AUD. 0019-2015

INFORME DE LOS RESULTADOS OBTENIDOS EN EL ESTUDIO SOBRE LA SEGURIDAD DE ACCESO A LA INFORMACIÓN DEL SISTEMA DE DESARROLLO HUMANO

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 2013.

1.2. Objetivo General

El objetivo del estudio consistió en coadyuvar en la gestión de la seguridad de la información, del Sistema de Desarrollo Humano.

1.3. Alcance y Periodo de Estudio

El estudio consistió en evaluar la razonabilidad, de la definición y alcance de los perfiles de acceso a la información, del sistema de Desarrollo Humano, durante el período del 01 de enero del 2013 al 31 de agosto del 2013 y se amplió en el caso de la revisión del cumplimiento de requisitos de las acciones de personal, hasta el 30 de abril 2014.

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), las Normas de Control Interno para el Sector Público[1], el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información[2], así como la demás normativa de Auditoría Interna de aceptación general.

1.4. Comunicación verbal de los resultados

En reunión celebrada el día 30 de enero del 2015, se comunicaron los resultados del presente informe al Máster Luis Adolfo González, jefe de Tecnologías de Información y al Lic. José Guido Masís Masís, Jefe de Desarrollo Humano, en la cual se efectuaron observaciones que en lo pertinente, una vez valoradas por esta Auditoría Interna, fueron incorporadas en el presente informe.

[1] Nº R-CO-9-2009 de la Contraloría General de la República. Publicada en la Gaceta N` 26 del 6 de febrero del 2009
[2] Nº R-CO- 26-2007 de la Contraloría General de la República, Publicada en la Gaceta N 119 del 21 de junio del 2007

2. RESULTADOS

2.1. Documentación de los perfiles de acceso al sistema de Desarrollo Humano y desconocimiento de la estructura de seguridad del mismo.

No se localizó documentación que detalle información importante relativa a los grupos de usuario con acceso, a los diferentes módulos del Sistema de Desarrollo Humano. Al respecto, existe una estructura de seguridad de acceso implementada, la cual consiste en grupos de usuarios que tienen acceso a los diferentes módulos, donde cada grupo tiene asignados privilegios sobre recursos del sistema como opciones de menú, botones de aplicación y datos. No obstante, tal como se indicó, esta estructura y sus accesos no están debidamente documentados y por lo tanto no se tiene información detallada de los atributos de los diferente grupos, como por ejemplo: justificación de su creación o existencia, opciones de menú que debe tener habilitadas y usuarios que deben pertenecer a cada uno de ellos, entre otros.

De acuerdo a lo indicado por el jefe de Desarrollo Humano, Lic. José Guido Masís Masís, una de las posibles causas por las que no se han documentado los accesos al Sistema de Desarrollo Humano, obedece a que las personas tanto internas como externas que diseñaron el esquema de seguridad actual ya no forman parte de la institución y por lo tanto se torna más difícil entender los criterios y justificaciones empleados en el momento de creación de los grupos de acceso al Sistema de Desarrollo Humano. Lo anterior, fue confirmado por el Lic. Eddy González Rodríguez, funcionario de Tecnologías de Información, encargado del sistema de Desarrollo Humano. Asimismo, al implementar en producción el sistema, no se confeccionó oportunamente la documentación de la estructura de seguridad, sino que se implementó directamente en el sistema que fue puesto en producción.

Aunado a lo anterior, se corroboró con el Lic. Masís y con el Lic. González que tanto el área de Desarrollo Humano como el área de Tecnologías de Información, desconocen detalles importantes de la estructura de seguridad del sistema de Desarrollo Humano, como por ejemplo, el por qué de la existencia de algunos grupos de usuarios, y cuáles opciones de menú y botones de aplicación deben tener habilitadas los diferentes grupos.

La situación descrita en los párrafos anteriores, limita el proceso de administración y control de los privilegios de acceso al sistema de Desarrollo Humano, pues no existe una base clara que establezca cuál es la asignación correcta de privilegios a los diferentes grupos definidos en el sistema.

La ausencia de esta base también imposibilita la comparación de la asignación real de permisos de acceso (que está implementada en el ambiente de producción) contra la asignación de accesos que realmente debería tener cada grupo de usuarios.

Adicionalmente, sin una base clara que establezca la asignación correcta de privilegios de acceso al sistema de Desarrollo Humano, no se puede precisar si los accesos asignados a un funcionario, efectivamente contemplan todos los accesos necesarios para que este ejerza sus funciones de acuerdo al cargo que desempeña y según lo establecido en el Manual de Cargos Institucional, o si por el contrario, tiene activos algunos privilegios que no forman parte de sus funciones. Dicha situación, no permite determinar si la asignación de privilegios de un usuario o grupo de usuarios, cumple con el principio de "necesidad de saber, o de menor privilegio", el cual establece que un usuario debe tener acceso únicamente a la información y operaciones del sistema necesarias para realizar su trabajo.

En el mismo orden de ideas, esta Auditoría corroboró que las solicitudes de acceso al sistema, son atendidas mediante la asignación del usuario a un grupo de usuario que tenga el acceso habilitado a la funcionalidad solicitada, lo que propicia que el usuario tenga derechos en todas las opciones de menú sobre las cuales tiene privilegio el grupo de usuario, aunque este no deba tenerlas. Dicha situación se contrapone con el principio de la necesidad de saber o de menor privilegio.

No obstante, ante las situaciones previamente descritas, esta Auditoría realizó una revisión manual de los principales grupos de usuario, según su nivel de riesgo y acceso y los miembros que pertenecen a cada uno de ellos, así como los privilegios de accesos que tiene asociado cada grupo de usuario. Con respecto a la revisión de los miembros pertenecientes a cada grupo de usuario, se concluyó que los miembros que pertenecen a cada uno de ellos, son en efecto los autorizados de acuerdo con las funciones que realizan y el cargo que desempeñan según el Manual de Cargos Institucional, lo anterior fue corroborado con el jefe de Desarrollo Humano, Lic. Masís Masís.

En lo que respecta a la revisión de los privilegios de acceso que tiene asociados cada grupo de usuario validado, se determinó que existe una seguridad razonable de que dichos privilegios han sido asignados a los grupos de usuario, de acuerdo con las funciones descritas en el Manual de Cargos para el puesto que desempeña cada uno de los miembros de los respectivos grupos. En este particular es importante mencionar que en el momento de la revisión, los grupos "coordinador recursos", "general medico" y "exfuncionarios" tenían asociados privilegios de acceso relacionados con la gestión de citas médicas, situación que fue subsanada al momento de la revisión. No obstante la revisión efectuada por la Auditoría, la cual fue realizada con base en información recopilada sobre funciones y tareas efectuadas por el personal, no existe una certeza razonable sobre la definición de grupos y perfiles, en virtud de que las pruebas efectuadas por la Auditoría no fueron exhaustivas sobre toda la estructura, sino sobre una muestra de los perfiles más riesgosos.

Con respecto al tema desarrollado, las Normas de Control Interno, en el Capítulo V: Normas sobre Sistemas de Información, señalan en lo de interés lo siguiente:

"5.8 Control de sistemas de información: El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter." (El subrayado no consta en el original)

Por otra parte, el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, en lo de interés señala:

"1.4.5 Control de acceso: La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:
(…)
d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.
e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones." (El subrayado no consta en el original)

Asimismo, la Política Acceso Lógico del IMAS, POL-EDI-11, publicada en Noviembre 2009, indica al respecto lo siguiente:

"9.1 Lineamientos:
A- Agrupamiento de usuarios: (…)
12. El Área de Tecnologías de Información creará en coordinación con el jefe o coordinador de cada unidad administrativa grupos de usuarios y concederá diferentes niveles de acceso a estos grupos (perfiles), según lo requieran sus funciones laborales.
13. Los usuarios deberán tener razones justificadas para obtener acceso a más información de la que se permita en el grupo al que pertenece, y en ese caso tendrá acceso estrictamente a la información que necesite para realizar sus labores.
14. El Área de Tecnologías de Información le concederá acceso a un usuario cuando el Jefe de Área o un Usuario especializado realice las actividades correspondientes para dicha solicitud. Estas peticiones serán archivadas y servirán de rastro de auditoría en el futuro. El acceso adicional será removido en cuanto el funcionario termine las labores para las cuales necesitaba este acceso.
15. Los dueños de los procesos (Gerentes, Coordinadores y otros funcionarios) son responsables por la revisión periódica de los privilegios otorgados a los funcionarios de

su Unidad y debe prontamente revocar aquellos privilegios que ya no son requeridos por los usuarios. La revisión debe llevarse a cabo periódicamente o cuando haya un cambio en la Institución, en los sistemas o en la importancia de los datos.
16. Es responsabilidad del Área de Tecnologías de Información proveer la información necesaria a los dueños de los procesos para realizar la revisión." (El subrayado no consta en el original)

2.2. Seguridad y Control Interno en el Sistema de Desarrollo Humano

2.2.1. Sobre el proceso de modificación de acceso a perfiles

En el sistema de Desarrollo Humano, no se localizaron controles que permitan identificar de manera automática, cuando se vence el período de un nombramiento temporal de un funcionario con acceso a los módulos del sistema. De acuerdo a lo indicado por el Jefe de Desarrollo Humano, Lic. José Guido Masís Masís, esta situación se da tanto en la asignación de accesos otorgados a los funcionarios de Desarrollo Humano para el uso de los módulos del Sistema de Desarrollo Humano, como en la asignación de accesos otorgados a las jefaturas de la Institución, para el uso del comúnmente llamado Módulo Remoto.

Ante la ausencia de una solución automatizada que contribuya a la notificación del vencimiento de un nombramiento temporal, se ha adoptado la práctica de realizar una revisión manual de las cuentas de usuarios, la cual consiste en validar visualmente la lista de usuarios registrados en el sistema de Desarrollo Humano y modificar de forma manual, los accesos a aquellas personas que el funcionario a cargo de la modificación de perfiles conoce que cambiaron sus funciones. No obstante, esta práctica no se aplica periódicamente.

La situación descrita, potencia el riesgo de que un usuario mantenga acceso a opciones del sistema que ya no le corresponde utilizar, pues no existen mecanismos confiables para eliminar los privilegios concedidos oportunamente, una vez que el funcionario deja de realizar las funciones que le fueron asignadas temporalmente.

Sobre este particular, producto de la revisión que efectuó esta Auditoría Interna a los principales privilegios de acceso que tiene habilitado cada grupo de usuario, se encontró el caso de los grupos de usuario descritos en la Tabla N°1, los cuales tenían habilitados privilegios de acceso a las opciones de menú relacionadas con citas médicas. No obstante, es importante recalcar que la revisión realizada refleja que en general los permisos críticos asignados responden razonablemente a las funciones de los cargos que ejercen los funcionarios que tienen este tipo de accesos, de conformidad con el Manual de Cargos institucional. Adicionalmente, la situación descrita en la Tabla N°1 fue subsanada durante la evaluación mediante la revocación de los privilegios de acceso a los grupos de usuario que por

sus funciones según el cargo que desempeñan, no deben tener accesos relacionados con citas médicas.

GRUPO DE USUARIO	USUARIOS MIEMBROS DEL GRUPO
coordinador recursos	No tiene miembros. Grupo eliminado durante la evaluación.
general medico	cleon (Catalina León Vázquez, doctora) trodriguezm (Tatiana Rodríguez Martínez, secretaria Desarrollo Humano)
exfuncionarios	mcespedesp (Mariela Céspedes Pol, funcionaria de Control Interno) esanchezu (Eduardo Sánchez Ugalde, funcionario archivo Desarrollo Humano)

Tabla N°1. Usuarios con acceso a opciones de menú relacionadas con Citas Médicas
Tomado del Sistema de Desarrollo Humano al 20/01/2014.

Sobre el particular, las Normas de Control Interno, en el Capítulo V: Normas sobre Sistemas de Información, señalan en lo de interés, lo siguiente:

> "5.8 Control de sistemas de información: El jerarca y los titulares subordinados, según sus competencias, deben disponer los controles pertinentes para que los sistemas de información garanticen razonablemente la calidad de la información y de la comunicación, la seguridad y una clara asignación de responsabilidades y administración de los niveles de acceso a la información y datos sensibles, así como la garantía de confidencialidad de la información que ostente ese carácter.
> 5.9 Tecnologías de información: El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y de amplio alcance." (El subrayado no consta en el original)

Por otra parte, el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, en lo de interés señala:

> "1.4.5 Control de acceso: La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:
> /…/
> f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios

de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.
k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI. (El subrayado no consta en el original)

Asimismo, la Política Acceso Lógico del IMAS, POL-EDI-11, publicada en Noviembre 2009, indica al respecto lo siguiente:

"9.1 Lineamientos:
A- Agrupamiento de usuarios: (…)
12. El Área de Tecnologías de Información creará en coordinación con el jefe o coordinador de cada unidad administrativa grupos de usuarios y concederá diferentes niveles de acceso a estos grupos (perfiles), según lo requieran sus funciones laborales.
13. Los usuarios deberán tener razones justificadas para obtener acceso a más información de la que se permita en el grupo al que pertenece, y en ese caso tendrá acceso estrictamente a la información que necesite para realizar sus labores.
14. El Área de Tecnologías de Información le concederá acceso a un usuario cuando el Jefe de Área o un Usuario especializado realice las actividades correspondientes para dicha solicitud. Estas peticiones serán archivadas y servirán de rastro de auditoría en el futuro. El acceso adicional será removido en cuanto el funcionario termine las labores para las cuales necesitaba este acceso.
15. Los dueños de los procesos (Gerentes, Coordinadores y otros funcionarios) son responsables por la revisión periódica de los privilegios otorgados a los funcionarios de su Unidad y debe prontamente revocar aquellos privilegios que ya no son requeridos por los usuarios. La revisión debe llevarse a cabo periódicamente o cuando haya un cambio en la Institución, en los sistemas o en la importancia de los datos.
16. Es responsabilidad del Área de Tecnologías de Información proveer la información necesaria a los dueños de los procesos para realizar la revisión." (El subrayado no consta en el original)

B- Creación y deshabilitación de cuentas de usuarios
17. La unidad de Recursos Humanos será responsable de informar al Área de Tecnologías de Información acerca de la contratación de cualquier funcionario a su área. Éste deberá enviar por escrito el nombre del usuario, fecha de ingreso, descripción de trabajo e información que necesita accesar para realizar sus labores.
18. Cuando un funcionario no labora más para la Institución o es cambiado de área, la unidad de Recursos Humanos deberá informar inmediatamente a al Área de Tecnologías de Información acerca de los cambios, para que se encargue de deshabilitar todas aquellas cuentas que el usuario posea." (El subrayado no consta en el original)

2.2.2. Administración de Cuentas de Usuario del Sistema de Desarrollo Humano

Se encontraron 3 cuentas de usuario activas en el sistema de Desarrollo Humano, correspondientes a personal que se encuentra inactivo, según la base de datos de Desarrollo Humano del IMAS.

No obstante lo anterior, para acceder a la información del sistema de Desarrollo Humano desde un sitio externo a la institución, es necesario tener además un usuario activo en el Active Directory y ninguno de estos usuarios tenían activo el acceso en el Active Directory. Las cuentas de usuario en esta condición pueden ser observadas con detalle en el **Anexo #1**.

La situación descrita es causada por la carencia de controles efectivos para ejecutar la gestión (establecimiento, emisión, suspensión, modificación y cierre) de cuentas de usuario y de los privilegios relacionados con los usuarios y grupos de usuario del sistema de Desarrollo Humano.

Con relación a lo expuesto anteriormente, el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, indica lo siguiente:

> "Capítulo I. Normas de aplicación general:
> 1.4.5 Control de acceso: La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe:
> (…)
> f. Implementar el uso y control de medios de autenticación (identificación de usuario, contraseñas y otros medios) que permitan identificar y responsabilizar a quienes utilizan los recursos de TI. Ello debe acompañarse de un procedimiento que contemple la requisición, aprobación, establecimiento, suspensión y desactivación de tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares." (El subrayado no consta en el original)

Adicionalmente, la Política del IMAS, POL-EDI-11 de Acceso Lógico, publicada en Noviembre 2009, al respecto señala:

> "B- Creación y deshabilitación de cuentas de usuarios
> 18. Cuando un funcionario no labora más para la Institución o es cambiado de área, la unidad de Recursos Humanos deberá informar inmediatamente a al Área de Tecnologías de Información acerca de los cambios, para que se encargue de deshabilitar todas aquellas cuentas que el usuario posea." (El subrayado no consta en el original)

De igual manera, la Política Uso de Palabras Claves del IMAS, POL-EDI-15, aprobada en Noviembre del año 2009, indica lo siguiente:

"29. Todas las claves de acceso relacionadas a un usuario deberán eliminarse en el momento en que el mismo deje de laborar para el IMAS." (El subrayado no consta en el original)

2.2.3. Administración de la Identidad Única de los Usuarios del Sistema de Desarrollo Humano

Se encontraron 7 funcionarios con dos nombres de usuario activos en el Sistema de Desarrollo Humano y que deben tener asignado únicamente una cuenta de usuario. Estos usuarios se indican con detalle en la siguiente tabla:

ID Usuario	Nombre Usuario
aalvarez	ALVAREZ JINESTA ALBERTO FRANCISCO
alavarez	ALVAREZ JINESTA ALBERTO FRANCISCO
lcalvo	CALVO CASTRO MARIA LORENA
LCalvo	CALVO CASTRO MARIA LORENA
denrique	DIAZ ENRIQUEZ MARIA AUXILIADORA
Denriquez	DIAZ ENRIQUEZ MARIA AUXILIADORA
wgamboa	GAMBOA PIZARRO WENDY PATRICIA
wpizarro	GAMBOA PIZARRO WENDY PATRICIA
jmasis	MASIS MASIS JOSE GUIDO
jmasism	MASIS MASIS JOSE GUIDO
GSotoQ	SOTO QUIJANO ADITA GABRIELA
gsotoq	SOTO QUIJANO ADITA GABRIELA
jumana	UMAÑA HERNANDEZ JOSUE ALBERTO
jumaña	UMAÑA HERNANDEZ JOSUE ALBERTO

Tabla N°2. Usuarios con dos nombres de usuario en el Sistema de Desarrollo Humano
Fuente: Sistema de Desarrollo Humano al 20/01/2014.

De acuerdo a lo indicado por el funcionario de Tecnologías de Información, encargado del Sistema de Desarrollo Humano, Lic. Eddy González Rodríguez, el caso de los usuarios 'jmasis' y 'jmasism' puede deberse a la herencia de la configuración anterior del sistema, en el cual los funcionarios de Desarrollo Humano debían tener dos usuarios por sus condiciones especiales de administradores y funcionarios en la utilización del sistema; en el caso de los demás usuarios no se determinó una causa que justifique la situación encontrada.

No obstante, la existencia de dos nombres de usuario asociados a la misma persona, genera el riesgo de incidentes de seguridad y además dificulta el monitoreo de las tareas efectuadas por el usuario dentro de los sistemas.

Sobre el particular, producto de las observaciones realizadas en la conferencia final, la situación descrita fue subsanada, lo cual se verificó durante la revisión que efectuó la Auditoría Interna al 13 de febrero del 2015.

3. CONCLUSIONES

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

3.1. Con respecto a los perfiles de acceso a la información del sistema de Desarrollo Humano, el aspecto más relevante determinado consiste en la ausencia de documentación de aspectos clave en su definición y alcance. Sobre la situación encontrada, es importante recalcar la importancia de que estos se encuentren formalmente documentados de manera que estén disponibles para su consulta y aplicación por parte de los sujetos interesados. Así mismo, es importante que cada modificación que se realice a la definición inicial, quede debidamente documentada y justificada.

3.2. De conformidad con las pruebas realizadas y los resultados obtenidos, se determinó que existen algunas oportunidades de mejora en la gestión de la seguridad del sistema de Desarrollo Humano que es necesario atender, para fortalecer el control interno, en aspectos puntuales como desactivación oportuna de usuarios y la remoción de privilegios de usuario asignados temporalmente .

4. RECOMENDACIONES

DISPOSICIONES LEGALES SOBRE RECOMENDACIONES

Esta Auditoría Interna respetuosamente se permite recordar al Jefe de Tecnologías de Información y al Jefe de Desarrollo Humano, 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, 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 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 JEFE DE DESARROLLO HUMANO

4.1 En conjunto con el área de Tecnologías de Información:

- **a.** Documentar formalmente los perfiles y privilegios de los usuarios del sistema de Desarrollo Humano. (Ver punto 2.1 del acápite de resultados)
- **b.** Efectuar una revisión de los permisos asignados efectivamente a los perfiles de usuario definidos y documentados en la recomendación anterior del presente informe, con el objetivo de que se efectúen las modificaciones necesarias a los derechos efectivos con que estos perfiles cuentan actualmente, en caso de determinar disconformidades con el perfil documentado previamente. (Ver punto 2.2.1 del acápite de resultados)

AL JEFE DE TECNOLOGÍAS DE INFORMACIÓN

4.2 En conjunto con el Área de Desarrollo Humano:

- **a.** Documentar formalmente los perfiles y privilegios de los usuarios del sistema de Desarrollo Humano, con el fin de realizar los aportes técnicos pertinentes. (Ver punto 2.1 del acápite de resultados)
- **b.** Efectuar una revisión de los permisos asignados efectivamente a los perfiles de usuario definidos y documentados en la recomendación anterior del presente informe, con el objetivo de que se efectúen las modificaciones necesarias a los derechos efectivos con que estos perfiles cuentan actualmente, en caso de determinar disconformidades con el perfil documentado previamente. (Ver punto 2.2.1 del acápite de resultados)

4.3 Deshabilitar en el sistema de Desarrollo Humano, así como en Active Directory, las cuentas de usuario pertenecientes al personal inactivo (ex funcionarios) de acuerdo a los registros de la base de datos de Desarrollo Humano. (Ver punto 2.2.2 del acápite de resultados)

4 PLAZOS DE RECOMENDACIONES

Para la implementación de las recomendaciones del informe, fueron acordados con la Administración (titulares subordinados correspondientes) los siguientes plazos y fechas de cumplimiento:

N° REC.	PLAZO	FECHA CUMPLIM.
4.1 a)	10 meses	30/12/2015
4.1 b)	11 meses	30/01/2016

N° REC.	PLAZO	FECHA CUMPLIM.
4.2 a)	10 meses	30/12/2015
4.2 b)	11 meses	30/01/2016
4.3	1 mes	31/03/2015

Hecho por
Licda. Sussan Aguirre Orozco
PROFESIONAL EJECUTORA

Revisado y aprobado
MATI. Wady Solano Siles
ENCARGADO DE PROCESO

AUDITORIA INTERNA
FEBRERO, 2015

INSTITUTO MIXTO DE AYUDA SOCIAL
AUDITORÍA INTERNA

ANEXO #1

CUENTAS DE USUARIO PERTENECIENTES A EXFUNCIONARIOS QUE SE ENCUENTRAN ACTIVAS EN EL SISTEMA DE DESARROLLO HUMANO

Información hasta el 05/11/2013

ID Usuario	Nombre Usuario	FEC SALIDA	ACTIVE DIRECTORY
kcortes	CORTES GOMEZ KAREN TATIANA	25/06/2013	NO
afuentesm	FUENTES MUÑOZ ARACELLY	08/08/2012	NO
nmonge	MONGE HIDALGO NELLY FRANCINI		NO

Fuente: Sistema Desarrollo Humano

Auditoría Interna
FEBRERO, 2015