AUD. 024-2011

INFORME DE LOS RESULTADOS OBTENIDOS EN EL ESTUDIO SOBRE LA EVALUACIÓN DE LA GESTIÓN DE RIESGOS DEL ÁREA DE TECNOLOGÍAS DE INFORMACIÓN

1. INTRODUCCIÓN

1.1. Origen del Estudio.

El estudio al que se refiere el presente informe, se llevó a cabo de conformidad con el Plan de Trabajo de la Auditoría Interna para el año 2010.

1.2. Objetivo General.

El objetivo general del estudio, consistió en evaluar la gestión de riesgos relacionados con las Tecnologías de Información y la suficiencia, validez y pertinencia del Control Interno en operación.

1.3. Alcance y Periodo de Estudio.

El estudio consistió en valorar la última evaluación de riesgos realizada por el Área de Tecnologías de Información y el último plan de implantación de medidas de tratamiento de riesgos, los cuales corresponden a los ejecutados en el 2009 y abarcó el periodo del 1 de enero del 2009 al 08 de noviembre del 2010, extendiéndose en los siguientes casos:
-En lo referente a la administración continua de riesgos de TI[1] se revisó el inventario de riesgos y planes de implementación de Tecnologías de Información realizado en el año 2005.
-En relación con el seguimiento a los planes de acción para la administración del riesgo de Tecnologías de Información hasta el 27 de julio del 2011 (hallazgo 2.3.1).

Adicionalmente, se dio seguimiento a las acciones emprendidas por la Gerencia General, Subgerencia Administrativa Financiera y Tecnologías de Información para ejecutar lo dispuesto en el informe de Auditoría AUD 012-2009, sobre los resultados obtenidos en el estudio de la Gestión de Riesgos del Área de Desarrollo Informático del IMAS de los años 2005 y 2007. El período del seguimiento efectuado abarcó acciones realizadas desde marzo del 2009 al 20 de octubre del 2010.

Para la realización del estudio, se consideraron las disposiciones del Manual de Normas Generales de Auditoría para el Sector Público (M-2-2006-CO-DFOE), el Manual de procedimientos de la Auditoría Interna, así como la demás normativa de Auditoría Interna de aceptación general.

[1] Unidad de Tecnologías de Información del IMAS.

1.4. Comunicación verbal de los resultados

En reunión celebrada el día 25 de noviembre del 2011, se comunicaron los resultados del presente informe a la MSc. Mayra Díaz Méndez, Gerente General, a la Lic. Guadalupe Sandoval Sandoval, Coordinadora de Control Interno, y al Lic. Luis Adolfo González Alguera, Coordinador de Tecnologías de Información, en la cual se efectuaron observaciones que en lo pertinente, una vez valoradas por esta Auditoría Interna, fueron incorporadas en el presente informe.

2. RESULTADOS

2.1. Sobre el seguimiento a las recomendaciones del informe AUD 012-2009

2.1.1. Grado de cumplimiento de las recomendaciones

De conformidad con la revisión efectuada, se determinó que de las 11 recomendaciones evaluadas; nueve se encuentran cumplidas y dos parcialmente implementadas (**Anexo Nº1)**, según se detalla en el siguiente cuadro:

Cuadro N º 1
Grado de cumplimiento de las recomendaciones

RESPONSABLE	TOTAL REC.	NIVEL DE CUMPLIMIENTO			
		CUMPLIDAS	%	PARCIALES	%
AUD 012-2009					
Gerencia General	3	4.1 4.2[2] 4.3	100%	0	0%
Subgerencia Administrativa Financiera	3	4.5 4.6	67%	4.4	33%
Tecnologías de Información	5	4.8 4.9 4.10 4.11	80%	4.7	20%
Efectividad de cumplimiento1[3]	**11**	**9**	**82%**	**2**	**18%**

En el siguiente gráfico se resume el grado de cumplimiento de las recomendaciones detalladas en el cuadro anterior:

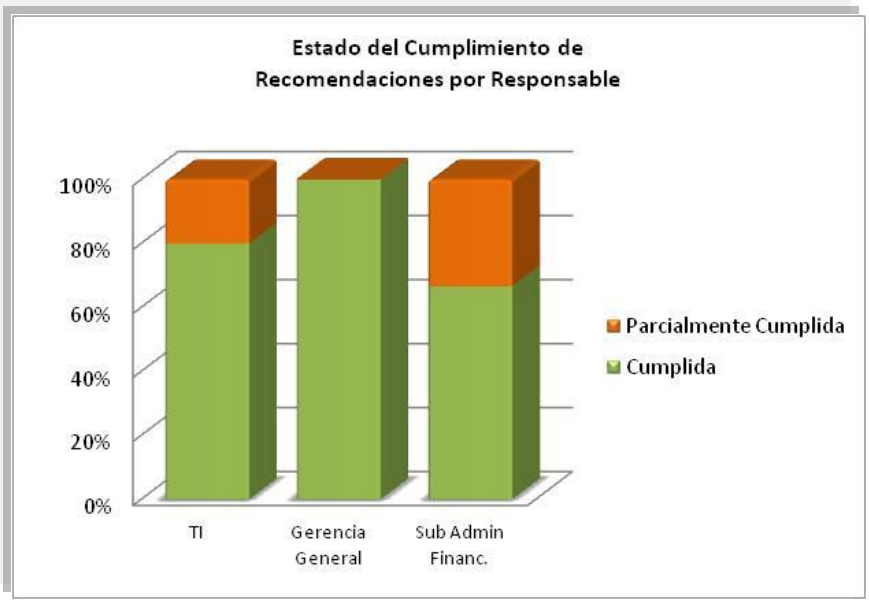
[2] De acuerdo con información brindada por la Lic. Guadalupe Sandoval Sandoval, Coordinadora de Control Interno y verificación realizada por la Auditoría Interna al 30 de noviembre del 2011, se determinó en relación con la recomendación 4.2 que durante el 2011 se ha realizado el seguimiento a los planes de administración de riesgos de Tecnologías de Información.

[3] La fórmula de este indicador de gestión se calcula dividiendo el número de recomendaciones "cumplidas", "parcialmente cumplidas" o "no cumplidas" entre la totalidad de recomendaciones evaluadas.

Gráfico N º 1
Grado de cumplimiento de las recomendaciones

Tal y como se observa en el gráfico siguiente, la Gerencia General ha implementado la totalidad de las recomendaciones, la Subgerencia Administrativa Financiera ha implementado el 67% de las recomendaciones y el 33% se encuentran parcialmente cumplidas. En el caso de Tecnologías de Información, el grado de cumplimiento es del 80% y el 20% está parcialmente cumplidas.

Gráfico #2. Estado de Cumplimiento de las Recomendaciones por Dependencia Responsable de Implementarlas



2.2. Sobre la validez de los resultados del proceso de identificación y valoración de riesgos del área de Tecnologías de Información.

2.2.1. Definición, identificación, evaluación y actualización de riesgos.

Si bien se ha realizado de manera coordinada entre la Unidad de Control Interno y Tecnologías de Información las siguientes fases:

- Fase 1. Identificación de riesgos (causa, evento consecuencia).
- Fase 2. Análisis (evaluación riesgo absoluto e identificación de controles, factores de riesgo).
- Fase 3. Evaluación de controles y priorización de riesgo
- Fase 4. Administración (Selección u análisis medidas)

Se determinó en relación con el proceso de identificación, análisis y evaluación de riesgos y controles las siguientes inconsistencias:

- Existen eventos documentados que corresponden a debilidades de control y no son riesgos. Un ejemplo de la situación anterior se muestra en la siguiente tabla:

Riesgo	Causa	Evento	Consecuencia
Riesgo vigente	Falta de planificación en la adquisición de software Descontrol en cuanto al vencimiento de licencias de software	La falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones	Bajo rendimiento de aplicaciones y sistemas Inconsistencia de operaciones en los sistemas y en la plataforma de TI.
Recomendación	Falta de planificación en la adquisición o actualización de software, falta de procedimientos formales, etc.	Ataque de virus	Pérdida de información, daños en el sistema, bajo rendimiento de aplicaciones y sistemas, etc.

- La Administración no tiene claro el significado del riesgo definido como “Niveles de seguridad de datos inconsistentes”.

- Se evidenció la existencia de riesgos repetitivos, a continuación y a manera de ejemplo, se indica un caso detectado:

Riesgo 1. "Proyectos a desarrollar por TI no son administrados adecuadamente para la maximización de los recursos y tiempos aceptables de desarrollo así como sean administración inadecuadamente."
Riesgo 2. "Proyectos administrados inadecuadamente"

- Se documentan en los formularios una serie de controles generales, sin que se especifique los mecanismos que operacionalizan el control. Esta situación dificulta la tarea de definir medidas concretas para administrar el riesgo.

- Se determinó la existencia de controles que no han sido evaluados, los cuales corresponden a los siguientes riesgos:
  - Deficiencias en los manuales de usuarios, operaciones y entrenamiento
  - Debilidades organizacionales para desarrollar y correr las aplicaciones requeridas.
  - Bitácoras o reportes de problemas que confirmen que los problemas ocurridos durante el procesamiento de información fueron considerados oportunamente y que se llevaron a cabo las acciones correctivas apropiadas.

  Esta situación no permite determinar si el riesgo está siendo administrado en forma adecuada y si los controles establecidos logran el objetivo de minimizar el riesgo.

- Adicionalmente, se determinó que la Unidad de Control Interno a la fecha de revisión no ha definido y comunicado formalmente lineamientos que indiquen como proceder para actualizar el mapa de riesgos ante la presencia de nuevos riesgos no considerados en la fase de identificación de riesgos y causados por cambios en el entorno que afectan la operación regular de Tecnologías de Información.

Con relación a lo comentado en los puntos anteriores, las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) D-3-2005-CO-DFOE emitido por la Contraloría General de la República, en lo de interés señalan lo siguiente:

- Apartado *4-Funcionamiento del Sistema Específico de Valoración del Riesgo Institucional:*

  4.2. Identificación de riesgos: "Se deberá identificar por áreas, sectores, actividades o tareas, de conformidad con las particularidades de la institución, lo siguiente:

a) Los eventos[4] que podrían afectar de forma significativa el cumplimiento de los objetivos institucionales. (…)
b) Las posibles causas, internas y externas, de los eventos identificados y las posibles consecuencias de la ocurrencia de dichos eventos sobre el cumplimiento de los objetivos.
c) Las formas de ocurrencia de dichos eventos y el momento y lugar en el que podrían incurrir. (…)"
4.3. Análisis de riesgos. **"**Para los eventos identificados se deberá determinar:
a) su posibilidad de ocurrencia,
b) la magnitud de su eventual consecuencia,
c) su nivel de riesgo,
d) sus factores de riesgo, y
e) las medidas para su administración.
El análisis de la consecuencia de los eventos identificados deberá considerar los posibles efectos negativos y positivos de dichos eventos.
El nivel de riesgo deberá obtenerse bajo dos escenarios básicos: sin medidas para la administración de riesgos y con aquellas existentes en la institución. El análisis que se realice puede ser cuantitativo, cualitativo o una combinación de ambos. (…)"

- Apartado *3.3-Ambiente de Apoyo:* "En cada institución deberá existir una estructura organizacional que apoye la operación del SEVRI, así como promoverse una cultura favorable al efecto. Para lo anterior, se deberá promover al menos: (…) b) Uniformidad en el concepto de riesgo en los funcionarios de la institución"

- Apartado *2.7-Responsabilidades del SEVRI*: "El jerarca y los respectivos titulares subordinados de la institución son los responsables del establecimiento y funcionamiento del SEVRI. Para lo anterior deberán: (…) e) Tomar las medidas necesarias tendientes a fortalecer y perfeccionar el Sistema y al cumplimiento de la presente normativa"

- Apartado *2.6- Características del SEVRI*: "El SEVRI que se establezca en cada institución deberá reunir características como las siguientes: (…) Flexibilidad: El Sistema se deberá diseñar, implementar y ajustar periódicamente a los cambios externos e internos de acuerdo con las posibilidades y características de cada institución.

[4] En las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) D-3-2005-CO-DFOE se define el término ***Evento*** como el incidente o situación que podría ocurrir en un lugar específico en un intervalo de tiempo particular.

- Apartado *2.4-Productos del SEVRI*: "El SEVRI deberá constituirse en un instrumento que apoye de forma continua los procesos institucionales. En este sentido, se deberá generar a través del SEVRI: a) Información actualizada sobre los riesgos institucionales relevantes asociados al logro de los objetivos y metas, definidos tanto en los planes anuales operativos, de mediano y de largo plazos, y el comportamiento del nivel de riesgo institucional". (Los subrayados no corresponden al original)

La situación comentada, es típica de un proceso de gestión de riesgos incipiente que va madurando conforme los ciclos de identificación, valoración y respuesta al riesgo, donde en cada iteración del proceso se refinan los resultados producto de la capacitación y comprensión de los conceptos asociados con la gestión de riesgo. No obstante, es importante atender y mejorar los aspectos evidenciados en el estudio, para evitar que se inviertan recursos en la atención de situaciones que no son las principales generadoras de riesgo en tecnologías de información, dejando descubiertas causas que si pueden ocasionar efectos catastróficos en la gestión institucional.

2.2.2. Gestión de Riesgos con medidas de administración "Externas"

No existen lineamientos formalmente definidos en el Marco Orientador del SEVRI para la gestión integral de riesgos con medidas de administración externas. Para el caso concreto de la Unidad de Tecnologías de información, el riesgo "Cobertura de seguros inadecuada" avalado por la Unidad de Control Interno y Tecnologías de Información, como parte del inventario de riesgos de Tecnologías de Información gestionado en el 2009, no se definieron medidas de administración por cuanto se consideró como riesgo externo.

Según indicó el Coordinador Luis Adolfo González, en relación con dicho riesgo "no tenemos competencia administrativa para poderlo administrar", por lo que señala a Proveeduría y Contabilidad como responsables de su implementación. Adicionalmente, la Coordinadora de Control Interno, indica que dicho riesgo tampoco es considerado en el inventario de riesgos de Proveeduría y Contabilidad. Dada esta condición, el riesgo permanece invariable sin que se implementen medidas de tratamiento del mismo.

Las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) D-3-2005-CO-DFOE emitido por la Contraloría General de la República, al respecto señalan en la sección *2.6 Características del SEVRI* lo siguiente: "El SEVRI que se establezca en cada institución deberá reunir características como las siguientes: (…) Integración: El Sistema se articula con el resto de los sistemas institucionales y apoya la toma de decisiones cotidiana en todos los niveles organizacionales." (El subrayado no consta en el original)

Así mismo, el Manual de Normas de Control Interno para el Sector Público, en su apartado *3.2 Sistema específico de valoración del riesgo institucional (SEVRI)*, en lo de interés señala: "El jerarca y los titulares subordinados, según sus competencias, deben establecer y poner en funcionamiento un sistema específico de valoración del riesgo institucional (SEVRI). El SEVRI debe presentar las características e incluir los componentes y las actividades que define la normativa específica aplicable[5]. Asimismo, debe someterse a las verificaciones y revisiones que correspondan a fin de corroborar su efectividad continua y promover su perfeccionamiento." (El subrayado no consta en el original)

De conformidad con lo expuesto, se mantiene la probabilidad de materialización de los riesgos considerados "externos" a la Unidad que los identifica y valora, al no establecer medidas concretas para su administración.

2.3. Sobre el cumplimiento de los planes de acción elaborados por las unidades administrativas como resultado del proceso de autoevaluación institucional del área de Tecnologías de Información

2.3.1. Seguimiento a los planes de acción para la administración del riesgo de Tecnologías de Información

De conformidad con las pruebas realizadas, se determinó que no se realiza un seguimiento periódico y una gestión continua y sistemática, para verificar el nivel de implementación y efectividad de las medidas de administración de Tecnologías de Información. Al respecto se evidenció lo siguiente:

Año 2009

a) En julio del 2009, Tecnologías de Información identifica sus riesgos y controles (AAI-092-2009) y control interno procede a realizar la revisión respectiva.
b) En octubre del 2009, Control interno envía a TI el informe de resultados de autoevaluación 2009, el informe de análisis y evaluación de riesgos 2009 y la matriz para que elaboren del plan de trabajo de las medidas de administración de riesgos.
c) En noviembre del 2009 TI remite a Control Interno el Plan de Administración del riesgo.

[5] "Directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)" (D-3-2005-CO-DFOE), aprobadas mediante resolución R-CO-64-2005 del 1º de julio de 2005, y publicadas en el Diario Oficial "La Gaceta" Nº 134 del 12 de julio de 2005.

Año 2010

d) En febrero del 2010, se inicia el proceso para la aprobación del "Informe de gestión de Riesgos 2009".
e) En correo electrónico de Junio del 2010, la Unidad de Control Interno informa a Tecnologías de Información acerca de su responsabilidad para comunicar y dar atención a los riesgos mediante las medidas de administración que fueron definidas y su responsabilidad en el cumplimiento de las disposiciones del SEVRI (Sistema Específico de Valoración del Riesgo Institucional) emitidas por la Contraloría General de la República.
f) En junio del 2010 se firma el "Contrato Servicios Profesionales para realizar la evaluación y seguimiento al funcionamiento del Sistema Específico de Valoración de Riesgos Institucional suscrito entre el IMAS y UMC Soluciones QYA Sociedad Anónima" cuyo objetivo fue realizar el seguimiento de las medidas de administración de riesgos y evaluar su impacto, entre otros; el cual tendría una vigencia de cuatro meses a partir del 21 de junio del 2010. No obstante, dicho contrato no se ejecuta dado que posteriormente la contratista solicita modificar el contrato y no se logra un acuerdo.
g) En diciembre del 2010 mediante acuerdo Nº577-2010 se aprueba el Informe de Priorización de Riesgos 2010 (gestión de riesgos 2009) por el Consejo Directivo
h) Durante el año 2010, no se evidencia que el Área de Tecnologías de información haya realizado gestiones para el cumplimiento del plan de Administración de Riesgos y que haya informado a la Unidad de Control Interno sobre su cumplimiento.
i) En diciembre del 2010, Control Interno solicita a TI (mediante oficio UCI-176-12-2010) el estado de implementación de las medidas de administración, las acciones respectivas realizadas y los resultados obtenidos de acuerdo con lo planificado, con la finalidad de obtener el primer seguimiento al plan de administración de riesgos.

Año 2011

j) En respuesta a la solicitud indicada en el punto anterior, en enero del 2011, Tecnologías de Información por medio del oficio TI-011-01-2011 remite un informe sobre el cumplimiento del Plan de Administración de Riesgos.
k) En marzo del 2011, por medio de correo electrónico Control Interno envía a Tecnologías de Información, el "instructivo análisis de efectividad de las medidas de administración y revisión de riesgos" con el objetivo de realizar la revisión de riesgos y análisis de la efectividad de las medidas de administración de riesgos, así como el instrumento para la identificación de riesgos "nuevos" para cuando lo requiera la unidad.

De conformidad con lo expuesto y en virtud de que se evidenció que desde Tecnologías de Información remitió a la Unidad de Control Interno en noviembre del 2009 el Plan de

Administración de Riesgos, hasta inicios del año 2011 se da seguimiento a la implementación del citado plan, se evidencia que el proceso de seguimiento a las medidas de administración no se realiza de forma sistemática y continua. Al respecto en las *directrices generales para el establecimiento y funcionamiento del SEVRI D-3-2005-CO-DFOE*, se define como SEVRI un *"conjunto organizado de componentes de la Institución que interaccionan para la identificación, análisis, evaluación, administración, revisión, documentación y comunicación de los riesgos institucionales".*

Adicionalmente, se carece de la característica de continuidad de proceso que establece la directriz antes mencionada, la cual indica que "los componentes y actividades del SEVRI se establecen de forma permanente y sus actividades se ejecutan de manera constante", dado que en noviembre del 2009 TI remite a Control Interno el Plan de Administración del riesgo y hasta el año 2011 se da seguimiento al plan de administración de riesgos.

Sobre el particular, las Directrices generales para el establecimiento y funcionamiento del sistema específico de valoración del riesgo institucional (SEVRI) D-3-2005-CO-DFOE emitido por la Contraloría General de la República, indican en lo de interés lo siguiente:

- *2.6-Características del SEVRI*: "El SEVRI que se establezca en cada institución deberá reunir características como las siguientes:
  Continuidad: Los componentes y actividades del SEVRI se establecen de forma permanente y sus actividades se ejecutan de manera constante."

- *2.7-Responsabilidad del SEVRI*: "El jerarca y los respectivos titulares subordinados de la institución son los responsables del establecimiento y funcionamiento del SEVRI. Para lo anterior deberán:
  b) Definir y ejecutar las actividades del Sistema indicados en la sección 4.
  c) Evaluar y dar seguimiento al Sistema para verificar su eficacia y eficiencia en relación con el objetivo indicado en la directriz 2.3.
  e) Tomar las medidas necesarias tendientes a fortalecer y perfeccionar el Sistema y al cumplimiento de la presente normativa.

- *3.3-Ambiente de Apoyo*: "(…) c) Actitud proactiva que permita establecer y tomar acciones anticipando las consecuencias que eventualmente puedan afectar el cumplimiento de los objetivos."

- *4.6-Revisión de Riesgos*: "En relación con los riesgos identificados, se deberá dar seguimiento, al menos, a:
  a) el nivel de riesgo;
  b) los factores de riesgo;
  c) el grado de ejecución de las medidas para la administración de riesgos;

d) la eficacia y la eficiencia de las medidas para la administración de riesgos ejecutadas.

La revisión de riesgos deberá ejecutarse de forma continua y la información que se genere en esta actividad deberá servir de insumo para:

a) Elaborar los reportes del SEVRI; b) ajustar de forma continua las medidas para la administración de riesgos; y c) evaluar y ajustar los objetivos y metas institucionales."

- 4.7. Documentación de riesgos. "Se deberá documentar la información sobre los riesgos y las medidas para la administración de riesgos que se genere en cada actividad de la valoración del riesgo (identificación, análisis, evaluación, administración y revisión). (…) Se deberá velar por que los registros sean accesibles, comprensibles y completos y que la documentación se realice de forma continua, oportuna y confiable. Toda esta información deberá servir de base para la elaboración de los reportes del SEVRI dirigidos a los sujetos interesados y podrá ser requerida por la Contraloría General de la República o la auditoría interna, por lo que deberá de estar actualizada en todo momento."

- 4.8. Comunicación de riesgos: "Se deberá brindar información a los sujetos interesados, internos y externos, y a la institución en relación con los riesgos institucionales. La comunicación deberá darse en ambas direcciones, mediante informes de seguimiento y de resultados del SEVRI que se elaboran periódicamente y mediante la operación de mecanismos de consulta a disposición de los sujetos interesados. " (Los subrayados no corresponden al original)

Adicionalmente, el Manual de Normas de Control Interno[6], en su apartado *3.2-Sistema específico de valoración del riesgo institucional (SEVRI),* en lo de interés señala:

El jerarca y los titulares subordinados, según sus competencias, deben establecer y poner en funcionamiento un sistema específico de valoración del riesgo institucional (SEVRI). El SEVRI debe presentar las características e incluir los componentes y las actividades que define la normativa específica aplicable. Asimismo, debe someterse a las verificaciones y revisiones que correspondan a fin de corroborar su efectividad continua y promover su perfeccionamiento. (El Subrayado no consta en el original)

[6] Normas de control interno para el Sector Público (N-2-2009-CO-DFOE) aprobadas mediante Resolución del Despacho de la Contraloría General de la República Nº R-CO-9-2009 del 26 de enero, 2009 y publicado en la Gaceta Nº 26 del 6 de febrero 2009.

Asimismo, en el documento Marco Orientador[7], en lo de interés señala:

- *2.1.2-Lineamientos:* "A los titulares subordinados y sus colaboradores les corresponde realizar un seguimiento continuo del plan con medidas para la administración del riesgo, con el fin de que éste sea ejecutado de acuerdo con la programación establecida."

- 3.2 Responsabilidades:
  "Titulares Subordinados:

  1) Ser el responsable de la Gestión de riesgos (identificación, análisis, evaluación y revisión) en la unidad bajo su responsabilidad.
  2) Proponer e implementar medidas de administración de riesgos, así como brindar la información al Equipo Técnico de Apoyo de Control Interno en el cumplimiento de las mismas.
  3) Dar seguimiento a las actividades de control que fueron definidas en su unidad para la administración de los riesgos.
  4) Ser responsable de las actividades de información y documentación de la administración del riesgo dentro de su unidad.

  Equipo Técnico de Apoyo de Control Interno:

  1) Brindar apoyo y asesoría a las unidades durante el proceso de valoración de riesgos.
  2) Elaborar propuestas de lineamientos y metodología para el fortalecimiento y desarrollo del SEVRI.
  3) Dar seguimiento a la implementación y funcionamiento del Sistema Específico de Valoración del Riesgo del IMAS.
  3) Dar seguimiento a las medidas de administración de riesgo implementadas por las diferentes unidades funcionales de los procesos de administración de riesgos.
  4) Administrar la herramienta informática, generar y comunicar información del SEVRI para la toma de decisiones.
  5) Buscar los mecanismos adecuados que permitan la comunicación dentro de la Institución y a los sujetos interesados del estado del SEVRI y las medidas que se han tomado para su fortalecimiento."

- 2.3.1. Procedimientos del Sistema Específico de Valoración del Riesgo Institucional: "(…) De esta manera, corresponde a los titulares subordinados en coordinación con el Equipo Técnico de Apoyo de Control Interno, realizar lo siguiente:

[7] Se refiere al documento denominado "Actualización del Marco Orientador y Fortalecimiento de Componentes del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), 2009" del IMAS.

Fase 5 Revisión de los Riesgos**:** "**Las medidas para la administración de riesgo seleccionadas deberán ejecutarse y evaluarse de forma continua**. Por lo que se realizará un seguimiento constante de su implementación y una vez que estas estén cumplidas con respecto a lo programado, se evaluará su eficacia y efectividad mediante el grado de afectación al nivel del riesgo. "

Actividad 10: "Para determinar el grado de ejecución de las medidas de administración, el Equipo Técnico de Apoyo de Control Interno solicitará un informe de avance a los responsables de la implementación de las medidas (jerarca o titular subordinado), conforme el plan de trabajo definido para cada una, para compararlo con lo programado, tanto en contenido como en tiempo. De existir un desfase se informará la situación al titular, el cual será responsable de hacer las correcciones pertinentes para lograr lo planeado. Lo anterior, con la finalidad de orientar y sugerir las acciones correctivas y ajustes necesarios, para concretar las mismas de forma que permitan asegurar un efectivo manejo del riesgo, concluyendo con un informe sobre el grado de ejecución de las medidas y resultados obtenidos con la implementación de estas. Los informes del seguimiento, una vez aprobados serán publicados de forma semestral en la Intranet para el acceso por parte de la comunidad institucional."

Actividad 11: "Para las medidas de administración que durante el seguimiento se determinen concluidas, el titular subordinado en coordinación con el Equipo Técnico de Apoyo de Control Interno realizará el análisis de: efectividad y eficacia de la medida de administración, efecto sobre los factores de riesgo y el nivel de riesgo una vez administrado o tratado."

Actividad 12: "Los titulares responsables con el apoyo del Equipo Técnico de Apoyo de Control Interno, realizarán la revisión de los riesgos tratados. Esta revisión de riesgos institucional, se hará de forma cíclica por áreas afines, de forma que permita medir el cumplimiento de los objetivos definidos, conforme se vayan implementando las medidas de administración." (Los subrayados no corresponden al original)

La causa de la situación expuesta, según indicó la Coordinadora de Control Interno obedece a que *"el seguimiento se contempló como una actividad a realizarse con la Contratación de Seguimiento y Evaluación al SEVRI, sin embargo no se ejecutó el contrato*[8] *por lo que no se ha realizado el seguimiento a la fecha, por parte de esta Unidad"*, aunado que no se comunicó formalmente acerca del grado de implementación

[8] Contrato Servicios Profesionales para realizar la evaluación y seguimiento al funcionamiento del Sistema Específico de Valoración de Riesgos Institucional suscrito entre el IMAS y UMC Soluciones Q Y A Sociedad Anónima.

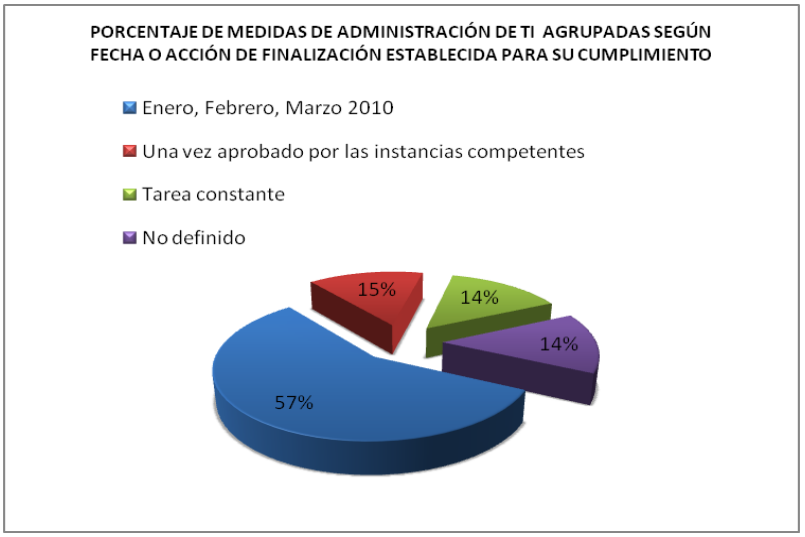
de las medidas de administración por parte de Tecnologías de Información, y a que hasta diciembre del 2010 mediante acuerdo Nº577-2010 se aprueba por parte del Consejo Directivo el "Informe de Priorización de Riesgos 2010" correspondiente a la gestión de riesgos realizada en el 2009.

Lo anterior provoca que no se pueda realizar un seguimiento periódico y una gestión continua y sistemática para verificar el nivel de implementación y efectividad de las medidas de administración, por lo que se expone a Tecnologías de Información a la materialización de riesgos críticos que pueden afectar significativamente la gestión Institucional, y a la inversión en recursos económicos y de personal para mantener controles o ejecutar medidas de administración que no ayudan a mitigar los riesgos significativamente.

2.3.2. Nivel de cumplimiento a las medidas de administración de Tecnologías de Información

Se evidenció que al 05 de noviembre del 2010 Tecnologías de Información no realiza una gestión y documentación formal que permita determinar el grado de implementación para cada una de las medidas de administración propuestas en el plan de administración de riesgos de su unidad, por lo que se desconoce el nivel de cumplimiento en función de las fechas establecidas para su finalización, lo anterior, a pesar de ciertas acciones que ha ejecutado Tecnologías de Información y que se pueden relacionar con algunas de las medidas de administración. A continuación se presenta un gráfico con el porcentaje de medidas de administración programadas para ejecutar por Tecnologías de Información durante el 2010.

Gráfico N º 3
Porcentaje de medidas de administración de TI a cumplir según período o acción establecida



Con respecto a lo comentado, las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) D-3-2005-CO-DFOE emitido por la Contraloría General de la República, indican en lo de interés lo siguiente:

- 2.6. Características del SEVRI. El SEVRI que se establezca en cada institución deberá reunir características como las siguientes:
  Continuidad: Los componentes y actividades del SEVRI se establecen de forma permanente y sus actividades se ejecutan de manera constante.
  Enfocado a resultados: Los componentes y actividades del sistema se establecen y desarrollan para coadyuvar a que la institución cumpla sus objetivos.

- *4.5-Administración de riesgos:* A partir de la priorización de riesgos establecida, se debe evaluar y seleccionar la o las medidas para la administración de cada riesgo, de acuerdo con criterios institucionales (…). Las medidas para la administración de riesgos seleccionadas deberán:
  a) Servir de base para el establecimiento de las actividades de control del sistema de control interno institucional.
  b) Integrarse a los planes institucionales operativos y planes de mediano y largo plazos, según corresponda.
  c) Ejecutarse y evaluarse de forma continua en toda la institución.

- *4.7-Documentación de riesgos:* Se deberá documentar la información sobre los riesgos y las medidas para la administración de riesgos que se genere en cada actividad de la valoración del riesgo (…). Se deberá velar por que los registros sean accesibles, comprensibles y completos y que la documentación se realice de forma continua, oportuna y confiable. Toda esta información deberá servir de base para la elaboración de los reportes del SEVRI dirigidos a los sujetos interesados y podrá ser requerida por la Contraloría General de la República o la auditoría interna, por lo que deberá de estar actualizada en todo momento. (Los subrayados no corresponden al original)

Asimismo, en el documento Marco Orientador[9], en lo de interés señala:

- 2.1.2. Lineamientos:
  "2-Cada una de las etapas del Sistema de Valoración del Riesgo se ejecutarán y será responsabilidad de los titulares subordinados y funcionarios en general, así como brindar la colaboración necesaria para su desarrollo.

[9] Marco Orientador denominado "Actualización del Marco Orientador y Fortalecimiento de Componentes del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), 2009" del IMAS.

7-A los titulares subordinados y sus colaboradores les corresponde realizar un seguimiento continuo del plan con medidas para la administración del riesgo, con el fin de que éste sea ejecutado de acuerdo con la programación establecida. “

- 2.3.1. Procedimientos del Sistema Específico de Valoración del Riesgo Institucional-Fase 5 Revisión de los Riesgos:
  “Las medidas para la administración de riesgo seleccionadas deberán ejecutarse y evaluarse de forma continua. Por lo que se realizará un seguimiento constante de su implementación y una vez que estas estén cumplidas con respecto a lo programado, se evaluará su eficacia y efectividad mediante el grado de afectación al nivel del riesgo”

- 3.2 Responsabilidades del Titular Subordinado:
  “1) Ser el responsable de la Gestión de riesgos (identificación, análisis, evaluación y revisión) en la unidad bajo su responsabilidad.
  2) Proponer e implementar medidas de administración de riesgos, así como brindar la información al Equipo Técnico de Apoyo de Control Interno en el cumplimiento de las mismas.
  3) Dar seguimiento a las actividades de control que fueron definidas en su unidad para la administración de los riesgos.
  4) Ser responsable de las actividades de información y documentación de la administración del riesgo dentro de su unidad.” (Los subrayados no corresponden al original)

Con respecto a la situación evidenciada, se determinó que la causa principal obedece a la cultura existente en la institución en relación con el SEVRI, pues no se ha logrado que los funcionarios tengan claridad e interioricen sus responsabilidades y deberes en la operación de este sistema. Como efecto de la situación descrita se provoca que no se tenga información oportuna sobre el estado de implementación de las medidas de administración, con lo cual no se conoce si los riesgos se mantienen en los niveles detectados al evaluarlos o se ha producido disminución en su probabilidad o impacto como producto de la implementación de alguna medida de tratamiento.

2.3.3. Lineamientos definidos en el Marco Orientador para iniciar el proceso de seguimiento

De conformidad con las pruebas realizadas, se determinó que a pesar de que en el marco orientador se definen las responsabilidades del Consejo Directivo, Titulares Subordinados y de la Unidad de Control Interno (nombrada anteriormente como Equipo Técnico de

Apoyo de Control Interno, ETACI), no se indica de forma clara y explícita cuando se puede iniciar el proceso de implementación, seguimiento y análisis de la efectividad de los planes de acción y si es necesaria o no la aprobación del informe de gestión de riesgos por el Consejo Directivo para iniciar el debido seguimiento, aún cuando los Titulares Subordinados son los responsables de implementar dichas medidas de administración y gestionar los riesgos de sus respectivas unidades o procesos.

Las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) D-3-2005-CO-DFOE emitido por la Contraloría General de la República, al respecto señalan:

- 2.7. *Responsabilidad del SEVRI*: El jerarca y los respectivos titulares subordinados de la institución son los responsables del establecimiento y funcionamiento del SEVRI. Para lo anterior deberán: (…)
  c) Evaluar y dar seguimiento al Sistema para verificar su eficacia y eficiencia en relación con el objetivo indicado en la directriz 2.3. (…)
  e) Tomar las medidas necesarias tendientes a fortalecer y perfeccionar el Sistema y al cumplimiento de la presente normativa. (…)"

- *3.2 Marco Orientador:* "La estrategia del SEVRI deberá especificar las acciones necesarias para establecer, mantener, perfeccionar y evaluar el SEVRI y los responsables de su ejecución. También deberá contener los indicadores que permitan la evaluación del SEVRI tanto de su funcionamiento como de sus resultados. La normativa interna que regule el SEVRI deberá contener en el ámbito institucional, al menos: los procedimientos del Sistema, los criterios que se requieran para el funcionamiento del SEVRI (…)".

- *3.3. Ambiente de apoyo: "*En cada institución deberá existir una estructura organizacional que apoye la operación del SEVRI, así como promoverse una cultura favorable al efecto. Para lo anterior, se deberá promover al menos: (…)
  c) Actitud proactiva que permita establecer y tomar acciones anticipando las consecuencias que eventualmente puedan Afectar el cumplimiento de los objetivos. (…)
  e) Mecanismos de coordinación y comunicación entre los funcionarios y las unidades internas para la debida operación del SEVRI." (Los subrayados no corresponden al original)

De conformidad con lo expuesto, la Unidad de Control Interno indicó que no se no tiene claridad sobre si puede iniciar el seguimiento sin la aprobación por parte del Consejo Directivo del Informe de Gestión de Riesgos 2009, aunque los responsables de la implementación y seguimiento de las medidas de administración sea el Titular

Subordinado, y consecuentemente que no se evalúe oportunamente la eficacia y efectividad de los planes de administración.

2.3.4. Suficiencia de los planes de acción

Se determinó que los planes de acción propuestos para mitigar los riesgos de Tecnologías de Información se encuentran incompletos de conformidad con los lineamientos definidos en el Marco Orientador para la gestión del SEVRI. Al respecto, se evidenció que los planes de acción no indican los recursos necesarios para ejecutar las medidas de administración. Adicionalmente, para la medida de administración "Adquisición de plataformas tecnológicas para la protección de código malicioso" no se indica la fecha de implementación, el responsable del monitoreo y la periodicidad para presentar el informe de avance.

Lo anterior, incumple lo dispuesto en el documento "Actualización del Marco Orientador y Fortalecimiento de Componentes del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)", específicamente en la sección 2.3.1. *Procedimientos del SEVRI*, actividad 8, donde señala que: "El Titular Subordinado responsable de su ejecución realizará un plan de trabajo para la implementación de cada medida de administración, el cual incluirá como mínimo: la descripción de la medida de administración, resultados esperados, tiempo de implementación, los responsables y recursos necesarios para llevarlas a cabo. Comunicará a los responsables de realizar acciones para la implementación de la misma y hará llegar el plan al Equipo Técnico de Apoyo de Control Interno, para su seguimiento. Las medidas de administración para los riesgos identificados en los planes operativos deberán integrarse dentro de esos planes institucionales. "(el subrayado no consta en el original)

Asimismo, las directrices generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) D-3-2005-CO-DFOE emitido por la Contraloría General de la República, en su apartado *4.7 Documentación de Riesgos* indica que (…) en relación con las medidas para la administración de riesgos deberá documentarse como mínimo su descripción, sus resultados esperados en tiempo y espacio, los recursos necesarios y responsables para llevarlas a cabo. Se deberá velar por que los registros sean accesibles, comprensibles y completos y que la documentación se realice de forma continua, oportuna y confiable (…). (El subrayado no consta en el original)

Sobre el particular, se determinó que la causa principal se originó al utilizar Tecnologías de Información el formato de plan de administración de riesgos proporcionado por la Unidad de Control Interno, que no contenía todos los requerimientos de información que deben suministrarse. Al respecto, la Coordinadora de la Unidad de Control Interno señaló

que efectivamente no contemplaron los respectivos lineamientos definidos en el marco orientador aunque si realizaron un estudio de viabilidad para cada medida de administración, donde se consideró que el costo no fuera mayor que el beneficio, no obstante no se analiza en función de términos económicos o descripción de recursos necesarios para su implementación.

2.3.5. Monitoreo de riesgos aceptados a nivel controlado

No se realiza un monitoreo de los riesgos aceptados a nivel controlado por parte de Tecnologías de Información. Al respecto, se evidenció que existen cuatro riesgos aceptados a nivel controlado por Tecnologías de Información y los cuales a la fecha de revisión no son monitoreados, dichos riesgos se detallan a continuación:

1. Clases de datos que hayan sido definidos de manera no apropiada
2. Niveles de seguridad de datos inconsistentes
3. Priorización de aplicaciones ocurridas en forma inconsistente con las expectativas de los usuarios
4. Las expectativas de desempeño de los usuarios no están siendo satisfechas, y que las modificaciones basadas en cambios de requerimientos no están siendo reflejadas en los planes de TI.

Con respecto a éste tema, el documento "Actualización del Marco Orientador y Fortalecimiento de Componentes del Sistema Específico de Valoración del Riesgo Institucional (SEVRI)", señala en la sección *2.3.2.3 Parámetros de aceptabilidad y administración del riesgo* lo siguiente*:*

"Se establecen los parámetros de aceptabilidad y administración del riesgo, con base en el nivel de riesgo residual, los riesgos que no se ubiquen dentro de la categoría de riesgo aceptable deberán administrarse de acuerdo con lo establecido en la Directriz 4.5 del SEVRI (el subrayado no consta en el original), como se indica en el siguiente cuadro:

Nivel de riesgo residual o controlado	Parámetros de aceptabilidad	Administración del riesgo
Extremo	Administrar, se deben establecer medidas de administración sin excepción	El nivel gerencial correspondiente (Gerencia General, Sub Gerencia Desarrollo Social y Sub Gerencia Administrativa Financiera), debe revisar y avalar las medidas de administración de riesgos propuestas por el Titular Subordinado.
Alto	Administrar, se deben establecer medidas de administración sin	El Titular Subordinado deberá definir medidas de administración que permitan minimizar el riesgo de ocurrencia o consecuencia del evento.

Nivel de riesgo residual o controlado	Parámetros de aceptabilidad	Administración del riesgo
	excepción	
Moderado	Administrar cuando su posibilidad de ocurrencia se encuentre dentro del rango de posible o probable.	El Titular Subordinado definirá las medidas de administración, según el parámetro de aceptabilidad. Si el riesgo no es administrado se realiza monitoreo constante de los factores de riesgo.
Bajo	**Aceptable**	**Para este nivel los riesgos se clasifican dentro del rango de aceptables, no se definirán medidas de administración. Requieren por parte del Titular Subordinado monitoreo constante de los factores de riesgo** (El subrayado no consta en el original)

La situación expuesta, se presenta según indicó el Coordinador de Tecnologías de Información porque "por error se envió un documento que contaba con esos riesgos, pero que más adelante se suprimieron", no obstante no se evidenció alguna comunicación formal que justificara dicha situación, por lo que en el Informe de Gestión de Riesgos 2009 presentado al Consejo Directivo para su aprobación y en el inventario de riesgos de Tecnologías de Información, se consideran los riesgos como aceptados a nivel controlado. Adicionalmente, la Unidad de Control Interno mediante correo con fecha del 08 de Junio del 2010 comunica a Tecnologías de Información el inventario de riesgos avalado tanto por la Unidad de Control Interno como por Tecnologías de Información, considerándose los riesgos citados, como aceptados a nivel controlado. Como consecuencia de lo anterior, el Área de Tecnologías no realiza un monitoreo de estos riesgos, con lo cual no se detecta si éstos aumentan su valor en el tiempo y por alguna razón requieren nuevamente ser tratados con medidas adicionales de control.

2.3.6. Administración continua del inventario de riesgos del año 2005 de Tecnologías de Información

Se determinó que los riesgos valorados como "medio", "bajo" o como "existe riesgo" del proceso de gestión de riesgos realizado durante el 2005, no fueron considerados para la evaluación de riesgos siguiente, para su administración y seguimiento continuo en el proceso de gestión de riesgos vigente, por lo que a la fecha de revisión, dichos riesgos no son incluidos en la herramienta ERA, sino que únicamente se consideran los identificados y valorados en el periodo siguiente.

Sobre el particular, el Manual de Normas Técnicas para la Gestión y Control de las Tecnologías de Información, en e apartado 1.3-Gestión de riesgos, en lo de interés señala:

"La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable." (El subrayado no consta en el original)

La situación expuesta según indicó el Lic. Luis Adolfo González, obedece por una recomendación de la Auditoría Interna, para analizar el inventario de riesgos de Tecnologías de Información considerando el modelo COBIT, por lo que al darle una perspectiva más general se provocó su omisión.

No obstante, las recomendaciones 4.4 y 4.8 del informe de Auditoría AUD 12-2009 sobre la Gestión de Riesgos del Área de Tecnología de información están enfocadas en la revisión y actualización de la estructura de riesgos considerando para ello como referencia los procesos del modelo COBIT, lo cual no necesariamente conlleva abandonar la estructura de riesgos que se tenía a la fecha, sino eventualmente su modificación y mejora.

La situación comentada, dificulta la comparación de resultados en el tiempo y ocasiona además que eventualmente se hayan eliminado del catálogo de riesgos, situaciones que realmente representan amenazas para el logro de objetivos del Área.

3. CONCLUSIONES

De conformidad con los resultados obtenidos en el presente estudio, esta Auditoría concluye lo siguiente:

1. A manera de resumen, las situaciones expuestas en los puntos 2.3.1 al 2.3.6 del presente informe, evidencian que no existe continuidad en el funcionamiento del SEVRI, y que además los canales de interacción entre sus diferentes componentes, por lo menos en el caso de la gestión del Área de Tecnologías de Información, no funcionan adecuadamente, con lo cual se afecta en forma sensible el funcionamiento sistémico del SEVRI, características esenciales de un sistema. Dadas estas condiciones, existe una alta probabilidad de que los objetivos que persigue lograr el SEVRI no se alcancen, y que se produzca un estancamiento que impida a los procesos adquirir un nivel mayor de madurez.

2. De las 11 recomendaciones dispuestas en el informe AUD 012-2009, el 82% (9) se han cumplido de forma total y el 18% (2) se encuentran parcialmente cumplidas. En virtud de lo anterior, y dada la relevancia de las recomendaciones que aún no han sido implementadas, se considera necesario que se dediquen mayores esfuerzos a efecto de

lograr el efectivo cumplimiento para las recomendaciones no cumplidas. En este sentido debe prestarse especial atención a los aspectos relevantes dispuestos en las recomendaciones.

3. En relación con la validez de los resultados del proceso de identificación y valoración de riesgos del área de Tecnologías de Información, se evidenció que durante las fases de identificación, análisis, priorización de riesgos y confección de planes de acción ha existido una buena coordinación entre la Unidad de Control Interno y Tecnologías de Información. No obstante, el estudio permitió determinar importantes deficiencias relacionadas principalmente con la identificación del evento generador del riesgo, con la definición y valoración de controles, con la actualización del inventario de riesgos y con la gestión integral de riesgos externos. Producto de lo anterior, se requieren acciones para atender directamente los eventos de riesgo con el fin de asegurar el funcionamiento de Tecnologías de Información y por ende de la Institución, y el evitar el invertir en recursos no efectivos para mitigar o disminuir la probabilidad de materialización de los riesgos.

4. El sistema Específico de Valoración de Riesgo Institucional del IMAS, adolece de una seria deficiencia en uno de los atributos más importantes del sistema: la continuidad. Esta situación imposibilita que la gestión de riesgos del IMAS sea sistémica, por lo que la probabilidad de materialización de los riesgos de Tecnologías de Información y eventualmente de otras unidades se mantiene sin cambios, debido a la ausencia de una cultura de autogestión de riesgos y de seguimiento por parte de la Unidad de Control Interno de la implementación de medidas de administración propuestas. Esta situación además expone a la Institución a sanciones por parte de los órganos de fiscalización superior de la Hacienda Pública, evidente incumplimiento de la normativa de control interno (Ley General de Control Interno, Directrices sobre funcionamiento de SEVRI, Normas de Control Interno del Sector Público, entre otras)

4. RECOMENDACIONES

DISPOSICIONES LEGALES SOBRE RECOMENDACIONES

Esta Auditoría Interna respetuosamente se permite recordar al Consejo Directivo, que de conformidad con lo preceptuado por el artículo 37 de la Ley General de Control Interno, Nº 8292, dispone de treinta días hábiles, contados a partir de la fecha de recibido de este informe, para ordenar la implantación de las recomendaciones.

Asimismo, se permite recordar a la Máster Mayra Díaz Méndez, en su calidad de Gerente General, al Lic. Luis Adolfo González Alguera, Coordinador de Tecnologías de Información y a la Licda. Guadalupe Sandoval Sandoval, Coordinadora de la Unidad de Control Interno, que de conformidad con lo preceptuado por el artículo 36 de la Ley General de Control Interno Nº 8292, disponen de diez días hábiles para ordenar la implantación de las recomendaciones, contados a partir de la fecha de recibido de este informe.

Al respecto, se estima conveniente transcribir a continuación, en lo de interés, lo que disponen los artículos 36, 37, 38 y 39 de la Ley Nº 8292:

> Artículo 36._ **Informes dirigidos a los titulares subordinados**. Cuando los informes de auditoría contengan recomendaciones dirigidas a los titulares subordinados, se procederá de la siguiente manera:
>
> a) El titular subordinado, en un plazo improrrogable de diez días hábiles contados a partir de la fecha de recibido el informe, ordenará la implantación de las recomendaciones. Si discrepa de ellas, en el transcurso de dicho plazo elevará el informe de auditoría al jerarca, con copia a la auditoría interna, expondrá por escrito las razones por las cuales objeta las recomendaciones del informe y propondrá soluciones alternas para los hallazgos detectados. /b) Con vista de lo anterior, el jerarca deberá resolver, en el plazo de veinte días hábiles contados a partir de la fecha de recibo de la documentación remitida por el titular subordinado; además deberá ordenar la implantación de recomendaciones de la auditoría interna, las soluciones alternas propuestas por el titular subordinado o las de su propia iniciativa, debidamente fundamentadas. Dentro de los primeros diez días de ese lapso, el auditor interno podrá apersonarse, de oficio, ante el jerarca, para pronunciarse sobre las objeciones o soluciones alternas propuestas. Las soluciones que el jerarca ordene implantar y que sean distintas de las propuestas por la auditoría interna, estarán sujetas, en lo conducente, a lo dispuesto en los artículos siguientes. /c) El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.
>
> Artículo 37. - **Informes dirigidos al jerarca.** Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente.

Artículo 38._ **Planteamientos de conflictos ante la Contraloría General de la República**. Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas. / La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, Nº 7428, de 7 de setiembre de 1994.

Artículo 39._ **Causales de responsabilidad administrativa.** El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable a la respectiva relación de servicios.

AL CONSEJO DIRECTIVO

4.1. Girar las instrucciones que correspondan y disponer las medidas que estimen pertinentes con el propósito de que las recomendaciones que se detallan en el Anexo Nº 1 al presente informe, sean debidamente implementadas, estableciendo un plazo razonable de cumplimiento; con el propósito de fortalecer los sistemas de control interno y atender de manera apropiada las responsabilidades establecidas en la Ley General de Control Interno, Nº 8292. (Ver punto 2.1.1 del acápite de resultados)

4.2. En su calidad de máximo Jerarca, responsable de la gestión del riesgo en el IMAS, ordenar a la Gerente General, realizar todas las acciones necesarias para que el Sistema Específico de Valoración de Riesgo Institucional, opere en forma sistémica y continua, de forma que las unidades implementen las medidas de tratamiento e informen a la Unidad de Control Interno y ésta última ejecute a su vez un seguimiento de la implementación de tales medidas. (Ver punto 2.3.1 del acápite de resultados)

A LA GERENTE GENERAL

4.3. Elaborar y someter a la aprobación del Consejo Directivo, las siguientes modificaciones del Marco Orientador de SEVRI:

a) Definir en el documento lineamientos que indiquen como proceder para actualizar el mapa de riesgos ante cambios en el entorno que afectan la operación regular de cada área, con el fin de anticipar la ocurrencia de eventos que provoquen consecuencias de alto impacto para la Institución. (Ver punto 2.2.1 del acápite de resultados)

b) Documentar de forma clara y explícita el o los responsables de iniciar el proceso de implementación, seguimiento y análisis de la efectividad de los planes de acción. Considerando que no es necesaria la aprobación del informe de gestión de riesgos por parte del Consejo Directivo para iniciar el proceso de implementación, seguimiento y análisis de la efectividad de los planes de acción; y la responsabilidad de los Titulares Subordinados en la implementación de los planes de acción, los cuales deben ser razonables y consecuentes según el riesgo a administrar y considerando el análisis de costo y beneficio en su diseño e implementación. (Ver punto 2.3.3 del acápite de resultados)

c) Incorporar en el Marco Orientador de forma clara y detallada las responsabilidades del Comité Gerencial de Control Interno en el proceso de revisión y aprobación de la gestión del riesgo institucional, y los plazos para su revisión. (Ver punto 2.3.3 del acápite de resultados)

d) Definir en el Marco Orientador del SEVRI lineamientos detallados que indiquen como proceder para documentar y atender de forma integral los riesgos definidos como externos. (Ver punto 2.2.2 del acápite de resultados)

A LA COORDINADORA DE CONTROL INTERNO

4.4. Realizar un seguimiento periódico y una gestión continua y sistemática a las medidas de administración de Tecnologías de Información con el fin de corroborar su cumplimiento y efectividad, en la mitigación de los riesgos identificados garantizando el funcionamiento sistemático del SEVRI. (Ver punto 2.3.1 del acápite de resultados)

4.5. Una vez aprobadas las modificaciones en el Marco Orientador del SEVRI contenidas en la recomendación 4.3, comunicar a las diferentes instancias involucradas en la gestión del SEVRI para su aplicación inmediata de acuerdo con sus responsabilidades. (Ver punto 2.2.1, 2.2.2 , 2.3.3 del acápite de resultados)

4.6. Según la modificación aprobada en el marco orientador, definir las medidas de tratamiento para el riesgo de Tecnologías de Información con planes de implementación "externos". (Ver punto 2.2.2 del acápite de resultados)

4.7. Actualizar en la herramienta ERA el inventario de riesgos de Tecnologías de Información, de acuerdo con la recomendación 4.10 del presente informe. (Ver punto 2.2.1 del acápite de resultados)

4.8. Aplicar lo dispuesto en la sección 2.3.1. Procedimientos del SEVRI, actividad 8, del Marco Orientador para la gestión del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), con el fin de garantizar la suficiencia de los planes de acción propuestos para mitigar los riesgos de TI. (Ver punto 2.3.4 del acápite de resultados)

4.9. Actualizar el inventario de riesgo vigente de Tecnologías de Información con el fin de integrar los riesgos valorados como "medio", "bajo" o como "existe riesgo" del proceso de gestión de riesgos realizado durante el 2005 con el fin de garantizar su administración continua y seguimiento periódico y sistemático. (Ver punto 2.3.6 del acápite de resultados)

AL COORDINADOR DE TECNOLOGÍAS DE INFORMACIÓN

4.10. Revisar el inventario de riesgos con el fin de corregir las siguientes deficiencias:

- Debilidades de control documentadas como riesgos.
- Especificar y/o modificar la definición conceptual del riesgo definido como "Niveles de seguridad de datos inconsistentes"
- Consolidar los riesgos repetitivos para eliminar duplicidades en el catálogo de riesgos.
- Detallar los controles documentados de forma general, especificando los mecanismos que operacionalizan los controles, con el fin de permitir determinar de manera concreta su evaluación y de servir de insumo para definir medidas de administración efectivas.
- Evaluar los controles no evaluados del inventario de riesgos 2009 y gestionar su actualización en la herramienta ERA. (Ver punto 2.2.1 del acápite de resultados)

4.11. Realizar una gestión continua de las medidas para la administración del riesgo de Tecnologías de Información, con el fin de que éste sea documentado y ejecutado de acuerdo con lo establecido y brindar de manera periódica información a la Unidad de Control Interno acerca de su nivel de cumplimiento. Se debe mantener dicha comunicación de forma periódica con la Unidad de Control Interno hasta que los

planes de acción sean implementados en su totalidad y se compruebe su eficacia en la mitigación de los riesgos; y hasta ubicar los riesgos de la unidad, en un nivel de riesgo aceptable. (Ver punto 2.3.2 del acápite de resultados)

4.12. Para los riesgos que se ubiquen dentro de la categoría de riesgo aceptable, realizar una revisión de éstos de conformidad con lo establecido en el marco orientador del SEVRI. (Ver punto 2.3.5 del acápite de resultados)

4.13. Aplicar lo dispuesto en la sección 2.3.1. Procedimientos del SEVRI, actividad 8, del Marco Orientador para la gestión del Sistema Específico de Valoración del Riesgo Institucional (SEVRI), con el fin de garantizar la suficiencia de los planes de acción propuestos para mitigar los riesgos de TI. (Ver punto 2.3.4 del acápite de resultados)

4.14. Actualizar el inventario de riesgo vigente de Tecnologías de Información con el fin de integrar los riesgos valorados como "medio", "bajo" o como "existe riesgo" del proceso de gestión de riesgos realizado durante el 2005 con el fin de garantizar su administración continua y seguimiento periódico y sistemático. (Ver punto 2.3.6 del acápite de resultados)

Hecho por
MATI. Karen Núñez Solano
PROFESIONAL EJECUTORA

Revisado y aprobado
MATI. Wady Solano Siles
COORDINADOR AUDITORIA

AUDITORIA INTERNA
DICIEMBRE, 2011

ANEXO 1

ESTUDIO SOBRE SEGUIMIENTO DE LAS RECOMENDACIONES CONTENIDAS EN EL INFORME AUD 012-2009.

En las siguientes tablas se detallan los resultados de la verificación realizada correspondiente a las recomendaciones parcialmente cumplidas:

Nº Recomendación: 4.4	**Condición: Parcialmente Cumplida**

Dirigida a: Subgerencia Administrativa Financiera / Responsable: Lic. Fernando Sánchez Matarrita

Revisar y actualizar la estructura de riesgos identificados en el Área de Desarrollo y Asesoría Informática e incorporar al menos los riesgos citados en el punto 2.1.3 del acápite de resultados del presente informe, actividad que debe integrarse dentro de la ejecución de actividades del Sistema Específico de Valoración de Riesgos Institucional. A la vez, comunicar a la Comisión de Control Interno Institucional los resultados obtenidos en esta revisión y actualización.

Resultados y valoración de la verificación realizada:

Con base en los resultados obtenidos en la verificación realizada por esta Auditoría se determinó que la recomendación indicada se encuentra "parcialmente cumplida". Lo anterior porque si bien Tecnologías de Información revisó y actualizó la estructura de riesgos del Área de Tecnologías de Información con base el modelo COBIT, no se incorporaron al menos los riesgos claves citados en el punto 2.1.3 del acápite de resultados del informe AUD 012-2009 (ver anexo 2).

Nº Recomendación: 4.7	**Condición: Parcialmente Cumplida**

Dirigida A: Tecnologías De Información / Responsable: Lic. Luis Adolfo González Alguera.

Elaborar y gestionar la aprobación de un plan de capacitación del personal del Área de Desarrollo Informático, el cual responda a las necesidades en materia de capacitación sobre las tecnologías que utiliza la Institución.

Resultados y valoración de la verificación realizada:

Con base en los resultados obtenidos en la verificación realizada por esta Auditoría se determinó que la recomendación indicada se encuentra "parcialmente cumplida". Lo anterior porque a pesar de que TI remite a Desarrollo Humano un plan de capacitación para su personal, éste no es aprobado por Desarrollo Humano (aunque a octubre del 2010 no habían enviado una respuesta formal a TI), ya que según se indicó en dicha unidad, el plan de capacitación se mantiene muy general, no brinda claridad de la inversión económica que se requiere, detalla técnicas de capacitación pero no considera actividades concretas de capacitación, y solicitan una gran cantidad de cursos (aproximadamente 23 cursos), por lo que debe coordinar con el Lic. Luis Adolfo González, la aplicación del *Formulario de Detección de Necesidades de Capacitación* con el fin de priorizar los cursos de capacitación en función de las necesidades específicas y prioritarias de la unidad, para su consideración en el presupuesto 2011.

Nº Recomendación: 4.7	**Condición: Parcialmente Cumplida**
Adicionalmente, Desarrollo Humano indicó que no se podía incluir en el presupuesto del 2010, ya que para considerarlo TI tenía que enviarlo aproximadamente en setiembre del 2009, a fin de reservar los recursos económicos correspondientes. Por otra parte, a octubre del 2010 Tecnologías de Información no había gestionado solicitudes de beca con el objeto de que los funcionarios a nivel individual se capacitaran en algunas de las actividades señaladas en el Plan de Capacitación de Tecnologías de Información 2010.	

ANEXO 2

CUADRO COMPARATIVO DE RIESGOS VIGENTES DE TECNOLOGÍAS DE INFORMACIÓN (INVENTARIO 2009) CONTRA LOS RIESGOS INCLUIDOS EN LA RECOMENDACIÓN 4.4 DEL INFORME AUD-012-2009

Con el fin de revisar si la estructura de riesgos del Área de Desarrollo incorpora al menos los riesgos citados en el punto 2.1.3, en la siguiente tabla se realiza una comparación de los riesgos citados en el punto 2.1.3 del informe AUD-012-2009 con los riesgos de Tecnologías de Información como resultado de la gestión del 2009, con el fin de analizar su respectiva correspondencia:

RIESGOS RECOMENDADOS INFORME AUD 012-2009	OBSERVACIONES	RIESGOS TI INVENTARIO 2009
a. Sub o sobre dimensionamiento en el desarrollo y adquisición de software.	Causa del punto BB	-
b. Diseño inadecuado en el desarrollo y adquisición de software.	Causa del punto C	-
c. Aceptación de software no acorde con las necesidades en el desarrollo y adquisición de software.	Riesgo Software no acorde con las necesidades …	5.Definición de datos de información sin responder a los requerimientos de los usuarios 6.Debilidades organizacionales para desarrollar y correr las aplicaciones requeridas 16.Priorización de aplicaciones ocurridas en forma inconsistente con las expectativas de los usuarios
d. Falta de oportunidad en la entrada en producción del desarrollo y adquisición de software.	Debilidad de control	-
e. Negación del servicio en la operación de instalaciones.	Ver punto O	-
f. Cambios no autorizados en la operación de instalaciones.	Debilidad de control	-
g. Ineficiente uso de los recursos en la operación de instalaciones.	Se repite con BB	-
h. Acceso no autorizado en la operación de instalaciones.	Ver punto t	-
i. Selección inadecuada de estrategias de aspectos técnicos y tecnológicos.	Ver puntos BB y N	-
j. Obsolescencia tecnológica.	Riesgo	**RECOMENDACIÓN NO CONSIDERADA**
k. Pérdida de información por fallas técnicas y tecnológicas.	Riesgo	**RECOMENDACIÓN NO CONSIDERADA**
l. Pérdida de confidencialidad en función de las relaciones con la información.	Ver punto T	-
m. Pérdida de integridad o confiabilidad de la información.	Riesgo	**RECOMENDACIÓN NO CONSIDERADA**
n. Carencia de estrategias y tácticas alineadas	Riesgo	4. Fallas en planificación a mediano y largo

RIESGOS RECOMENDADOS INFORME AUD 012-2009	OBSERVACIONES	RIESGOS TI INVENTARIO 2009
con la institución.		plazo para satisfacer los objetivos Institucionales. 10. Un marco referencial de control débil que ponga en duda el compromiso de la administración en cuanto al fomento de un ambiente de control interno positivo a través de la organización. 11. Lagunas, traslapes, etc. en la estructura organizacional.
o. Deficiente entrega de servicios de TI de acuerdo con las prioridades del negocio.	Riesgo	1.La no existencia de acuerdos de niveles servicio **RECOMENDACIÓN CONSIDERADA PARCIALMENTE**
p. Deficiente destino de los esfuerzos de utilizar los sistemas de TI de manera productiva y segura.	Ver punto BB	-
q. Ineficiente monitoreo y evaluación de la calidad y cumplimiento de los requerimientos de control.	Riesgo	8.Bitácoras o reportes de problemas que confirmen que los problemas ocurridos durante el procesamiento de información fueron considerados oportunamente y que se llevaron a cabo las acciones correctivas apropiadas **RECOMENDACIÓN CONSIDERADA PARCIALMENTE**
r. Ineficiente medición del desempeño de TI para detectar preventivamente problemas.	Riesgo	**RECOMENDACIÓN NO CONSIDERADA**
s. Ineficiente planeación y organización previa a adquirir e implementar un sistema.	Causa de punto BB	-
t. Ineficiente administración de las claves o passwords de acceso a los sistemas (seguridad de la información).	10. Acceso no autorizado de información. Ver h.	2. Accesos inapropiados por parte de los usuarios a los recursos del sistema.
u. Deficiente mantenimiento de los sistemas institucionales.	Riesgo	**RECOMENDACIÓN NO CONSIDERADA**
v. Incumplimiento de regulaciones	Riesgo	**RECOMENDACIÓN NO CONSIDERADA**
w. Administración de proveedores y contratación global (el fracaso de proyectos cuantiosos en TI).	Riesgo	13.Cobertura de seguros inadecuada **RECOMENDACIÓN CONSIDERADA PARCIALMENTE**
x. Detección de fraudes y falta de Integridad Interna.	Riesgo Fraude	**RECOMENDACIÓN NO CONSIDERADA**
y. Hacking y Virus (gusanos, troyanos, phishing, software de espionaje).	Riesgo Ataque de virus	7.La falta de software actualizado para la detección de virus o de procedimientos formales para prevenir, detectar, corregir y comunicar contaminaciones
z. Ignorancia del nivel de dependencia y vulnerabilidad de TI del negocio	Riesgo Dependencia de	**RECOMENDACIÓN NO CONSIDERADA**

RIESGOS RECOMENDADOS INFORME AUD 012-2009	OBSERVACIONES	RIESGOS TI INVENTARIO 2009
(Heterogeneidad en la ejecución de procesos).	personal clave de TI	
aa. Ignorancia del nivel de oportunidades y pérdidas en las inversiones TI.	Causa de punto BB	-
bb. Ineficiencia en el uso de los recursos (pérdida económica) y el hurto de activos (recursos informáticos): robo de identidad, demandas legales, manejo de activos TI, falta de clasificación y valorización de la información, información privilegiada de la institución.	Riesgo	9.Proyectos a desarrollar por TI no son administrados adecuadamente para la maximización de los recursos y tiempos aceptables de desarrollo así como sean administración inadecuadamente 12.Proyectos administrados inadecuadamente **RECOMENDACIÓN CONSIDERADA PARCIALMENTE**
cc. Limitación de crecimiento u optimización o innovación (selección de sistemas basados en parámetros de hoy, selección de sistemas basados en tecnologías de punta o de corta vida, falta de levantamientos de los procesos de negocios en forma previa, alta dependencia de terceros, implementaciones desastrosas, espionaje industrial, dificultad de cumplir con requerimientos más complejos y capacidad de respuesta).	Causa de punto J	-