INFORME FINAL

EXAMEN ESPECIAL

MINISTERIO DE HACIENDA

DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES-DGIC

1. ANTECEDENTES

La Resolución CGR N° 520 del 24 de noviembre de 2005 "*Por la cual se aprueba la metodología para la elaboración de Informe y Dictamen de la Contraloría General de la República*", estableció la necesidad de evaluar la confiabilidad de los controles implementados para el resguardo del Sistema Integrado de Administración de Recursos del Estado, evaluación que será incluida por la Contraloría General de la República en el Informe y Dictamen sobre el Informe Financiero del ejercicio fiscal 2013, elaborado por el Ministerio de Hacienda en cumplimiento del artículo 282 de la Constitución Nacional y del artículo 69 de la Ley N° 1535/99 "*De Administración Financiera del Estado".*

Para el mejor cumplimiento de los fines enunciados en el párrafo anterior, en la Resolución CGR N° 125 de fecha 28 de febrero de 2014, la Contraloría General de la República dispuso la realización de un Examen Especial a la Dirección General de Informática y Comunicaciones, dependiente de la Subsecretaría de Estado de Administración Financiera del Ministerio de Hacienda, correspondiente al ejercicio fiscal 2013.

En la Nota CGR N° 06246 de fecha 4 de julio de 2014, se remitió a la Entidad auditada la Comunicación de Observaciones elaborada como resultado del Examen Especial a la Dirección General de Informática y Comunicaciones, dependiente de la Subsecretaría de Estado de Administración Financiera del Ministerio de Hacienda, correspondiente al ejercicio fiscal 2013, para que, en un plazo perentorio de 10 (diez) días presente el Descargo correspondiente.

Se deja constancia que la Dirección General de Informática y Comunicaciones del Ministerio de Hacienda, no presentó los descargos a las observaciones formuladas por esta auditoría.

2. ALCANCE DEL EXAMEN

El examen especial incluyó el análisis de los controles internos implementados en el ejercicio fiscal 2013 por el Departamento de Seguridad de la Información, dependiente de la Dirección General de Informática y Comunicaciones del MH, con el fin de mantener la seguridad de la información administrada por la entidad; el cumplimiento de las medidas señaladas en el Plan de Mejoramiento presentado por el Ministerio de Hacienda para la implementación de las recomendaciones formuladas en los Informes Finales de los Exámenes Especiales practicados sobre los ejercicios fiscales 2006 al 2012.

El examen practicado por los Auditores de la CGR fue realizado de conformidad a las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) que son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI), las cuales son

compatibles con las establecidas en las Normas Internacionales de Auditoría (NIA), las Normas de Auditoría aplicables al Sector Público, y el Manual de Auditoría Gubernamental del Paraguay, que contiene disposiciones para las actividades en materia de control gubernamental, fundamento principal de referencia para las actividades de fiscalización y control por parte de la CGR, además el 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 se cumpla con requisitos éticos, se planifique y se realice la Auditoría para obtener certeza razonable que la información y documentación auditada no contengan exposiciones erróneas. Igualmente, que las operaciones a las cuales ellas corresponden hayan sido ejecutadas de conformidad a las disposiciones legales vigentes y demás normas aplicables.

El resultado del presente informe, surge del análisis de los documentos proveídos a los auditores para su estudio y que son de exclusiva responsabilidad de los funcionarios de la Dirección General auditada.

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

3. OBJETIVO DEL EXAMEN

Analizar y evaluar que la planificación, administración y coordinación de los sistemas de información y comunicaciones cuenten con directivas y procedimientos de funcionamiento y mantenimiento de los sistemas para asegurar la operación en línea entre los organismos y entidades del Estado a través de la Red Nacional de Comunicaciones, la confiabilidad de los controles internos y el cumplimiento de las recomendaciones formuladas en Exámenes Especiales anteriores.

4. AUTORIDADES DE LA INSTITUCIÓN

A continuación se detalla la nómina de las autoridades de la Dirección General de Informática y Comunicaciones durante, en funciones durante el ejercicio fiscal 2013.

Nombre y Apellido	Cargo	Dependencia	Disposición legal de designación	Presta Servicios en el cargo	
				Desde	Hasta
Sr. Juan Carlos Ferreira Matto	Encargado de la Atención del Despacho	Director General de Informática y de Comunicaciones	Resolución SSEAF N° 214-12	01/01/13	Actualidad
Sr. Edgar Rafael Vivero Bareiro	Jefe	Departamento de Sistemas Informáticos	Resolución MH N° 25-08	02/01/08	Actualidad
Sr. Enrique Poletti Pietrafesa	Jefe	Departamento de Seguridad Informática	Resolución MH N° 25-08	02/01/08	Actualidad
Sr. Derlis Alfredo Samudio Coronel	Jefe	Departamento de Comunicaciones	Resolución MH N° 25-08	02/01/08	Actualidad
Sr. Gustavo R. Pineda	Jefe	Departamento de Soporte Técnico	Resolución MH N°25-08	02/01/08	Actualidad

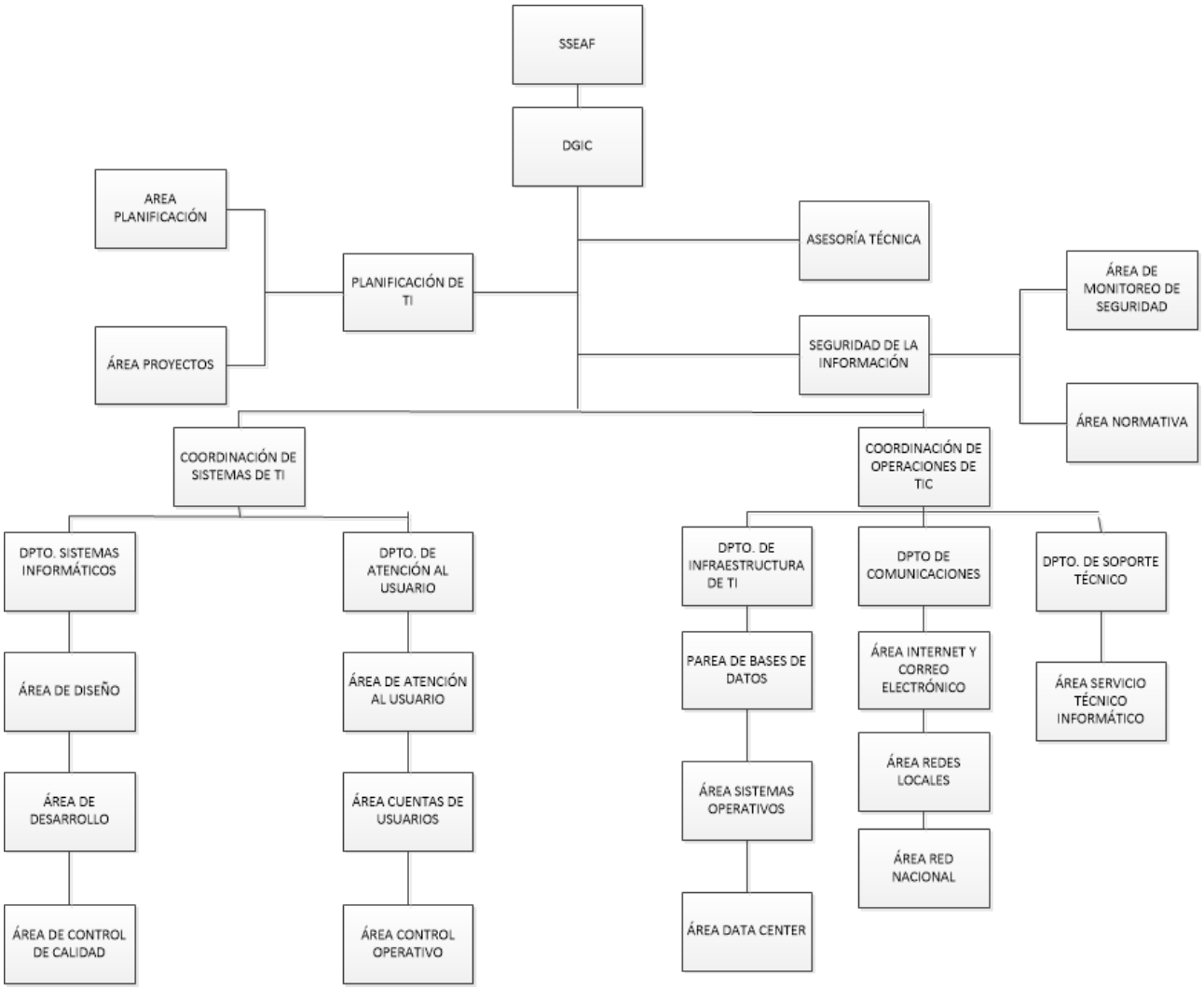
Nombre y Apellido	Cargo	Dependencia	Disposición legal de designación	Presta Servicios en el cargo	
Sr. Diego Manuel Quintana Yegros	Jefe Interino	Departamento de Atención al Usuario	Resolución MH N° 106-08	22/10/08	14/01/14
Sra. Miriam Teresa Gómez de Malwitz	Jefa	Departamento de Planificación	Resolución MH N° 140-09	22/04/09	Actualidad
Sr. Enrique Poletti Pietrafesa	Encargado de la Atención del Despacho sin perjuicio de sus actuales funciones	Departamento de Infraestructura de TI	Resolución SSEAF N°39/13	08/03/13	13/11/13
Sra. Graciela Benítez de Román	Encargado de la Atención del Despacho	Departamento de Infraestructura de TI	Resolución SSEAF N° 145-13	13/11/13	Actualidad
Sr. Diego Manuel Quintana Yegros	Jefe	Departamento de Atención al Usuario	Resolución MH Nº 12-2014	14/01/14	Actualidad

Fuente: Memorándum DGIC N° 117/14, de fecha 17/06/14 -Dirección General de Informática y Comunicaciones

5. DISPOSICIONES LEGALES

5.1 Constitución Nacional de la República del Paraguay.
5.2 Ley Nº 276/94 "*Orgánica y Funcional de la Contraloría General de la República"*.
5.3 Ley Nº 1535/99 "*De Administración Financiera del Estado*".
5.4 Decreto N° 8127/00 "*Por el cual se establecen las disposiciones legales y administrativas que reglamentan la implementación de la Ley 1535/99 de Administración Financiera- SIAF".*
5.5 Resolución MH N° 290/12."*Por la cual se modifica el Organigrama y el Manual de Organización, Funciones y Cargos de la DGIC".*
5.6 Otras disposiciones vigentes aplicables.

6. ORGANIGRAMA ESTRUCTURAL DE LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES



7. DESARROLLO DEL EXAMEN

Para una mejor comprensión del presente Informe se han desarrollado los siguientes capítulos:

CAPÍTULO I - CONTROL INTERNO IMPLEMENTADO POR EL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO II - SEGUIMIENTO A LAS RECOMENDACIONES DE AUDITORIAS ANTERIORES

CAPÍTULO III - CONCLUSIONES Y RECOMENDACIONES

INTRODUCCIÓN

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

De forma a asegurar la operación en línea entre el Ministerio de Hacienda y las entidades de la Administración Central, la ley 1535/99 de Administración Financiera del Estado, establece que estarán a cargo de la Dirección General de Informática y Comunicaciones las funciones de planificación, administración y coordinación de los sistemas de información y comunicaciones del área de administración de recursos de los organismos y entidades del Estado y la red Metropolitana.

Para el logro del objetivo mencionado se implementó el Sistema Integrado de Administración Financiera (SIAF) de forma a integrar y armonizar las tareas derivadas de la administración de recursos asignados a las entidades.

En cumplimiento de las funciones de control asignadas por la Constitución Nacional, concordantes con las disposiciones legales, Ley Nº 276/94 “Orgánica y Funcional de la Contraloría General de la República”, se dispuso por Resolución CGR Nº 125 de fecha 28 de febrero de 2014, la realización de un Examen Especial a efectos de opinar sobre la razonabilidad en el manejo de los registros informáticos del Sistema Integrado de Administración de Recursos del Estado.

CAPÍTULO I

1. CONTROL INTERNO IMPLEMENTADO POR EL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN.

En la Resolución MH N° 290 de fecha 26 de setiembre de 2012 fue modificado el organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones, dependiente de la Subsecretaría de Estado de Administración Financiera del Ministerio de Hacienda.

El Departamento de Seguridad de la Información paso a formar parte del *staff* y a depender directamente de la Dirección General.

Los funcionarios del Departamento de Seguridad de la Información fueron entrevistados de manera a verificar los controles implementados y la adecuación al Manual de Organización y Funciones del Departamento. En ese procedimiento se pudo evidenciar cuanto sigue:

1.1. No son gestionados los riesgos en todos los proyectos y procesos

Se realiza la gestión de riesgos en los proyectos y procesos en los que el Departamento de Seguridad de la Información tiene participación, pero no en todos.

En la Resolución MH Nº 290/12 fue modificado el Organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones, y en ella quedó establecida como función específica del Departamento de Seguridad de la Información, "*gestionar los riesgos de TIC y proponer acciones de mitigación*".

Al ser requerida a la Dirección General de Informática y Comunicaciones sobre ese particular, respondió que "*Se gestionan los riesgos pero no en todos los procesos*", "*En base a la matriz de riesgos de procesos de la DGIC se identificaron acciones de mitigación. Las mismas se incluyen en los planes de trabajo de la DGIC. Asimismo en los proyectos en los que se tiene participación se aplican criterios de seguridad con el objeto de mitigar riesgos".*

La Dirección General de Informática y Comunicaciones no cuenta con procedimiento aprobado que obligue a incluir al Departamento de Seguridad de la Información en todos los proyectos y procesos de forma que le permita evaluar los riesgos, solo participa en algunos casos. Esta situación podría afectar que la emisión de la información no sea confiable, integra y esté disponible para los usuarios de la misma.

CONCLUSIÓN

El hecho de no realizar la gestión de riesgos en todos los proyectos y procesos, dificulta la identificación de los elementos relacionados con el riesgo, aumenta las vulnerabilidades y, además, no pueden ser establecidas acciones de mitigación y prevención.

RECOMENDACIÓN

Elaborar procedimientos adecuados de manera a incluir al Departamento de Seguridad de la Información en todos los proyectos y procesos que afecten la actividad de la Dirección de forma que se realice una adecuada gestión de riesgos y reducir los efectos negativos que podrían ocasionar los mismos a las actividades de la DGIC.

1.2. No se evalúa el nivel de riesgo de seguridad de información de proveedores que procesen información restringida y confidencial.

Se pudo evidenciar que el Departamento de Seguridad de la Información no evalúa el nivel de riesgo en la incorporación de proveedores que procesan información restringida y confidencial.

La ya aludida Resolución MH Nº 290/12 que modificó el Organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones, asignó a esa Dirección la función de "*evaluar el nivel de riesgo de seguridad de información de proveedores que procesen información restringida y confidencial y recomienda acciones de mitigación*".

Al requerimiento la Dirección General de Informática y Comunicaciones sobre ese particular, explicó que "s*i bien es cierto que existe una cláusula de confidencialidad en los contratos, no existe un procedimiento, política ni esquema organizacional, que obligue a las distintas áreas a comunicar a este Departamento sobre el acceso de proveedores a activos de la organización".*

El Departamento de Seguridad de la Información no participa en la contratación de todos los proveedores que manejan información restringida y confidencial. Esta situación limita una adecuada gestión de los riesgos de la información utilizada.

CONCLUSIÓN

Al no realizar la gestión de riesgos en la incorporación de proveedores que manejan información restringida o confidencial, no pueden ser identificados todos los riesgos relacionados con la seguridad de la información, aumentan las vulnerabilidades y se dificulta el establecimiento de acciones de mitigación y prevención.

RECOMENDACIÓN

Elaborar procedimientos de manera a incluir al Departamento de Seguridad de la Información en los procesos que incluyan la incorporación de proveedores que manejan información sensible y confidencial de forma a salvaguardar la confidencialidad, integridad y disponibilidad de la información administrada por la institución.

1.3. No son evaluados los riesgos de modo continuo respecto a la seguridad de la información.

No se cuenta con un proceso continuo de evaluación de riesgo de seguridad de la información.

En la modificación del Organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones dispuesta en la ya aludida Resolución MH Nº 290/12 se dispuso asignar como función específica, "*Evalúa de modo continuo los riesgos en cuanto a la seguridad de la información, de los procesos y la tecnologías implantadas y recomienda acciones de mitigación*".

Al ser requerido a la Dirección General de Informática y Comunicaciones sobre ese aspecto, respondió que "*Se evalúa los procesos en los que se tiene participación, si bien no existe una metodología, sin embargo no existe un procedimiento, política ni esquema organizacional, que obligue a las distintas áreas a dar participación a este departamento en procesos y tecnologías implantadas*".

El Departamento de Seguridad de la Información no realiza una evaluación continua de riesgos de seguridad, generándose vulnerabilidades que pueden afectar a la información y a las tecnologías implantadas.

CONCLUSIÓN

La falta de una evaluación de riesgos de modo continuo dificulta la identificación oportuna de amenazas que podrían impedir el cumplimiento de los objetivos de la Institución.

RECOMENDACIÓN

Elaborar políticas y procedimientos de manera a dar participación al Departamento de Seguridad de la Información en procesos de tecnologías implantadas, de forma a lograr una mejora continua de gestión de riesgos para identificar oportunamente las amenazas y dar cumplimiento a los objetivos de la institución.

1.4. Las políticas de seguridad incluyen procesos generales pero sin definir procedimientos específicos para cada proceso incluido en las mismas.

Se evidenció que la Resolución Nº 210 de fecha 26 de diciembre de 2012 aprobó la "Política de Seguridad de la Información" de la Subsecretaria de Estado de Administración Financiera del Ministerio de Hacienda. En ella se incluyen controles generales de Tecnología de Información. Sin embargo, no se cuenta con políticas referentes a la Administración de Recursos de Tecnología de la Información, Clasificación y Niveles de Seguridad de la Información, Gestión de Monitoreo y Reportes de Eventos de Seguridad.

En la Política de Seguridad de la Información aprobada, se indica, a un nivel general, que deben hacerse controles sobre la Administración de Recursos de Tecnología de la Información, Clasificación y Niveles de Seguridad de la Información, Gestión de Monitoreo y Reportes de Eventos de Seguridad, de forma general. Asimismo, en el Manual de Organización y Funciones del Departamento de Seguridad de la Información, le asigna la función de *: Definir los niveles de clasificación de la información y la documentación de la DGIC y monitorear el cumplimiento de las Políticas relativas a la seguridad de la información; Evaluar de modo continuo los riesgos en cuanto a la seguridad de la información, de los procesos y las tecnologías implantadas y recomendar acciones de mitigación; Recibir informes de los eventos e incidentes (inclusive señales de alertas de seguridad) recabar información y proponer medidas correctivas."*

Requerido al respecto, la Dirección General de Informática y Comunicaciones informó que, "*Se aprobó las políticas en el 2012, Auditoría Interna Informática recomendó que las políticas sean adecuadas anualmente y se incluyan procesos a nivel inferior"*. "*En el plan de trabajo de cada año se incluye las tareas correspondientes a la elaboración/actualización de políticas/procedimientos".*

Las Políticas de Seguridad con que cuenta la Institución no indican procedimientos específicos a seguir para mantener la seguridad de los activos creando brechas que pueden afectar al logro de los objetivos del Departamento de Seguridad.

CONCLUSIÓN

El hecho de no institucionalizar las buenas prácticas en la administración de tecnologías de la información hace que el logro de los objetivos institucionales se vea dificultado, corriendo riesgos, tanto sobre la información administrada, como sobre los equipamientos, situación que podría, ante eventualidades, afectar a los activos de la institución.

RECOMENDACIÓN

Utilizar como base las Políticas de Seguridad de la Información e implementar políticas, procedimientos, normas y reglamentaciones complementarias para controlar la estandarización, la calidad de las operaciones, y evitar desviaciones en el logro de los objetivos y de las metas propuestas. Formalizar las documentaciones y socializar con las áreas competentes.

1.5. No son registrados todos los incidentes de seguridad en el Sistema de Gestión de Seguridad de la Información

En la Resolución DGIC–SSEAF Nº 022/12 se aprobó el procedimiento de gestión de incidentes, en cuya Tarea 30, se incluye el proceso de registro de incidentes de Tecnología de Información. Este procedimiento es cumplido de forma parcial ya que no todos los incidentes que se producen son registrados.

En la Resolución MH Nº 290/12, que modificó el Organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones, se le asigna al Departamento de Seguridad de la Información la función específica de, *"Recibir informes de los eventos e incidentes (inclusive señales de alertas de seguridad, recabar información y proponer medidas correctivas",* así mismo, en las Políticas de Seguridad aprobada por Resolución Nº 210 de fecha 26 de diciembre de 2012 en el punto 3.1 Reglas Generales-Obligaciones, 3.1.7 Gestión de Monitoreo y Reporte de Eventos de Seguridad Informática, a) Reporte de Actividades de Seguridad se indica *"El área de Administración de Seguridad Informática debe asegurar que los posibles incidentes de seguridad sean definidos y comunicados de forma clara, de manera que los problemas de seguridad sean atendidos de forma apropiada por medio del proceso de Gestión de Incidentes de Seguridad de TI".* Sin embargo, se informó que *"La falta de adherencia al procedimiento ha hecho que no sean registrados la totalidad de los incidentes".*

Se cuenta con el Procedimiento de Gestión de Incidentes, pero la falta de apego al mismo hace que no sean registrados la totalidad de los incidentes de seguridad que se producen, lo que hace que no se lleve un completo histórico de incidentes. Esta situación podría afectar a la eficiencia y rapidez de respuesta en caso en que sean requeridos.

CONCLUSIÓN

Al no llevar un registro detallado de todos los incidentes de seguridad, no se puede evitar que el mismo evento vuelva a ocurrir. Tampoco se cuenta con el histórico completo de todos los incidentes y las soluciones propuestas, de forma que se pueda resolver el problema con mayor eficiencia y rapidez.

RECOMENDACIÓN

Velar por el cumplimiento del "Procedimiento de Gestión de Incidentes" aprobado en la Resolución DGIC–SSEAF N° 022/10 y crear conciencia sobre la importancia del mismo y de la utilidad del registro de los incidentes de seguridad producidos de manera que ese registro sirva de herramienta de apoyo al control de la seguridad de la información.

1.6. El control de la aplicación de las normativas de acceso físico a las áreas de la DGIC no es ejercido por el Departamento de Seguridad de la Información

Se pudo evidenciar que el Departamento de Seguridad de la Información no realiza el control de la aplicación de políticas, normativas y procedimientos relativos a: acceso físico a las áreas y a los recursos de tecnologías de información.

En la modificación del Organigrama y el Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones dispuesta en la Resolución MH Nº 290/12, se le asigna la función específica al Departamento de Seguridad de la información, *"Controlar la aplicación de políticas, normativas y procedimientos relativos a: acceso físico a las áreas y a los recursos de tecnologías de información".* Igualmente, en el punto 3.1.9., "Administración del Ambiente Físico", b) Acceso Físico de la "Política de Seguridad de la Información", se indica, *"El área de Administración de Seguridad Informática de la DGIC conjuntamente con el Departamento de Seguridad de la Dirección General de Administración y Finanzas, deben definir e implementar procedimientos para otorgar, limitar y revocar el acceso de funcionarios a locales, edificios y áreas de acuerdo con las necesidades de la institución, incluyendo las emergencias. El acceso a locales, edificios y áreas debe ser justificado, autorizado, registrado y monitoreado. Esto aplica para todas las personas que accedan a las instalaciones incluyendo funcionarios, visitantes, proveedores o cualquier tercera persona".*

Al ser requerido al respecto la Dirección General de Informática y Comunicaciones, respondió que, "*El acceso físico no es controlado por el departamento ya que las funciones lo indican como un área normativa", "Se ha participado del proceso de elaboración de normativas de acceso al edificio, si bien el proceso en si es de responsabilidad de otra área de la organización. Si se participa, gradualmente, del proceso de acceso a los recursos de TI".*

El Manual de Organización, Funciones y Cargos y las Políticas de Seguridad de la Información, establecen que el Departamento de Seguridad de la Información debe realizar el control sobre el cumplimiento de la normativa de acceso físico a las áreas de la Dirección General de Informática y Comunicaciones. No se ha evidenciado el cumplimiento a cabalidad de estas normas, así mismo, su incumplimiento podría afectar negativamente a la Institución en caso de eventos no previstos.

CONCLUSIÓN

La falta de control sobre la aplicación de las políticas, normativas y procedimientos relativos a: acceso físico a las áreas y a los recursos de tecnologías de información, produce brechas de seguridad que pueden afectar a los activos y a la información que se administra, y producir serios daños a la Institución.

RECOMENDACIÓN

Realizar un control periódico de la aplicación de las normas y reglamentos establecidos para el control de acceso físico de la Institución y evitar perjuicio que se puede producir por esta falencia.

1.7. El Manual de Organización, Funciones y Cargos asigna al Departamento de Seguridad de la Información una función normativa

El Manual de Organización, Funciones y Cargos designa al Departamento de Seguridad de la Información como un área normativa, es decir no desempeña específicamente funciones de control, que están distribuidas en varios departamentos de la DGIC: al Departamento de Atención al Usuario corresponde la gestión de usuarios; al Departamento de Comunicaciones, las gestiones de acceso, etc. Además, existen funciones en el Manual que no son desempeñadas por los funcionarios del Departamento de Seguridad de la Información, así como también realizan funciones que no están incluidas en el mismo.

El Manual de Organización, Funciones y Cargos de la Dirección General de Informática y Comunicaciones en vigencia, indica como objetivo del Departamento de Seguridad de la información "*salvaguardar la confidencialidad, integridad y disponibilidad de los datos, sistemas de información, servicios y documentación bajo responsabilidad de la DGIC".*

El Jefe de Departamento de Seguridad de la Información manifestó, que las funciones del Departamento no están formalizadas para que el área realice funciones específicas de seguridad, debido a que el Manual de Funciones del Departamento lo considera como área normativa.

CONCLUSIÓN

La ausencia de controles adecuados de seguridad provoca riesgos para la confidencialidad, integridad y disponibilidad de la información y demás activos de la institución.

RECOMENDACIÓN

Adecuar el Manual de Organización, Funciones y Cargos del Departamento de Seguridad de la Información a las exigencias de seguridad de la institución, de forma a que se cumpla con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de los datos, sistemas, servicios y documentación bajo responsabilidad de la DGIC.

CAPITULO II

SEGUIMIENTO A LAS RECOMENDACIONES

RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 261/13	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**
Falta de procedimientos para mantener actualizado el diccionario de datos y las reglas de sintaxis. Recomendación Arbitrar medidas para la elaboración de procedimientos de actualización del diccionario de datos.	Fue remitido por la DGIC el "Procedimiento del Ciclo de Vida de Sistemas- Control de Cambios", en el mismo se detalla la actividad de actualización de documentación de Sistemas con relación al Diagrama Entidad Relación (DER) y el Lenguaje de Definición de Datos (DDL).	En proceso	En el plan de mejoramiento presentado a la CGR, se asigna el primer trimestre de 2014 como plazo para el cumplimiento de la recomendación. Dicho cumplimiento se verificará en auditorias posteriores.
Los cambios realizados en los sistemas no se reflejan inmediatamente en el diccionario de datos ni en las reglas de sintaxis. Recomendación a) 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. b) Fomentar el uso estandarizado del diccionario de datos entre los diferentes usuarios del Área de Desarrollo de Sistemas.	El procedimiento de ciclo de vida de sistemas y control de cambios, indica la actualización de la documentación al producirse una modificación en los sistemas. La puesta en producción de dicho procedimiento se daría en el primer trimestre del 2014.	En proceso	La Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditorías posteriores.
No se cuenta con un esquema de clasificación de datos ni con niveles de seguridad para los datos almacenados en los sistemas. 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.	En el plan de mejoras presentado se verifica el periodo de ejecución diciembre de 2014 para *"Realizar un mapeo de la información generada por el SIAF y establecer la clasificación de las direcciones rectoras".*	Pendiente	La Institución no se adecuó a la recomendación.
SEGUIMIENTO DE LAS RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y			

COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 261/13	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**
No posee un listado definido de usuarios de red ni propietarios de datos y sistemas. 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.	La Institución manifiesta que "se ha migrado la plataforma de usuarios de dominio a una nueva infraestructura la cual permite la identificación y administración de los usuarios del dominio de la SSEAF. (se adjunta el listado de usuarios de dominio de la SSEAF activos a la fecha. Resumen de cuenta de servicios). Propietario de Sistemas y Datos: acorde a la Ley 1535/99 y su decreto reglamentario las Direcciones de la SSEAF son las rectoras de los sistemas del SIARE (se adjunta las Políticas de Seguridad de la Información de la SSEAF aprobada por Res. 210/12	Superada	La Institución dio cumplimiento a la recomendación.
No se cuenta con políticas de acceso a la información a nivel interno. Implementar políticas de acceso a la información con reglas claras de administración, que permitan minimizar inconvenientes que puedan afectar al sistema.	La Institución expone como acción de mejoramiento: "Implementación gradual del Manual de administración de cuentas de usuarios finales en la sección 7.4 Movimiento del personal que contempla los ingresos, retiro, traslados y ausencias programadas".	En proceso	La completa implementación del Manual de Administración de Cuentas de Usuarios finales será verificado en auditorías posteriores.
No se tiene identificado al personal clave. Definir e identificar al personal clave, a fin de reducir el riesgo de dependencia de un solo personal que desempeña una función de trabajo crítica. Asignar personal de respaldo para dichos puestos, de tal manera que se eviten inconvenientes en caso de ausencia o retiro de los mismos. Insistir con el pedido de personal de tal forma a mitigar estos inconvenientes	La Institución remitió la Resolución DGIC Nº 37/2013 en la cual se constituye el Comité Técnico y el Personal clave de la Adm. De recursos críticos de TI. No se cuenta aún con personal suficiente que sirva de respaldo para los puestos claves.	En proceso	Su cumplimiento será verificado en auditoría posterior.
No se realizan revisiones sobre las pistas de auditoría. 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.	La Institución remite como acción de mejoramiento: "Prever mecanismos de control interno en forma permanente sobre las pistas de auditoría. Implementar una herramienta para centralizar los registros de auditoría de base de datos. Asignar al Dpto. de Seguridad la gestión de los registros de auditoría".	Pendiente	La Institución no se adecuó aún a la recomendación.

SEGUIMIENTO DE LAS RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 261/13	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**

Los privilegios otorgados para el acceso a los sistemas no están acordes con el Manual de Organización, Funciones y Cargos. 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.	La Institución prevé como acción de mejoramiento: "Establecer un mecanismo para otorgar participación al Departamento de Seguridad en la gestión de usuario en la DGIC".	Pendiente	La Institución no se adecuó aún a la recomendación.
La documentación de los sistemas no está actualizada. 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.	La Institución emite como acción de mejoramiento: "Incorporar la tarea de actualización de documentación referente a los DER, en el procedimiento ciclo de vida de sistemas- control de cambios por cada FMA". La Institución remitió el procedimiento Ciclo de Vida de Sistemas y Control de Cambios se prevé como actividad "Actualizar las documentaciones con relación al Diagrama Entidad Relación (DER) y el Lenguaje de Definición de Datos (DDL)".	En proceso	Su cumplimiento será verificado en auditoría posterior.
Personal insuficiente para cumplir funciones primordiales. Dotar a la DGIC del personal necesario que garantice la disponibilidad, integridad y confiabilidad del sistema.	Se tuvo evidencia del pedido de contratación de personal realizado por la Institución.	Pendiente	La Institución no se adecuó a la recomendación

SEGUIMIENTO DE LAS RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 186/12	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**
No se cuenta con una adecuada segregación de funciones.	La Institución remitió la matriz de responsabilidades de	En proceso	Su cumplimiento será verificado en auditoría

Evaluar requerimiento de personal De forma regular, cuando existan cambios en la institución o se asignen proyectos, de tal manera a garantizar que la institución cuente con los recursos para cumplir adecuada y apropiadamente con las metas y los objetivos dispuestos.	personal de la DGIC, aprobado por Resolución MH Nº009/14, del 3 de marzo de 2014; la Resolución DGIC-MH Nº 011/13 de fecha 13 de febrero de 2013 en el cual se asigna la custodia de cuentas de administración al Dpto. de Seguridad de la Información; se remitió además el Manual de administración de cuentas de usuarios finales, aprobado por resolución DGIC_SSEAFG Nº035/13.		posterior.
Grave carencia de personal para el manejo de los sistemas administrados por la DGIC. Incorporar en el menor tiempo posible, la cantidad necesaria de personal capacitado para llevar adelante la Administración de los Sistemas Informáticos y los proyectos comprometidos a la Dirección, de manera a precautelar la integridad y continuidad de los sistemas.	La Institución remitió evidencia de la gestión realizada para la contratación de personal, no se tuvo evidencia del cumplimiento.	En proceso	Su cumplimiento será verificado en auditorías posteriores.
No se prevé el nombramiento o contratación de personal capacitado para el manejo de los nuevos sistemas creados a través de proyectos. Recomendar la evaluación de requerimientos de personal para cada proyecto, de manera que se solucionen los inconvenientes que devienen de dicha situación, de manera a garantizar que la institución cuente con los recursos para cumplir adecuada y apropiadamente las metas y los objetivos dispuestos.	La Institución remitió evidencia de la gestión de personal realizada, no se tuvo evidencia del cumplimiento de lo observado.	En proceso	La Institución se encuentra en proceso de cumplimiento de la recomendación.

SEGUIMIENTO DE LAS RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 186/12	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**
No se tiene establecido el tiempo aproximado para el cumplimiento de las solicitudes, el tiempo promedio de atención y posterior ejecución es de 28 días.	La Institución remitió el *"Procedimiento Ciclo de Vida de sistemas- Control de cambios"* y la Resolución SSEAF N° 24/2014 por la cual se aprueba,	Superada	La Institución se adecuó a la recomendación.

Impulsar los mecanismos necesarios de manera a obtener una rápida gestión con respecto a los plazos establecidos para el cumplimiento de las solicitudes de modificación de datos y aplicaciones.	en el manual se detalla la estimación de tiempo de desarrollo y las prioridades.		
Incluir a todas las entidades que no se encuentran conectadas en línea, al Sistema Integrado de Administración Financiera (SIAF).	Se encuentra en proceso de desarrollo el Sistema de Distribución de Ingresos a ser implementado por las municipalidades.	En proceso	Su cumplimiento será verificado en auditorias posteriores
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 Dirección General de Informática y Comunicaciones. Solicitar a las instancias administrativas agilizar los trámites de confirmación de los cargos gerenciales y aceptación de comisionamientos en tiempo y forma.	Se tuvo evidencia que los trámites administrativos de cargos superiores fueron realizados en tiempo.	Superada	La Institución se adecuó a la recomendación.
El jefe de Departamento de Atención al Usuario Interina desde el 22/10/08 a la fecha. Confirmar en el puesto o nombrar un jefe del departamento de Atención al Usuario, de tal forma que se puedan tomar las decisiones y corregir las deficiencias del área.	La Institución remitió la Resolución MH 012/14, en la cual se confirma en el cargo al Jefe de Atención al Usuario.	Superada	La Institución se adecuó a la recomendación.
Manual de Procedimientos para la gestión de proyectos sin aprobarse. Iniciar los trámites necesarios para elaborar el correspondiente manual de procedimiento, su posterior seguimiento, aprobación y puesta en práctica.	La Institución remitió copia del Manual de Gestión de Proyectos aprobado por Resolución DGIC Nº 063/12 y del Procedimiento de "Gestión de Proyectos", de implementación gradual, aprobado por Resolución DGIC Nº 03/13.	Superada	La Institución se adecuó a la recomendación.

SEGUIMIENTO DE LAS RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 023/11	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**
No se encuentran separadas las funciones que desempeñan los funcionarios en el departamento Separar funciones dentro de cada una de las áreas del Departamento de Sistemas para asegurar un mayor control. Implementar controles	Se implementó el Mecanismo de Revisión por pares Circular DSI Nº 02/2013. No se tuvo evidencia de la separación de funciones.	Pendiente	No se tuvo evidencia del cumplimiento de la recomendación.

compensatorios hasta tanto la observación sea subsanada, considerando el monitoreo de las actividades y supervisión de los administradores.			
No se realizan monitoreos preventivos de los sistemas. Incluir en el plan anual de monitoreo, el monitoreo preventivo de los sistemas, de manera a reducir riesgos que eventualmente puedan producirse	Sin avances al respecto.	Pendiente	No se recibió evidencia del cumplimiento de la recomendación. La recomendación sigue pendiente de cumplimiento.
No se cuenta con documentación actualizada relativa a los programas de aplicación. Proceder a actualizar la documentación de los sistemas y programas de aplicación de tal manera que sirva como instrumento de apoyo y guía para cuando sea necesario. Mantener actualizada dicha documentación a medida se desarrollen los cambios.	La Institución remitió el procedimiento "Ciclo de Vida de Sistemas- Control de Cambios" en el cual se detalla las tareas de actualización de documentación de sistemas. Resolución SSEAF Nro. 24/2014.	En proceso	Su cumplimiento será verificado en auditoría posterior.
Administración de riesgos. Elaborar y aprobar un Plan de Contingencias que incluya guías para su utilización, procedimientos para los distintos casos, definición de los encargados de ejecutar los procedimientos.	La DGIC cuenta con una política de marco de trabajo de continuidad de TI aprobada en el 2013. Se ha iniciado un proyecto a fin de contratar un servicio de contingencia con un proveedor externo.	En proceso	En la evidencia remitida se observa que la Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en revisiones posteriores.

SEGUIMIENTO DE LAS RECOMENDACIONES FORMULADAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA RESULTANTES DEL EXAMEN ESPECIAL A LA DIRECCIÓN GENERAL DE INFORMÁTICA Y COMUNICACIONES DEL MINISTERIO DE HACIENDA, EN CUMPLIMIENTO DE LA RESOLUCIÓN CGR N° 261/13			
RECOMENDACIONES DE LA CGR EXAMEN ESPECIAL RESOLUCIÓN 311/06	**MEDIDAS ADOPTADAS POR LA DGIC**	**SITUACIÓN ACTUAL**	**COMENTARIO DE LA CGR**
Seguridad Física. Adecuar a las Ordenanzas Municipales aplicables a la seguridad física del edificio, en el menor tiempo posible, y contar con salidas de emergencia, atendiendo siempre de no debilitar la seguridad de acceso a las áreas críticas de la Dirección. Se deberán implementar, periódicamente los planes de	La Institución remitió evidencia de los trabajos que se vienen realizando para el cumplimiento de la recomendación. No se tuvo evidencia del cumplimiento total del mismo.	En proceso	Por la documentación recibida se evidencia que la Institución se encuentra en proceso de cumplimiento de la recomendación. Su cumplimiento será verificado en auditorias posteriores.

contingencia.			
Proyecto de reingeniería del SIAF. Culminar en tiempo y forma la reingeniería Sistema Integrado de Administración Financiera (SIAF).	La Institución remitió evidencia de los trabajos que se vienen realizando para el cumplimiento de la recomendación. *-Dic/2013: TORs revisados por un consultor externo contratado por el BID.* *-Ene/2014: Determinación y priorización de actividades en el POA del Proyecto PROFOMAF II. Ref.: SIME Nº 4476/14.* *- Marzo/2014: Definición de la arquitectura para nuevos sistemas (revisado).* *- Marzo/2014: elaboración y revisión de TORs por la DGIC y las Direcciones de la SSEAF.*	En proceso	Su cumplimiento será verificado en Auditorías posteriores.

CONCLUSIÓN

De un total de 24 recomendaciones realizadas por la Contraloría General de la República en Informes Finales de Exámenes Especiales practicados en ejercicios fiscales 2006 al 2012, 5 fueron cumplidas, que representa el 20.83 % del total; 6 no fueron cumplidas, que corresponden también al 24 % del total y, 13 se encuentra en proceso de cumplimiento, es decir, 54.16 % del total. La Institución se encuentra en un lento proceso de cumplimiento a las acciones correctivas.

Están en proceso puntos importantes que pueden eventualmente constituir riesgo relevante en cuanto a la confiabilidad, integridad y disponibilidad de la información de los sistemas. Entre los puntos principales están: la reingeniería del Sistema Integrado de Administración Financiera, la contratación de personal para mejorar la gestión y lograr la segregación de funciones.

En consideración a las pruebas obtenidas se puede señalar que, durante el ejercicio fiscal 2013, se evidenciaron riesgos en cuanto a la confiabilidad, integridad de la información administrada en el Sistema Integrado de Administración Financiera.

RECOMENDACIÓN

La Dirección General de Informática y Comunicaciones deberá continuar arbitrando 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).

CAPITULO III

CONCLUSIONES Y RECOMENDACIONES FINALES

1. CONTROL INTERNO IMPLEMENTADO POR EL DEPARTAMENTO DE SEGURIDAD DE LA INFORMACIÓN.

1.1. No son gestionados los riesgos en todos los proyectos y procesos

CONCLUSIÓN

El hecho de no realizar la gestión de riesgos en todos los proyectos y procesos, dificulta la identificación de los elementos relacionados con el riesgo, aumenta las vulnerabilidades y, además, no pueden ser establecidas acciones de mitigación y prevención.

RECOMENDACIÓN

Elaborar procedimientos adecuados de manera a incluir al Departamento de Seguridad de la Información en todos los proyectos y procesos que afecten la actividad de la Dirección de forma que se realice una adecuada gestión de riesgos y reducir los efectos negativos que podrían ocasionar los mismos a las actividades de la DGIC.

1.2. No se evalúa el nivel de riesgo de seguridad de información de proveedores que procesen información restringida y confidencial.

CONCLUSIÓN

Al no realizar la gestión de riesgos en la incorporación de proveedores que manejan información restringida o confidencial, no pueden ser identificados todos los riesgos relacionados con la seguridad de la información, aumentan las vulnerabilidades y se dificulta el establecimiento de acciones de mitigación y prevención.

RECOMENDACIÓN

Elaborar procedimientos de manera a incluir al Departamento de Seguridad de la Información en los procesos que incluyan la incorporación de proveedores que manejan información sensible y confidencial de forma a salvaguardar la confidencialidad, integridad y disponibilidad de la información administrada por la institución.

1.3. No son evaluados los riesgos de modo continuo respecto a la seguridad de la información.

CONCLUSIÓN

La falta de una evaluación de riesgos de modo continuo dificulta la identificación oportuna de amenazas que podrían impedir el cumplimiento de los objetivos de la Institución.

RECOMENDACIÓN

Elaborar políticas y procedimientos de manera a dar participación al Departamento de Seguridad de la Información en procesos de tecnologías implantadas, de forma a lograr una mejora continua de gestión de riesgos para identificar oportunamente las amenazas y dar cumplimiento a los objetivos de la institución.

1.4. Las políticas de seguridad incluyen procesos generales pero sin definir procedimientos específicos para cada proceso incluido en las mismas.

CONCLUSIÓN

El hecho de no institucionalizar las buenas prácticas en la administración de tecnologías de la información hace que el logro de los objetivos institucionales se vea dificultado, corriendo riesgos, tanto sobre la información administrada, como sobre los equipamientos, situación que podría, ante eventualidades, afectar a los activos de la institución.

RECOMENDACIÓN

Utilizar como base las Políticas de Seguridad de la Información e implementar políticas, procedimientos, normas y reglamentaciones complementarias para controlar la estandarización, la calidad de las operaciones, y evitar desviaciones en el logro de los objetivos y de las metas propuestas. Formalizar las documentaciones y socializar con las áreas competentes.

1.5. No son registrados todos los incidentes de seguridad en el Sistema de Gestión de Seguridad de la Información

CONCLUSIÓN

Al no llevar un registro detallado de todos los incidentes de seguridad, no se puede evitar que el mismo evento vuelva a ocurrir. Tampoco se cuenta con el histórico completo de todos los incidentes y las soluciones propuestas, de forma que se pueda resolver el problema con mayor eficiencia y rapidez.

RECOMENDACIÓN

Velar por el cumplimiento del "Procedimiento de Gestión de Incidentes" aprobado en la Resolución DGIC–SSEAF N° 022/10 y crear conciencia sobre la importancia del mismo y de la utilidad del registro de los incidentes de seguridad producidos de manera que ese registro sirva de herramienta de apoyo al control de la seguridad de la información.

1.6 El control de la aplicación de las normativas de acceso físico a las áreas de la DGIC no es ejercido por el Departamento de Seguridad de la Información

CONCLUSIÓN

La falta de control sobre la aplicación de las políticas, normativas y procedimientos relativos a: acceso físico a las áreas y a los recursos de tecnologías de información, produce brechas de seguridad que pueden afectar a los activos y a la información que se administra, y producir serios daños a la Institución

RECOMENDACIÓN

Realizar un control periódico de la aplicación de las normas y reglamentos establecidos para el control de acceso físico de la Institución y evitar perjuicio que se puede producir por esta falencia.

1.7 El Manual de Organización, Funciones y Cargos asigna al Departamento de Seguridad de la Información una función normativa

CONCLUSIÓN

La ausencia de controles adecuados de seguridad provoca riesgos para la confidencialidad, integridad y disponibilidad de la información y demás activos de la institución.

RECOMENDACIÓN

Adecuar el Manual de Organización, Funciones y Cargos del Departamento de Seguridad de la Información a las exigencias de seguridad de la institución, de forma a que se cumpla con el objetivo de salvaguardar la confidencialidad, integridad y disponibilidad de los datos, sistemas, servicios y documentación bajo responsabilidad de la DGIC.

1.8 Seguimiento a las recomendaciones

CONCLUSIÓN

De un total de 24 recomendaciones realizadas por la Contraloría General de la República en Informes Finales de Exámenes Especiales practicados en ejercicios fiscales 2006 al 2012, 5 fueron cumplidas, que representa el 20.83 % del total; 6 no fueron cumplidas, que corresponden también al 24 % del total y, 13 se encuentra en proceso de cumplimiento, es decir, 54.16 % del total. La Institución se encuentra en un lento proceso de cumplimiento a las acciones correctivas.

Están en proceso puntos importantes que pueden eventualmente constituir riesgo relevante en cuanto a la confiabilidad, integridad y disponibilidad de la información de los sistemas. Entre los puntos principales están: la reingeniería del Sistema Integrado de Administración Financiera, la contratación de personal para mejorar la gestión y lograr la segregación de funciones.

En consideración a las pruebas obtenidas se puede señalar que, durante el ejercicio fiscal 2013, se evidenciaron riesgos en cuanto a la confiabilidad, integridad de la información administrada en el Sistema Integrado de Administración Financiera.

RECOMENDACIÓN

La Dirección General de Informática y Comunicaciones deberá continuar arbitrando 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).

Es nuestro informe.

Asunción, de agosto de 2014.

Econ. Carlos Ramírez
Auditor

Ing. José Arzamendia
Auditor

Ing. Mabel Arriola
Jefa de Equipo

Lic. Teresa Torres
Supervisora
Directora de Área

Lic. Yassir Admén R.
Director
Dirección Asesoría Técnica

Lic. Gladys Fernández
Directora General
Dirección General de Economía

Asunción, 07 AGO. 2014

Nota CGR Nº 06849

Ref.: Informe Final – Resolución CGR Nº 125/14.

SEÑOR MINISTRO:

Tengo el agrado de dirigirme a Su Excelencia con el objeto de poner a su conocimiento el Informe Final resultante de los trabajos dispuestos por Resolución CGR Nº 125/14 Examen Especial a la Dirección General de Informática y Comunicaciones, dependiente de la Subsecretaría de Administración Financiera del Ministerio de Hacienda, correspondiente al ejercicio fiscal 2013.

La evaluación emitida en el presente informe es el resultado del análisis de los documentos proveídos a los auditores para su estudio, los cuales constituyen exclusiva responsabilidad de los funcionarios de la institución auditada.

La institución deberá implementar las medidas necesarias a fin de regularizar totalmente las situaciones observadas, para lo cual tendrá que elaborar y poner en marcha un Plan o Programa de Mejoramiento, el que deberá ser presentado a la Contraloría General de la República en versión magnética e impresa en un plazo no mayor a 30 (treinta) días, a partir de la recepción del informe, de acuerdo al modelo expuesto en el sitio web de la Contraloría, www.contraloria.gov.py/formularios/. La evaluación del mismo se realizará cuando este Organismo Superior de Control así lo crea conveniente.

Al respecto, este Organismo Superior de Control señala que el ente auditado es el responsable de informar de la recepción del Informe Final a las personas afectadas de la administración anterior.

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

CONTRALORÍA GENERAL DE LA REPÚBLICA

CONTRALORÍA GENERAL DE LA REPÚBLICA

ALFREDO DAVID BARÚA M.
Secretario General

OSCAR RUBÉN VELÁZQUEZ GADEA
Contralor General
de la República

A SU EXCELENCIA
GERMAN HUGO ROJAS IRIGOYEN, MINISTRO
MINISTERIO DE HACIENDA

MINISTERIO DE HACIENDA
61175/2014

ORVG/O/epa