación de la Alta Dirección para implementar el sistema

- Informes difundidos por entidades subcontratadas encargadas de proveer el mantenimiento de los sistemas

- Otros documentos relacionados con la DMO y/o su sistema (por ejemplo, diapositivas, textos, metas e informes anuales de gestión de deuda)

- Número de empleados de la DMO que son usuarios del sistema y que cuentan con perfil de acceso

- Número de empleados de TI y especificaciones del puesto (definición de funciones) tanto para la DMO como para el personal de TI

- Lista de empleados con acceso a sala de servidores

- Descripción del perfil de acceso al PDMIS

- Especificación formal de forma y periodicidad de actualización del Sistema Operativo, firewalls y software antivirus

- Opciones de obstáculos físicos y herramientas automáticas para prevenir el acceso no autorizado a mainframes, estaciones de trabajo, servidores y otras instalaciones de la DMO;

- Ubicación de cada sala dentro y fuera de la DMO

- Lista de personal, estaciones de trabajo, y servidores

- Asignación de presupuesto para los últimos 5 años

- Lista de capacitación previa tanto para el uso del PDMIS (personal de la DMO) como para la actualización en TI (personal de TI)

- Reglas, prácticas y descripciones intrínsecas definidas para evitar daños por inestabilidad eléctrica, fuego, polvo, agua, alimentos, temperaturas o humedad extremas, o electricidad estática.

- Especificaciones sobre el funcionamiento de la fuente de alimentación ininterrumpida (si la hay)

- Registros de incidentes acerca de las exigencias de la DMO sobre errores del PDMIS o informes de las instrucciones de uso

- Informes de registro de incidentes de seguridad

- Lista de modificaciones al programa PDMIS en los últimos 12 meses

- Registros e informes de pruebas anteriores de la BCP y del DRP y eventos ocurridos

- Documentación de aplicación y de usuario

- Condiciones de uso de cada aplicación

- Manual de procedimientos para atender errores de procesamiento;

- Muestra de datos para volver a ejecutar operaciones de comprobación de cálculos y controles de las aplicaciones.

Procedimientos

- Estudio de la documentación del sistema (manuales y condiciones de uso) para conocer los principales procesos de deuda llevados a cabo en sistemas de información; si la documentación de procesos de la DMO es insuficiente, el equipo de auditoría debe revisar y mapear los procesos;
- Verificar la existencia de normas jurídicas relacionadas con el uso, mantenimiento, y gestión empresarial del PDMIS;
- Identificar, en auditorías previas, los hallazgos relacionados con puntos débiles en los flujos de la operación de deuda pública y/o en sistemas de gestión de deuda pública;
- Identificar los principales controles generales basados en la documentación del sistema;
- Identificar los principales controles de aplicaciones basados en la documentación del sistema: controles de entrada, procesamiento y salida de datos;
- Llevar a cabo una evaluación del riesgo en estos principales controles generales y de aplicación para evaluar qué riesgos afectan estos sistemas y la severidad de su impacto en la gestión de la deuda pública;

- Determinar cuáles de los sistemas repercuten en funciones y datos críticos, tales como entrada, procesamiento y salida de datos, lista de acreedores, cálculos de deuda pública, presentación de informes, y toma de decisiones;

- Identificar los controles internos implementados para mitigar o disminuir los riesgos identificados;
- Clasificar los sistemas y procesos basados en la evaluación del riesgo y determinar el alcance de la auditoría;
- Estimar recursos y calendario;
- Organizar entrevistas con el jefe de la unidad de TI, los directivos y cuerpo técnico responsables de trabajar en el desarrollo/mantenimiento/operación del sistema;
- Desarrollar la matriz para la auditoría de controles generales y de aplicación y determinar las pruebas a ser llevadas a cabo. (Véase la matriz sugerida en el Apéndice III).

La EFS debe responder a las siguientes preguntas

- ¿Cuáles son los Sistemas de Información para la Gestión de la Deuda Pública y qué papel juega cada sistema en la gestión de la deuda pública?

- ¿El PDMIS fue desarrollado exclusivamente por la DMO, o se adquirió de un tercero? En el caso de este último, ¿se ha hecho alguna personalización para satisfacer necesidades específicas de la DMO?
- ¿A quién debe entrevistarse sobre temas de controles generales de TI en la DMO?
- ¿A quién debe entrevistarse para aclarar los controles de aplicación del PDMIS?
- ¿Quiénes son los principales usuarios del PDMIS?
- ¿Cuáles son los controles generales y de aplicación del PDMIS?
- ¿Los controles internos son capaces de disminuir los riesgos de los sistemas de información que puedan afectar a la gestión de la deuda pública?
- ¿Cuáles son los mayores riesgos relacionados con la entrada, procesamiento y salida de datos del PDMIS?
- ¿Qué pruebas relacionadas con los controles generales y de aplicación deben implementarse?

APÉNDICE II: MATRIZ DE PRUEBAS PARA CONTROLES GENERALES

CONTROLES GENERALES		
Los objetivos de los controles generales son salvaguardar los datos, proteger los programas de aplicación y garantizar el funcionamiento continuo de las operaciones computacionales en caso de interrupciones inesperadas.		
REQUISITO / FUNCIONALIDAD	**CONTROL GENERAL**	**PROCEDIMIENTOS DE PRUEBA SUGERIDOS**
Preguntas generales	Las acciones del sector TI deben ser conformes con la misión de la DMO Debe existir un monitoreo sobre el desempeño del PDMIS teniendo en cuenta los objetivos de DMO Debe realizarse periódicamente una auditoría interna sobre las operaciones de la DMO y del PDMIS	Revisar muestras de decisiones o notas de la Dirección, relacionadas con acciones de TI, para asegurar que sean claras, bien fundamentadas yconformes con la misión de la DMO Evaluar las medidas de desempeño del PDMIS contra indicadores esperados y asegurarse que la Alta Dirección reconoce estas medidas Evaluar informes de auditorías internas previas sobre los controles generales de TI para identificar deficiencias graves Evaluar tanto la cantidad relativa como la capacidad de las estaciones de trabajo y otros dispositivos de TI, y asegurar que el personal cuente con las habilidades necesarias Evaluar los montos relativos de asignación presupuestaria, y compararlos con períodos anteriores y sectores de TI de otras entidades de gobierno

Controles Organizacionales	La Dirección de la DMO o del Ministerio de Finanzas debe tener el compromiso de desarrollar y mantener un buen entorno general de TI Personal de la DMO y de TI debe tener capacitación periódica y adecuada, que incluya conciencia de la seguridad Debe existir un programa de capacitación Debe haber políticas escritas y procedimientos estándar, relacionado a lo siguiente: • Seguridad de la Información • Recursos humanos • Servicios de TI de terceros • Administración del cambio • Acceso físico y lógico • Planeación de continuidad escritos del negocio y recuperación ante desastres Las políticas y procedimientos deben actualizarse periódicamente Las políticas deben difundirse adecuadamente por los Altos Dirección de la DMO	Entrevistar a la Alta Dirección de la DMO sobre su interés en las TI para evaluar su compromiso con el desarrollo y mantener un buen entorno general de TI Revisar la evidencia que indique que se ha impartido capacitación Entrevistar a usuarios de la DMO y el personal de TI acerca de: • la frecuencia de la capacitación • necesidades de conocí-miento/ capacitación • conocimiento de las políticas Evaluar la idoneidad de las políticas y procedimientos respecto a los servicios de TI Observar si personal de la DMO trabaja de acuerdo a procedimientos estándar (establecidos en un manual)

Controles Organizacionales (cont.)	Los empleados de la DMO deben conocer estas políticas Debe existir una documentación de procedimientos que abarque todas las actividades de gestión de la deuda El Organismo debe implementar una adecuada segregación de funciones para asegurar que los usuarios no tengan más autoridad que la que requieren sus puestos	
Controles Físicos	El acceso físico al mainframe y a los servidores debe limitado (a través del uso puerta, cerradura, etc.) Debe haber supervisión por video Las ventanas de la sala donde se encuentran el mainframe y los servidores deben protegerse contra acceso forzado Debe tener acceso a la sala de servidores sólo quién esté autorizado	Verificar la existencia y funcionamiento eficaz de obstáculos físicos para prevenir el acceso no autorizado a mainframe, servidores y estaciones de trabajo de la DMO Verificar si los procedimientos administrativos del personal para prevenir el acceso no autorizado a, e interferencia con, los servicios de TI operan como fueron establecidos Con el fin de identificar cualquier debilidad en los controles automáticos, observar cómo operan las herramientas electrónicas- tales como cerraduras electrónicas, sistema de bloqueo de teclas, cámaras y otros medios que limiten el acceso físico a servidores - y otras infra-estructuras críticas En el caso de sistemas de bloqueo de teclas, verificar si se comparten contraseñas entre los empleados

Controles Lógicos	Si se externalizan los servicios de TI de deuda pública, el contrato debe determinar controles adecuados para garantizar que un tercero no tenga acceso a secretos comerciales, datos importantes y estrategias de deuda pública No debe haber ex empleado, persona no contratada por la DMO o usuario “virtual” con un perfil de acceso activo Los derechos de acceso deben ser revisados periódicamente Los antivirus, firewall, y softwares de intrusión malware actualizados deben estar en funcionamiento Debe haber una actualización sistemática del sistema operativo de estación(es) de trabajo y servidor(es) El Organismo debe definir sus procedimientos para autorizar, revocar o modificar el control de acceso cuando las condiciones cambien (nuevas contrataciones, rescisiones, cambio de funciones, etc.)	Evaluar si los perfiles de acceso se basan en las funciones del empleado Verificar que ningún ex empleado, persona no contratada por la DMO tenga un perfil de acceso activo Verificar si existen firewalls, antivirus actualizados, detectores de malware y de intrusión. Verificar si el sistema operativo se actualiza sistemáticamente en las estación(es) de trabajo y servidor(es) Evaluar si se está aplicando adecuadamente la política de contraseñas Verificar si los procedimientos están definidos y documentados

Controles de Entorno	Debería haber tuberías (agua, calefacción, electricidad, etc.) por toda la sala de servidores Debe haber detectores de agua, calor y humedad Debe haber un sistema contra inundaciones en la sala de servidores Debe haber dispositivos de detección de humo/ fuego Debe haber un piso elevado o estar ubicado el equipo de 15 a 20 cm por encima del suelo en los estantes Debe haber una fuente de alimentación ininterrumpida para sostener el funcionamiento del mainframe y los servidores	Inspeccionar y evaluar las condiciones del entorno en la sala de servidores de base de datos Verificar la existencia y el mantenimiento efectivo de dispositivos utilizados para evitar incendios, inundaciones, y humedad Verificar la existencia y funcionamiento eficaz de las fuentes de alimentación alternativas para evitar la interrupción en los servicios de TI
Controles de Cambios a Programas	La gerencia de TI debe mantener un registro de auditoría de problemas opera-clonales, incidentes y errores El registro debe rastrear cada incidente desde la causa subyacente hasta la resolución No debe haber preguntas de instrucción importantes referentes al PDMIS sin resolver en la mesa de ayuda	Evaluar el tiempo dedicado a resolver las exigencias de la DMO relacionadas con instrucciones de uso o fallas en el funcionamiento del PDMIS Identificar las fallas más frecuentes del PDMIS y sus causas probables Comparar los cambios previos contra procedimientos estándar

Controles de Cambios a Programas **(cont.)**	Debe haber escalamiento de problemas para eventos críticos y un nivel apropiado de respuesta basada en la prioridad del evento Debe haber un informe de incidentes de seguridad, brindado a los directores de la DMO Los cambios previos deben seguir los procedimientos estándar Si se utiliza un sistema de gestión de la deuda des-estandarizado, el Organismo debe tener documentados los propios procedimientos para control de cambios y señalar quién está autorizado para realizar cambios en el sistema El Organismo debe rastrear y monitorear todos los câmbios al sistema de deuda (pistas de auditoría)	

BCP y DRP	Debe haber un BCP y un DRP establecidos por la DMO El personal responsable de la continuidad operacional debe conocer sus funciones y responsabilidades La debilidad en pruebas anteriores de la BCP y DRP, o eventos actuales, así como las acciones llevadas a cabo por la DMO para atender tales debilidades deben reportarse. La documentación de préstamos deben guardarse en un lugar seguro donde los documentos están protegidos contra robo, incendio, inundación u otros incidentes que la pudieran dañar o destruir	Evaluar la consistencia y la integridad de los planes de la BCP y del DRP y determinar si están actualizados Evaluar los informes sobre pruebas previas de los planes de la BCP, del DRP y del plan de contingencia Verificar si los planes BCP y DRP son difundidos adecuadamente a todo el personal Verificar si los respaldos fuera de sitio están en buenas condiciones y puedan ser utilizados para reiniciar el sistema en caso de falla

APÉNDICE III: MATRIZ DE PRUEBAS PARA CONTROLES DE APLICACIÓN

ESTÁNDARES DE DOCUMENTACIÓN		
Los objetivos de las normas de documentación apropiadas son asegurar que los controles operarán sobre una base continua, así como disminuir el riesgo de error.		
REQUISITO / FUNCIONALIDAD	**CONTROLES DE APLICACIÓN**	**PROCEDIMIENTOS DE PRUEBA SUGERIDOS**
Controles de la Documentación	La documentación de la aplicación debe ser lo suficientemente integral (con todas las funcionalidades de la aplicación y funcionamiento relacionado)	Verificar la documentación
	La documentación debe ser actualizada para reflejar las modificaciones a la aplicación	Verificar la documentación
	Los controles de la aplicación incluidos en la documentación deben ser implementados y estar funcionando eficazmente	Verificar una muestra de controles de aplicación especificados en los controles de la doce- tentación y verificar si se aplican de acuerdo con la documentación y si operan eficazmente
Respaldo de la Documentación	Se debe contar con una copia de resguardo de la documentación	Verificar el resguardo de la documentación

CONTROLES DE ENTRADA		
El objetivo de los controles de entrada es asegurar la autorización, exactitud, integridad y oportunidad de los datos introducidos en una aplicación.		
REQUISITO / FUNCIONALIDAD	**CONTROL DE APLICACIONES**	**PROCEDIMIENTOS DE PRUEBA SUGERIDOS**
Campos de entrada obligatoria	La aplicación no debe permitir la confirmación de la operación si algún campo de entrada obligatorio no ha sido llenado	Confirmar la operación omitiendo algunos datos necesarios y verificar que la transacción no sea procesada Aplicar esta prueba a los siguientes procesos: registro de contrato, activación de contrato, registro de emisión de valor, etc.
Entrada de datos correcta y adecuada	La aplicación no acepta entrada de datos incorrectos o inadecuados	Verificar el formato de datos en la base de datos Revisar las especifica-cines de entradas y Verificar algunas en la aplicación Intentar ingresar datos incorrectos o añade-cuados, verificar que los datos no sean aceptados, y que se genere un mensaje de error. Aplicar estas pruebas a los siguientes procesos: registro de contrato, activación de contrato, registro de emisión de valor, actualización de índices,reembolso de valor, etc.
	La aplicación no permite la duplicación de datos	Tratar de registrar un contrato o un título de deuda con el mismo nombre de uno ya existente, y verificar que los datos no sean aceptados y que se genere un mensaje de duplicidad
	Para tasas de interés de contratos, no debe haber periodos sobrepuestos o al descubierto con respecto a la aplicabilidad de las tasas de interés	Verificar en la base de datos si hay períodos con tasas de interés superpuestas o descubiertas

Entrada de datos correcta y adecuada (cont.)	En caso de un contrato de donación, la aplicación debe permitir la entrada del desembolso dado que, en este caso, no existen operaciones de amortización ni de intereses	Tratar de ingresar el desembolso de un contrato de donación y verificar si la aplicación no requiere operaciones de interés ni de amortización
	En la pantalla de captura de desembolsos, cuando el usuario busca contratos para aplicar un desembolso, la aplicación debe solamente mostrar contratos con Estado “activo” en la fase de desembolso o de desembolso y amortización	Tratar de ingresar un desembolso verificarla fase de los contratos mostrados por la aplicación
	Si la tasa de interés es flotante, la aplicación debe requerir la inclusión del índice	Verificar si la aplicación requiere la inclusión de un índice cuando se selecciona el régimen de tasa de interés flotante
	La aplicación no debe permitir la entrada de cifras decimales para la cantidad de valores emitidos	Tratar de ingresar cifras decimales para la cantidad de valores emitidos y verificar que no lo permita la aplicación
	La aplicación debe permitir la creación de un valor bursátil antes de su emisión	Simular la creación de un valor bursátil sin realizar su emisión
Integralidad de la Información	Toda información relevante de deudas debe ser introducida en la aplicación	Verificar si todos los datos de deuda importantes se introducen en la aplicación, por ejemplo, operaciones de crédito, garantías, préstamos, tasas de interés, y tipo de cambio
Compatibilidad entre fechas	La fecha de inicio para el cálculo de la tasa de compromiso debe ser anterior a la fecha de terminación del proyecto	Tratar de introducir una fecha de inicio, para el cálculo de la tasa de compromiso, posterior a la fecha de terminación del proyecto, verificar que los datos no sean aceptados y que se genere un mensaje de error

Compatibilidad entre fechas (cont.)	La fecha de inicio de vigencia debe ser anterior a la fecha de terminación del proyecto	Tratar de introducir una fecha de inicio de vigencia, para el cálculo de la tasa de compromiso, posterior a la fecha de terminación del proyecto y verificar bloqueo y mensaje de error
	La fecha de inicio de vigencia debe ser anterior a la fecha límite de desembolso	Tratar de introducir una fecha de inicio de vigencia posterior a la fecha límite de desembolso y verificar que los datos no sean aceptados y que se genere un mensaje de error
	La fecha límite de desembolso tiene que ser anterior a la fecha de terminación del proyecto	Tratar de introducir una fecha de límite de desembolso posterior a la fecha de terminación del proyecto, y verificar que los datos no sean aceptados y que se genere un mensaje de error
	Para obtener el Informe de Vencimientos, la fecha final de vencimiento de un valor bursátil debe ser posterior a su fecha de inicio	Tratar de introducir una fecha de inicio posterior a la fecha vencimiento de un valor y verificar que se genere un mensaje de error
	La aplicación no debe aceptar fechas futuras para las operaciones	Tratar de realizar algunas operaciones mediante la inserción de una fecha futura, y verificar que los datos no sean aceptados y que se genere un mensaje de error. Aplicar esta prueba a los siguientes procesos: registro de contrato, activación de contrato, registro de emisión de valores, actualización de índices, reembolso de valores, registro de desembolsos, adiciones a contratos, etc.
	La fecha de emisión de valores debe ser anterior a su fecha de vencimiento	Tratar de introducir una fecha de emisión posterior a la fecha de vencimiento, y verificar que los datos no sean aceptados y que se genere un mensaje de error

Compatibilidad entre fechas (cont.)	Al registrar un pago de amortización, en los casos en que la cantidad o la fecha introducida difieran de los de la aplicación, esta debe desplegar un mensaje informando al usuario de tal situación, antes de que se pueda confirmar la operación	Registrar un pago con fecha o valor diferente de los de la aplicación y verificar si la aplicación despliega un mensaje
	Si la fecha de liquidación es diferente de la fecha de vencimiento, la aplicación debe requerir que sean llenados los campos de “justificación” o de “endoso de acreedor”	Ingresar distintas fechas para vencimiento y liquidación y verificar si la aplicación requiere de una justificación o endoso
	Desembolsos programados no deben ener períodos sobrepuestos, po ejemplo, la fecha inicial del segundo desembolso no puede ser anterior a la fecha del primer desembolso	Tratar de ingresar una fecha de segundo desembolso anterior a la fecha del primero y verificar que los datos no sean aceptados y que se genere un mensaje de error

Seguridad en entrada de datos y operaciones	La aplicación no debe permitir que personas no autorizadas ingresen ciertos datos y lleven a cabo ciertas operaciones	Verificar la existencia de “tokens” (dispositivos) y otros requisitos para un perfil específico de usuario. Tratar de introducir datos y realizar ciertas operaciones sin tener el perfil adecuado y verificar que no está permitido. Aplicar esta prueba a los siguientes procesos: registro de contrato, activación de contrato, registro de emisión de valores, cambios de índices, reembolso de valores, registro de pagos, etc.
	La aplicación debe registrar una bitácora de acceso en caso de captura manual de datos	Verificar la existencia de bitácoras de acceso restringido y asegurar que las bitácoras no puedan ser vistas o ni modificadas por personas no autorizadas
	La aplicación no debe permitir el cambio de valor de un contrato vigente	Tratar de cambiar el valor de un contrato vigente y verificar que esto no sea permitido
	La aplicación debe impedir la modificación de datos y la eliminación de los contratos con estado de “cancelado” o “concluido”	Tratar de modificar y borrar algunos datos de una muestra de contratos con estado “cancelado” o “concluido” y verificar que esto no sea permitido
	La aplicación no debe permitir la eliminación de un contrato vigente, a menos que el contrato esté siendo negociado o inactivo	Tratar de eliminar un contrato vigente que no está en negociación y verificar que esto no sea permitido
	La aplicación no debe permitir la exclusión indebida de un valor bursátil emitido, a menos que no haya ninguna operación vinculada al valor	Tratar de eliminar un valor emitido que no esté vinculado a una operación y verificar que esto no sea permitido.

Seguridad en entrada de datos y operaciones (cont.)	La aplicación debe requerir autorización dual para realizar operaciones importantes	Importantes requieren autorización dual para ser completadas. Aplicar esta prueba a los siguientes procesos: activación de contrato, emisión de valores, pago de amortizaciones, reembolso de valores, cambios a valor de contrato, pago de cupones, reversión de pagos, cambios a tasas de interés, etc.
	La aplicación sólo debe aceptar entrada de datos de fuentes reconocidas; el préstamo capturado debe ser conforme al acuerdo y normas aceptadas	Verificar que los datos clave sean capturados dos veces y que un mensaje de error se produzca cuando los datos sean diferentes.
	La aplicación debe permitir la disminución de un valor contractual siempre y cuando no sea mayor que el valor del “saldo a ser desembolsado”	Intentar disminuir el valor del contrato en un monto mayor al saldo a ser desembolsado, y verificar que los datos no sean aceptados y que se genere un mensaje de error
	La aplicación debe registrar todas las transacciones una única vez	Realizar algunas transacciones idénticas (por ejemplo: pago de una amortización) y verificar que las transacciones no sean procesadas y que no se dupliquen en la base de datos
	Al registrar un pago, si se revoca el permiso del usuario, la aplicación debe informar sobre la revocación solamente cuando el usuario trate de ingresar el pago permitiendo así que se registre en la bitácora tanto el intento fallido como los datos que pretendía introducir el usuario	Tratar de registrar un pago con un permiso revocado, y verificar que los datos no sean registrados y que el intento se registren la bitácora

Seguridad en entrada de datos y operaciones (cont.)	En el caso de transferencia automática de archivos entre aplicaciones, el PDMIS deber mantener los datos originales, recibidos de otras aplicaciones por un período preestablecido por la DMO.	Verificar los datos conservados transferidos desde otras aplicaciones para garantizar que estén cifrados o protegidos contra daño, pérdida o violación
	La aplicación no debe permitir la modificación de tasas de interés de una parcialidad ya pagada y toda alteración de tasa de interés necesita una segunda aprobación para completarse	Intentar modificar la tasa de interés de una parcialidad ya pagada y verificar que los datos no sean aceptados; verificar además, si la aplicación requiere de una segunda aprobación para cambiar una tasa de interés
Compatibilidad entre valores	El valor del tramo debe ser menor al del contrato	Tratar de ingresar un valor de tramo mayor al del contrato, y verificar que los datos no sean aceptados y que se genere Un mensaje de error
	El valor de recompra debe ser menor al valor emitido	Tratar de efectuar un Reembolso por un valor mayor al emitido; y verificar que los datos no sean aceptados y que se genere un mensaje de error
	La aplicación muestra una alerta sobre pagos insuficientes o pagos en exceso antes de su procesamiento	Simular un pago insuficiente o en exceso y verificar la existencia de una alerta
Documentos de origen	Debe existir un rastro de documentos de origen para las entradas a efectos de garantizar la autenticidad de la captura de datos	Seleccionar algunos datos capturados y verificar si tienen el documento de origen respectivo (por ejemplo, contrato de préstamo, correo, etc.)

CONTROLES DE PROCESAMIENTO		
El objetivo de los controles de procesamiento es asegurar que los datos sean procesados con exactitud a través de la aplicación y que ningún dato sea añadido, perdido o alterado durante el procesamiento.		
REQUISITO / FUNCIONALIDAD	**CONTROL DE APLICACIONES**	**PROCEDIMIENTOS DE PRUEBA SUGERIDOS**
Indicación de estado apropiado	La aplicación debe cambiar el estado del contrato después de un desembolso total	Simular la terminación de desembolso y verificar si cambia el estado del contrato de “desembolso” a “totalmente desembolsada”
	La aplicación debe cambiar el estado del valor bursátil cuando se confirma su emisión	Simular una confirma- cien de emisión de valor y verificar si el estado del valor cambia de “inactivo” a “activo”
	La aplicación debe cambiar el estado del contrato o del valor bursátil después del pago total	Simular el último pago y verificar si cambia el estado del contrato o del valor
	La aplicación debe prever al menos las siguientes fases: • Desembolso: en esta fase se crean los desembolsos • totalmente desembolsado: no se permiten desembolsos en esta fase • concluido: en esta fase, los desembolsos no reciben operación financiera alguna y no se permite la modificación de datos	Crear un contrato, tratar de realizar un desembolso en cada fase, y verificar que los datos no sean aceptados y que se genere un mensaje de error

Indicación de estado apropiado (cont.)	La aplicación debe contener reglas para que el estado del contrato (activo o inactivo) sea compatible con las fases (desembolso, completamente desembolsado, amortización, desembolso y amortización, concluido) con el fin de evitar la contradicción en la información; por ejemplo, un contrato en estado inactivo no puede estar en fase de Desembolso o Amortización	Simular algunos cambios de estado de contrato y fases de contrato, y verificar si son compatibles
	La aplicación debe contener un programa para actualizar las fases del contrato, por ejemplo, cuando el saldo a desembolsar es igual a cero, la aplicación debe modificar la fase de "Desembolso a Totalmente Desembolsado	Simular las condiciones necesarias para cambiar la fase del contrato y verificar si ocurre el cambio
Cálculo correcto	La aplicación debe realizar los cálculos correctamente	Verificarlos cálculos al volver a procesar. Aplicar la prueba de cálculo a siguiente información: deuda (contractual y titulizada), vencimiento, calendario de amortización (fechas y valores), valor de la comisión de los agentes, flujo de pago de valores, valor financiero de reembolso, etc.

Cálculo correcto (cont.)	Después de algunos cambios en los datos de entrada, la aplicación debe actualizar los datos	Hacer algunos cambios de entrada y verificar la actualización de los datos, por ejemplo: • simular un pago y verificar si se actualizó el saldo y el flujo de amortización • cambiar algunos índices y verificar si se actualizó el monto del valor de la deuda
	La aplicación debe contener, en su programación, al menos los siguientes métodos para el cálculo de parcialidades: distribución uniforme, interés simple, parcialidad, aplicación de precio, aplicación de amortización constante, canasta de divisas Pool Unit (Banco Internacional de Reconstrucción y Fomento, BIRF) y canasta de divisas de la Unión Aduanera Centroamericana, UAC (Banco Interamericano de Desarrollo, BID)	Verificar los métodos que el sistema utiliza para calcular las parcialidades; la precisión de los métodos se puede verificar empleando datos de muestra
	Siempre que se cambia el campo Valor Contratado, la aplicación debe volver a calcular automáticamente el campo Saldo del Contrato por Desembolsar	Cambiar el campo Valor Contratado y verificar si el campo Saldo del Contrato por Desembolsar se ha actualizado correctamente

Cálculo correcto (cont.)	La aplicación debe generar automáticamente las fechas de las parcialidades empleando uno de los siguientes métodos posibles: • fecha inicial y número fijo de parcialidades • fecha inicial, fecha final y número decreciente de parcialidades • fecha inicial, fecha final y número fijo de parcialidades • fecha inicial y número de períodos • períodos	Ingresar los datos requeridos por cada método posible y verificar si las fechas de las parcialidades son correctas
	Cuando la fecha de la parcialidad es en un día no laborable (inhábil), la aplicación debe ofrecer dos opciones: adelantar la fecha para el siguiente día laborable o recorrerla al anterior	Configurar una parcialidad con la fecha de un día no laborable y verificar si la aplicación permite cambiar la fecha al día laborable anterior o al siguiente
	El sistema debe actualizar automáticamente el valor nominal de los valores cuando haya un cambio en el indizador respectivo	Cambiar el indizador (confecciona dar de índices) de un valor y verificar si se actualiza el valor nominal respectivo
	En caso de pago de un monto inferior al calculado por la aplicación, se debe mostrar un mensaje al momento de captura del pago; el mensaje debe repetirse hasta la fecha de vencimiento de la siguiente parcialidad.	Simular un pago menor al monto calculado por la aplicación y verificar la existencia de un mensaje y si este se repite hasta la fecha de la siguiente parcialidad

Cálculo correcto (cont.)	En su base de datos, el sistema debe diferenciar los valores con emisión simulada	Dentro de la base de datos, verificar si se diferencian los valores simulados y si se ignoran en los cálculos de la deuda y su vencimiento
	Cuando un usuario elimina un valor bursátil, la aplicación debe eliminar los importes respectivos en la base de datos	Eliminar un valor y verificar si su monto se elimina de la base de datos
	Los valores con estado "Cancelado" no deben considerarse en el cálculo de valores de deuda (por ejemplo, tasa interna de retorno, vencimiento, etc.), es decir, después de que se cancelan,los importes respectivos deben ser excluidos permanentemente de la base de datos	Cambiar el estado de un valor a "cancelado" y verificar si su importe es excluido de los cálculos (de existencia/stock, vencimiento, etc.)
	La aplicación debe tratar de manera diferente las parcialidades con pagos vencidos	Verificar si la aplicación está calculando correctamente todos los cargos sobre parcialidades vencidas
Control adecuado de errores de procesamiento	Los errores de procesamiento de días/ semanas atrás no deben quedarse sin resolver	Verificar si hay algún criterio en relación con el número de días que toma la resolución de errores en el sistema, así como la existencia de mensajes de error, y discutir, con los administradores del sistema y de la deuda, las medidas adoptadas para corregir cualquier fallas
	De ocurrir un error de procesamiento, la aplicación debe cancelar el proceso y almacenar en la base de datos fecha, hora y la razón técnica del problema	Simular un error de proceso y verificar si la aplicación almacena en la base de datos la fecha, hora y la razón técnica del problema

Registro correcto	La aplicación debe permitir a los administradores de deuda registrar correctamente el flujo de efectivo (asociado con préstamos en moneda extranjera y nacional, actividades de cobertura y comerciales, garantías y préstamos) para todas las transacciones	Realizar una transacción y verificar si su registro es correcto y exacto
	La aplicación debe mantener un historial de las transacciones llevadas a cabo durante la vida del contrato e incluir detalles sobre los campos de acreedor, valor contratado, fecha de cierre del proyecto, y fechas límite de desembolso	Seleccionar algunos contratos y verificar si cada uno cuenta con un historial de todas las transacciones efectuadas durante su vida, con todos los detalles necesarios
	La aplicación debe tener una bitácora para cada instrumento de deuda	Verificar si las transacciones históricas relacionadas con un contrato o valor bursátil coinciden en su bitácora de deuda
Programa Correcto de Tareas	La aplicación debe tener un inicio automático para tareas en horarios establecidos por la DMO para actualizar índices, deuda, etc.	Verificar la existencia de arranques automáticos y si este proceso funciona apropiadamente
	Para un tipo de valor cuya amortización se realice con la misma frecuencia que el interés (precio, por ejemplo), el sistema debe asegurar que tanto el interés como la amortización tengan el mismo calendario de pagos	Crear un valor con amortización e interés en la misma frecuencia y Verificar si tiene el mismo calendario de pagos

Pistas de auditoría	Debe mantenerse una pista de auditoría del PDMIS para habilitar el seguimiento a los contratos o valores de la deuda, desde la firma/emisión hasta su reembolso	Verificar la existencia de la pista de auditoría para una muestra de contratos y valores, desde el registro/ emisión hasta el reembolso
CONTROLES DE SALIDA		
El objetivo de los controles de salida es garantizar la integridad, así como la distribución correcta y oportuna de las salidas.		
REQUISITO / FUNCIONALIDAD	**CONTROL DE APLICACIONES**	**PROCEDIMIENTOS DE PRUEBA SUGERIDOS**
Control sobre los usuarios de la información	La aplicación debe tener una bitácora de informes para registrar los nombres de los usuarios que han solicitado informes, así como las fechas y horas de las solicitudes.	Pedir algunos informes y verificar si la aplicación registra las solicitudes
	La aplicación debe pedir autorización especial para cargar ciertos informes (especialmente aquellos que contengan información sensible)	Tratar de generar estos informes
Informes oportunos y confiables	La aplicación debe generar informes predefinidos (clasificados por bono, préstamo y tramo, por ejemplo vencimiento, estado, fuente de financiamiento, tipo de financiamiento, crédito, tipo de instrumento, términos, facturas sin pagar, etc.)	Tratar de generar algunos informes predefinidos

Informes oportunos y confiables **(cont.)**	La aplicación debe generar informes apropiadamente, asegurando la integralidad e integridad de la información	Verificar si los informes se generan de acuerdo a los términos de uso Verificar si los informes presentan números de página y totales. Aplicar esta prueba a los informes siguientes: Informe de Vencimiento (para deuda contractual y titulizada), Informe de Saldo Pendiente, Informe de Recepción, etc.
	La aplicación debe permitir la emisión de informes, tanto globales (todos los títulos de deuda) como específicos, tales como: • Por estado de valores (emitido, cancelado, canjeado, etc.) • Para eventos en cierto rango de fechas (emisiones, reembolsos, etc.) • Para stock de corto y largo plazo • Por posición de la cartera • Por el tipo de valor • Por intervalo de vencimiento, etc.	Intento de generar informes, globales o específicos, usando como criterio, los datos a continuación: • Estado de valores (emitido, cancelado, canjeado, etc.) • Eventos en un cierto rango de fechas (emisiones, reembolsos, etc.) • Stock de corto y largo plazo • Posición de la cartera • Tipo de valor • Intervalo de vencimiento, etc.
	Los informes deben presentar información completa y correcta	Generar informes y volver a realizar los cálculos Aplicar esta prueba a los siguientes informes: Informe de Vencimiento (para deuda contractual y titulizada), Informe de Saldo Pendiente, Informe de Recepción, etc.

Informes oportunos y confiables **(cont.)**	Los informes deben presentar exactamente la misma información cómo se presenta en las pantallas de la aplicación	Comparar la consistencia de los informes con la información presentada en las pantallas de la aplicación Aplicar esta prueba a los siguientes informes: Informe de Vencimiento (para deuda contractual y titulizada), Informe de Saldo Pendiente, Informe de Recepción, etc.
	Los valores presentados en los Informes informe de Vencimiento, Saldo Pendiente y Existencias (Stock) deben coincidir	Comparar la consistencia de estos informes
	El sistema debe ser capaz de generar informes sobre los totales de la deuda, en forma individual y agregada, con pronóstico de servicio de la deuda para préstamos y títulos existentes y futuros	Intentar generar tales informes Verificar si los informes abarcan tanto las operaciones de deuda existentes como las previstas
	La aplicación debe generar automáticamente informes diarios de financiera sobre todos los informes “activos”; también debe los contratos generación manual de tratar de generar informes para contratos específicos	Verificar la generación automática de agenda para todos contratos activos y permitir la informes manuales para contratos específicos
Transferencia de datos correcta	La transferencia de datos entre aplicaciones y/o fases de procesamiento debe ser precisa y completa	Simular una transferencia de datos entre aplicaciones y verificar la exactitud y la integralidad de los datos

Mensajes de salida útiles	Cuando un usuario accede a la aplicación, se debe mostrar un mensaje con la siguiente información: • Contratos por vencer en los próximos cinco días • Contratos con pagos de parcialidades vencidas • Contratos con parcialidades pagadas parcialmente • Contratos con fechas de desembolso vencidas • Contratos con fecha límite de desembolso de 5 días (la aplicación debe enviar un mensaje diario hasta que se haga el desembolso, se cancele el importe a desembolsar, o se modifique el plazo límite)	Acceder a la aplicación y verificar si muestra todos estos mensajes
	La aplicación debe indicar el estado del cálculo, como "cálculo en ejecución" o "cálculo finalizado"	Solicitar la ejecución de un cálculo y verificar si la aplicación indica el estado de la operación
	Al final de la generación de un informe, la aplicación debe mostrar un mensaje indicando que la generación concluyó o bien mostrar el informe solicitado	Solicitar un informe y verificar si la aplicación muestra un mensaje informando que la operación concluyó o despliega el informe solicitado
	La aplicación debe indicar el estado de la generación de informes, como "en proceso" o "finalizado"	Generar un informe y verificar si la aplicación indica el estado de la operación

Mensajes de salida útiles (cont.)	Si ocurre cualquier alteración en las tasas de interés, la aplicación debe mostrar un mensaje de alerta	Cambiar las tasas de interés y verificar la existencia de un mensaje de alerta
	Antes de procesar la eliminación o el canje de un título de deuda, la aplicación debe mostrar una pantalla con la información que está siendo eliminada o canjeada para que el usuario pueda confirmar la operación	Tratar de canjear o eliminar un título de deuda y verificar si la aplicación muestra un mensaje para el usuario a fin de confirmar la operación.

FIGURA 1: AUDITORÍAS A LA DEUDA PÚBLICA POR EFS: EL CASO DE BRASIL

Auditoría realizada por el Tribunal de Cuentas de la Unión de Brasil al Sistema Integrado de Deuda (SID) del Gobierno Federal de Brasil en 2014

Teniendo en cuenta que el Sistema Integrado de Deuda (SID) está siendo probado para deuda titulizada interna, el equipo auditor decidió centrarse sólo en la prueba de procesos relacionados con la gestión de la deuda externa (titulizada y contractual). Las observaciones y los hallazgos de auditoría fueron los siguientes:

Estrategia y Gestión General del Sistema de TI;

Según su Manual de operaciones, una vez que el SID haya sido totalmente implementado, ofrecerá las siguientes funciones:

a) una amplia gama de cálculos, como el valor nominal actualizado, precio unitario, stock (tanto de deudas contractuales como de títulos de deuda), planeación financiera de contratos, tarificación de contratos y bonos y vencimientos;

b) una variedad de búsquedas de informes, tanto de registro de datos como de resultados de cálculos;

c) operaciones financieras, tales como emisión de bonos, reembolsos de contratos, canje, y transferencia, entre otros;

d) un registro de información utilizado en toda su extensión en los distintos módulos de negocios.

Con respecto a la gestión general y la estrategia de sistemas de TI, las principales observaciones y hallazgos de la auditoría fueron:

- No existe programa de capacitación para los sistemas de gestión de deuda pública más utilizados, Sistema de Ejecución de Presupuesto y Finanzas (Sistema de Execução Orçamentária e Financeira, SEORFI) y SID.

- No hay fecha prevista para la plena implementación del SID, incluyendo la deuda interna titulizada.

- Algunas operaciones importantes como activación de contrato, reembolsos, reversión de reembolsos, modificación de tasas de interés, o modificación de valores de contrato se llevan a cabo por una sola persona. El sistema no plantea la necesidad de aprobación ni de doble autorización. La seguridad de las operaciones se basa exclusivamente en la idoneidad del perfil, lo que crea un problema de segregación de funciones.

- Otro problema de segregación de funciones se refiere a la falta de personal para el desarrollo del SID; el personal de la DMO se encuentra desarrollándolo, a la par de la ejecución de las funciones habituales de la oficina.

- La evaluación de vulnerabilidad ante riesgos operacionales inherente a los procesos de TI ha sido desarrollada, pero la evaluación para la mitigación de estos riesgos no ha ocurrido aún.

Controles de Seguridad y de Entorno;

En cuanto a controles de seguridad y de entorno, las principales observaciones y resultados de la auditoría fueron:

- La DMO no ha designado al Gerente de Seguridad de la Información y de Comunicaciones, y el Comité de Seguridad de Información, responsable por el nombramiento del gerente, no comenzó a trabajar eficazmente.

- No hay una BCP formalizada, y se están revisando los procesos de trabajo de gestión de la deuda pública con el fin de preparar la BCP.

- Los análisis del equipo de auditoría identificaron la existencia de tres usuarios genéricos activos, lo que dificulta las buenas prácticas de TI, con base en el artículo 11.2.1 de ISO / IEC 27002: 2005, que recomienda el uso de identificación única de usuario para asegurar la responsabilidad de las acciones de cada usuario en el sistema.

- Aunque la definición del acceso al SID debe realizarse sólo a través de un certificado digital A3, y accederse por número de identificación nacional y su contraseña debe ser una excepción, el análisis de la base de datos de los usuarios del SID indica que no existe fecha límite para el uso de la excepción.

- El análisis de la base de datos de los usuarios de SID indica falla en el proceso de revisión de acceso del usuario.

- El equipo de auditoría también detectó fallas en el mantenimiento automático de rutina diario de la base de datos del usuario del SID.

- El SID no registra pistas de auditoría para la mayoría de sus transacciones y, como resultado, la DMO no realiza revisiones periódicas de pistas generadas por el sistema y tampoco monitorea las transacciones en el SID.

- El SID no tiene una función de auditoría para rutinariamente genere, almacene y analice la bitácora del sistema.

- El equipo de auditoría notó la falta de un plan de prueba, y de los resultados asociados en la mayoría de los sistemas empleados por la DMO, SEORFI y SID.

- El equipo de auditoría no ha recibido confirmación de la creación real de un equipo para dar respuesta a incidentes en redes de cómputo, responsable de recibir, revisar y responder a los incidentes de seguridad.

- El equipo de auditoría notó la falta de un Plan de Continuidad de Servicios de TI, que es el documento debidamente formalizado que describe las iniciativas de continuidad para todos los servicios de TI a cargo de la agencia o entidad.

Controles Operacionales y Documentación

En cuanto a controles operacionales y documentación, las principales observaciones y hallazgos de la auditoría fueron:

- La interfaz no es muy amigable, por lo que los usuarios del SID requieren mayor conocimiento previo respecto al sistema.

- No hay manual de usuario del SID.

- La velocidad de procesamiento de los cálculos requeridos es baja. Esto evita la generación simultánea de cálculos e informes. Al haber múltiples usuarios simultáneos en el sistema, esto puede disminuir la eficacia del mismo. El equipo de auditoría sugirió que la DMO evalúe mejoras para aumentar la capacidad de procesamiento del sistema.

CONTROLES DE APLICACIÓN

Después de que el equipo de auditoría llevó a cabo las pruebas de control de entrada, procesamiento y salida en el SID para la deuda pública externa, los hallazgos de la auditoría y observaciones fueron:

- Muchos de los mensajes de error no son claros y a veces no aparecen al usuario.

- A través de pruebas de control de aplicación de entrada, el equipo de auditoría encontró varios mensajes de error que no explicaban la causa del error.

- Mediante pruebas de control de aplicación de procesamiento para la deuda contractual externa, el equipo de auditoría encontró una diferencia de cifras en el Informe Financiero del Flujo de Efectivo (Cash Flow Financial Report), refiriéndose a una reversión que no fue considerada en el informe. En pruebas de aplicación del control de salida, el equipo de auditoría identificó que, si la captura de datos no es correcta, la aplicación no genera algunos informes de deuda contractual, como era de esperarse, pero la aplicación tampoco señala este error al usuario. A través de pruebas de aplicación de control de salida el equipo de auditoria identificó errores en los informes de deuda contractual debido al uso de índices desactualizados por parte del sistema.

- Algunos informes informe de deuda contractual fueron emitidos con información incompleta.

Recomendaciones

Teniendo en cuenta los hallazgos de la auditoría y las observaciones reportadas, el equipo de auditoría recomienda que, en 90 días, el Secretariado de la Tesorería Nacional desarrolle, un plan de acción que contenga el calendario para la implementación de los siguientes puntos:

- Establecer la fecha prevista para la plena implementación del SID, incluyendo la deuda interna titulizada. Designar al Gerente de Seguridad de la Información y de Comunicaciones y al Comité de Seguridad de Información (Information Security Committee). Formalizar la BCP. Formalizar el Plan de Continuidad de los Servicios de TI. Creación de un Equipo de Atención y Respuesta a Incidentes en Redes Informáticas (Incident Response Team for Computer Networks). Evaluar y mitigar los riesgos operacionales de TI.

- Revisar el mantenimiento rutinario automático diario de la base de datos de usuarios del SID;

- Revisar el proceso de revisión de acceso del usuario del SID.

- Revisar el proceso de concesión de acceso al usuario genérico de SID. Establecer procedimientos para la revisión periódica de pistas de auditoría generadas por el SID. Brindar bitácora de registro de acceso a las aplicaciones por parte del SID. Revisar los mensajes de error del SID. Desarrollar el manual de usuario del SID. Revisar la rutina de generación de informes del SID.

FIGURA 2: AUDITORÍAS DE DEUDA PÚBLICA POR EFS: EL CASO DE MOLDAVIA

Evaluación de Control de Aplicación llevada a cabo por el Tribunal de Cuentas de la República de Moldavia

La aplicación del SIGADE cuenta con suficientes controles integrados que comprueban automáticamente si la entrada de datos fue realizada con precisión. Sin embargo, hay algunos aspectos que causan preocupación y deben ser atendidos: los operadores pueden introducir datos en los clasificadores del sistema y en otras tablas del sistema, lo que puede afectar la exactitud e integridad de los datos debido a duplicación o eliminación de registros.

Recomendación n° 15: Revisar los derechos de los operadores respecto al ingreso, modificación o eliminación de datos en el clasificador de la base de datos del SIGADE, o identificar tales operaciones que resulten en la duplicidad de datos o su ingreso erróneo.

Además de los informes estándar establecidos en la aplicación del SIGADE, un gran número de informes de carácter genérico se han desarrollado en "Excel", incluyendo la mayor parte de los aspectos requeridos. No todos los tipos de informes se empelan sistemáticamente. La mayoría de los informes requeridos se generan en "Excel". Sin embargo, existen informes que se generan manualmente a partir de los datos obtenidos de otros informes. La revisión de datos en los informes de "Excel" es preocupante. La generación de informes es un procedimiento complicado que podría verse afectado drásticamente por errores humanos. Más aún, los informes generados podrían ser modificados sin autorización, y estos errores pueden ocurrir en otros informes consolidados que sean importantes, mismos que deben contar con una máxima seguridad y representar la actividad primaria de la División General de Deuda Pública.

Como resultado de esto, algunas deficiencias menores podrían afectar críticamente la confiabilidad y exactitud de los datos de informes importantes sobre las actividades de la División General de Deuda Pública.

Recomendación n° 16: Considerar la optimización y automatización del proceso para modificar de informes a ser generados. Identificar el modo para generar automáticamente informes consolidados, eliminando la posibilidad del error humano. Considerar el migrar a la versión 6.0.

BIBLIOGRAFÍA

Organización de Entidades Fiscalizadoras Superiores de Asia (ASOSAI). Proyecto de Investigación. *IT Audit Guidelines– 6th Edition*, Septiembre de 2003.

Gallegos, Frederick. Senft, Sandra. Manson, Daniel P. Gonzalez, Carol. *Information Technology Control and Audit– Second Edition*, Auerbach Publications, EUA 2004

Oficina del Contralor y Auditor General de la India. *Information Technology Audit - General Principles. (IT Audit Monograph Series # 1).*

Fondo Monetario Internacional y el Banco Mundial. Directrices Revisadas para la Gestión de la Deuda Pública. 1 de abril de 2014.

Organización Internacional de Entidades Fiscalizadoras Superiores. *ISSAI 300: Principios Fundamentales de la Auditoría de Desempeño*, Septiembre 2019.

Organización Internacional de Entidades Fiscalizadoras Superiores. *ISSAI 3000: Norma para la Auditoría de Desempeño*, basada en las normas de auditoría y experiencia práctica de la INTOSAI. Julio de 2004.

Iniciativa para el Desarrollo de la INTOSAI. WGITA. *Handbook on IT Audit For Supreme Institutions*. Febrero de 2014.

Parker, Xenia Ley. Auditorías de Tecnologías de la Información *(Information Technology Audits)*, CCH Incorporated, EUA 2006.

Sitio web del Departamento de Seguridad Interna de los Estados Unidos: http://www.dhs.gov.

Oficina de Rendición de Cuentas Gubernamental de Estados Unidos. Manual Federal de Auditoría de Controles de Sistemas de información *(Federal Information System Controls Audit Manual – FISCAM)*, GAO-09-232G. Febrero de 2009.