INDICE

MINISTERIO DE HACIENDA

"EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEPENDIENTE DEL MINISTERIO DE HACIENDA"

ANTECEDENTES

La Contraloría General de la República, por Resolución CGR Nº 261 de fecha 3 de abril de 2013, dispuso la realización de un *"Examen Especial a la Dirección General de Informática y Comunicaciones dependiente del Ministerio de Hacienda, correspondiente al ejercicio fiscal 2012",* en cumplimiento de las funciones y atribuciones de control, vigilancia y fiscalización de los bienes públicos y del patrimonio del Estado establecidas por la Constitución Nacional y la Ley Nº 276/93 "Orgánica y Funcional de la Contraloría General de la República".

ALCANCE Y OBJETIVO DEL EXAMEN

Se realizó el Examen Especial a la **Dirección General de Informática y Comunicaciones**, al cierre del ejercicio fiscal 2012, a efectos de opinar sobre los controles utilizados para el resguardo de los datos del Sistema Integrado de Contabilidad (SICO).

Los procedimientos de auditoría tuvieron como objetivo fundamental obtener evidencia razonable sobre la confiabilidad y efectividad del ambiente de control tecnológico que permita expresar una opinión sobre la seguridad del mismo.

El alcance se enmarcó en la verificación de los controles utilizados por la Dirección General de Informática y Comunicaciones, para el resguardo de los datos del Sistema Integrado de Contabilidad (SICO), de manera a obtener evidencia razonable sobre la confiabilidad y efectividad del ambiente de control tecnológico, el cual permita expresar una opinión sobre la seguridad del mismo en el ejercicio fiscal 2012.

Fue realizado conforme a las Normas del Manual de Auditoría Gubernamental (Tesareko) y la utilización de pruebas de cumplimiento, además de procedimientos basados en el COBIT- *Control Objetives for Information and Related Technology* (Objetivos de Control para la Información y Tecnologías

relacionales). Estas normas requieren, que el Examen se planifique y efectúe con el objeto de obtener la certeza razonable de que la información y los antecedentes del mismo no contengan exposiciones erróneas, igualmente que los procedimientos a los cuales correspondan se hayan efectuado de conformidad con las disposiciones legales reglamentarias y demás normas aplicables para el sector informático.

Este Informe surge como resultado de la aplicación de procedimientos de Auditoría y el análisis de los documentos proveídos a los auditores para su estudio, que son de exclusiva responsabilidad de los funcionarios de la Institución intervinientes en la ejecución y formalización de las operaciones examinadas.

El trabajo de los auditores no incluyó una revisión detallada e integral de todas las operaciones, por tanto, no se puede considerar como una exposición de todas las eventuales deficiencias o de todas las medidas que podrían adoptarse para corregirlas.

1. **Naturaleza Jurídica de la Institución**

La Dirección General de Informática y Comunicaciones es un órgano técnico del Ministerio de Hacienda, jerárquicamente depende de la Sub Secretaria de Estado de Administración Financiera.

La Ley 1535/99 de Administración Financiera del Estado, en el Art. Nº 81 designa a la Dirección General de Informática y Comunicaciones como la institución encargada de la planificación, administración y coordinación de los sistemas de información y comunicaciones, de manera a asegurar la operatividad en línea entre los organismos y entidades del Estado.

Teniendo en cuenta el período analizado al cierre del ejercicio fiscal 2012, con la finalidad de confirmar y evaluar los procedimientos administrativos y legales que atañen al manejo del SIARE en general y al SICO en particular, ésta Auditoria ha considerado las siguientes disposiciones legales:

- Decreto Nº 8127/00 *"Por el cual se establecen las disposiciones Legales y Administrativas que reglamentan la implementación de la Ley Nº 1535/99 de "Administración Financiera del Estado" y el funcionamiento del Sistema Integrado de Administración Financiera–SIAF"*

- Decreto Nº 5154 de fecha 13 de setiembre de 1999 *"Por el cual se aprueba el funcionamiento del sistema integrado de Administración Financiera–SIAF, en el ámbito del sector público conforme a las disposiciones establecidas en al presente ordenamiento"*

- Resolución M.H. Nº 290/2012, de fecha 26 de setiembre de 2012, "*Por la cual se modifica el Organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones, dependiente de la Subsecretaria de Estado de Administración Financiera de este Ministerio".*

Capítulo I

Grado de cumplimiento del plan de mejoramiento-Seguimiento a las recomendaciones de ejercicios anteriores

I.1 Antecedentes

Por Expediente Externo Nº 31693 de fecha 8 de noviembre de 2012, la Dirección General de Informática y Comunicaciones del Ministerio de Hacienda, presenta el Plan de Mejoramiento elaborado para el cumplimiento de las recomendaciones derivadas del Examen Especial realizado por la Contraloría General de la República, correspondiente al ejercicio fiscal 2012.

A continuación se expone el grado de cumplimiento de las mismas:

I.1 Evaluación de las recomendaciones Dirección General de Informática y Comunicaciones

Recomendación: elaborar un Manual de Cargos y Funciones, en la brevedad posible, cuidando de definir adecuadamente los perfiles requeridos y necesarios para la Dirección General de Informática y Comunicaciones (DGIC).
Respuesta: *"Insistir en la aprobación del Manual de Organización, Funciones y Cargos, presentado a las autoridades en octubre de 2010".*
Grado de cumplimiento: por Resolución M.H.Nº 290/12, de fecha 26 de setiembre de 2012, se modifica el organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones. La Institución se adecuó a la recomendación.

Recomendación: adecuación a las Ordenanzas Municipales aplicables a la seguridad física del edificio.
Respuesta: *"Contratación de Consultoría para la Aprobación y Regularización de Planos Municipales y Proyectos de Prevención de Incendios ".*
Grado de cumplimiento: se contrató a una empresa de Consultoría para la aprobación y regularización de planos municipales y prevención contra incendios, por Contrato MH Nº 181/2012. Su cumplimiento será verificado en auditoría posterior.

Recomendación: acciones de contingencia.
Respuesta: *"Diseño del sitio de contingencia. Consultoría para la elaboración de especificaciones técnicas para construcción del sitio alternativo"*.
Grado de cumplimiento: se recibió copia de la Resolución MH N° 358/11, por la cual se autoriza a la DGIC, la utilización de una propiedad del Ministerio para sede del nuevo Data Center. Se recibió además copia de la documentación que avala la finalización de la Consultoría. Su cumplimiento será verificado en auditoría posterior.

Recomendación: proyecto de Reingeniería del SIAF
Respuesta: *"El proyecto SPIR (Generación de Reportes Gerenciales) se encuentra en proceso de desarrollo y pruebas. El proyecto de reingeniería del SIAF, se ha elaborado los TORs para el llamado de manifestación de Interés para pre-calificación de las empresas, previo al llamado a licitación".*
Grado de cumplimiento: si bien se ha evidenciado la finalización del proyecto SPIR, este constituye un sistema gerencial que contiene información del SIARE e interfaces con otros sistemas, es por tanto, complementario del SIARE. No se tuvo documentación que avale la continuidad de la reingeniería del SIAF. La Institución no se adecuó aún a la recomendación.

Recomendación: incluir a todas las entidades al SIAF.
Respuesta: *"Las Municipalidades son autónomas, las acciones que realiza la SSEAF son: Mejora en los equipos de comunicación para soportar el incremento de usuarios. Sistema de ingresos (SDI con financiamiento de GTZ-GIZ), con un módulo para registro y envío de información contable y de ejecución por parte de las municipalidades a la DGCP. Elaboración de TORs para inicio de llamado para el Desarrollo del Sistema de Gestión Municipal (inicialmente 6 municipios). Plazo del proyecto dic-2015".*
Grado de cumplimiento: se pudo verificar la remisión de los Términos de Referencia para la actualización tecnológica de la Red Metropolitana del Sector Público, a la Subsecretaría de Estado de Administración Financiera y la puesta en producción del Sistema SDI para transferencia de royalties; no se ha constatado la implementación del módulo contable. La Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditoría posterior.

Recomendación: identificador y mapa de riesgos de los procesos de la Dirección General de Informática y Comunicaciones.
Respuesta: *"El llamado para la contratación de una consultoría de Gestión de Riesgos se ha declarado desierta. Se realizará un siguiente llamado".*
Grado de cumplimiento: se constató la finalización de la Consultoría de Gestión de Riesgos de Tecnología de Información, evidenciándose entre los documentos el plan de implementación de gestión de riesgos y el plan de gestión de riesgos por áreas, en los cuales se identifica el nivel de riesgo y el riesgo residual. La Institución se ha adecuado a la recomendación.

Recomendación: informe sobre contratos de mantenimiento de conexiones, de las instituciones conectadas al SIAF.
Respuesta: *"Actualización de la normativa de la RMSP para contemplar el mantenimiento preventivo, correctivo y de mejora de los enlaces OEEs. Aprobación de la normativa".*
Grado de cumplimiento: se pudo comprobar que ha sido elaborado un borrador de la Normativa de la Red Metropolitana del Sector Público, que se encuentra en proceso de revisión por las instancias correspondientes. La Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditoría posterior.

Recomendación: consultoría para el Desarrollo y Mantenimiento de aplicaciones del SIARE.
Respuesta: *"En proceso de evaluación técnica de oferta del llamado al Concurso de ofertas".*
Grado de Cumplimiento: se suscribió el contrato de mantenimiento Nº 168/11, con vigencia hasta noviembre de 2012, y la presentación de los términos de referencia para el siguiente llamado.

Recomendación: no existe una buena comunicación de roles y responsabilidades a los funcionarios de DAU.
Respuesta: "*Solicitar cursos de adiestramiento en cuanto al manejo y la atención a usuarios. Socializar el manual de procedimientos. Verificar procedimientos y actualizar según corresponda*".

Grado de cumplimiento: se comprobó la emisión de los Términos de Referencia para el llamado a la "Consultoría para el diagnóstico del Servicio de Asistencia al Usuario y Capacitación en Atención y Servicio al Cliente", pero no se pudo evidenciar la realización de la misma. Se procedió a la socialización del Manual de Procedimientos del DAU. La Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditoría posterior.

Recomendación: DAU no realiza rotación de funcionarios dentro del área.
Respuesta: *"Generar procedimientos de rotación de funcionarios del área de Atención al Usuario".*
Grado de cumplimiento: se evidenció la rotación de puestos, sin que se cuente con procedimiento formalizado para la realización de la misma. Su cumplimiento será verificado en auditoría posterior.

Recomendación: No se realiza control de funcionarios dentro del DAU, lo cual afecta a la calidad de los servicios.
Respuesta: *"Generar procedimientos para tratar de garantizar la calidad de los servicios ofrecidos".*
Grado de cumplimiento: se evidenció el pedido de personal, pero no se constató el cumplimiento de la recomendación. La Institución no se adecuó a la recomendación.

Recomendación: no se cuenta con una normativa para la realización del mantenimiento y reparación de la fibra óptica.
Respuesta: *"Actualización de la normativa de la RMSP para contemplar el mantenimiento preventivo, correctivo y de mejoras de los enlaces OEEs. Aprobación de la normativa. Realizar el mantenimiento preventivo y correctivo de la RMSP".*
Grado de cumplimiento: se comprobó la elaboración de un borrador de la Normativa de la Red Metropolitana del Sector Público, que se encuentra en proceso de revisión por las instancias correspondientes. La Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditoría posterior.

Recomendación: no se cuentan con documentos legales que confirmen o no, los cargos de Director General y confirmaciones de cargos de los funcionarios destacados en la DGIC.
Respuesta: *"Solicitar a las instancias administrativas agilizar los trámites de confirmación de los cargos gerenciales y aceptación de comisionamientos en tiempo y forma".*
Grado de cumplimiento: se recibió documentación que confirmó el pedido a las instancias administrativas, de acelerar los trámites de confirmación de comisionamientos. La Institución se adecuó a la recomendación.

Recomendación: el jefe de DAU interina desde el 22/10/2008.
Respuesta: *"Solicitar a las instancias administrativas el llamado a concurso para el cargo de Jefe del Dpto. de Atención al Usuario".*
Grado de cumplimiento: no se tuvo evidencia de la confirmación en el cargo ni nombramiento para cubrir dicho puesto. La Institución no se adecuó a la recomendación.

Recomendación: plan anual de trabajos sin aprobarse.
Respuesta: *"Promover la aprobación del plan anual de trabajos ante las autoridades".*
Grado de cumplimiento: se ha recibido copia del Plan de trabajo y proyectos priorizados; Cronograma de implementación del MECIP; Plan operativo anual de seguridad informática; Plan de optimización de la infraestructura de servicios; Resolución DGIC/SSEAF Nº 011/11, de revisión de normativas y procedimientos. La Institución se adecuó a la recomendación.

Recomendación: manual de procedimientos para la gestión de proyectos sin aprobarse.
Respuesta: *"Elaborar el procedimiento de gestión de proyectos. Aprobar el procedimiento de gestión de proyectos. Insistir en la incorporación de recursos que permitan la gestión y el seguimiento de los proyectos".*
Grado de cumplimiento: se evidenció la aprobación del Manual de Gestión de Proyectos TIC de la Dirección General de Informática y Comunicaciones. La Institución se adecuó a la recomendación.

Recomendación: no se encuentran separadas las funciones que desempeñan los funcionarios en el departamento.
Respuesta: *"Insistir en la solicitud de incorporación de recursos que permitan: separar funciones dentro de cada una de las áreas del departamento de sistemas informáticos. Incorporar mecanismos de revisión por pares".*
Grado de cumplimiento: no se evidenció el cumplimiento el de esta recomendación. La Institución no se adecuó a la recomendación.

Recomendación: no se realiza monitoreo preventivo de los sistemas
Respuesta: *"Insistir en la incorporación de recursos, para asignar actividades de monitoreo preventivo de los sistemas".*
Grado de cumplimiento: la Institución no se adecuó a la recomendación.

Recomendación: manual de gestión de seguridad informática en etapa de aprobación.
Respuesta: *"Insistir en la aprobación de las Políticas de Seguridad a las autoridades de la institución. Seguimiento de las tareas realizadas y las observaciones visualizadas en el informe de monitoreo".*
Grado de cumplimiento: se recibió copia de la Resolución Nº 210/12 "Por la cual se aprueba la Política de Seguridad de la Información…". La institución se adecuó a la recomendación.

Recomendación: no se cuenta con documentación actualizada relativa a los programas de aplicación.
Respuesta: *"Insistir en la solicitud de incorporación de recursos, para asignar actividades de actualización y compilación de la documentación de los sistemas y programas de aplicación a medida que se realizan. Mantener la documentación actualizada conforme se desarrollen los cambios por parte de consultorías (Esta acción ya se viene realizando sistemáticamente)"*.
Grado de cumplimiento: su cumplimiento será verificado en auditoría posterior.

Recomendación: la actual estructura organizacional no está adecuada a las necesidades de la Institución.
Respuesta: *"Cumplido. Manual aprobado según la Resolución M.H.Nº 290 de fecha 26 de Setiembre de 2012".*

Grado de cumplimiento: se evidenció que, por Resolución M.H.Nº 290 de fecha 26/09/12, se modificó el organigrama y el Manual de Organización, Funciones y Cargos de la DGIC. La Institución se adecuó a la recomendación.

Recomendación: no se cuenta con una adecuada segregación de funciones.
Respuesta: *"Manual aprobado Ref. Resol.MH Nº 290/12. Con la implementación del Manual vigente, de acuerdo a los perfiles y cargos se avanzará en la segregación de funciones, y solicitará los profesionales específicos para cada área. Ver Plan de Mejoras de la Dirección Administrativa de MH relativa a incorporación de personal para la DGIC. SIME Nº 39.296".*
Grado de cumplimiento: no se evidenció el cumplimiento de la recomendación.

Recomendación: se tiene dependencia del personal clave.
Respuesta: *"Insistir en la incorporación de profesionales, para las áreas críticas de la DGIC. Remitir los niveles de riesgos de estas áreas, para una mayor disposición por parte de la DA en cuanto a la contratación. Ver Plan de Mejoras de la Dirección Administrativa de MH relativa a incorporación de personal para la DGIC. SIME Nº 39.296".*
Grado de cumplimiento: no se evidenció el cumplimiento de la recomendación.

Recomendación: no se cuenta con procedimientos establecidos para evaluar los requerimientos de personal de forma periódica.
Respuesta: *"Insistir en la incorporación de RRHH de acuerdo a los cambios en la Institución o los nuevos proyectos tecnológicos. Ver Plan de Mejoras de la Dirección Administrativa de MH relativa a incorporación de personal para la DGIC. SIME Nº 39.296".*
Grado de implementación: no se evidenció el cumplimiento de la recomendación.

Recomendación: la Institución no cuenta con Plan de Continuidad.
Respuesta: *"Contratar consultoría de apoyo para la elaboración de Plan de Recuperación de Desastres (DRP) para la DGIC".*
Grado de cumplimiento: se recibió copia del documento por el cual se solicitó la contratación de la consultoría. La Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditoría posterior.

Recomendación: no son administrados los controles internos adecuados para controlar el acceso físico al área del data center de la DGIC.
Respuesta: *"Ver plan de mejoras de la Dirección Administrativa de MH relativa a la inducción sobre la Normativa de Control de Acceso. Solicitud de personal de seguridad para control de acceso al Data Center de la DGIC. Ref: SIME 305/12 y SIME 34.260.*
Cumplido: personal de seguridad incorporado a partir del 1º de octubre. Definir responsable de la Administración del Data Center y sus sistemas de control".
Grado de cumplimiento: se recibió copia de la Resolución DGIC-SSEAF por la cual se aprobó la Versión 2 de la Normativa de acceso al edificio de la DGIC y al Data Center. Se asignó a un funcionario de seguridad el control de acceso al mismo. La institución se adecuó a la recomendación.

Recomendación: grave carencia de personal para el manejo de los sistemas administrados en la DGIC.
Respuesta: *"Ver plan de mejoras de la Dirección Administrativa de MH relativa a la incorporación de RRHH".*

Grado de cumplimiento: no se evidenció el cumplimiento de esta recomendación

---

Recomendación: no se prevé el nombramiento o contratación de personal capacitado para el manejo de los nuevos sistemas creados a través de los proyectos.
Respuesta: *"Ver plan de mejoras de la Dirección Administrativa de MH relativa a la incorporación de RRHH".*
Grado de cumplimiento: no se tuvo evidenció el cumplimiento de esta recomendación.

Recomendación: el SIARE tiene limitaciones con respecto a navegadores y sistema operativo.
Respuesta*: "Navegadores: hay una nueva versión del Mozilla Firefox "compatible" con los sistemas del SIARE, pueden encontrar en: \\dcint\server nt\FirefoxMH\ FirefoxMH-14.0.2-windows-x86.exe". Se encuentra en proceso de contratación la "consultoría para la "Revisión y actualización del Sistema de Administración Financiera- SIAF". TOR's adjunto como evidencia del Cap. I-Seguimiento del Plan de Mejoras-VI.15- Documentación de los Sistemas".*
Grado de cumplimiento: la Institución no se adecuó a la recomendación.

Recomendación: no se tiene establecido un tiempo aproximado para el cumplimiento de las solicitudes, el tiempo promedio de atención y posterior ejecución es de 28 días.

Respuesta: *"Se ha incorporado en el procedimiento del Ciclo de Vida de Sistemas Control de Cambios cuyo formulario es de Mantenimiento de Aplicaciones (FMA) el tiempo estimado de desarrollo de acuerdo impacto y el diagnóstico previo de la solicitud de requerimiento dicho tiempo es evaluado por el Jefe de Departamento. Pendiente de aprobación de la SSEAF de la versión 3.0 del Procedimiento "Control de Cambios". SIME Nº 39.102/12 Nota DGIC 584/12 de fecha 24/Set/12".*

Grado de cumplimiento: la Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditoría posterior.

Recomendación: no son seguidos todos los procedimientos establecidos en el Sistema de Gestión de Calidad. Código DF-GI-7.3-120 Versión 00.

Respuesta: *"Implementar el uso de recibos para solicitudes de creación de usuarios".*

Grado de cumplimiento: la institución se ha adecuado a la recomendación.

Recomendación: el reporte del Sistema, con respecto al perfil de usuario, presenta una descripción incompleta y no apropiada para los usuarios ajenos al manejo del sistema.

Respuesta: *"Cumplido, ya realizado en JUPE, SINARH y SIAF. Formularios de Modificación de Datos: SIAU Nº 2802. Memorándum DAU Nº 11/2010 y Memo DSI Nº 127/2012".*

Grado de cumplimiento: la institución se ha adecuado a la recomendación.

I.3 Evaluación de las recomendaciones de Dirección General de Contabilidad Pública - Ministerio de Hacienda

Recomendación: las Municipalidades de la República del Paraguay, no se encuentran conectados al Sistema Integrado de Administración Financiera (SIAF), que comprende un conjunto de sistemas, normas básicas y procedimientos administrativos a los que se ajustan los distintos organismos y dependencias del estado, para programar, gestionar, registrar y evaluar los ingresos y el destino de los fondos públicos.

Respuesta: *"Cabe resaltar que a pesar de que las Municipalidades no se encuentran conectadas al Sistema Integrado de Administración Financiera (SIAF) …"*

Grado de cumplimiento: se pudo evidenciar que se encuentra en proceso la puesta en marcha del Sistema de Gestión Municipal (SIGEM).

Recomendación: el Departamento de Municipalidades no tiene definido un plan anual de trabajos aprobado formalmente.

Respuesta: "*Elaboración de un Plan Anual de Trabajos para el Departamento de Administración de Municipalidades. En proceso de Certificación de Calidad ISO 9001 del proceso de Emisión de Constancias a Municipalidades de la República por la rendición de cuentas de carácter cuatrimestral y anual.*"

Grado de cumplimiento: no se tuvo evidencia del cumplimiento de la recomendación, la Institución no se ha adecuado a la recomendación.

Recomendación: el Departamento de Apoyo Informático de la Dirección General de Contabilidad Pública no dispone de un Manual de Procedimientos formalmente aprobado a ser utilizado para cada situación.

Respuesta: "*Solicitar la contratación de una Consultoría para la elaboración de un Manual de Procedimientos para el Departamento de Apoyo Informático*".

Grado de cumplimiento: no se recibió evidencia del cumplimiento de esta recomendación.

Conclusión del Capítulo I

Tras el análisis de cada uno de los puntos definidos en el Plan de Mejoramiento, presentado por la Dirección General de Informática y Comunicaciones del Ministerio de Hacienda, se observó que la institución se encuentra en un proceso de mejora, dando cumplimiento parcial a las acciones correctivas.

Se encuentran pendientes de cumplimiento puntos importantes que pueden eventualmente constituir riesgo relevante en cuanto a la confiabilidad, integridad y disponibilidad de la información administrada por el sistema. Entre los puntos principales pendientes de cumplimiento están: la reingeniería del Sistema Integrado de Administración Financiera, la contratación de personal necesario para mejorar la gestión y la adecuada segregación de funciones.

En consideración a las pruebas obtenidas se puede señalar que, durante el ejercicio fiscal 2012, se evidenciaron riesgos en cuanto a la confiabilidad de la información administrada en el Sistema Integrado de Administración Financiera.

Recomendación

La Dirección General de Informática y Comunicaciones deberá arbitrar medidas administrativas que permitan la contratación de personal necesario de manera a mitigar los riesgos asociados con las debilidades señaladas en el informe y proseguir con la reingeniería del SIAF.

Las máximas autoridades del Ministerio de Hacienda deberán asumir el compromiso para el mejoramiento institucional, de manera a minimizar los riesgos que pudieran afectar, tanto a la entidad como a las demás instituciones conectadas al Sistema Integrado de Administración Financiera (SIAF).

Capítulo II

II.1 Definición de la Arquitectura de información

II.1.1 Falta de procedimientos para mantener actualizado el diccionario de datos y las reglas de sintaxis.

Se cuenta con diccionario de datos y reglas de sintaxis, diseñados en los inicios del SIAF (Sistema Integrado de Administración Financiera). Existe un diccionario de datos para las aplicaciones que utilizan Oracle y otro diccionario de datos para las aplicaciones realizadas con el lenguaje de programación JAVA. No se dispone de procedimiento aprobado para realizar las actualizaciones a los mismos.

El artículo 1º de la Ley 1535 de Administración Financiera del Estado, menciona en los principios generales que "Esta ley regula la administración financiera del Estado, que comprende el conjunto de sistemas, las normas básicas y los procedimientos administrativos a los que se ajustarán sus distintos organismos y dependencias para programar, gestionar, registrar, controlar y evaluar los ingresos y el destino de los fondos públicos…."; debido a la importancia de toda la información administrada por los sistemas, tanto para el Ministerio de Hacienda como para los demás entes del estado y considerando que no se ha presentado descargo a la observación, esta auditoría se ratifica en la observación.

Conclusión

El diccionario de datos es un instrumento que contiene las características lógicas de los datos que se van a utilizar en el sistema informático, en él se encuentra toda la lista de elementos que forman parte del flujo de datos mismo; al no contar con procedimientos para la actualización del diccionario de datos, se corren serios riesgos en cuanto a la solidez del diseño, protección de datos, la centralización de la información y la correcta utilización de las reglas de sintaxis del sistema.

Recomendación

Arbitrar medidas para la elaboración de procedimientos de actualización del diccionario de datos.

II.1.2 Los cambios realizados en los sistemas no se reflejan inmediatamente en el diccionario de datos ni en las reglas de sintaxis.

El diccionario de datos esta accesible a las áreas de desarrollo y prueba. Los cambios realizados son documentados, pero los mismos no son reflejados inmediatamente en el diccionario de datos.

El artículo 1º de la Ley 1535 de Administración Financiera del Estado, menciona en los principios generales que *"Esta ley regula la administración financiera del Estado, que comprende el conjunto de sistemas, las normas básicas y los procedimientos administrativos a los que se ajustarán sus distintos organismos y dependencias para programar, gestionar, registrar, controlar y evaluar los ingresos y el destino de los fondos públicos…."*; debido a la importancia de toda la información administrada por los sistemas, tanto para el Ministerio de Hacienda como para las instituciones conectadas a la Red Metropolitana, y considerando que no se ha presentado descargo a la observación, esta auditoría se ratifica en la observación.

Conclusión

El diccionario de datos es una lista organizada de todos los datos del sistema; al no estar actualizado el diccionario de datos, se corren riesgos en cuanto a la solidez del diseño, protección de datos, la centralización de la información.

Recomendación

Actualizar en forma permanente el diccionario que contenga las reglas de sintaxis, el esquema de clasificación y los niveles de seguridad de los datos del sistema, de manera a prevenir incompatibilidades. Además, tomar las medidas necesarias que permitan que esos datos sean compartidos entre las aplicaciones y el sistema.

Fomentar el uso estandarizado del diccionario de datos entre los diferentes usuarios del Área de Desarrollo de Sistemas.

II.1.3 No se cuenta con un esquema para la clasificación de datos ni con niveles de seguridad para los datos almacenados en los sistemas.

Por Resolución Nº 210 de fecha 26 de diciembre del 2012 se aprueba la "Política de Seguridad de la Información". En el punto 3.1.2. Clasificación y Niveles de Seguridad de la Información, se menciona que "La información generada por los funcionarios de la institución debe ser clasificada de acuerdo a su nivel de confidencialidad". A la fecha no se cuenta con un esquema para la clasificación de datos.

En el descargo, la Institución manifiesta: "*Sin observación. Por Resolución MH Nº 196/2013 se crea la Unidad de Seguridad de la Información, entre cuyas funciones están "el establecimiento de los mecanismos que determinen la Clasificación y los Niveles de Seguridad de los Datos y Sistemas Informáticos administrados por la SSEAF", conjuntamente con la DGIC. La Unidad se encuentra en proceso de implementación. Se adjunta copia de la Resolución mencionada".*

A la realización de esta auditoría no se tuvo evidencia del inicio de los trabajos para suplir esta falencia y por la importancia de la información administrada, esta auditoría se ratifica en la observación.

Conclusión

Sin una adecuada clasificación de los datos administrados en el sistema no se definen los niveles apropiados de seguridad ni los controles adecuados, lo cual podría afectar a la confidencialidad e integridad de la información administrada.

Recomendación

Establecer un esquema de clasificación a todos los datos del sistema, basado en que es tan crítica y sensible la información de la institución; utilizar este esquema para aplicar los controles de acceso y resguardar la información que es administrada.

II.1.4 No posee un listado definido de usuarios de red ni propietarios de datos y sistemas.

Actualmente se cuenta con el listado de usuarios de aplicaciones, no así con el listado de usuarios de la red; según lo expuesto, se está trabajando en el listado actualmente, pero no tuvo evidencia al respecto.
Para identificar a los propietarios de sistemas, se basan en la Ley Nº 1535 de Administración Financiera, el cual define que los responsables de la aplicación del decreto reglamentario son las instituciones afectadas a la ley. No se tiene identificado a los propietarios de sistemas a nivel inferior; tampoco a los propietarios de datos.
Se considera imprescindible contar con todas las medidas de seguridad para proteger la información administrada por la Institución y considerando que no se ha presentado descargo a la observación, esta auditoría se ratifica en la misma.

Conclusión

Al no identificar adecuadamente a los usuarios que acceden a la red interna, las responsabilidades no están definidas y se corren riesgos en cuanto a la integridad y seguridad de la información.
Con la ausencia de una identificación adecuada de propietarios de datos y sistemas a nivel interno, se corren serios riesgos de seguridad, ya que no están definidas las responsabilidades ni se delimitan las acciones, y se dificultan los controles para la protección de los activos de información.

Recomendación

Aplicar mecanismos formales que faciliten el proceso de Rendición de Cuentas y posibiliten la identificación de los usuarios de datos, de sistemas y de red, delimitando las responsabilidades en el manejo de la información y resguardando la integridad y consistencia de los datos almacenados electrónicamente.

II.1.5 No se cuenta con políticas de acceso a la información a nivel interno.

Si bien el acceso a los datos está definido por privilegios, no se cuenta con una política aprobada para el manejo del mismo.
En el descargo la Institución manifiesta: "*Las Políticas han sido definidas en el Manual de Administración de Cuentas de Usuarios Finales, recientemente aprobado por Resolución DGIC Nº 035/13 del 11/07/13. En proceso de implementación gradual*".

Considerando que en el ejercicio fiscal auditado no se contaba con el "*Manual de Administración de Cuentas de Usuarios Finales"* y la importancia de la correcta administración de la información para la entidad, esta auditoría se ratifica en la observación.

Conclusión

Al no establecer reglas claras para el acceso a la información, se corren riesgos de seguridad que pueden afectar a la integridad y consistencia, de los datos administrados por la institución.

Recomendación

Implementar políticas de acceso a la información con reglas claras de administración, que permitan minimizar inconvenientes que puedan afectar al sistema.

II.2 Definición de la organización de Tecnología de Información

II.2.1 No se tiene identificado al personal clave.

La Institución no tiene identificado al personal clave ni se cuenta con programas de reemplazo de personal.

No se ha presentado descargo a la observación por lo cual, esta auditoría se ratifica en la misma.

Conclusión

Al no tener identificado al personal clave de tecnología de la información, se corren riesgos en la seguridad, ya que no se puede determinar adecuadamente quien administra los sistemas ni establecer responsabilidades, de forma a asegurar la transparencia y establecer los controles adecuados.

Recomendación

Definir e identificar al personal clave de tecnología de la información, de manera a disminuir la dependencia en una sola persona que realiza funciones críticas y lograr la efectividad, eficiencia y el soporte oportuno ante los requerimientos constantes.

II.3 Garantizar la seguridad de los sistemas

II.3.1 No se cuenta con políticas para el tratamiento de perfiles de usuario en caso de permisos, vacaciones, despidos.

La Institución no cuenta con políticas para el tratamiento de los perfiles de usuario, de manera a garantizar la suspensión, modificación, cierre de cuentas de usuario y los privilegios relacionados en caso de permisos, vacaciones, despidos etc.

En el descargo la Institución menciona: "*Las Políticas han sido definidas en el Manual de Administración de Cuentas de Usuarios Finales, recientemente aprobado por Resolución DGIC Nº 035/13 del 11/07/13. En proceso de implementación gradual".*

Considerando que en el ejercicio fiscal auditado no se contaba con el "*Manual de Administración de Cuentas de Usuarios Finales"* y la importancia de la correcta administración de la información para la entidad, esta auditoría se ratifica en la observación.

Conclusión

Al no establecer reglas claras para el tratamiento de los perfiles de usuario en caso de permisos, vacaciones, despidos, se corren riesgos de seguridad que pueden eventualmente afectar a la integridad, confiabilidad y disponibilidad, de la información administrada por la institución.

Recomendación

Considerando que actualmente se dispone de un *Manual de Administración de Cuentas de Usuarios Finales*; con el fin de mitigar está debilidad se deben establecer las medidas necesarias en la brevedad posible. Se debe realizar transferencia de conocimiento, reasignar responsabilidades y bloquear/eliminar los privilegios de acceso, de manera que los riesgos sean minimizados y se garantice la continuidad del servicio sin inconvenientes.

II.3.2 No se realizan revisiones sobre las pistas de auditoría.

No se cuentan con pistas de auditoría centralizada. Solo se tienen pistas de auditoría que le ofrece el Oracle y algunas aplicaciones JAVA. No se realizan revisiones sobre las mismas, tampoco se cuenta con un encargado para realizar dicha revisión. Se solicitó por Memorándum Nº 04/2013, de fecha 17 de junio de

2013, copia de pistas de auditoría del periodo 01/05/12 al 01/06/12 a lo cual por Memorándum DS 44/13 de fecha 21 de junio de 2013 se respondió "no existen pistas de auditoría para el periodo indicado".

En el descargo la Institución manifiesta: *"Sin observaciones con respecto a las pistas de auditoría del periodo indicado. Conforme al Plan de Trabajo de Seguridad del presente ejercicio, aprobado por Resolución DGIC Nº 02/13, se realizó la incorporación en la herramienta ACL de las tablas faltantes para los procesos críticos del SIARE. Se adjunta el Informe Nº 08 del Dpto. de Seguridad de la Información de fecha 22/Marzo/13".*

Considerando que el ejercicio fiscal auditado es 2012, esta auditoría se ratifica en la observación.

Conclusión

La falta de adecuados controles internos, lleva a serios riesgos en la seguridad, lo cual podría eventualmente afectar a la confiabilidad e integridad de la información administrada por la Institución.

Recomendación

Prever mecanismos de control interno en forma permanente sobre las pistas de auditoría, y realizar seguimiento de los movimientos del sistema, estableciendo que toda acción ejecutada sea procesada, almacenada y presentada sin transgresión. Identificar quien o quienes tengan permiso para realizar revisiones sobre las pistas de auditoría, y cuánto tiempo se retienen los registros.

II.3.3 Los privilegios otorgados para el acceso a los sistemas no están acordes con el Manual de Organización, Funciones y Cargos.

Por Memorándum Nº 04/2013, de fecha 17 de junio del 2013 se solicitó un informe si los privilegios otorgados están acordes al Manual de Organización, Funciones y Cargos, a lo cual por Memorándum DS 44/13 de fecha 21 de junio del 2013 se respondió "Los privilegios se otorgan de conformidad con el Manual de Procedimientos DAU, en el apartado Reglamento de Gestión de Usuario", en la misma hace mención a los requisitos para la gestión de usuarios no así a la asignación de privilegios en el sistema de acuerdo a las funciones que cumplen en la institución.

En el descargo la Institución manifestó cuanto sigue: *"Este punto se trata en el Manual de Administración de Cuentas de Usuario Finales, recientemente aprobado por* Resolución DGIC Nº 035/13 del 11/07/13. En proceso de implementación gradual".

Considerando que en el ejercicio fiscal auditado año 2012, no se cuenta con controles adecuados, esta auditoría se ratifica en la observación.

Conclusión

La falta de una adecuada gestión de privilegios, trae asociado el mal manejo de la información administrada por los sistemas y el eventual riesgo a la integridad, confiabilidad y confidencialidad de los datos.

Recomendación

Implementar reglas de acceso para establecer la correlación entre los usuarios, sus funciones y los datos a los que pueden acceder.
Implementar control de acceso a los usuarios basado sobre el menor privilegio. Esto está referido al otorgamiento de los accesos requeridos para ejecutar funciones específicas; de ser necesario permiso adicional también debe ser documentado.

II.4 Desarrollo y mantenimiento de software de aplicación

II.4.1 La documentación de los sistemas no está actualizada.

Se cuenta con un Procedimiento de Control de Cambios aprobado por Resolución Nº 2 de fecha 4 de enero de 2011, del Ministerio de Hacienda; en la actividad 120 –Documentación, tiene como tarea "Actualizar la documentación de Programas"; en Hoja de Entrevistas Nº 1 de fecha 13/06/13, se consultó "La documentación de los Sistemas está actualizada", a lo cual se respondió de forma negativa, la documentación de los sistemas no se encuentra actualizada a la fecha.

La Institución no presentó descargo a la observación, por lo cual esta auditoría se ratifica en la misma.

Conclusión

La falta de una documentación actualizada de los sistemas, trae consigo inconvenientes como: utilización no efectiva del sistema y problemas para el mantenimiento futuro del sistema.

Recomendación

Mantener actualizada la documentación de los sistemas, para asegurar la utilización efectiva y su mantenimiento futuro. Implementar procedimientos que permitan que la documentación de los sistemas sea almacenada fuera del sitio, que posibiliten su recuperación en caso de desastre.

II.5 Administración de Recursos Humanos

II.5.1 No se cuenta con políticas para la selección de personal para el área de informática.

No se cuenta con políticas para la selección de personal para el área de informática ni se realiza entrenamiento inicial al personal nuevo.

En su descargo la Institución manifiesta: "*Se adjunta copia de la Resolución MH Nº 139/2012 del 26/Abril/2012, que aprueba las "Políticas de Talento Humano" y la Resolución MH Nº 187/2011 que aprueba el Reglamento Interno de Selección para el Ingreso y Promoción de Funcionarios y Personal Contratado".*

Se aceptan como válidas las informaciones y documentaciones remitidas por DGIC en el descargo sobre este punto.

II.5.2 Personal insuficiente para cumplir funciones primordiales.

Se siguen presentando problemas de insuficiencia de personal para el cumplimiento de funciones claves. El Jefe de Departamento de Seguridad Informática se encuentra a su vez como Jefe Interino del Departamento de Infraestructura.

La Institución no presentó descargo a la observación, por lo que esta auditoría se ratifica en la misma.

Conclusión

Al no contar con personal suficiente que pueda llevar adelante las funciones primordiales, se corren riesgos de que los sistemas no estén disponibles, no sean íntegros ni confiables.

Recomendación

Dotar a la DGIC del personal necesario que garantice la disponibilidad, integridad y confiabilidad del sistema.

Capítulo III

Conclusiones y Recomendaciones Finales

1. Conclusión Final

Realizado el análisis de cada uno de los puntos expuestos en este informe podemos emitir las siguientes opiniones:

La Dirección General de Informática y Comunicaciones se encuentra en un lento proceso de mejora; siguen pendientes de cumplimiento, puntos importantes que pueden eventualmente constituir riesgo relevante para la confiabilidad, integridad y disponibilidad de la información que es administrada en los sistemas. Entre ellos los más relevantes son: la reingeniería del SIAF, la contratación de personal necesario para mejorar la gestión y lograr una adecuada segregación de funciones.

Tomando en cuenta las evidencias obtenidas, queda comprobado que durante el ejercicio fiscal 2012, se corrieron riesgos que pondrían eventualmente a la información administrada en los sistemas.

2. Recomendaciones Finales

Recomendaciones del Capítulo I

La Dirección General de Informática y Comunicaciones deberá arbitrar medidas administrativas que permitan la contratación de personal necesario de manera a mitigar los riesgos asociados con las debilidades señaladas en el informe y proseguir con la reingeniería del SIAF.

Las máximas autoridades del Ministerio de Hacienda deberán asumir el compromiso para el mejoramiento institucional, de manera a minimizar los riesgos que pudieran afectar, tanto a la entidad como a las demás instituciones conectadas al Sistema Integrado de Administración Financiera (SIAF).

Recomendaciones del Capítulo II

- Arbitrar medidas para la elaboración de procedimientos de actualización del diccionario de datos.
- Actualizar en forma permanente el diccionario que contenga las reglas de sintaxis, el esquema de clasificación y los niveles de seguridad de los datos del sistema, de manera a prevenir incompatibilidades. Además, tomar las medidas necesarias que permitan que esos datos sean compartidos entre las aplicaciones y el sistema.

- Fomentar el uso estandarizado del diccionario de datos entre los diferentes usuarios del Área de Desarrollo de Sistemas.
- Establecer un esquema de clasificación a todos los datos del sistema, basado en que es tan crítica y sensible la información de la institución; utilizar este esquema para aplicar los controles de acceso y resguardar la información que es administrada.
- Aplicar mecanismos formales que faciliten el proceso de Rendición de Cuentas y posibiliten la identificación de los usuarios de datos, de sistemas y de red, delimitando las responsabilidades en el manejo de la información y resguardando la integridad y consistencia de los datos almacenados electrónicamente.
- Implementar políticas de acceso a la información con reglas claras de administración, que permitan minimizar inconvenientes que puedan afectar al sistema.
- Definir e identificar al personal clave de tecnología de la información, de manera a disminuir la dependencia en una sola persona que realiza funciones críticas y lograr la efectividad, eficiencia y el soporte oportuno ante los requerimientos constantes.
- Considerando que actualmente se dispone de un Manual de Administración de Cuentas de Usuarios Finales; con el fin de mitigar está debilidad se deben establecer las medidas necesarias en la brevedad posible. Se debe realizar transferencia de conocimiento, reasignar responsabilidades y bloquear/eliminar los privilegios de acceso, de manera que los riesgos sean minimizados y se garantice la continuidad del servicio sin inconvenientes.
- Prever mecanismos de control interno en forma permanente sobre las pistas de auditoría, y realizar seguimiento de los movimientos del sistema, estableciendo que toda acción ejecutada sea procesada, almacenada y presentada sin transgresión.
- Identificar quien o quienes tengan permiso para realizar revisiones sobre las pistas de auditoría, y cuánto tiempo se retienen los registros.
- Implementar reglas de acceso para establecer la correlación entre los usuarios, sus funciones y los datos a los que pueden acceder.
- Implementar control de acceso a los usuarios basado sobre el menor privilegio. Esto está referido al otorgamiento de los accesos requeridos para ejecutar funciones específicas; de ser necesario permiso adicional también debe ser documentado.
- Mantener actualizada la documentación de los sistemas, para asegurar la utilización efectiva y su mantenimiento futuro. Implementar procedimientos que permitan que la documentación de los sistemas sea

almacenada fuera del sitio, que posibiliten su recuperación en caso de desastre.

- Dotar a la DGIC del personal necesario que garantice la disponibilidad, integridad y confiabilidad del sistema.

Plan de Mejoramiento e informe

- Elevar a la Contraloría General de la República en un plazo no mayor a 120 días, un nuevo informe sobre las medidas a ser adoptadas para subsanar las observaciones mencionadas del Plan de Mejoramiento presentado, adecuándolo en base a documentos aprobados y finales, a fin de poder realizar un seguimiento efectivo a las actividades de mejoramiento de la Dirección General de Informática y Comunicaciones, dependiente del Ministerio de Hacienda.

ES NUESTRO INFORME.

Asunción, 23 de septiembre de 2013

José Arzamendia
Auditor

Econ. Carlos Ramírez
Auditor

Ing. Sonia Cattebeke
Auditor

Ing. Mabel Arriola
Jefe de Equipo

Lic. Yassir Admén Ramírez
Director

DUPLICADO

Asunción, 03 OCT. 2013

Nota CGR Nº L - 4072

Ref: Resolución CGR N° 261/13, Examen Especial a la Dirección General de Informática y Comunicaciones- Ministerio de Hacienda

Señor Ministro:

Me dirijo a Vuestra Excelencia a efectos de remitir adjunto el Informe Final en el marco del trabajo dispuesto por Resolución CGR N° 261 de fecha 3 de abril de 2013, **"POR LA CUAL SE DISPONE LA REALIZACIÓN DE UN EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES, DEPENDIENTE DEL MINISTERIO DE HACIENDA, CORRESPONDIENTE AL EJERCICIO FISCAL 2012".**

La evaluación emitida en el presente informe es el resultado del análisis de los documentos que han sido proveídos a los auditores para su estudio, los cuales son de exclusiva responsabilidad de los funcionarios de la Dirección General de Informática y Comunicaciones, dependiente del Ministerio de Hacienda, que intervinieron en la ejecución y formalización de las operaciones examinadas.

Hago propicia la ocasión para saludar a Vuestra Excelencia con distinguida consideración.

ALFREDO DAVID BARÚA M.
Secretario General

OSCAR RUBÉN VELÁZQUEZ GADEA
Contralor General
de la República

A Su Excelencia
Lic. GERMÁN HUGO ROJAS IRIGOYEN, Ministro
Ministerio de Hacienda

ORVG/D/ma

RECIBIDO
04 OCT 2013
M.C.E
MINISTERIO DE HACIENDA

MINISTERIO DE HACIENDA
S.I.M.E. Nº 47 595/2013