Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

AUD 017-2020

INFORME DE LOS RESULTADOS OBTENIDOS EN EL ESTUDIO SOBRE LA EVALUACIÓN DE LA SEGURIDAD LÓGICA DEL SISTEMA NACIONAL DE INFORMACIÓN Y REGISTRO ÚNICO DE BENEFICIARIOS DEL ESTADO

TABLA DE CONTENIDO

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

RESUMEN EJECUTIVO

AUD 017-2020

INFORME DE LOS RESULTADOS OBTENIDOS EN EL ESTUDIO SOBRE LA EVALUACIÓN DE LA SEGURIDAD LÓGICA DEL SISTEMA NACIONAL DE INFORMACIÓN Y REGISTRO ÚNICO DE BENEFICIARIOS DEL ESTADO

¿Qué examinamos?

La gestión de la seguridad de la información del Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (SINIRUBE), en las siguientes áreas consideradas relevantes: evaluación de la disponibilidad, confidencialidad e integridad de la información; evaluación de la razonabilidad de la definición y alcance de los perfiles de acceso a la información; y cumplimiento de la normativa técnica y legal relacionada con la gestión de la seguridad de la información del sistema.

La auditoría abarcó el periodo comprendido de junio del 2018 a junio del 2019, ampliándose cuando se consideró necesario.

¿Por qué es importante?

Por la relevancia de fortalecer la gestión de la seguridad de la información del SINIRUBE, en cuanto a la disponibilidad, confidencialidad e integridad de la información.

¿Qué encontramos?

Se determinó que el Órgano Desconcentrado SINIRUBE, se encuentra en un proceso de implementación de políticas y procedimientos relacionados con la seguridad de la información. Asimismo, se determinó la ausencia de lineamientos formales para la modificación, desactivación y eliminación de usuarios. Por otra parte, se detectaron debilidades de control relacionadas a la gestión de contraseñas; integridad de los datos almacenados en la base de datos del SINIRUBE y vigencia de los contratos de confidencialidad.

¿Qué sigue?

Con el propósito de corregir las deficiencias de gestión determinadas, se recomendó al Director Ejecutivo del SINIRUBE, establecer las medidas de control pertinentes, con la finalidad de asegurar la seguridad de la información del SINIRUBE.

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

AUD 017-2020

INFORME DE LOS RESULTADOS OBTENIDO EN EL ESTUDIO SOBRE LA EVALUACIÓN DE LA SEGURIDAD LÓGICA DEL SISTEMA NACIONAL DE INFORMACIÓN Y REGISTRO ÚNICO DE BENEFICIARIOS DEL ESTADO

1. INTRODUCCION

1.1. Origen del estudio

El presente estudio se originó en atención al Plan de Trabajo de la Auditoría Interna para el año 2018.

1.2. Objetivo general

Evaluar la seguridad de la información del Sistema Nacional de Información y Registro Único de Beneficiarios del Estado (en adelante, SINIRUBE).

1.3. Alcance y periodo del estudio

El estudio consistió en evaluar la seguridad lógica del SINIRUBE. El periodo del estudio comprendió de junio del 2018 a junio del 2019 y se extendió en los casos que se consideró necesario.

El estudio se llevó a cabo de conformidad con lo dispuesto en las Normas para el Ejercicio de la Auditoría Interna en el Sector Público, las Normas Generales de Auditoría para el Sector Público, el Manual de Procedimientos de la Auditoría Interna del IMAS, así como la demás normativa de auditoría de aplicación y aceptación general.

1.4. Comunicación de resultados

En reunión celebrada el día 07 de octubre del 2020, se comunicaron los resultados del presente informe al Máster Erikson Álvarez Calonge, Director Ejecutivo del SINIRUBE, en la cual se efectuaron observaciones que en lo pertinente, una vez valoradas por esta Auditoría Interna, fueron incorporadas en el apartado de recomendaciones del presente informe.

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

2. RESULTADOS

2.1. Seguridad de la Información del SINIRUBE

2.1.1 Políticas y procedimientos de Seguridad de la Información

Se determinó que el Órgano Desconcentrado SINIRUBE, carece de un marco normativo en materia de seguridad de la información para el Sistema Nacional de Información y Registro Único de Beneficiarios del Estado. No obstante, se comprobó la existencia de tres políticas relacionadas al Control de Acceso Lógico, Desarrollo y Mantenimiento de Software; y Carga de Información.

Además, no se obtuvo evidencia de los planes de contingencia que garanticen razonablemente el continuo funcionamiento del SINIRUBE, en caso de materialización de algún evento adverso que origine la suspensión severa de este.

Sobre el particular, es importante mencionar el artículo 61 del Reglamento a la Ley N° 9137 Creación del Sistema Nacional de Información y Registro Único de Beneficiarios del Estado, que cita textualmente:

> *El SINIRUBE deberá documentar e implementar políticas de seguridad de la información, y los procedimientos correspondientes, para lograr los niveles de seguridad requeridos, de acuerdo al análisis de riesgos que se realice de la información que contienen las bases de datos, además, debe establecer las medidas de seguridad relacionadas con los siguientes aspectos:*
>
> *a) La implementación de un marco de seguridad de la información*
> *b) El compromiso del personal con la seguridad de la información.*
> *c) La seguridad física y ambiental.*
> *d) La seguridad en las operaciones y comunicaciones.*
> *e) El control de acceso.*
> *f) La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.*
> *g) La continuidad de los servicios de TI.*
> *h) El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.*
> *i) El manejo de la documentación.*
> *j) La terminación normal de contratos, su rescisión o resolución.*
> *k) La salud y seguridad del personal de TI*

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

Por otra parte, la norma 5.8 “Control de sistemas de información” de las Normas de Control Interno para el Sector Público, establece:

> *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.*

Asimismo, la norma 1.4 “Gestión de la seguridad de la información” de Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de República, dispone:

> *La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*
>
> *Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos y considerar lo que establece la presente normativa (…)*

De igual forma, la sub norma 1.4.7 “Continuidad de servicios de TI” del precitado cuerpo normativo, indica:

> *La organización debe mantener una continuidad razonable de sus procesos y su interrupción no debe afectar significativamente a sus usuarios. Como parte de ese esfuerzo debe documentar y poner en práctica, en forma efectiva y oportuna, las acciones preventivas y correctivas necesarias con base en los planes de mediano y largo plazo de la organización, la evaluación e impacto de los riesgos y la clasificación de sus recursos de TI según su criticidad.*

Complementariamente, las buenas prácticas establecidas en COBIT 5, señala en lo de interés, lo siguiente:

> *(…)*
> ***APO13 Gestionar la Seguridad*** *Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.*
> *(…)*
>
> ***DSS04 Gestionar la Continuidad*** *Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.*
> *(…)*

En relación con lo expuesto, como parte de las pruebas realizadas y la evidencia recopilada, esta Auditoría Interna determinó que la situación descrita se encuentra en proceso de implementación por parte del SINIRUBE. Lo anterior, según información suministrada por el Máster Erickson Alvarez Calonge, Director Ejecutivo del SINIRUBE, mediante correo electrónico del 11 de setiembre del 2020, en el cual indicó lo siguiente:

> *"(…) Hemos estado en proceso de implementación de la normativa aprobada por el Consejo Rector de SINIRUBE y por esta Dirección, todo esto de acuerdo al trabajo realizado en Conjunto con PWC."*

Adicionalmente, mediante correo electrónico del 18 de setiembre del 2020 el Máster Alvarez Calonge remitió a esta Auditoría, un archivo en formato Excel con el inventario de la normativa del SINIRUBE, en el cual se detalla las políticas, procedimientos e instructivos implementados a setiembre del 2020. Ver **Anexo Nº 1** adjunto al presente informe.

2.1.2. Solicitud de modificación, desactivación y eliminación de usuarios

En la revisión efectuada de los convenios y contratos de confidencialidad para el acceso a la información del SINIRUBE suscritos entre el SINIRUBE y las instituciones públicas, se determinó la ausencia de una cláusula o lineamiento que establezca como parte de las obligaciones de dichas instituciones, informar al SINIRUBE sobre la modificación, desactivación o eliminación de cuentas de usuario.

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

Asimismo, el SINIRUBE no cuenta con un procedimiento formal establecido que regule entre otras, las actividades relacionadas con la modificación, suspensión temporal y la eliminación de usuarios, el control, mantenimiento e inactividad de usuarios.

Por tanto, la situación indicada, imposibilita el poder garantizar que el proceso de solicitud de modificación, suspensión y eliminación de las cuentas de usuario, sea totalmente funcional y controlado**.**

En relación con lo anterior, la norma 5.8 "Control de Sistemas de Información" de las Normas de Control Interno para el Sector Público, establece lo siguiente:

> *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.*

Además, los incisos a, c, d, e y f de la Norma 1.4.5 "Control de acceso" de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, indican lo siguiente:

> *La organización debe proteger la información de accesos no autorizados.*
> *Para dicho propósito debe:*
>
> *a. Establecer un conjunto de políticas, reglas y procedimientos relacionados con el acceso a la información, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación.*
> *c. Definir la propiedad, custodia y responsabilidad sobre los recursos de TI.*
> *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.*
> *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*

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

tales medios de autenticación, así como para su revisión y actualización periódica y atención de usos irregulares.

Complementariamente, y como sana práctica, se debe indicar que el Estándar Internacional ISO/IEC 27002, establece:

9.2.1 Registro y cancelación de usuarios

Control

Se debería implementar un proceso formal de registro y de cancelación de usuarios para habilitar la asignación de derechos de acceso.

Guía de implementación

El proceso de gestión de identificación (ID) de usuarios debería incluir:

a) la utilización de una ID única de usuario para hacer que los usuarios queden vinculados y sean responsables de sus acciones; el uso de IDs compartidas debería permitirse solamente cuando sea necesario por razones de negocio u operativas, y debería ser aprobado y documentado;
b) la desactivación o eliminación inmediata de los IDs de los usuarios que han dejado la organización (ver apartado 9.2.6);
c) la identificación y eliminación o desactivación periódica de IDs de usuarios redundantes;
d) asegurarse de que las IDs de usuarios redundantes no se otorguen a otros usuarios.

9.2.5 Revisión de los derechos de acceso de los usuarios

Control

Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios en intervalos regulares.

Guía de implementación
La revisión de los derechos de acceso debería considerar lo siguiente:

a) los derechos de acceso de usuarios deberían revisarse a intervalos regulares, y luego de cualquier cambio, tal como una promoción, una degradación, o una terminación del empleo;
b) los derechos de acceso de usuario deberían ser revisados y reasignados cuando se mueve de un rol a otro dentro de la misma organización;
c) las autorizaciones para derechos de acceso privilegiados deberían revisarse a intervalos más frecuentes;
d) debería verificarse la asignación de privilegios a intervalos regulares para garantizar que no se obtengan privilegios no autorizados;
e) los cambios en las cuentas privilegiadas deberían registrarse para su revisión periódica.

9.2.6 Eliminación o ajuste de los derechos de acceso

Control

Los derechos de acceso de todos los empleados y de los usuarios de partes externas a la información y a los recursos de procesamiento de la información deberían ser eliminados al finalizar el empleo, contrato o acuerdo, o ajustados en caso de cambios.

Guía de implementación

Cuando ocurre la desvinculación, los derechos de acceso de un individuo a la información y los activos asociados con recursos de procesamiento y servicios de información, deberían eliminarse o suspenderse. Esto determinará si es necesario eliminar los derechos de acceso. Los cambios en la relación laboral deberían estar reflejados en la eliminación de todos los derechos de acceso que no fueron aprobados para el nuevo puesto. Los derechos de acceso que deberían eliminarse o ajustarse incluyen aquellos para acceso físico y lógico. La eliminación o el ajuste se pueden hacer mediante eliminación, revocación o reemplazo de las claves, tarjetas de identificación, recursos de procesamiento de información o suscripciones. Cualquier documentación que identifique los derechos de acceso de los empleados y contratistas debería reflejar la eliminación o el ajuste de los derechos de acceso. Si un empleado o usuario de tercera parte que se marcha ha conocido las contraseñas para IDs de usuarios que permanecen activos, éstas deberían cambiarse al momento de la desvinculación o cambio de cargo, contrato o acuerdo.

Los derechos de acceso a la información y a los activos asociados con los recursos de procesamiento de información, deberían reducirse o eliminarse antes de que el empleo termine o cambie, dependiendo de la evaluación de los factores de riesgo tales como:

a) si la desvinculación o cambio es iniciado por el empleado, usuario de tercera parte, o por la dirección y la razón de la desvinculación;
b) las responsabilidades actuales del empleado, usuario de tercera parte o cualquier otro usuario;
c) el valor de los activos accesibles actualmente.

2.2. Gestión de contraseñas

De la revisión efectuada al sistema de gestión de contraseñas del SINIRUBE, se determinaron una serie de deficiencias de control que se detallan a continuación:

a) Se comprobó que el sistema no obliga a los usuarios a cambiar sus contraseñas en el primer acceso. Asimismo, se constató que cuando el usuario recibe la contraseña temporal mediante la cuenta de correo electrónico servicios@sinirube.go.cr, esta también es visualizada por el Bach. Guillermo Vásquez Hernández, funcionario del Área SINIRUBE, responsable de administrar dicha cuenta.

b) También, se determinó que el sistema carece de un control que permita cambiar las contraseñas periódicamente y/o con base en cierto número predeterminado de accesos.

c) Además, se examinó que el sistema permite al usuario repetir contraseñas previamente utilizadas.

En relación con lo anterior, las Normas de Control Interno para el Sector Público, en lo de interés, señalan lo siguiente:

(...)
4.1 Actividades de control *El jerarca y los titulares subordinados, según sus competencias, deben diseñar, adoptar, evaluar y perfeccionar, como parte del SCI, las actividades de control pertinentes, las que comprenden las políticas, los procedimientos y los mecanismos que contribuyen a asegurar razonablemente la operación y el fortalecimiento del SCI y el logro de los objetivos institucionales. (...)*

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

El ámbito de aplicación de tales actividades de control debe estar referido a todos los niveles y funciones de la institución. En ese sentido, la gestión institucional y la operación del SCI deben contemplar, de acuerdo con los niveles de complejidad y riesgo involucrados, actividades de control de naturaleza previa, concomitante, posterior o una conjunción de ellas. Lo anterior, debe hacer posible la prevención, la detección y la corrección ante debilidades del SCI y respecto de los objetivos, así como ante indicios de la eventual materialización de un riesgo relevante.
(…)

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. (…)* (Los subrayados no corresponden al texto original)

Asimismo, el inciso a. de la norma 1.4.5 "Control de acceso" de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información de la Contraloría General de República, indica lo siguiente:

(…)
La organización debe proteger la información de accesos no autorizados.
Para dicho propósito debe:
a) ***Establecer un conjunto de*** *políticas,* ***reglas*** *y procedimientos* ***relacionados con el acceso a la información****, al software de base y de aplicación, a las bases de datos y a las terminales y otros recursos de comunicación. (…)* (El subrayado y negrita no corresponden al texto original)

Adicionalmente, y como sana práctica, se debe indicar que el Estándar Internacional ISO/IEC 27002 en su apartado 9.4.3 "Sistema de gestión de contraseñas" establece:

Control
Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurarse de la calidad de las contraseñas.

Guía de implementación
Un sistema de gestión de contraseñas deberá:

a) *imponer el uso de contraseñas e ID de usuario individuales con el fin de mantener la rendición de cuentas;*
b) *permitir a los usuarios seleccionar y cambiar sus propias contraseñas e incluir un procedimiento de confirmación para tener en cuenta los errores de entrada;*
c) *forzar la selección de contraseñas de calidad;*
d) forzar a los usuarios a cambiar sus contraseñas en su primer acceso (log-on);
e) forzar los cambios regulares de contraseña y cuando sea necesario;
f) mantener un registro de las contraseñas anteriores utilizadas e impedir su reutilización;
g) *no mostrar las contraseñas en la pantalla cuando se están introduciendo;*
h) *guardar archivos de contraseñas separados de los datos del sistema de aplicaciones;*
i) *guardar y transmitir las contraseñas en formas protegidas.* (El subrayado y negrita no corresponden al texto original)

Lo anterior, es causado por la inexistencia de controles automáticos que garanticen una adecuada gestión de contraseñas, lo que consecuentemente expone al Área del SINIRUBE a la perdida de uno de sus activos más valioso, la información.

2.3. Inconsistencias en los registros almacenados en la base de datos del SINIRUBE

Según el análisis realizado a la base de datos del SINIRUBE, específicamente lo referente a la asignación de los perfiles de usuario, se detectaron las siguientes inconsistencias:

a) Existen 5 registros con descripción "NULL" en el campo ROL.
Los casos encontrados en esta condición se muestran en la siguiente tabla:

CÉDULA	NOMBRE	ENTIDAD	ROL
115130831	KAREN HERNANDEZ BADILLA	INSTITUTO MIXTO DE AYUDA SOCIAL	NULL
109040145	ANDREA CAROLINA BEJARANO CAMACHO	INSTITUTO MIXTO DE AYUDA SOCIAL	NULL
701560103	CHARLENE CHEVEZ MONTERO	CAJA COSTARRICENSE DEL SEGURO SOCIAL (RNC)	NULL
503880402	PRISCILA MARIA ELIZONDO MORENO	INSTITUTO MIXTO DE AYUDA SOCIAL	NULL
602440090	MARIA ISABEL CARVAJAL CARMONA	INSTITUTO MIXTO DE AYUDA SOCIAL	NULL

Tabla N°1. Usuarios sin rol definido en la base de datos del SINIRUBE

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

Adicionalmente, se identificó que 2 de los 5 registros anteriores presentan accesos al sistema de información, a pesar de tener asignado el Rol "NULL".
El detalle de estos casos se presenta a continuación:

CÉDULA	NOMBRE	ENTIDAD	ROL	CANTIDAD ACCESOS
701560103	CHARLENE CHEVEZ MONTERO	CAJA COSTARRICENSE DEL SEGURO SOCIAL (RNC)	NULL	13
503880402	PRISCILA MARIA ELIZONDO MORENO	INSTITUTO MIXTO DE AYUDA SOCIAL	NULL	8

Tabla N°2. Usuarios con accesos al sistema sin rol definido en la base de datos del SINIRUBE

b) Existen 2 registros a los cuales se les asignó el perfil "ALTO", sin que tuvieran un perfil definido en el documento denominado "Formulario de Acceso al Sistema de Información" utilizado para la creación del usuario.
Los casos encontrados en esta condición se muestran en la siguiente tabla:

CÉDULA	NOMBRE	ENTIDAD	ROL
205380041	FRANCINY TERESITA CORDERO ABARCA	CAJA COSTARRICENSE DEL SEGURO SOCIAL (RNC)	ALTO
203300662	GLADYS MARGARITA CASTRO CRUZ	CAJA COSTARRICENSE DEL SEGURO SOCIAL (RNC)	ALTO

Tabla N°3. Usuarios sin rol definido en el formulario de acceso al SINIRUBE

c) Además, se identificaron registros con información inconsistente y campos incompletos en el perfil "Consulta Pública". Asimismo, se comprobó que dicho perfil permite registrar texto y numero en el campo cedula.

Al respecto, en consulta verbal realizada al personal del Tecnologías de Informacion del SINIRUBE sobre las razones o causas de tales errores, se indicó, que muchos de los errores son de digitación y falta de uniformidad en cuanto al contenido de los campos y la información que representan.

Las inconsistencias antes mencionadas, son considerados riesgos que afectan la confiabilidad de la información.

Sobre el particular, la norma 4.3 "Administración de los datos" de las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, dispone literalmente lo siguiente:

La organización debe asegurarse de que los datos que son procesados mediante TI corresponden a transacciones válidas y debidamente autorizadas, que son

procesados en forma completa, exacta y oportuna, y transmitidos, almacenados y desechados en forma íntegra y segura.

2.4. Vigencia de los contratos de confidencialidad

Se determinó que aunque los contratos de confidencialidad suscritos entre el SINIRUBE, las instituciones y las personas funcionarias solicitantes del acceso a la información del sistema SINIRUBE, se suscribieron por un plazo de 1 año con posibilidad de prorrogarse a solicitud de la institución participante, esta Auditoría no obtuvo evidencia de que se hayan gestionado las prórrogas respectivas para la ampliación de la vigencia de dichos contratos.

Asimismo, se comprobó que aún cuando dichos contratos están vencidos, las instituciones y las personas funcionarias mantienen el acceso al sistema. La causa de la situación expuesta, obedece a que no se han realizado revisiones periódicas de las vigencias de los contratos de confidencialidad, lo que debilita el control interno y aumenta el riesgo de usos no autorizados.

Con respecto a lo anterior, el Máster Erikson Álvarez Calonge, Director Ejecutivo del SINIRUBE, mediante correo electrónico del 18 de setiembre del 2020, indicó en lo de interés, lo transcrito a continuación:

> *"(...) a) Con respecto a lo anterior, indicar las razones y/o justificaciones que motivaron que los contratos se realicen anualmente y no se prorroguen de manera automática.*
> *R/La motivación es para que las instituciones se vean obligadas a revisar si los usuarios a los que le solicitaron acceso todavía laboral (sic) en la institución, en el mismo puesto y función que motivo la solicitud del Acceso. (...)*
>
> *c) Indicar si el acceso al sistema SINIRUBE caduca cuando se vence la vigencia del contrato de confidencialidad.*
> *R/Así debe de ser, sin embargo por ser esta la primera vez que se esta realizando dicho proceso, lo estamos gestionando vía oficio y se les ha dado un tiempo para la renovación de los contratos. Para la semana del 21 de Septiembre, se inhabilitaran todos los accesos cuyos contratos de confidencialidad estén vencidos. (...)"*

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

Adicionalmente, es importante mencionar el artículo 8 de la Ley General de Control Interno, N° 8292, que cita textualmente:

> *Concepto de sistema de control interno. Para efectos de esta Ley, se entenderá por sistema de control interno la serie de acciones ejecutadas por la administración activa, diseñadas para proporcionar seguridad en la consecución de los siguientes objetivos: (...) d) Cumplir con el ordenamiento jurídico y técnico. (El subrayado no consta en el original)*

Por otra parte, la cláusula décima del contrato de confidencialidad suscrito entre el SINIRUBE y las instituciones, señala en lo de interés, lo siguiente:

> *"(...)* ***DÉCIMA:*** *El presente contrato rige a partir de su suscripción y por un plazo de 1 año, el cual podrá ser prorrogado a solicitud del Jerarca (...). Lo anterior mantiene vigente las obligaciones y responsabilidades de confidencialidad y protección de la información a la cual tuvo acceso la persona usuaria, esto según la normativa vigente en temas de protección y acceso a la información. (...)"*

En relación con lo expuesto, en la conferencia final celebrada el día 07 de octubre del 2020, la Auditoría Interna presentó al SINIRUBE el resultado supracitado relacionado con el acceso al sistema de conformidad con la vigencia del contrato de confidencialidad. Posteriormente, el día 14 de octubre del 2020, el Director Ejecutivo del SINIRUBE remitió a este Despacho las pruebas que evidencian la implementación de un control en el código de programación de dicho sistema que permite deshabilitar automáticamente los usuarios que presenten contratos de confidencialidad vencidos.

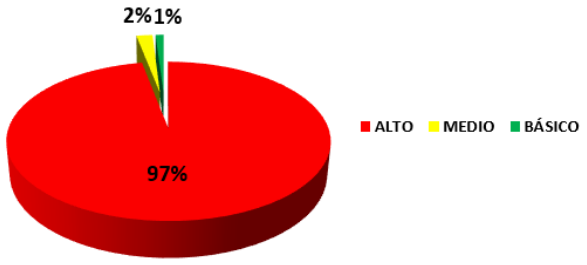
2.5. Definición de perfiles de usuario y documentación soporte para la creación de usuarios

De conformidad con la revisión efectuada por esta Auditoría, se determinaron una serie de deficiencias de control que se detallan a continuación:

a) Se constató que de los 791 usuarios activos en el SINIRUBE al 28 de junio del 2019, un 97% (769) tiene asignado el perfil de usuario "Alto", un 2% (17) tiene asignado el perfil de usuario "Medio" y un 1% (5) tiene asignado el perfil de usuario "Básico".

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

GRAFICO Nº 1:
PERFILES DE USUARIO SINIRUBE



En relación con lo anterior es importante destacar que el 97% de los usuarios asignados al perfil de usuario "Alto" sugiere una definición de perfiles no acorde al requerimiento de seguridad, dado que la mayor cantidad de usuarios pueden consultar en el sistema toda la información disponible de la población beneficiaria que recibe ayuda del Estado.

Con respecto a este tema, se determinó que la causa de la situación descrita obedece a que las instituciones participantes solicitan el perfil de acceso "Alto" mediante el "Formulario de acceso al sistema de información" establecido por el SINIRUBE, quien según la descripción de las funciones de la persona solicitante del acceso y las justificaciones del rol solicitado indicado en dicho formulario, procede con la asignación del rol.

Por tanto, se genera el riesgo de acceso a información sensible, al no limitar los privilegios asignados a los usuarios al mínimo necesario en el sistema SINIRUBE.

b) Se determinó que los expedientes donde se custodian los formularios para la solicitud de acceso a la información del SINIRUBE y los contratos de confidencialidad, los cuales son los documentos que soportan la creación de usuarios, no se encuentran ordenados cronológicamente ni foliados.

Lo anterior, obedece a la ausencia de lineamientos específicos para la organización, utilización, disponibilidad y acceso de los documentos soporte para la creación de usuarios.

Por tanto, dicha situación afecta la confiabilidad de dichos expedientes, pues no cuentan con una medida de control tendiente a salvaguardar su integridad.

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

De conformidad con lo expuesto anteriormente, las "Normas de control interno para el Sector Público", en lo de interés, señalan lo siguiente:

> *"(...) 5.5 Archivo institucional. El jerarca y los titulares subordinados, según sus competencias, deben implantar, comunicar, vigilar la aplicación y perfeccionar políticas y procedimientos de archivo apropiados para la preservación de los documentos e información que la institución deba conservar en virtud de su utilidad o por requerimiento técnico o jurídico. En todo caso, deben aplicarse las regulaciones de acatamiento obligatorio atinentes al Sistema Nacional de Archivos.*
>
> *Lo anterior incluye lo relativo a las políticas y procedimientos para la creación, organización, utilización, disponibilidad, acceso, confidencialidad, autenticidad, migración, respaldo periódico y conservación de los documentos en soporte electrónico, así como otras condiciones pertinentes. (...)*
>
> *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. (...)"*

De igual forma, la sub norma *5.7.4*, del precitado cuerpo normativo, establece lo siguiente:

> *"(...) 5.7.4 Seguridad. Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran. (...)"*

3. CONCLUSIONES

En relación con la seguridad de la información del sistema SINIRUBE, el estudio permitió determinar importantes deficiencias que aumentan la probabilidad de ocurrencia riesgos que afecten la disponibilidad, confidencialidad e integridad de la información almacenada en dicho sistema.

Adicionalmente, se identificaron una serie de debilidades relacionadas con la gestión de acceso de usuarios, vigencia de los contratos de confidencialidad, definición de perfiles de usuario y gestión de contraseñas, que son necesarias atender, para fortalecer el control interno en operación, en el marco de un proceso de mejora continua del servicio prestado por dicha Área a las instituciones del sector social.

Expuesto lo anterior, se considera necesario que la Administración implemente una serie de medidas preventivas y correctivas que solventen las debilidades presentadas en el estudio, con tal propósito en el capítulo siguiente se formulan las recomendaciones que se consideran pertinentes.

4. RECOMENDACIONES

Esta Auditoría Interna respetuosamente se permite recordar que de conformidad con lo preceptuado por el artículo 36 de la Ley General de Control Interno, Nº 8292, disponen de diez días hábiles, contados a partir de la fecha de recibo de este informe, para ordenar la implantación de las recomendaciones que les correspondan.

Al respecto, se estima conveniente transcribir a continuación, en lo de interés, lo que disponen los artículos 12, 36, 38 y 39 de la Ley Nº8292:

> **Artículo 12.-Deberes del jerarca y de los titulares subordinados en el sistema de control interno.** En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes: …/c) Analizar e implantar, de inmediato, las observaciones, recomendaciones y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan. /…
>
> **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 DIRECTOR EJECUTIVO DEL SINIRUBE

4.1. Elaborar un plan de implementación para que se incorpore en los convenios suscritos entre el SINIRUBE y las instituciones asociadas, una cláusula que establezca como parte de las obligaciones de dichas instituciones comunicar al SINIRUBE la modificación, suspensión y eliminación de cuentas de usuario. (Ver punto 2.1.2 del acápite de resultados)

4.2. De conformidad con lo expuesto en el punto 2.2 del acápite de resultados del presente informe, establecer en el sistema de información, controles de seguridad en la gestión

de contraseñas del sistema SINIRUBE, que permitan obligar a los usuarios a cambiar sus contraseñas en el primer acceso; cambiar las contraseñas periódicamente y/o con base en cierto número predeterminado de accesos y mantener un registro de las contraseñas anteriores utilizadas e impedir su reutilización. (Ver punto 2.2 del acápite de resultados)

4.3. De conformidad con lo expuesto en el punto 2.3 del acápite de resultados del presente informe, corregir en la base de datos del SINIRUBE las inconsistencias relacionadas con la asignación de perfiles, a efecto de asegurar la confiabilidad de la información almacenada en dicha de base de datos. (Ver punto 2.3 del acápite de resultados)

4.4. Realizar las gestiones pertinentes para subsanar la deficiencia determinada en el punto 2.4 de forma que todos los usuarios con una cuenta activa tengan vigente el contrato de confidencialidad respectivo. Asimismo, inhabilitar aquellas cuentas de usuario que una vez efectuada la actualización de los contratos, no tengan vigente para el usuario respectivo, un contrato de confidencialidad. (Ver punto 2.4 del acápite de resultados)

4.5. Establecer medidas de control eficientes con el fin de corregir las deficiencias expuestas en el apartado 2.5 de acápite de resultados del presente informe, para lo cual:

a) Revisar la definición y asignación de los perfiles de acceso al sistema SINIRUBE. (Ver inciso a) del punto 2.5 del acápite de resultados)
b) Establecer lineamientos para mantener ordenados y foliados los expedientes físicos donde se custodia la documentación que soporta la creación de usuarios. (Ver inciso b) del punto 2.5 del acápite de resultados)

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° Recomendación	Plazo (meses)	Fecha Cumplimiento
4.1.	2	30/11/2020
4.2.	2	30/11/2020
4.3.	1	30/10/2020
4.4.	2	30/11/2020
4.5.	2	30/11/2020

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

EVELYN MARIA CAMPOS PADILLA (FIRMA)
Firmado digitalmente por EVELYN MARIA CAMPOS PADILLA (FIRMA)
Fecha: 2020.10.15 14:21:37 -06'00'

Hecho por:
Licda. Evelyn Campos Padilla
PROFESIONAL EN AUDITORIA

WADY BERNY SOLANO SILES (FIRMA)
Firmado digitalmente por WADY BERNY SOLANO SILES (FIRMA)
Fecha: 2020.10.15 14:29:08 -06'00'

Revisado y aprobado por:
MATI. Wady Solano Siles
COORDINADOR UNIDAD GESTIÓN TECNOLOGÍAS

AUDITORIA INTERNA
OCTUBRE, 2020

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

AUDITORIA INTERNA
ANEXO Nº 1

Tipo Documento	Código Documento	Instrumento SINIRUBE
Estándar	ES-SINIRUBE-001	Estándar de gestión de la calidad
Estándar	ES-SINIRUBE-002	Estándar de seguridad física de los recursos de T.I
Instructivo	IN-SINIRUBE-006	Marco de Seguridad de TI
Instructivo	IN-SINIRUBE-001	Metodología de administración de proyectos
Instructivo	IN-SINIRUBE-002	Metodología de desarrollo de Software
Instructivo	IN-SINIRUBE-003	Plan de capacitación y concientización de T.I
Instructivo	IN-SINIRUBE-004	Plan para la gestión de la capacidad y disponibilidad
Instructivo	IN-SINIRUBE-005	Requisitos de la seguridad durante el ciclo de vida del desarrollo
Instrumento	IS-SINIRUBE-001	Herramienta de gestión PTIC
Instrumento	IS-SINIRUBE-002	Inventario de T.I
Política Institucional	PI-SINIRUBE-001	Política de control de acceso lógico
Política Institucional	PI-SINIRUBE-002	Política de carga de información
Política Institucional	PI-SINIRUBE-003	Desarrollo y Mantenimiento Software
Política Institucional	PI-SINIRUBE-004	Control de Acceso
Política Institucional	PI-SINIRUBE-005	Adm. Terceros
Política Institucional	PI-SINIRUBE-006	Des. Seguro
Política Institucional	PI-SINIRUBE-007	Escritorio Limpio
Política Institucional	PI-SINIRUBE-008	Software Malicioso
Política Institucional	PI-SINIRUBE-009	Control Cripto.
Política Institucional	PI-SINIRUBE-010	Seguridad de Informacion
Política Institucional	PI-SINIRUBE-011	Cont. Negocio

Instituto Mixto de Ayuda Social
Teléfono (506) 2202-4184
Fax (506) 2202-4194
Apartado postal 6213-1000

Tipo Documento	Código Documento	Instrumento SINIRUBE
Política Institucional	PI-SINIRUBE-012	Contraseña
Política Institucional	PI-SINIRUBE-013	Dest. Datos
Procedimiento Interno	PR-SINIRUBE-001	Procedimiento Atención de Usuarios
Procedimiento Interno	PR-SINIRUBE-002	Procedimiento para la gestión de respaldos
Procedimiento Interno	PR-SINIRUBE-003	Procedimiento de control interno
Procedimiento Interno	PR-SINIRUBE-004	Procedimiento Revisión de Cumplimiento Regulatorio de TI
Procedimiento Interno	PR-SINIRUBE-005	Procedimiento Gestión y control de terceros de T.I
Procedimiento Interno	PR-SINIRUBE-006	Procedimiento para el Ingreso de Terceros
Procedimiento Interno	PR-SINIRUBE-007	Procedimiento Gestión de Cambios
Procedimiento Interno	PR-SINIRUBE-008	Procedimiento Gestión de Incidentes
Procedimiento Interno	PR-SINIRUBE-009	Procedimiento Gestión de Problemas
Procedimiento Interno	PR-SINIRUBE-010	Procedimiento de Ingreso y Salida de Equipos
Procedimiento Interno	PR-SINIRUBE-011	Procedimiento de Solicitud de Acceso
Procedimiento Interno	PR-SINIRUBE-012	Proceso de seguimiento de los procesos de TI