AUD. 020-2014

INFORME DE LOS RESULTADOS OBTENIDOS EN EL ESTUDIO SOBRE LA SEGURIDAD DE ACCESO A LA INFORMACIÓN DE LOS SISTEMAS SIPO/SABEN

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 Identificación de la Población Objetivo (en adelante SIPO) y del Sistema de Atención de Beneficiarios (en adelante SABEN).

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 de los sistemas SIPO/SABEN, durante el periodo del 01 junio 2012 al 31 de enero del 2013 y se amplió en los siguientes casos:

- En la revisión de usuarios activos en base de datos y en aplicaciones SIPO/SABEN hasta el 11 de marzo 2013.
- En la revisión de casos de personas que no son funcionarios de la institución, que tienen perfiles en el sistema y que pueden autorizar resoluciones hasta el 15 de junio del 2013.

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

[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

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 01 de abril del 2014, se comunicaron los resultados del presente informe a la Máster Mayra Díaz Méndez, Gerente General, al Lic. Juan Carlos Dengo González, Sub Gerente de Desarrollo Social, al Lic. Berny Vargas Mejía, Asesor Jurídico General, al Máster Luis Adolfo González, jefe de Tecnologías de Información y al Lic. José Guido Masís Masís, Jefe Área 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.

Así mismo, en reunión celebrada el día 10 de abril del 2014 con el Gerente del Área Regional de Desarrollo Social Brunca, Lic. Wilberth Antonio Hernandez Vargas, se comunicaron los resultados del presente informe, específicamente en lo relacionado al "*Convenio de cooperación suscrito entre el Instituto Mixto de Ayuda Social y el Centro de Estudios y Capacitación Cooperativa Responsabilidad Limitada (CENECOOP R.L.) para el préstamo de funcionarios o empleados que realicen acciones tendientes al cumplimiento de los fines sociales que establece la Ley 4760*". Las observaciones efectuadas, fueron valoradas por esta Auditoría Interna e incorporadas en el presente informe.

2. RESULTADOS

2.1. Documentación de los perfiles de acceso a SABEN/SIPO

A pesar de que la Auditoría recibió vía correo electrónico el documento "Perfiles de acceso a SIPO.docx", remitido por la Lcda. Silvana Nunnari Saballos, Responsable Técnico de Sistemas de Investigación e Información Social, los perfiles de acceso a SABEN/SIPO aún no han sido documentados formalmente y comunicados a los usuarios que así lo requieren.

Con respecto al documento "Perfiles de acceso a SIPO.docx" mencionado en el párrafo anterior, éste no incluye todos los perfiles creados en la base de datos para SIPO, ni establece de forma clara, cuáles accesos de aplicación deberían tener cada perfil y cuáles puestos, según el Manual de Cargos, están ligados a cada perfil. Adicionalmente, no cuenta con la aprobación de la Gerencia General y por lo tanto, tampoco ha sido comunicado formalmente.

[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

Es importante mencionar que mediante el acuerdo de Consejo Directivo Nº 067-02-2013, del 18 de febrero 2013, se otorgó a la Gerencia General y Subgerencia de Desarrollo Social, un plazo de 60 días (el cual venció el 22 de mayo del 2013) para el cumplimiento de la documentación de los perfiles con su respectiva relación con los usuarios, según el Manual del Cargos vigente en la institución, fecha de actualización del documento, depuración y comunicación formal del mismo; sin embargo, a la fecha no se tiene la documentación.

De conformidad con el seguimiento efectuado, mediante el oficio GG 1793-09-2013, del 18 de setiembre del 2013, la Gerente General, Msc. Mayra Díaz Méndez indicó que los perfiles de acceso a SIPO y perfiles de acceso a SABEN "(...) *se encuentran en estos momentos en revisión por parte de las unidades de Planificación y Asesoría Jurídica, una vez que se tengan las revisiones correspondientes, la Gerencia traslada el documento a la Unidad correspondientes para que realice los ajustes que correspondan. Dicha Unidad una vez realizado los ajustes, deberá trasladar el documento con los ajustes, (Versión Final del Documento) a la Gerencia para su revisión y aprobación"*. Posteriormente mediante oficio SIIS-10-2013, suscrito por la Lcda. Silvanna Nunnari Saballos, como responsable técnico de la secretaría técnica de Sistemas de Información Social, se hace del conocimiento de la Gerente General que: "*…las nuevas funciones para adaptar los perfiles deben contar con la aprobación por parte del área de Desarrollo Humano así como del Consejo Directivo, y de acuerdo con la nueva estructura, ya que esto da origen a la creación de nuevos cargos"*.

No obstante las gestiones realizadas, al 19 de marzo del 2014 no se tiene conocimiento del avance de la revisión y aprobación de los documentos mencionados.

La carencia de documentación sobre la definición de perfiles en los sistemas evaluados, limita el proceso de administración y control de los perfiles, pues no se tiene una base clara sobre cual es la asignación correcta de privilegios a los diferentes perfiles definidos en los sistemas.

Según lo indicado por la Lcda. Silvanna Nunnari Saballos, Responsable Técnico de Sistemas de Investigación e Información Social, la documentación de perfiles no se ha realizado debido a varios factores, entre ellos el programa de trabajo del área que coordina, correspondiente al inicio de año, el cual estuvo saturado de actividades urgentes, definición concreta de responsables de administración del SIPO por parte de las instancias superiores y varios cambios que se generaron producto de la reestructuración organizacional.

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." (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 SIPO/SABEN.

2.2.1. Administración de cuentas de usuario de la base de datos SIPO/SABEN

Se identificaron 67 cuentas de usuario activas en la base de datos de SIPO/SABEN, correspondientes a personal que según la base de datos de Desarrollo Humano del IMAS, se encuentra inactivo. La lista de estas 67 cuentas de usuario se puede apreciar con detalle en el **Anexo #1**.

Para acceder a la información del sistema SABEN desde un sitio externo a la institución, es necesario tener además un usuario activo en el Active Directory; sobre particular, se determinó que 4 usuarios de los 67 indicados en el párrafo anterior, tienen activo el acceso en el Active Directory, incrementando así el riesgo de acceso no autorizado y de aprobación de transacciones no autorizadas, por personas que ya no forman parte del personal interno o externo de la Institución, pero que mantiene derechos de acceso a los sistemas y bases de datos.

Las personas que mantienen cuenta de usuario activa en SABEN y que además mantienen cuenta en Active Directory, son las siguientes:

USUARIO	NOMBRE	APELLIDO 1	APELLIDO 2	INSTITUCIÓN	PERFIL	FEC SALIDA
elmermp	ELMER	MONDRAGON	PRIETO	IMAS	Epis_sab	04/08/2008
enidaf	ENID	ABARCA	FLORES	IMAS	Tecnicos_Financieros	13/09/2007
josevb	JOSE	VILLALOBOS	BALLESTERO	IMAS	Profesional_Ejecutor	02/06/2009
marjoriesv	MARJORIE	SALAS	VILLALOBOS	ASEDEMASA	Digitadores	25/12/2010

Lo anterior, es causado por la carencia y claridad de lineamientos y controles efectivos para ejecutar la gestión (establecimiento, emisión, suspensión, modificación y cierre) de cuentas de usuario y de los privilegios relacionados con los usuarios internos y externos del SIPO y SABEN.

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)

2.2.2. Administración de contraseñas para los usuarios SABEN/SIPO

Se identificó que las contraseñas de acceso para los sistemas SIPO y SABEN, se asignan inicialmente de forma temporal por el Administrador de Base de Datos y estos sistemas no obligan a su modificación durante el primer ingreso al sistema, por lo que el usuario puede mantener indefinidamente dicha contraseña (la contraseña temporal) para acceder a los sistemas. Según análisis efectuado en la base de datos del SIPO/SABEN, se comprobó que los usuarios del sistema no tienen la práctica de modificar periódicamente sus contraseñas, algunas de las cuales datan incluso del año 2000. Lo anterior, a pesar de lo indicado en la política POL-EDI-15, Política de uso de palabras claves, punto 18, el cual indica:

"Cuando se crea un nuevo usuario en alguno de los sistemas, el Área de Desarrollo Informático asigna una contraseña temporal, la cual debe ser modificada la primera vez que el usuario ingrese al sistema." (El subrayado no consta en el original)

La situación indicada, aumenta la probabilidad de que se revelen las claves de acceso y que se produzcan accesos no autorizados a los sistemas SIPO/SABEN, los cuales eventualmente pueden tener consecuencias de alto impacto, como pérdidas de información y otras que afecten la capacidad de operación de la Institución.

La causa principal de dicha situación, obedece a que no se ha advertido a los usuarios de los riesgos en el uso de contraseñas y seguridad de los sistemas. Asimismo, la situación es motivada por la ausencia de un control automático en las aplicaciones computarizadas, que obliguen a los usuarios a renovar sus contraseñas periódicamente.

Esta situación causa el incumplimiento de la política: Uso de Palabras Claves del IMAS (POL-EDI-15, aprobada en Noviembre 2009), para la aplicación de la seguridad, con respecto al uso y administración de contraseñas.

Sobre el particular, las Normas de Control Interno, 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 otro lado, el Manual de Normas Técnicas para la Gestión y Control de las Tecnologías de Información, indica:

> "1.4.2 Compromiso del personal con la seguridad de la información. "El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe:
> a. Informar y capacitar a los empleados sobre sus responsabilidades en materia de seguridad, confidencialidad y riesgos asociados con el uso de las TI.
> b. Implementar mecanismos para vigilar el debido cumplimiento de dichas responsabilidades.
> (…)

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."

2.2.3. Administración de la identidad única de los usuarios de base de datos SIPO/SABEN

Se identificaron 6 funcionarios con dos nombres de usuario activos y que por sus funciones y el perfil al que pertenecen, deben tener asignado únicamente una cuenta de usuario.

Adicionalmente, se identificaron 7 usuarios genéricos que ya no se utilizan y que aún se encuentran activos en la base de datos.

Es importante mencionar que durante la realización del estudio, específicamente el día 24 de abril del año 2013, ambas situaciones fueron corroboradas y corregidas por el Administrador de Base de Datos, Bach. Carlos González Quesada.

2.2.4. Usuarios de SIPO que tienen asignado un perfil de usuario SABEN

Se identificó la existencia de 28 usuarios del sistema SIPO que fueron "matriculados" en el sistema SABEN y por lo tanto, tienen asociado un perfil de usuario de acuerdo con la Tabla de Límites de Autoridad Financiera. Es importante mencionar que en su mayoría, estos usuarios tienen perfil de consulta o digitador.

De acuerdo con la validación realizada con la Licda. Silvanna Nunnari Saballos, Responsable Técnico de Sistemas de Información e Investigación Social, con el Lic. Carlos Barberena Galvez, analista de Sistemas de Información y con el Bach. Carlos González Quesada, Administrador de Base de Datos, estos usuarios no deberían tener asociado un perfil de usuario en el SABEN, debido a que por sus funciones no lo necesitan. La lista de usuarios en esta condición puede apreciarse en el **Anexo #2**.

Adicionalmente, según lo indicado por la Licda. Nunnari Saballos, y por el Bach. González Quesada y de conformidad con la evidencia recolectada por esta Auditoría, el Area de Desarrollo Humano, en ocasiones no comunica oportunamente a los funcionarios del área de Sistemas de Información Social o de Tecnologías de Información, encargados de habilitar y

deshabilitar usuarios, cuando una persona cambia de puesto. Cuando esta comunicación es oportuna, el profesional (tanto del área de Sistemas de Información e Investigación Social como de Tecnologías de Información) debe estar pendiente de las fechas de vencimiento de cada asignación para modificarla manualmente.

Cuando por sus funciones, un usuario del sistema SIPO debe estar "matriculado" en el sistema SABEN (para efectos de visualizar información, básicamente), este debe de asignarse al perfil de acceso "*Técnico Social*", el cual se constituye en el perfil de menor privilegio y por lo tanto, no tiene derechos sobre las autorizaciones, de acuerdo con la Tabla de Límites de Autoridad Financiera

Los usuarios en esta condición son los siguientes:

USUARIO BD	NOMBRE	APELLIDO 1	APELLIDO 2	NOM GERENCIA	PERFIL BASE DATOS	PERFIL_SABEN
gsandoval	GUADALUPE	SANDOVAL	SANDOVAL	ARDS NORESTE	Supervisores	SUBGERENTE DESARROLLO SOCIAL
yadirapp	ANA	PIZARRO	PALMA	ARDS HEREDIA	Epis_sab	GERENTE REGIONAL
ivaniaaa	IVANIA	ARGUELLO	ABARCA	HUETAR ATLANTICA	Epis_sab	GERENTE REGIONAL
silvannan	SILVANA	NUNNARI	SABALLOS	NIVEL CENTRAL	Supervisores	GERENTE REGIONAL
yadelyac	YADELY	ABARCA	CUBILLO	ARDS CHOROTEGA	Epis_sab	GERENTE REGIONAL

Si bien es cierto, un usuario puede acceder a la aplicación en aquellas opciones de menú que el perfil de base de datos le permita, el tener habilitados otros privilegios que no está ocupando, podría generar información confusa sobre los accesos reales que tiene o debe tener un usuario. Así mismo, un usuario que tenga asociado un perfil con mayores privilegios de acceso o diferente del que debe tener, podría accesar, accidental o intencionalmente, a la información y realizar transacciones importantes que en definitiva no le corresponden.

Lo anteriormente expuesto, se origina en la ausencia de documentación de los perfiles de base de datos y la revisión periódica de esos perfiles.

Con relación a lo expuesto, 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:
> (…)
> 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.

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

> "9.1 Lineamientos:
> A- Agrupamiento de usuarios: (…)
> 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. (…)
> 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.

2.3. Acceso a la información SIPO/SABEN

2.3.1. Existencia de usuarios con perfiles en SABEN distintos al cargo que desempeñan.

Se identificó la existencia de 8 funcionarios con perfiles en el sistema SABEN que según el cargo que ostentan (con base en el Manual de Cargos vigente en la institución), tienen asignado un perfil que no corresponde con el cargo que desempeñan. Lo anterior, de conformidad con la prueba realizada y la validación efectuada con la Licda. Silvanna Nunnari Saballos, Responsable Técnico de Sistemas de Información e Investigación Social.

Los funcionarios que tienen asignado un perfil que no corresponde con el cargo que ocupan en la institución son los siguientes:

FUNCIONARIO	PERFIL SIPAS	ESTADO DH	DESCRIP. CARGO	LUGAR TRABAJO
MEJIAS SANCHEZ JAMILETH MARIA DEL C	Tecnicos_Financieros	Activo	PROFESIONAL EN CONTABILIDAD	CONTABILIDAD
SANDOVAL SANDOVAL GUADALUPE	Gerentes_SAB	Activo	JEFE DE CONTROL INTERNO	CONTROL INTERNO
VARGAS VARELA LUIS ALBERTO	Tecnicos_Financieros	Inactivo	TRABAJADOR CALIFICADO 2	GER. REG. NORESTE
CHAVES BOLAÑOS MARYI VANESSA	Profesional_Ejecutor	Inactivo	TECNICO GENERAL 3,(I.B.S.)	CEDES HEREDIA
MOYA HIDALGO DIEGO	Profesional_Ejecutor	Activo	ASISTENTE GER. GEN. Y SUBGERENCIAS	SUB-GERENCIA DESARROLLO SOCIAL
QUIROS CAMACHO JEANNETE	Profesional_Ejecutor	Activo	ENCUESTADOR/DIGITADOR	U.L.D.S. PAVAS
SOLANO VALVERDE NIDYA	Profesional_Ejecutor	Activo	PROF. LIC. EN EVAL. Y SEG. DE PROGRAMAS	PROGRAMA AVANCEMOS
SOLORZANO FERNANDEZ LUCIA	Profesional_Ejecutor	Inactivo	PROF.ASESOR EQUIP.PROG.DES.SOC	CEDES ALAJUELA

La existencia de usuarios con accesos a perfiles que no corresponde a sus funciones, permite el eventual ejercicio de actividades que se encuentran fuera del rango de sus competencias.

Así mismo, la existencia de usuarios con accesos a perfiles que no corresponden a sus funciones, podría generar una incorrecta segregación de funciones, la cual se materializa cuando dentro de los privilegios de acceso asignados existen tareas que se complementan entre sí para realizar una operación.

Lo anteriormente expuesto, inobserva lo indicado en el punto 2.5.3, de las Normas de Control Interno, el cual indica:

> "2.5.3 Separación de funciones incompatibles y del procesamiento de transacciones: El jerarca y los titulares subordinados, según sus competencias, deben asegurarse de que las funciones incompatibles, se separen y distribuyan entre los diferentes puestos; así también, que las fases de autorización, aprobación, ejecución y registro de una transacción, y la custodia de activos, estén distribuidas entre las unidades de la institución, de modo tal que una sola persona o unidad no tenga el control por la totalidad de ese conjunto de labores. Cuando por situaciones excepcionales, por disponibilidad de recursos, la separación y distribución de funciones no sea posible debe fundamentarse la causa del impedimento. En todo caso, deben implantarse los controles alternativos que aseguren razonablemente el adecuado desempeño de los responsables." (El subrayado no consta en el original)

Así mismo, el punto 5.8, Capítulo V: Normas sobre Sistemas de Información, indica 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)

Adicionalmente, el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, en el punto 1.4.5, señala lo siguiente:

> "1.4.5. Control de Acceso: La organización debe proteger la información de accesos no autorizados. Para dicho propósito debe: (…)

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. (…)" (el subrayado no consta en el original)

2.3.2. Procedimiento para modificar el acceso a los perfiles de base de datos SABEN/SIPO

Se carece de controles automatizados para la administración, control y revisión regular del estado de las cuentas de usuario de funcionarios internos y externos. Sobre este particular, el sistema SABEN no permite identificar de manera automática cuando se vence el período de un nombramiento temporal y los derechos de acceso del usuario deben removerse de forma manual una vez finalizado el período.

Ante la ausencia de un procedimiento formalmente establecido, se ha adoptado la práctica de realizar una revisión manual de las cuentas de usuarios. Esta consiste en validar visualmente la lista de usuarios registrados en la base de datos SIPO/SABEN, contra la lista de funcionarios de la institución y se ejecuta de forma manual, ya que no existe forma de realizar la asociación automática a través de un identificador único por que el formato de la base de datos de Desarrollo Humano y la base de datos del sistema SIPO/SABEN es diferente. No obstante, esta práctica no se aplica periódicamente.

Adicionalmente, el área de Desarrollo Humano, en ocasiones no comunica oportunamente a los funcionarios del área de Sistemas de Información Social o de Tecnologías de Información, encargados de habilitar y deshabilitar usuarios, cuando una persona cambia de puesto. Cuando esta comunicación es oportuna, el profesional (tanto del área de Sistemas de Información e Investigación Social como de Tecnologías de Información) debe estar pendiente de las fechas de vencimiento de cada asignación para modificarla manualmente.

Esta modificación manual del estado de las cuentas de usuario y no recibir de forma oportuna la comunicación sobre el estado de un colaborador interno o externo, podría ocasionar que eventualmente se dejen de lado accesos que debían ser atendidos y regresados a su condición anterior, o que no sean asignados los permisos, conforme las funciones del personal, establecidos con claridad en el Manual de Cargos vigente en la institución.

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)

2.4. Administración de convenios de cooperación para el préstamo de funcionarios al IMAS.

Se identificaron las siguientes situaciones con respecto a los convenios que el IMAS suscribió con las cooperativas COOPELESCA R.L y CENECOOP R.L.:

- Si bien, la cláusula décimo tercera de ambos convenios se refiere al tema de la solución de diferencias, rescisión, resolución y finiquito, no se identifica claramente cuál es el proceso a seguir en caso de que una de las partes desee rescindir el convenio durante su vigencia, cuando el caso de recisión sea diferente al de solución de conflictos, como lo es por ejemplo el incumplimiento de alguna de las partes de lo establecido en el convenio.

- Los convenios suscritos entre el IMAS y las empresas que prestan funcionarios para el estudio y aprobación de beneficios, no especifican el cargo que va a desempeñar el funcionario que estará a préstamo.

  Al respecto, el Lic. José Guido Masís Masís, jefe de Desarrollo Humano, indicó que la situación comentada dificulta al área de Desarrollo Humano realizar la identificación y solicitud de atestados, de acuerdo al cargo que la persona va a desempeñar, así mismo indica que la situación ha sido comentada a la Gerencia General en diferentes ocasiones,

tanto en forma verbal como mediante oficio (como es el caso del DH-1711-09-2012, con fecha del 24 de setiembre de 2012).

En el mismo orden de ideas, el Lic. Berny Vargas Mejías, Asesor Jurídico de la Institución, indicó a esta Auditoría que en distintas ocasiones se ha comentado el tema de manera verbal con las partes involucradas. Así mismo, indicó que mediante oficio AJ-0566-05-2013 con fecha del 20 de mayo del 2013, se recomendó al Presidente Ejecutivo en ese momento, Dr. Fernando Marín Rojas, lo siguiente:

> "Esta Asesoría Jurídica ha estado confeccionando los convenios de préstamo de funcionarios con las empresas que esa Presidencia Ejecutiva ha instruido y que previamente se han coordinado por su persona o por el Licenciado Roy Vargas Solano, sin embargo operativamente es necesario solicitarle, que en la misma instrucción que se hace a esta Instancia Asesora se consigne el cargo que presuntamente ocuparía el funcionario prestado y el lugar en que desarrollará sus funciones a lo interno del IMAS./ Lo anterior porque al momento de remitir el convenio firmado a Desarrollo Humano, para que proceda a corroborar si los atestados del interesado se adecúan a un puesto en el IMAS, se ha evidenciado que no se ha sabido el cargo a equiparar, consecuentemente no se ha podido determinar si los atestados son o no suficientes./Lo anterior tiene un efecto jurídico importante, porque el IMAS podría estar extralimitando las funciones de estos funcionarios, por lo que se espera su respuesta para mitigar el riesgo."

Con relación al oficio precitado, el Asesor Jurídico General indicó que al 09 de abril del presente año, no se había recibido respuesta por parte del señor ex-Presidente Ejecutivo.

En relación con lo indicado por el señor Asesor Jurídico en el oficio de cita, en el sentido de que es necesario que se verifique si los atestados de los funcionarios que vienen a laborar al IMAS en calidad de préstamo, cumplen con los requisitos para el cargo que van a desempeñar, el pronunciamiento vertido por la Procuraduría General de la República, vertido mediante oficio C-229-2011, del 13 de setiembre de ese año, indica en lo de interés lo siguiente:

> "…/De ahí que la Administración Pública, incluida la del IMAS, se encuentra facultada para reclutar trabajadores sociales o de otras

> disciplinas para que laboren como funcionarios ad honorem de la institución./ Lo que sí es importante mencionar es que los requisitos establecidos en el ordenamiento jurídico para ocupar el cargo en mención, deben observarse independientemente del carácter remunerado o no del nombramiento"

Como puede observarse, efectivamente resulta necesario que al materializar el acuerdo de préstamo de un colaborador para que ejecute labores como funcionario del IMAS, se conozca el cargo que va a desempeñar, de forma que previo a entrar en funciones sea posible verificar que la persona cumple con los requisitos establecidos por el ordenamiento jurídico para ocupar el cargo en mención.

- De acuerdo con información suministrada por el Lic. Wilberth Antonio Hernandez Vargas, Gerente del Área Regional de Desarrollo Social Brunca, las funcionarias a préstamo mediante el convenio con la empresa CENECOOP R.L., ofrecieron servicio en el IMAS hasta el mes de diciembre del año 2012 y no existe un documento formal donde la empresa CENECOOP R.L. comunique al IMAS que no podía continuar enviando a las funcionarias prestadas a través del convenio por falta de presupuesto, sino que la comunicación fue realizada de manera verbal. Dicho convenio tiene una vigencia de un año, la cual venció en agosto del 2013; sin embargo, es prorrogable automáticamente por periodos iguales, salvo que las partes dispongan no continuarlo con expresa indicación dentro del último mes antes de que opere la prórroga.

  Sobre este particular, es importante mencionar que el 30 de abril del año en curso, mediante oficio ARDSB-09-0220-04-2014, el Lic. Hernández Vargas remitió a la Subgerencia de Desarrollo Social, el informe requerido de acuerdo con lo establecido en la cláusula Décimo Tercera del Convenio con la empresa CENECOOP R.L., para su resolución, recisión o finiquito, según corresponda.

- La funcionaria prestada al IMAS mediante convenio suscrito con la empresa CENECOOP R.L., Cindy María Gómez Ortiz, ya no labora para la entidad debido a lo indicado en el párrafo anterior. Sin embargo, ésta Auditoría comprobó que su usuario en SIPO/SABEN continúa activo en el perfil "*Profesional_Ejecutor*". Dicha situación genera una probabilidad de que se materialice el riesgo de fraude o acceso a información de SIPO/SABEN por personal no autorizado, debido a que ya no forma parte del personal interno o externo de la Institución, pero mantiene derechos de acceso a los sistemas, base de datos y Active Directory.

Al respecto, el Manual de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, sobre el particular indica lo siguiente:

"Capítulo I. Normas de aplicación general:
1.4.2 Compromiso del personal con la seguridad de la información. El personal de la organización debe conocer y estar comprometido con las regulaciones sobre seguridad y confidencialidad, con el fin de reducir los riesgos de error humano, robo, fraude o uso inadecuado de los recursos de TI. Para ello, el jerarca, debe:
(…)
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos
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 de Acceso Lógico del IMAS - POL-EDI-11, publicada en Noviembre 2009, al respecto señala:

"B- Creación y deshabilitación de cuentas de usuarios: (…)
19. La unidad de Recursos Humanos será responsable de avisar mediante orden de Área de Desarrollo Informático 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.
20. 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 Desarrollo Informático acerca de los cambios, para que se encargue de deshabilitar todas aquellas cuentas que el usuario posea." (El subrayado no consta en el original)

Así mismo, en el "*Convenio de cooperación suscrito entre el Instituto Mixto de Ayuda Social y el Centro de Estudios y Capacitación Cooperativa Responsabilidad Limitada (CENECOOP R.L.) para el préstamo de funcionarios o empleados que realicen acciones tendientes al cumplimiento de los fines sociales que establece la Ley 4760*" , se indica lo siguiente en las cláusulas:

"Décima Tercera: De la solución de diferencias, rescisión, resolución y finiquito. (…)

Sea para la rescisión, la resolución o el finiquito, será necesario que la Subgerencia de Desarrollo Social cuente con un informe del titular subordinado encargado de verificar el cumplimiento de las obligaciones del convenio que así lo recomiende.
(…)
Décima Quinta: De la vigencia. El plazo de vigencia para la presente relación jurídica es de un año, prorrogable automáticamente por períodos iguales, según acuerdo de las partes, salvo que dispongan no continuarlo con expresa indicación dentro del último mes de que opere la prórroga."

3. CONCLUSIONES

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

3.1. De conformidad con las pruebas realizadas y los resultados obtenidos, se determinó que existen algunas deficiencias en la gestión de la seguridad de los sistemas de información SIPO/SABEN, que es necesario subsanar para fortalecer el control interno en la gestión de la seguridad de la información.

3.2. Con respecto a la definición y alcance de los perfiles de acceso a la información de los sistemas SIPO/SABEN, 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 las áreas interesadas. Así mismo, es importante que cada modificación que se realice a la definición inicial, quede debidamente documentada y justificada.

3.3. De acuerdo a las pruebas realizadas y los resultados obtenidos, la asignación y alcance de los perfiles SIPO/SABEN es razonable, salvo algunas situaciones específicas determinadas con algunos usuarios del sistema SIPO "matriculados" en el sistema SABEN y funcionarios con perfil de mayores privilegios al que deberían de tener.

3.4. Finalmente, con respecto a los convenios de cooperación para el préstamo de funcionarios al IMAS, existen aspectos que se considera conveniente subsanar, para garantizar razonablemente que se cumple con los requerimientos que el ordenamiento jurídico impone para formalizar y gestionar estas iniciativas de cooperación.

4. RECOMENDACIONES

DISPOSICIONES LEGALES SOBRE RECOMENDACIONES

Esta Auditoría Interna respetuosamente se permite recordar a la Gerente General, al Subgerente de Desarrollo Social, al Asesor Jurídico, al Jefe de Tecnologías de Información y al Jefe del Area 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 CONSEJO DIRECTIVO

4.1. Disponer que en los convenios de préstamo de funcionarios al Instituto, se indique expresamente el cargo y el lugar donde desempeñaría sus actividades el funcionario a préstamo.

A LA GERENTE GENERAL

4.2. Tramitar en un plazo no mayor de 30 días, los documentos correspondientes a la documentación de los Perfiles de Acceso del Sistema SABEN y del Sistema SIPO, con el fin de dar cumplimiento a la recomendación 4.5 del AUD 027-2010, instruido mediante acuerdo de Consejo Directivo Nº 067-02-2013, del 18 de febrero 2013 y en el que se otorgó un plazo de 60 días el cual venció el 22 de mayo del año 2013. (Ver punto 2.1 del acápite de resultados)

AL SUBGERENTE DE DESARROLLO SOCIAL

4.3. Concordar el perfil de acceso de aquellos funcionarios que de acuerdo a sus funciones y a la Tabla de Límites de Autoridad Financiera, tienen asociado en el sistema SABEN un perfil de usuario con mayores privilegios al que deben tener. (Ver punto 2.2.4 del acápite de resultados).

4.4. Asignar el perfil correcto que deben tener, de acuerdo al cargo y funciones que desempeñan, los usuarios descritos en el punto 2.3.1 del acápite de resultados del presente informe.

4.5. Realizar las gestiones que correspondan con relación al "*Convenio de cooperación suscrito entre el Instituto Mixto de Ayuda Social y el Centro de Estudios y Capacitación Cooperativa Responsabilidad Limitada (CENECOOP R.L.) para el préstamo de funcionarios o empleados que realicen acciones tendientes al cumplimiento de los fines sociales que establece la Ley 4760*". (Ver punto 2.4 del acápite de resultados)

AL JEFE DE TECNOLOGÍAS DE INFORMACIÓN

4.6. Deshabilitar en la base de datos SABEN/SIPO, 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 2.2.1 del acápite de resultados)

4.7. Implementar controles automáticos en los sistemas SABEN/SIPO, que obliguen al usuario a realizar el cambio de contraseña de forma periódica. (Ver punto 2.2.2 del acápite de resultados)

4.8. Deshabilitar del registro de usuarios activos de SABEN, aquellos funcionarios que son usuarios de SIPO y que por sus funciones no deben estar matriculados en SABEN. (Ver punto 2.2.4 del acápite de resultados).

4.9. Establecer en la aplicación SABEN, controles que deshabiliten de forma oportuna, la asignación temporal de privilegios con base en una fecha de finalización de los mismos. (Ver punto 2.3.2 del acápite de resultados)

4.10. Deshabilitar en el Active Directory y en la base de datos SABEN/SIPO, la cuenta de usuario perteneciente a Cindy María Gómez Ortiz, funcionaria prestada mediante convenio con la empresa CENECOOP R.L. (Ver punto 2.4 del acápite de resultados)

AL JEFE DEL ÁREA DE DESARROLLO HUMANO

4.11. Comunicar oportunamente a las áreas responsables de la asignación y reasignación de privilegios de acceso a las aplicaciones (Sistemas de Investigación e Información Social y Tecnologías de Información), cuando una persona ingresa a la institución o se cambia de puesto. (Ver punto 2.3.2 del acápite de resultados)

5. 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.
4.2	30 días	30/06/2014
4.3	90 días	31/08/2014
4.4	90 días	31/08/2014
4.5	90 días	31/08/2014
4.6	30 días	30/06/2014
4.7	90 días	31/08/2014
4.8	30 días	30/06/2014
4.9	90 días	31/08/2014
4.10	10 días	30/05/2014
4.11	60 días	31/07/2014

Hecho por
Licda. Sussan Aguirre Orozco
PROFESIONAL EJECUTORA

Revisado y aprobado
MATI. Wady Solano Siles
ENCARGADO DE PROCESO

AUDITORIA INTERNA
MAYO 2014

INSTITUTO MIXTO DE AYUDA SOCIAL
AUDITORÍA INTERNA

ANEXO #1

EXFUNCIONARIOS QUE SE ENCUENTRAN ACTIVOS EN LA BASE DE DATOS SABEN/SIPO
Información hasta el 11/03/2013

USUARIO	NOMBRE	APELLIDO 1	APELLIDO 2	INSTITUCIÓN	PERFIL	FEC SALIDA
elmermp	ELMER	MONDRAGON	PRIETO	IMAS	Epis_sab	04/08/2008
enidaf	ENID	ABARCA	FLORES	IMAS	Tecnicos_Financieros	13/09/2007
josevb	JOSE	VILLALOBOS	BALLESTERO	IMAS	Profesional_Ejecutor	02/06/2009
marjoriesv	MARJORIE	SALAS	VILLALOBOS	ASEDEMASA	Digitadores	25/12/2010
adrianavm	ADRIANA	VALVERDE	MORA	IMAS	Profesional_Ejecutor	01/11/2008
amarilysbe	AMARILYS	BARRANTES	ENRIQUEZ	IMAS	Asistente_Adm_Cedes	07/09/2010
anaas	ANA	ARCE	SANDI	MUNICIPALIDAD DE CARTAGO	Digitadores	15/05/2012
anaas	ANA	ARCE	SANDI	MUNICIPALIDAD DE CARTAGO	Digitadores	15/05/2012
anacs	ANA	CAMACHO	SANCHEZ	IMAS	Profesional_Ejecutor	16/12/2007
bayardopg	BAYARDO	PEREZ	GONZALEZ	IMAS	Profesional_Ejecutor	01/03/2007
bernysb	BERNY	SANCHEZ	BALLESTERO	IMAS	Profesional_Consultor	30/08/2005
carmenab	CARMEN	ARGUELLO	BOGANTES	IMAS	Tecnicos_Administrativos	24/10/2008
cesarab	CESAR	ARRIETA	BRIZUELA	IMAS	Tecnicos_Administrativos	01/10/2009
cinthiapm	CINTHIA	POVEDA	MEDINA	IMAS	Asistente_Adm_Cedes	01/02/2010
dayanacs	DAYANA	CARMONA	SANCHEZ	IMAS	Profesional_Ejecutor	01/01/2010
dayannapu	DAYANNA	PIEDRA	UGARTE	IMAS	Tecnicos_Administrativos	24/01/2010
diegovl	DIEGO	VIQUEZ	LIZANO	IMAS	Profesional_Consultor	15/03/2007
efrenrg	EFREN	RODRIGUEZ	GONZALEZ	IMAS	Profesional_Ejecutor	02/08/2007
erickvr	ERICK	VALERIO	RAMIREZ	IMAS	Digitadores	15/04/2006
evelynlh	EVELYN	LOPEZ	HERNANDEZ	IMAS	Profesional_Ejecutor	11/05/2006
evelynvs	EVELYN	VARGAS	SALAZAR	IMAS	Digitadores	17/08/2007
franciscohh	FRANCISCO	HERNANDEZ	HERNANDEZ	IMAS	digitador_imas	30/04/2012
franciscohh	FRANCISCO	HERNANDEZ	HERNANDEZ	IMAS	digitador_imas	30/04/2012
franciscome	FRANCISCO	MADRIGAL	ESQUIVEL	IMAS	Tecnicos_Financieros	21/01/2009
gloriajr	GLORIA	JIMENEZ	RAMIREZ	IMAS	Consulta	30/10/2009
guillermocc	GUILLERMO	CAMPOS	CRUZ	IMAS	digitador_imas	04/06/2008
hanniaav	HANNIA	ARIAS	VALVERDE	IMAS	Consulta	14/08/2007

USUARIO	NOMBRE	APELLIDO 1	APELLIDO 2	INSTITUCIÓN	PERFIL	FEC SALIDA
hanniarc	HANNIA	ROJAS	CASTRO	IMAS	Tecnicos_Administrativos	01/04/2008
heidyvl	HEIDI	VILLEGAS	LOPEZ	IMAS	Asistente_Adm_Cedes	04/07/2006
ivanmp	IVAN	MORA	POVEDA	IMAS	Consulta	30/11/2007
ivanniasr	IVANNIA	SANABRIA	RIVERA	IMAS	Profesional_Ejecutor	31/05/2007
jannethss	JANNETH	SWEILL	SWEILL	IMAS	Digitadores	01/12/2004
jeannettere	JEANNETTE	RAMIREZ	ESQUIVEL	IMAS	Profesional_Ejecutor	15/10/2006
jessicagq	JESSICA	GRANADOS	QUESADA	IMAS	Profesional_Ejecutor	12/12/2006
jorgerl	JORGE	RODRIGUEZ	LOPEZ	IMAS	Asistente_Adm_Cedes	16/11/2006
josegm	JOSE	GONZALEZ	MONTIEL	IMAS	Presupuesto	15/05/2008
juaname	JUANA	MEMBREÑO	ESCALANTE	IMAS	Tecnicos_Administrativos	31/03/2008
karinavd	KARINA	VALLE	DIAZ	IMAS	Digitadores	01/10/2007
karlavar	KARLA	VASQUEZ	RODRIGUEZ	HOLCIM	Digitadores	15/03/2004
laurabm	LAURA	BOGANTES	MORA	IMAS	Consulta	22/12/2006
lauraba	LAURA	BRENES	ALFARO	IMAS	Profesional_Ejecutor	01/02/2009
lillianhv	LILLIAN	HERRERA	VILLALOBOS	IMAS	Profesional_Ejecutor	01/01/2009
luciasf	LUCIA	SOLORZANO	FERNANDEZ	IMAS	Profesional_Ejecutor	16/11/2008
marcoag	MARCO	ARCE	GAMBOA	IMAS	Consulta	16/06/2008
margaritafg	MARGARITA	FERNANDEZ	GARITA	IMAS	fideicomiso	01/06/2011
mariaac	MARIA	ALVAREZ	CANTON	IMAS	Consulta	23/10/2007
mariarga	MARIA	GARRO	ABARCA	IMAS	Asistente_Adm_Cedes	18/03/2008
maritzamh	MARITZA	MARIN	HERRERA	IMAS	Profesional_Ejecutor	16/01/2008
marolyncp	MAROLYN	CARRILLO	PERALTA	IMAS	Tecnicos_Administrativos	24/11/2006
nellyce	NELLY	CASTILLO	ESPINOZA	IMAS	Asistente_Adm_Cedes	09/10/2007
patriciabv	PATRICIA	BALTODANO	VASQUEZ	IMAS	Profesional_Ejecutor	25/02/2011
raulpm	RAUL	PEREZ	MORALES	IMAS	Tecnicos_Administrativos	15/06/2009
rebecaaj	REBECA	ARGUEDAS	JIMENEZ	IMAS	Digitadores	03/03/2006
robertohg	ROBERTO	HENRIQUEZ	GUTIERREZ	CENTRO INT. DE INVERSIONES CIISA	Digitadores	10/01/2005
sandrabv	SANDRA	BOLIVAR	VARGAS	IMAS	Profesional_Consultor	01/11/2009
silviabb	SILVIA	BOLAÑOS	BOLAÑOS	IMAS	grp_archivistica	30/03/2008
sofiamu	SOFIA	MARTINEZ	UREÑA	IMAS	Profesional_Ejecutor	23/05/2006
sofiazv	SOFIA	ZUÑIGA	VALERIO	IMAS	Profesional_Ejecutor	18/09/2009
susanass	SUSSY	ARIAS	HERNANDEZ	IMAS	Digitadores	01/01/2009
vanessachb	VANESSA	CHAVEZ	BOLAÑOS	IMAS	Profesional_Ejecutor	06/09/2008
wendygp	WENDY	GAMBOA	PIZARRO	IMAS	Asistente_Adm_Cedes	26/07/2008
wilsonmc	WILSON	MENA	CORDERO	IMAS	Tecnicos_Administrativos	15/02/2005

USUARIO	NOMBRE	APELLIDO 1	APELLIDO 2	INSTITUCIÓN	PERFIL	FEC SALIDA
yahairagg	YAHAIRA	GARCIA	GUZMAN	IMAS	Digitadores	15/09/2006
yorlenmm	YORLEN	MARCHENA	MARTINEZ	IMAS	Tecnicos_Administrativos	26/07/2008
yorlenmr	YORLEN	MARCHENA	MARTINEZ	IMAS	Tecnicos_Administrativos	26/07/2008
yorlenyra	YORLENY	RAMIREZ	ALVARADO	IMAS	Profesional_Ejecutor	05/08/2005
zulmarp	ZULMA	RUIZ	PIZARRO	IMAS	Profesional_Ejecutor	01/03/2008

Fuente: Base de datos SIPO/SABEN
Auditoría Interna
Mayo 2014 2013

INSTITUTO MIXTO DE AYUDA SOCIAL
AUDITORÍA INTERNA

ANEXO #2

USUARIOS SIPO QUE TIENEN ASOCIADO UN PERFIL SABEN Y NO DEBEN TENERLO
Información hasta el 11/03/2013

USUARIO BD	NOMBRE	APELLIDO 1	APELLIDO 2	NOM GERENCIA	PERFIL BASE DATOS	PERFIL_SABEN
adrianarm	ADRIANA	RAMIREZ	MAYORGA	ARDS PUNTARENAS	Digitadores	TECNICO SOCIAL
alfonsodr	ALFONSO	DURAN	RETANA	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
anaas	ANA	ARCE	SANDI	ARDS CARTAGO	Digitadores	TECNICO SOCIAL
anarv	ANA	RODRIGUEZ	VARGAS	NIVEL CENTRAL	Digitadores	TECNICO SOCIAL
bernardobv	BERNARDO	BENAVIDES	VIQUEZ	NIVEL CENTRAL	Digitadores	TECNICO SOCIAL
blancass	BLANCA	SANCHEZ	SERRANO	ARDS CARTAGO	Consulta	TECNICO SOCIAL
dagellesv	DAGELLE	SAENZ	VARGAS	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
gabrielabq	GABRIELA	BARQUERO		ARDS SUROESTE	Digitadores	TECNICO SOCIAL
geimycc	GEIMY	CORTES	CORDERO	ARDS HEREDIA	grp_archivistica	TECNICO SOCIAL
ginnettemp	GINNETTE	MORA	PRADO	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
gloriajr	GLORIA	JIMENEZ	RAMIREZ	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
ivanmp	IVAN	MORA	POVEDA	ARDS CARTAGO	Consulta	TECNICO SOCIAL
jenniferav	JENNIFER	ANCHIA	VARGAS	ARDS SUROESTE	grp_archivistica	TECNICO SOCIAL
jennyjg	JENNY	JAMES	GRAHAMS	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
juande	JUAN	DUARTE	ESQUIVEL	ARDS BRUNCA	Digitadores	TECNICO SOCIAL
luisrm	LUIS	ROJAS	MADRIGAL	NIVEL CENTRAL	Digitadores	TECNICO SOCIAL
marcoam	MARCO	ARAYA	MONTEZUMA	ARDS SUROESTE	grp_archivistica	TECNICO SOCIAL
marianelachr	MARIANELA	CHAVES	RAMIREZ	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
marjoriesv	MARJORIE	SALAS	VILLALOBOS	NIVEL CENTRAL	Digitadores	TECNICO SOCIAL
mayrato	MAYRA	TENCIO	ORTIZ	ARDS BRUNCA	Consulta	TECNICO SOCIAL
randallcs	RANDALL	CENTENO	SOTO	ARDS HEREDIA	Digitadores	TECNICO SOCIAL
robertohg	ROBERTO	HENRIQUEZ	GUTIERREZ	ARDS NORESTE	Digitadores	TECNICO SOCIAL
sayirajv	SAYIRA	JIMENEZ	VARGAS	ARDS ALAJUELA	Consulta	TECNICO SOCIAL
shirleymn	SHIRLEY	MORA	NAVARRO	NIVEL CENTRAL	Digitadores	TECNICO SOCIAL

USUARIO BD	NOMBRE	APELLIDO 1	APELLIDO 2	NOM GERENCIA	PERFIL BASE DATOS	PERFIL_SABEN
teresitapb	TERESITA	PICADO		ARDS SUROESTE	Digitadores	TECNICO SOCIAL
vilmavg	VILMA	VALVERDE	GARCIA	NIVEL CENTRAL	Consulta	TECNICO SOCIAL
wendymh	WENDY	MONGE	H	NIVEL CENTRAL	grp_archivistica	TECNICO SOCIAL
yorlenelm	YORLENE	LOAIZA	MATA	ARDS CARTAGO	Digitadores	TECNICO SOCIAL

Fuente: Base de datos SIPO/SABEN
Auditoría Interna
Noviembre, 2013