INSTITUTO COSTARRICENSE DE ACUEDUCTOS Y ALCANTARILLADO

AUDITORÍA INTERNA

AUDITORÍA DE CÁRACTER ESPECIAL PARA EVALUAR LA SEGURIDAD DEL SISTEMA COMERCIAL INTEGRADO EN CUANTO A LOS PERFILES

ICI-2021-04

2021

Tabla de contenido

RESUMEN EJECUTIVO

¿Qué examinamos?

La Auditoría especial se realiza al Sistema *Comercial integrado (OPEN) relacionado con el proceso de facturación, en específico evalúa la existencia de lineamientos, políticas, procedimientos, disposiciones para la administración de perfiles, roles y privilegios que mantiene el sistema.*

En la evaluación se tomaron en consideración aspectos fundamentales como los procedimientos de solicitud, modificación y eliminación de usuarios. Además de aspectos propios de la caracterización de perfiles, roles y privilegios asignados a los usuarios, de forma adicional se analiza las cuentas ID de usuarios, la integridad de datos de creación o modificación de usuarios, el grado de documentación existente para la adecuada operación y administración funcional (Dirección del Sistema Comercial Integrado) del sistema.

En complemento se evalúa el cumplimiento de la normativa aplicable a cada función que se desarrolla en la administración funcional del sistema comercial, el riesgo asociado a las funciones incompatibles y el conocimiento de los administradores de las funciones que desempeñan.

De forma adicional se incorpora los resultados de una encuesta practicada a los usuarios del sistema, a efectos de evaluar el grado de conocimiento del perfil asignado y las funciones establecidas, la capacitación o conocimiento del sistema que se tiene versus el perfil asignado y la supervisión ejercida.

¿Por qué es importante?

El sistema de trámite, registro, facturación y cobro de los servicios que presta el AyA, representan en el país más de 600,000 clientes los cuales se relacionan de forma directa con el sistema comercial conocido con el nombre OPEN, para cada uno de los procesos que se ejecutan en el sistema en la mayoría de los casos se requiere la interacción de un funcionario (usuario del sistema)con cada proceso que se ejecuta, los cuales pueden ir desde un lector, un analista de facturación, un analista de atención al cliente, un notificador, personal de atención de ordenes de servicio, proceso legal, y cobradores externos.

La definición y creación de perfiles del sistema OPEN, corresponde al personal de administración funcional (Dirección Comercial Nacional), con base en los diferentes procesos que se ejecutan en las áreas operativas. Ahora bien, la solicitud de asignación la realiza los encargados comerciales con base en la experiencia y conocimiento de las funciones que se desean que sean ejecutadas por parte de los usuarios, en armonía con el conocimiento que se tiene de las prerrogativas (privilegios) asignados a cada perfil que existe en el sistema. En este sentido queda claro que la definición, administración de perfiles es una labor de la administración funcional de la Dirección Comercial Nacional y no de los encargados. Por su parte, los encargados de las áreas usuarias si pueden y deben solicitar cual perfil debe tener cada usuario en el sistema, no así cuales son las características propias de cada perfil de usuario por cuanto es una labor propia de la Dirección Comercial Nacional.

En este sentido la adecuada administración para la creación, modificación y eliminación de usuarios es una actividad importante dentro proceso mismo de la comercialización de los servicios.

Existen premisas importantes que definen cual debe ser las generalidades de creación y asignación de perfiles o derechos de lo que debo o puedo hacer en los sistemas de información como lo puedan ser: "el principio de necesidad de saber o menor privilegio", "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".

El estudio realizado es de importancia para que el Instituto asegure razonablemente los recursos financieros y técnicos necesarios; así como el sistema de control interno que le facilite operar de forma eficiente y cumplir con los objetivos encomendados por su Ley Constitutiva.

¿Qué encontramos?

La Auditoría permitió verificar el cumplimiento de lo dispuesto por la Junta Directiva de AyA en el acatamiento de la definición y puesta en marcha de una política de seguridad que permitiera a la administración establecer en forma adecuada cuales eran los principios y reglas que aplican para los temas de seguridad de los sistemas, equipos, instalaciones, red de comunicaciones, accesos y otros, que interactúan con las TI, determinándose que a pesar que el Comité de Gerencia para finales del año 2019 aprobó y sometió a consideración las políticas de seguridad a la Junta Directiva, las cuales fueron aprobadas por este órgano, se evidenció que la administración superior no realizó las gestiones necesarias para divulgar y poner en práctica las políticas aprobadas.

De forma adicional la auditoria permitió determinar la existencia de falta de documentación necesaria para la administración funcional del sistema, determinándose que la falta de información compromete los requerimientos propios y necesarios para poder ejercer esta función, de forma adicional se pudo determinar que la Dirección Comercial Nacional no cuenta con el personal necesario para la adecuada administración funcional.

Así mismo, se determinaron inconsistencia de usuarios con ID diferentes para un mismo funcionario, además de funcionarios que deberían estar inactivos en el sistema con claves activas como consecuencia de realizar nuevas funciones, jubilaciones, renuncias y despidos.

Por otra parte, se encontraron perfiles y roles que no se encuentran definidos en los manuales del sistema, así como más de 28,000 objetos de definición de privilegios que no mantienen ningún tipo de documentación, entre otros aspectos que debilitan el control interno como lo es la falta de separación de funciones entre desarrollo/mantenimiento y el ambiente de producción, permitiéndose a personal de estas áreas poder acceder al sistema en producción.

Un aspecto fundamental de la evaluación realizada, lo fue el hecho de que se determinara la existencia en el nivel de usuarios de base de datos y mantenimiento de sistemas el que este personal realice la inclusión de registros, lo cual compromete la seguridad del sistema.

***¿Qué sigue**?*

Debido a lo expuesto se giran recomendaciones a las autoridades con la competencia suficiente de poner en práctica lo dejado de implementar o en su defecto se adecuen los procedimientos existentes a lo que la norma dispone, en fortalecimiento de cada uno de los procedimientos automatizados o manuales que existan en la administración funcional del sistema y seguridad lógica del mismo.

Para cada recomendación se solicita el o los documentos necesarios y suficientes que acrediten el cumplimiento de lo solicitado.

Con las recomendaciones dadas la Auditoría Interna aporta valor agregado en la mejora de los procesos y subprocesos institucionales y coadyuva con la Administración en el logro de los objetivos institucional del sistema de control interno, específicamente en el componente de sistemas de información. A su vez, se dan recomendaciones para mejorar los controles, los procesos de dirección y los riesgos.

ES-09-2021
INFORME Nro.ICI-2021-04

AUDITORÍA DE CÁRACTER ESPECIAL PARA EVALUAR LA SEGURIDAD DEL SISTEMA COMERCIAL INTEGRADO EN CUANTO A LOS PERFILES

1. INTRODUCCIÓN.

1.1 Origen de la auditoria.

La auditoría se efectuó de conformidad con las competencias conferidas a la Auditoria Interna en la Ley General de Control Interno N. 8292, en cumplimiento del Plan de Trabajo Anual 2021 y en cumplimiento a la disposición Nro. 9 del OF-0080-IA-2021 remitido el 10 de febrero de 2021 por la Autoridad Reguladora de Servicios públicos (ARESEP).

1.2 Objetivo general.

Identificar y evaluar los permisos u autorizaciones otorgados a los diferentes usuarios o grupo de usuarios del Sistema Comercial integrado (OPEN), tomando en consideración la asignación de privilegios a cada perfil creado en el sistema según las funciones asignadas, para evaluar el cumplimiento de lo en el bloque de legalidad y las sanas prácticas en materia de seguridad.

1.3 Objetivos específicos.

a) Determinar si el jerarca y los titulares subordinados formalizaron y divulgaron las políticas, lineamientos, procedimientos para la definición, control y administración de usuarios del sistema Comercial OPEN.
b) Evaluar si el perfil es conforme a las funciones desarrolladas.
c) Determinar la existencia de funcionarios no activos con perfiles activos.
d) Identificar roles y privilegios no autorizados.
e) Comprobar la existencia de perfiles asignados a funcionarios que no deban existir en el sistema en producción.
f) Evaluar las transacciones y registro de quien, cuando, y que modificó cada usuario en los datos que se almacenan las tablas del sistema, con respecto al perfil asignado.

1.4 Alcance de la Auditoría

La auditoría abarcó los datos en Open al 30 de junio del 2021 En lo que fuera de interés se amplía el periodo de análisis a efectos de cumplir con el objetivo del estudio

1.5 Criterio de auditoría

Los criterios de Auditoria relativos al análisis y fundamento legal para la asignación de perfiles de usuario y su administración fueron presentados en fecha 21 de junio del 2021. Posteriormente se remitieron los criterios al Gerente General con el oficio AU-2021-00503 del 6 de julio del 2021 y no se recibieron observación alguna.

1.6 Metodología Aplicada.

La auditoría se realizó de acuerdo con lo establecido en la Ley General de Control Interno Nro.8292, las Normas Generales de Auditoría para el Sector Público y Manual de Políticas y Procedimientos de la Auditoría Interna de AyA.

La metodología empleada se enfocó en la aplicación de técnicas de auditoría, tales como: solicitudes de información, revisión y análisis de documentos, encuestas, análisis de la información que se registra en las tablas de datos del OPEN en materia de administración funcional (Dirección del Sistema Comercial Integrado) y normativa aplicable al objeto de estudio.

La encuesta se aplicó a más de 100 usuarios del sistema a nivel las seis regiones en la que se utiliza el OPEN. Se obtuvieron 61 respuesta.

La encuesta aplicada tuvo como fin el determinar el grado de conocimiento que mantienen los usuarios de las características funcionales que le permite los privilegios asignados en el perfil de usuario según sus funciones, de igual forma el determinar el grado de capacitación o adiestramiento recibido, así como la supervisión que recibe de sus labores, entre otros aspectos propios del proceso de asignación y administración de perfiles que mantiene el sistema OPEN.

Con respecto al análisis de datos que se evaluaron, se evaluaron los registros que se almacenan en las tablas de la base de datos identificadas con los nombres: usuarios, perfiles, usuarios_perfil, perfil_objeto, objetos y car_var, en el análisis se utilizaron las herramientas tecnológicas ACL Lenguaje para consultas de auditoría y Power BI herramienta de visualización y análisis de datos.

1.7 Limitaciones que afectaron la ejecución de la auditoría

A continuación, se detallan las limitaciones presentadas durante la ejecución de la auditoría:

La imposibilidad de poder actualizar el licenciamiento de uso de la herramienta tecnológica ACL.

La falta de conocimiento en las estructuras aprobadas para la documentación y preparación de papeles de trabajo de los estudios desarrollados por la Auditoria Interna, afecto la discusión, revisión y programación actividades del estudio

1.8 Aspectos de la Ley General de Control Interno N.°8292

En atención a recomendaciones emitidas por la Contraloría General de la República y en aras de cumplir con la legislación vigente, sobre todo con el fin de fortalecer los canales de información entre los titulares subordinados y la Auditoría Interna, se transcribe los artículos Nro. 36, 37, 38 y 39 de la Ley General de Control Interno, publicada en la Gaceta Nro.169 del 4 de setiembre de 2002.

> *"[…]*
>
> ***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.*
>
> *El acto en firme será dado a conocer a la auditoría interna y al titular subordinado correspondiente, para el trámite que proceda.*
>
> *"**ARTÍCULO 38.** —Planteamiento 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, N° 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.
El jerarca, los titulares subordinados y los demás funcionarios públicos incurrirán en responsabilidad administrativa, cuando debiliten con sus acciones el sistema de control interno u omitan las actuaciones necesarias para establecerlo, mantenerlo, perfeccionarlo y evaluarlo, según la normativa técnica aplicable".

1.9 Conferencia final de los resultados de la Auditoría

Los resultados de la auditoría se expusieron a través de video conferencia el día 16 de noviembre de 2021, a la Gerencia General Eric Alonso Bogantes Cabezas, Ana Cristina Pereira Meneses, Dirección de TI Miguel Cordero Leiva, Luis Fernando Ulate Vargas, Dirección Comercial Nacional Armando Rodríguez Angulo, Patricia Zeledón Villalta, Luis Guillermo Solano Espinoza, Funcionarios del Área Metropolitana Alejandro Calderón Acuña, Adriana Zamora Amador, Luis Fernando Cubillo Lobo, Paola Campos Porras, Silvia Quesada Campos, de la Unidad de Control Interno Sonia Murillo Hurtado, Dirección Jurídica Rodolfo Lizano Rojas, Dirección de Capital Humano Yolanda Salas Hernández, Sub Gerencia Sistemas Periféricos Natalie Montiel Ulloa, Eduardo Solano Campos, de la Junta Directiva Federico Avilés Chaves, Fabio Vincenzi Guilá, Gerardo Morera Rojas, Yolanda Acuña Castro y de la Auditoría Interna Karen Espinoza Vindas, Marco Espinoza Rosales y Luis Fernando Vindas Murillo

El informe borrador se remitió con el oficio AU-2021-970 de 17 de noviembre de 2021.El 2 de diciembre se recibieron de parte de la Gerencia General las observaciones al informe borrador con el oficio GG-2021-04549.

Las observaciones fueron analizadas por la Auditoría Interna. En el Anexo Nro.2 se encuentra el análisis realizado.

2. RESULTADOS

2.1 El Jerarca no cuenta con un asesor en tecnología de información (TI)

En la actualidad no existe una comisión o comité que asesore a la Junta Directiva en materia de tecnología de información.

Se determina que en Minuta No. 16-2017 de fecha: 14/07/17el Consejo Gerencial acuerda:

> *"(…) Tema 3: Conformación Comisión de Tecnologías de Información (GG-DSI-2017-00512)".*

Las Normas de Control Interno del Sector Público (NCISP) que los sistemas de información deben estar integrados a nivel organizacional y ser coherentes con los objetivos institucionales y, en consecuencia, con los objetivos del SCI.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (NTGCTI), emitidas por la Contraloría General de la República[1], norma que la Junta Directiva debe apoyar sus decisiones sobre asuntos estratégicos de TI en la asesoría de una representación razonable de la organización que coadyuve a mantener la concordancia con la estrategia institucional, a establecer las prioridades de los proyectos de TI, a lograr un equilibrio en la asignación de recursos y a la adecuada atención de los requerimientos de todas las unidades de la organización.

Con el acuerdo 2019-468 tomado en sesión extraordinaria 2019-074 del 3 de diciembre de 2019 y comunicado el 4 de diciembre de 2019, la Junta Directiva aprobó el documento denominado "Conformación y funcionamiento de la comisión de Tecnologías de Información y Comunicaciones" (Comisión de TI) del Instituto Costarricense de Acueductos y Alcantarillados, adscrita al Consejo Gerencial Institucional y conformada por las siguientes áreas y sus representantes.

En diciembre del año 2019, la Junta Directiva de AyA mediante acuerdos conoce y aprueba el documento denominado "Conformación y funcionamiento de la comisión de Tecnologías de Información y Comunicaciones" (Comisión de TI) del Instituto Costarricense de Acueductos y Alcantarillados, adscrita al Consejo Gerencial Institucional.

El anterior acuerdo es tomado como parte de la Normativa regulatoria establecida por la Contraloría General de la Republica antes de enero 2022, en el entendido que la organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o

[1] Que se derogan el enero del 2022, por la entrada en vigencia de la normativa que emita el Ministerios de Ciencia; Innovación, Tecnología y Telecomunicaciones.

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

modificación no autorizados, daño o pérdida u otros factores disfuncionales.

De igual forma para noviembre del 2021 el Ministerio de Ciencia y Tecnología comunica el Marco Normativo de Gobierno y Gestión de las Tecnologías de Información, que sustituyen (N-2-2007-CODFOE) derogadas por la Contraloría General de la República mediante la resolución N° R-DC-17-2020 del diecisiete de marzo del dos mil veinte. Las nuevas normas técnicas de Tecnologías de Información entrarán en vigor a partir del 1 de enero del 2022.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información establecido por el Ministerio de Ciencia y Tecnología mantienen su base en las sanas prácticas, además de lo que en esta materia dispone o propone el COBIT 19, para los entes que acojan este marco regulatorio, en este sentido el AyA debe realizar un análisis de las brechas que puedan existir entre lo ya caminado en la disposición y las nuevas disposiciones, a efectos de tener la claridad necesaria del esfuerzo a realizar en cumplimiento de lo dispuesto.

El hecho de no haberse implementado como corresponde la Comisión de Tecnologías de Información debilito la toma decisiones en los diferentes niveles de la administración, conllevando el tener que declararse desiertos procesos de contratación aumentado los riesgos asociados a los sistemas computarizados y el hardware asociado a los sistemas.

2.2 Cumplimiento de los roles y responsabilidades definido en las políticas de TI aprobadas por la Junta Directiva.

A pesar de que existen las aprobaciones requeridas en el nivel de Junta Directiva para el cumplimiento de las Normas de la Contraloría General de la República, se tiene que las mismas no fueron implementadas como corresponde, en esta norma aprobada por Junta Directiva se tiene:

Tabla 1

Detalle de normativa

Acuerdo	Detalle
2019-469	“Políticas estratégicas para la gestión de las tecnologías de información y de comunicaciones - TIC'S - del Instituto Costarricense de Acueductos y Alcantarillados
2019-470	“Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados”.
2019-471	Perfiles para los oficiales de Seguridad de la Información y Ciberseguridad, y se trasladan a la Dirección Gestión de

Acuerdo	Detalle
	Capital Humano, para su inclusión en el Manual de Puestos y la gestión de las plazas respectivas
	Oficial de Ciberseguridad, sea parte de la Dirección de Sistemas de Información. En tanto no se cuente con la Plaza para el nombramiento de una persona que se dedique en forma exclusiva a esta función, las actividades se distribuirán entre las diferentes áreas de la Dirección. Oficial de Seguridad de la Información, la Gerencia General, la Subgerencia de Ambiente, Investigación y Desarrollo y la Dirección de TI, realizarán una valoración para identificar el área a la cual deberá pertenecer. En tanto no se tenga esta definición y no se cuente con la Plaza para el nombramiento de una persona que se dedique en forma exclusiva a estas funciones, las actividades las asumirá la Unidad de Control Interno, como parte de la Administración del Sistema de valoración de riesgo – Sevri. Los oficiales de seguridad de la información y de ciberseguridad, serán parte del Comité de Seguridad institucional que está promoviendo la Subgerencia de Ambiente, Investigación y Desarrollo. •Las funciones del Comité de Seguridad de TI, las asumirá el Consejo de Gerencia, en tanto se concreta un Comité de seguridad institucional.

Fuente: autoría propia a partir de la información puesta en el sitio Web de la Junta Directiva

Con respecto a lo dispuesto en acuerdo 2019-471 en específico a: "*En tanto no se tenga esta definición y no se cuente con la Plaza para el nombramiento de una persona que se dedique en forma exclusiva a estas funciones, las actividades las asumirá la Unidad de Control Interno, como parte de la Administración del Sistema de valoración de riesgo – Sevri*.", de lo anterior se tiene que mediante memorando PRE-UCI-2020-00008 del 27 de febrero del 2020, la encargada de la Unidad de Control Interno de AyA, comunica a la Presidencia Ejecutiva y Gerencia General de ese entonces, con respecto a la asignación de las nuevas funciones de oficial de seguridad: "*En atención al memorando de la referencia, y agradeciendo el nombramiento que se me hiciera como Oficial de Seguridad de la Información, debe hacer manifiesta mi preocupación y oposición a dicho nombramiento, debido a que como es de conocimiento de Ustedes, esta Unidad no cuenta con la capacidad instalada para asumir las funciones de Oficial de Seguridad de la Información, tal y como lo indica el acuerdo del Consejo Gerencial, debido a que no poseo personal que me apoye como para asumir el correspondiente compromiso".* De lo indicado por la

Licda. Murillo Hurtado en referencia a no poder ejercer esa responsabilidad que se le asignó, se determinó que no existió ninguna gestión de parte de la Gerencia General para poder asignar a otra área la tarea de Oficial de Seguridad de la Información, incumpliéndose lo dispuesto por Junta Directiva.

De igual forma se determinó con respecto a lo que dispone el acuerdo 2019-470 en referencia a: ***El responsable del Área de Recursos Humanos*** *o quién desempeñe esas funciones, cumplirá la función de notificar a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan. Asimismo, tendrá a su cargo la notificación de la presente Política a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los Compromisos de Confidencialidad (entre otros) y las tareas de capacitación continua en materia de seguridad de la información.* Con respecto a esta asignación, la Dirección de Capital Humano en cumplimiento a lo dispuesto por Junta Directiva, indico con memorando **GG-DCH-2021-03238** del 1 de noviembre del 2021:

> "(…) *nos permitimos informar que el Acuerdo de Junta Directiva que se indica, no ha sido recibido en esta Dirección según los registros que se llevan.*
>
> *Asimismo, hemos consultado a la Dirección de Sistemas de Información en relación con el tema de "Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados"* a lo cual se nos ha indicado que *"es un tema institucional que se elevó en su momento a la Gerencia General para que se implemente institucionalmente en alguna dependencia como un proceso independiente de dicha Dirección. Es indispensable señalar que a esta Dirección no se le ha solicitado o instruido en la temática a la fecha."*

Por lo anterior se puede determinar con plena certeza que lo aprobado y dispuesto por la Junta Directiva en materia de seguridad de las TI, a la fecha de este informe, no han sido divulgadas, promovidas e implementadas, a pesar que la política se dictamina como: *"La Política de Seguridad de la Información que se dictaminada en cumplimiento de las disposiciones legales vigentes, con el objeto de gestionar adecuadamente la seguridad de la información, los sistemas informáticos y el ambiente tecnológico del AyA. Debe ser conocida y cumplida por todo el personal del AyA, tanto se trate de funcionarios políticos como técnicos, y sea cual fuere su nivel jerárquico y su situación contractual".*

Sin embargo, a pesar del comentario anterior se debe indicar que se le preguntó al actual director de Sistemas de Información en relación con la implementación de la política de seguridad a lo que contestó: *"Le informo que en la Dirección de Sistemas de información se desarrolló en el año 2018 una plataforma de seguridad (ADS) para las aplicaciones, lo que ha sido sin duda un punto clave para facilitar y fortalecer la gestión para la seguridad en los sistemas desarrollados a lo interno o a la medida, y aparte de estandarizar lo referente al trato de nivel de acceso, reduce el tiempo de*

desarrollo de las aplicaciones por la existencia de un componente preconstruido para incrustarlo y adecuarlo en cada sistema". Ahora bien, de lo informado por el Lic. Cordero Leiva se debe indicar que la política aprobada va más allá de lo informado por él, además de que en lo que respecta a la divulgación, capacitación a todo el personal no se indica ninguna acción al respecto.

A mayor abundamiento se debe indicar que La Dirección del Sistema Comercial Integrado no conoce ni aplica lo dispuesto en acuerdo de Junta Directiva 2019-470. Políticas de seguridad & TI, lo que informa el Director Comercial Nacional, en repuesta dada en memorando No.GG-SCI-2021-00593 el 3 de setiembre de 2021, en el cual se refiere a que *realizó la consulta a la Dirección de Sistemas de Información a efectos de que le informaran con respecto las estrategias de divulgación, comunicación y capacitación que se hayan ofrecido para materializar el cumplimiento de dicho acuerdo, toda vez que el acuerdo no era conocido por su persona en calidad de Director Comercial Nacional,* indicando que de la consulta realizada: *no obtuvo respuesta de la Dirección de TI.*

Las NTGCT establecen en cuanto a la ***Gestión de la seguridad de la información***:

> *"1.4* ***Gestión de la seguridad de la información*** *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 en relación con los siguientes aspectos:*
>
> - *La implementación de un marco de seguridad de la información.*
> - *El compromiso del personal con la seguridad de la información.*
> - *La seguridad física y ambiental.*
> - *La seguridad en las operaciones y comunicaciones.*
> - *El control de acceso.*
> - *La seguridad en la implementación y mantenimiento de software e infraestructura tecnológica.*
> - *La continuidad de los servicios de TI.*
>
> *Además, debe establecer las medidas de seguridad relacionadas con:*
>
> - *El acceso a la información por parte de terceros y la contratación de servicios prestados por éstos.*

- *El manejo de la documentación.*
- *La terminación normal de contratos, su rescisión o resolución.*
- *La salud y seguridad del personal.*

Las medidas o mecanismos de protección que se establezcan deben mantener una proporción razonable entre su costo y los riesgos asociados.

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.
c. Establecer, cuando corresponda, acuerdos de confidencialidad y medidas de seguridad específicas relacionadas con el manejo de la documentación y rescisión de contratos".

De la auditoría se pude determinar que no existió una coordinación previa al momento de formular las políticas, de tal forma que permitiera determinar las involucrados conforme las funciones y responsabilidades institucionales; y claro está la cantidad de recurso y disponibilidad. Por parte de los funcionarios que conforman el Comité de Seguridad y quien preside este órgano, hacen que el cumplimiento a lo dispuesto por la Contraloría General de la República en las NTGCT, se cumpla únicamente en el contar con las políticas que establece la norma, no así en la implementación y conocimiento de esta, según se regula.

Un aspecto que pudo afectar la atención de los acuerdos se determinó, que lo fue la rotación de personal en el nivel de la Gerencia General y Subgerencia General, Subgerencia de Investigación y Desarrollo y otras, además de Presidencia Ejecutiva y Dirección de Sistemas de información lo que incidido directamente en el que se implementara la Política. Por último, se debe indicar que la propuesta de asignar algunas de las responsabilidades de la política a la Unidad de Control Interno, no necesariamente fue una decisión apropiada para las condiciones o requerimientos que se deseaban, más aún el no haber propuesto otra área para la atención de la política a la Junta Directiva, hizo que las acciones necesarias para la implementación no se ejecutaran.

La Política de seguridad establece que la administración de la seguridad de la información es parte fundamental de los objetivos y actividades del AyA, el efecto

de no implementarla de forma apropiada incide directamente en el riesgo asociado a los sistemas, redes, equipos, información e instalaciones que soportan las TI. Es fundamental el conocimiento y el compromiso de los funcionarios con la política que regulan el accionar en esta materia. En la medida que este conocimiento no exista, imposibilita el pedir y exigir responsabilidad en este tema.

2.3 Deficiencias encontradas en el grado de capacitación y conocimiento del perfil asignado a los usuarios del sistema OPEN con respecto a las funciones asignadas.

A efectos de determinar el grado de conocimiento de las características asignadas a cada perfil en función de las actividades desarrolladas por los funcionarios que desempeñan funciones en el sistema comercial, se desarrolló y aplicó una encuesta anónima.

De los resultados de la encuesta se pudo determinar:

- El 35% de los funcionarios encuestados manifiesta no conocer las características del perfil asignado para las funciones que realiza.
- El 24%, indica no conocer cuál es el nombre del perfil asignado
- El 46% no recuerda haber firmado la boleta de TERMINOS Y CONDICIONES PARA EL USO DE CLAVES Y PERFILES.
- El 100% de los encuestados, indican que alguien les supervisa su trabajo.
- El 46% indica no haber recibido, ni recibir una capacitación adecuada para el uso del sistema comercial OPEN con respecto a las funciones asignadas.

Las NTGCT establecen en la norma 1.4.2, lo relacionado con el ***Compromiso del personal con la seguridad de la información:***

A mayor abundamiento, las Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados, establecen:

> *"Política 3.2:* ***Capacitación del Usuario***
>
> *Formación y Capacitación en Materia de Seguridad de la Información*
>
> *Todos los empleados del AyA y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el AyA recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del AyA. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.*
>
> *Política 6:* ***Control de Accesos Generalidades*** *El acceso por medio de un sistema de restricciones y excepciones a la información es la base*

de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento".

De igual forma, estipula el contrato de TERMINOS Y CONDICIONES PARA EL USO DE CLAVES Y PERFILES, el cual en principio es firmado por cada usuario que es creado en el sistema comercial:

"(…)
en cuanto a que "toda operación que se realice quedará registrada en los sistemas de seguridad que poseen: El Open SCI, Datamart Comercial, Archivo Histórico y SIGOS. Este registro electrónico es la prueba ante cualquier instancia administrativa o judicial, de que la operación fue realizada por el usuario asignado.

Acepto el Perfil de _____ conforme a las tareas asignadas, el día
Nombre y apellido del funcionario y firma", lo anterior aunado a que un 46% de los que respondieron la encuesta indicaron no recordar el haber firmado el contrato de términos y condiciones de uso de claves y perfiles.
(…)"

En cuanto a las posibles causas que originan los resultados de la encuesta se tiene que:

1. Los efectos que causó la facturación por estimados en el año 2020 y el gran número de comunicados que existieron por parte de la Gerencia General, Dirección Comercial y reuniones virtuales confundieron al personal en la tramitología para la resolución de casos.

2. Falta de un programa de capacitación adecuado y permanente para el adiestramiento, manejo y operación del sistema con base en el perfil asignado, hace que el funcionario no cuente con el conocimiento adecuado para las labores que se le asignan. (…)"

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

Las modificaciones al sistema o la incorporación de nuevas operativas, como la aplicación del transitorio, o el prorrateo de consumos, ajustes por normativa, sin la debida capacitación afectan de forma directa el accionar diario de los funcionarios que interactúan con los abonados y los sistemas automatizados, más aún cuando por ejemplo estas rutinas presentan hechos que comprometen la atención, como lo es el caso de que se facture el impuesto al valor agregado en recibos con consumos menores a 30 m^3, que han sido ajustados.

Se tiene que, dentro de los efectos de una inadecuada capacitación de lo que puedo realizar en el sistema OPEN, conforme las funciones del funcionario público aumentan el riesgo de que las adecuaciones que se realicen a las facturas puestas al cobro se ajusten de forma indebida y con ello, se afecte el cumplimiento de proteger y conservar el patrimonio público contra cualquier pérdida, despilfarro, uso indebido, irregularidad o acto ilegal. A su vez, se potencia el riesgo de una atención equivocada al público que reclama o realiza una gestión cualquiera ante la Institución.

2.4 Usuarios con más de una cuenta activa asignada en el sistema Comercial

De la muestra revisada al 21 de setiembre del 2021, se determina que los siguientes usuarios mantienen varias cuentas activas con diferente nomenclatura de acceso al sistema comercial integrado OPEN, la información se extrae de la tabla usuarios:

1. Alvarez Alfaro Rudy AYAC2034, AYA04121, código UNICOM 4211

SEGURIDAD SGC	AYA2034	Rudy Alvarez Alfaro	*4411*	*4411*
MANUAL	AYA04121	Alvarez Alfaro Rudy	*4211*	*4211*
SEGURIDAD SGC	AYAC2034	Alvarez Alfaro Rudy	*4211*	*4211*

Tabla usuario_perfil

USUARIO	F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
AYA77504	*04/04/2011 00:00:00*	SEGURIDAD SGC	AYAC2034	JEFE OFI_COM_1	vb

Autoría: propia se extrae de la información que contiene la tabla usuarios del sistema OPEN

2. Dayana Rodriguez Galeano AYA26011, AYA72602 código UNICOM 1213 y 1312
3. Edgar Trejos Alvarado AYA6499, AYA499, AYA62999 código UNICOM 1110, 1200, 1211
4. Fabricio Murillo Rojas DCM00165, DCM00190 código UNICOM 1111
5. Gerardo Noguera Valverde AYA 60942, AYA60904 código UNICOM 3211
6. Gerardo Quiros Ulloa AYA6860, AYA68600 código UNICOM 1200

7. José Aniceto Acuña Garro AYA00647, AYA6471, AYA6470, AYA6472, AYA6473, AYA6474 código UNICOM 1111, 1213, 1313, 1413, 1312, 1111
8. Jairo Stevens Adams AYAC2133, AYA0920 código UNICOM 4311
9. Johnny Arauz Díaz AYA05155, AYA5155 código UNICOM 3711, 3411
10. Jonny Badilla Duarte AYA00992, AYA992 código UNICOM 5112, 5911
11. Jorge Chaves Campos AYA04374, AYA4374 código UNICOM 2411
12. Jorge Rodriguez Zeledon AYA01104, AYA01048 código UNICOM 1111
13. Julio Ramirez Torres AYAC0246, AYA69978 código UNICOM 1213, 1110
14. Luis Granados Solis AYA94880, AYA39488 código UNICOM 3311
15. Luis Paulino Chacon Salas AYA25921, AYA32592, AYA22592 código UNICOM 1126, 1300, 1200
16. Marco Tulio Cruz Campos AYA24976, AYA24976 código UNICOM 1400, 1413
17. Orlando Alvarado Arias AYA3211, AYA2290 código UNICOM 1111, 1100
18. Rafael Rodriguez Soto AYA73689, AYA73683 código UNICOM 1126
19. Rodrigo Meneses Obando AYAAYA52, AYA52697 código UNICOM 1413
20. Victor Ureña Ureña AYA88032, AYA8032 código UNICOM 1313, 1110

En anexo Nro.2 se informa el detalle de las características de cada uno de los ID de funcionarios asociados a cada uno de los usuarios del sistema.

Con respecto al tema de definición de las políticas de acceso establecidas por el AyA, el Acuerdo de Junta Directiva N. 2019-470 dispone:

Las Políticas de seguridad TI, aprobadas se norma lo que corresponde el control de acceso en la política 6

> ***"Política 6: Control de Accesos***
>
> ***Generalidades***
>
> *El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.*
>
> *Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.*
>
> *La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto, es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces,*

en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Objetivo

a. Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
b. Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
c. Controlar la seguridad en la conexión entre la red del AyA y otras redes públicas o privadas.
d. Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
e. Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
f. Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

Alcance
La política definida en este documento se aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los sistemas de información, bases de datos o servicios de información del AyA, cualquiera sea la función que desempeñe.

Los propietarios de la información estarán encargados de:

a. Evaluar los riesgos a los cuales se expone la información con el objeto de:

1. Determinar los controles de accesos, autenticación y utilización a ser implementados en cada caso.
2. Definir los eventos y actividades de usuarios a ser registrados en los sistemas de procesamiento de su incumbencia y la periodicidad de revisión de los mismos.

b. Aprobar y solicitar la asignación de privilegios a usuarios.

c. Llevar a cabo un proceso formal y periódico de revisión de los derechos de acceso a la información y conjunto con el Oficial de Seguridad de la Información.

Reglas de control de acceso

Las reglas de control de acceso especificadas deberán:

a. *Indicar expresamente si las reglas son obligatorias u optativas*

b. ***Establecer reglas sobre la premisa "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente**".*

c. Controlar los cambios en los rótulos de información que son iniciados automáticamente por herramientas de procesamiento de información, de aquellos que son iniciados a discreción del usuario.

d. Controlar los cambios en los permisos de usuario que son iniciados automáticamente por el sistema de información y aquellos que son iniciados por el administrador.

e. Controlar las reglas que requieren la aprobación del administrador o del propietario de la información de que se trate, antes de entrar en vigencia, y aquellas que no requieren aprobación.

Política 6.2: Administración de accesos de usuarios
Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Registro de Usuarios

El Oficial de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

1. *Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.*

2. *Verificar que el usuario tiene autorización del propietario de la información para el uso del sistema, base de datos o servicio de información.*

3. *Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la política de seguridad del AyA, por ejemplo, que no compromete la separación de tareas.*

4. *Entregar a los usuarios un detalle escrito de sus derechos de acceso.*

5. *Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.*

6. *Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.*

7. *Mantener un registro formal de todas las personas registradas para utilizar el servicio.*

8. *Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del AyA o sufrieron la pérdida/robo de sus credenciales de acceso.*

9. *Efectuar revisiones periódicas con el objeto de: a. Cancelar identificadores y cuentas de usuario redundantes*

10. *Inhabilitar cuentas inactivas por más de 60 días.*

11. *Eliminar cuentas inactivas por más de 120 días.*

12. *En el caso de existir excepciones, deberán ser debidamente justificadas y aprobadas.*

13. *Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.*

14. *Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados".*

La falta de una rutina en el sistema OPEN que valide la existencia del nombre de un usuario permite que se den casos como los que se citan. En específico a los usuarios del OPEN, se debe indicar que si existe una rutina en el nivel de generar su clave de acceso "ID" (AYAXXXX, DCMXXXX, etc.) la cual no permite el que se duplique el ID, no así el nombre de funcionario.

En este sentido se debe indicar que no existe una labor de calidad de datos, de parte de las áreas involucradas (Dirección Comercial Nacional, y del mismo usuario), por cuanto se considera difícil o casi imposible de manejar para un mismo usuario, cual clave debe utilizar para una función específica cuando se cuenta con 6 usuarios definidos como el caso de José Aniceto Acuña Garro con usuario: AYA00647, AYA6471, AYA6470, AYA6472, AYA6473, AYA6474 código UNICOM 1111, 1213, 1313, 1413, 1312, 1111, todos ellos con diferente oficina.

Por otra parte, se determinó que el usuario AYAD0003 Reyner Arguedas Chaves, funcionario de la Empresa ATESA responsable de la carga de usuarios para el subsistema SIGOS, desarrolló el día 23 de mayo de 2018, la carga masiva de datos de usuarios, y que dentro de las actividades realizadas registró un número significativo de usuarios duplicados con ID de identificador de usuario diferentes lo cual refleja que no existió una depuración adecuada de los datos de carga. Al igual en consulta realizada a la Dirección de Sistemas de Información en específico el Lic. Enrique Angulo encargado de mantenimiento del sistema comercial, informó que existen dos lugares en donde se incluyen datos de usuarios en el sistema OPEN, uno en la Dirección Comercial Nacional y otro en la Dirección de Sistemas de información de

parte del personal de mantenimiento del sistema y administradores de base de datos a solicitud del área funcional, aspecto que facilita el que se presenten este tipo de inconsistencias.

Asimismo, se indica que el sistema y su lógica de roles obliga a que se tenga que crear varios usuarios para un mismo funcionario, a manera de ejemplo, el rol de notificador, lector, resolución de ordenes de servicio, etc., este aspecto para personal de campo, implica que para cada función deba mantener un usuario diferente esto ocurre con mayor incidencia en las zonas de periféricos donde las labores de los funcionarios es variada (poli funcionabilidad), de igual forma por la lógica como trabaja el sistema cuando un funcionario que deba trabajar en una labor determinada en una oficina cantonal con un centro técnico específico, que deba ayudar a otra oficina en las mismas funciones, se debe crearse un nuevo usuario con un ID diferente con centro técnico diferente y oficina cantonal diferente.

De lo descrito, se determina que la lógica aplicada en la creación y asignación de roles a usuarios no es la apropiada en una sana administración de base de datos.

Como efecto se tiene, que la administración de usuarios se vuelva difícil de controlar y evaluar, además de que una posible conversión de datos se vuelva más compleja y con algún grado de probabilidad de fallos, mantenimiento de programas y rutinas de sistemas difícil y complejas.

Además de que, con lo actuado por personal ajeno a la Administración Funcional (Dirección del Sistema Comercial Integrado) se incumple con lo que dispone la norma en cuanto a la separación de funciones entre desarrollo, pruebas, y producción del sistema, al estar personal de mantenimiento incluyendo datos o carga de datos en el sistema.

2.5 Registro de transacciones realizadas por funcionarios no autorizados a realizar modificaciones, inclusiones, o borrado de datos de usuarios.

Se determinó de la auditoría que los siguientes usuarios externos han creado de forma inapropiada usuarios, en contrario a lo que regula el manual de Manual Usuario del Sistema de Seguridad de la aplicación SGC ADM-93-03-M02 (ver figura nro.1). Según lo indicado por el director Comercial Nacional con el memorando No.GG-SCI-2021-00593 del 3 de septiembre del 2021 existen dos funcionarios encargados del Sistema de Seguridad. El programa que ejecuta la función inclusión, modificación en el registro de datos de la base de datos del Sistema Comercial (OPEN SCI) en la inclusión de usuarios es efectivamente SEGURIDAD SGC.

Figura 1

Cantidad de usuario creados por personal externo

Fuente: Open SCI

De lo anterior se debe indicar con especial énfasis, que el usuario AYAD0003 modificó o incluyó 398 registros, recordando como se mencionó con antelación que no es funcionario del AYA, sino más bien es un funcionario de la Empresa ATESA, empresa contratada para el mantenimiento del sistema OPEN. A su vez, se indicó que es probable que esa acción de registro en la tabla del sistema obedece a la carga inicial de usuarios del sistema SIGOS en el año 2018.

La anterior condición debió ser supervisada y documentada, aspecto que no se pudo comprobar que existiera la documentación necesaria y requerida en este tipo de trabajos desarrollados por terceros

En esta misma condición se encuentra el usuario AYAD0002, con 110 registros.

Con respecto a la carga masiva de datos, las sanas practicas disponen que cuando se tenga que realizar este tipo de labores, sea el Desarrollador de la Base de Datos (DBA)el que realice las mismas.

El usuario DBA no existe en el sistema con ese nemónico, sin embargo, mantiene un registro de 3 registros. Al respecto, la encargada del módulo de seguridad del sistema comercial en referencia a este usuario y se obtuvo la siguiente respuesta:

> *“efectivamente en ocasiones cuando falla el sistema o se pega los contactamos, ya que la aplicación es vieja (…)”*

De igual forma se le pregunto al funcionario de la Dirección de Sistemas de Información si el registro de usuario DBA, era un usuario definido por la administración de base de la siguiente forma:

> *"en las únicas que puede salir ese dato me parece que son las tablas de modificación de perfiles y usuarios.*
> *(…)*
> *efectivamente... eso sucede porque en ocasiones la aplicación les falla; ya que es muy vieja. Entonces ellos nos llaman para que les colabore con algún cambio.... se les pone DBA, MANUAL para que quede la evidencia que fuimos nosotros y que se realizó de esa forma*
> *(…)*
> *el usuario DBA no existe, se pone así para identificar que no fueron los compañeros de comercial los que realizaron el cambio de oficina o perfil de un usuario. En TI habemos 3 personas que tenemos el rol de DBA. Los 3 tenemos usuarios diferentes, en mi caso es JLEIVA. De los 3 yo soy el que más a realizado algún tipo de cambio a nivel de usuarios a solicitud de comercial. (…)"*

Lo anterior deja claro que los usuarios de administración de base de datos modifican registros, incumpliendo con este accionar lo que disponen las regulaciones propias de la administración funcional, sanas prácticas y regulaciones de seguridad como lo son la separación de funciones.

Y así sucesivamente se registran una cantidad significativa de registros realizadas por diferentes usuarios los cuales no corresponden a los indicados en el memorando No.GG-SCI-2021-00593 por el Lic. Armando Rodriguez director Comercial Nacional.

Ejemplo:
AYA, GARCE, GARCE1, GARCE", GUSTAVO, MANUAL, etc. Valga indicar, que para los anteriores nombres de usuarios no se logró evidenciar a quien corresponde el ID registrado en las tablas.

Ahora bien, con No.GG-SCI-2021-00692 del 22 de octubre del 2021 la Licda. Patricia Zeledón Villalta, informa en relación con algunos de los funcionarios que aparecen con ID de usuario que registra transacciones en la base de datos, de la siguiente forma:

> *"(…)*
> *Con respecto al usuario AYAC0001 y AYAC0002; estos no existen en la base de datos, ni en la tabla usuarios y usuario perfil, como se evidencia en las pantallas que se adjuntan a continuación.*
> *Con respecto al usuario AYAC0003 este no existe en la base de datos; sin embargo, en la tabla usuario y usuario perfil si existen con valores 0 en el centro técnico, unidad comercial y perfil.*
> *Con respecto al usuario JLEIVA, este existe en la base de datos como parte de las funciones de administración de las bases de datos. En la tabla usuario y usuario perfil no está registrado ya que no requiere usar la*

aplicación del OPEN.
Con respecto al usuario DBA; estos no existen en la base de datos, ni en la tabla usuarios y usuario perfil.
Con respecto al usuario AYA; estos no existen en la base de datos, ni en la tabla usuarios y usuario perfil.
Con respecto al usuario SYSTEM, estos se crean de forma automático al crear la base de datos ORACLE y se le otorga el rol de DBA. Es una cuenta administrativa.

Sobre los usuarios indicados no existen registros de estos documentos físicos ni digitales en los archivos de esta Dirección. (…)"

De lo comentado por la encargada queda claro que existen funcionarios tanto internos como externos (contratados) que están interactuando con el sistema OPEN en el nivel de administración funcional, sin que exista al menos el documento formal de asignación de perfil y el conocimiento de las responsabilidades que se contraen con el AyA con el uso y administración del ID asignado, más aún no se tuvo conocimiento de reportes, controles o cualesquiera otro mecanismos de control que permitieran a la administración funcional (Dirección del Sistema Comercial Integrado) dar seguimiento y vigilancia a lo actuado por estos usuarios.

Ahora bien, con respecto a la administración de cuentas de usuarios y los perfiles asignados, se tiene que las NTGCTI disponen en la norma 1.4, lo correspondiente a la *Gestión de la seguridad de la información y a su vez, se norma*:

*"**1.3 Gestión de riesgos** La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable.*

***"1.4.5 Control de acceso** 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.

b. Clasificar los recursos de TI en forma explícita, formal y uniforme de acuerdo con términos de sensibilidad.

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

j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.

k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI".

***"1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica** La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información. Para ello debe:*

a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.
b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.
c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.
d. Controlar el acceso a los programas fuente y a los datos de prueba".

*"**4.1 Definición y administración de acuerdos de servicio** La organización debe tener claridad respecto de los servicios que requiere y sus atributos, y los prestados por la Función de TI según sus capacidades.*

El jerarca y la Función de TI deben acordar los servicios requeridos, los ofrecidos y sus atributos, lo cual deben documentar y considerar como un criterio de evaluación del desempeño. Para ello deben:

(…)
c. Definir con claridad las responsabilidades de las partes y su sujeción a las condiciones establecidas.
d. Establecer los procedimientos para la formalización de los acuerdos y la incorporación de cambios en ellos.
e. Definir los criterios de evaluación sobre el cumplimiento de los acuerdos.
f. Revisar periódicamente los acuerdos de servicio, incluidos los contratos con terceros".

*"**4.3 Administración de los datos** 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".

*"**4.6 Administración de servicios prestados por terceros** La organización debe asegurar que los servicios contratados a terceros satisfagan los requerimientos en forma eficiente. Con ese fin, debe:*

a. Establecer los roles y responsabilidades de terceros que le brinden servicios de TI.
b. Establecer y documentar los procedimientos asociados con los servicios e instalaciones contratados a terceros.
c. Vigilar que los servicios contratados sean congruentes con las políticas relativas a calidad, seguridad y seguimiento establecidas por la organización.
d. Minimizar la dependencia de la organización respecto de los servicios contratados a un tercero.
e. Asignar a un responsable con las competencias necesarias que evalúe periódicamente la calidad y cumplimiento oportuno de los servicios contratados".

*"**5.2 Seguimiento y evaluación del control interno en TI** El jerarca debe establecer y mantener el sistema de control interno asociado con la gestión de las TI, evaluar su efectividad y cumplimiento y mantener un registro de las excepciones que se presenten y de las medidas correctivas implementadas".*

Por su parte las NCISP establecen:

*"**1.5 Responsabilidad de los funcionarios sobre el SCI** De conformidad con las responsabilidades que competen a cada puesto de trabajo, los funcionarios de la institución deben, de manera oportuna, efectiva y con observancia a las regulaciones aplicables, realizar las acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del SCI".*

***"2.5.2 Autorización y aprobación** La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales".*

***"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".

***"4.5.1 Supervisión constante** El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos".*

***"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".*

A mayor abundamiento, el Acuerdo de Junta Directiva N. 2019-470: Esta junta directiva aprueba el documento denominado "Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados"

*"**Política 6.17: Identificación y autenticación de los usuarios** Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.*

En circunstancias excepcionales, cuando existe un claro beneficio para el AyA, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del propietario de la información de que se trate".

*"**Política 5.5: Separación entre instalaciones de desarrollo e instalaciones operativas** Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.*

Para ello, se tendrán en cuenta los siguientes controles:

a. Ejecutar el software de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, o directorios.
b. Separar las actividades de desarrollo y prueba, en entornos diferentes.
c. Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
d. Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas.
e. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la conexión.
f. Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
g. ***El personal de desarrollo no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos".*** (El resaltado no pertenece al original)

Para el caso que no puedan mantener separados los distintos ambientes en forma física, deberán implementarse los controles indicados en el punto "Separación de Funciones".

"Política 7: Desarrollo y mantenimiento de sistemas Generalidades *El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.*

Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

Por otro lado, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software".

Objetivos
a. Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.
b. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en

la cual se apoyan.
c. Definir los métodos de protección de la información crítica o sensible.

Alcance
Esta política se aplica a todos los sistemas informáticos, tantos desarrollos propios o de terceros, y a todos los sistemas operativos y/o software de base que integren cualquiera de los ambientes administrados por el AyA en donde residan los desarrollos mencionados".

Así las cosas, se determina que la causa principal identificada por la cual el personal de administración funcional (Dirección del Sistema Comercial Integrado) solicita a personal de mantenimiento del sistema o administración de base de datos del sistema OPEN el que realice actualización, inclusión y otro tipo de transacciones en las tablas asociadas al módulo de seguridad, radica en que el módulo o componente de desarrollado para la administración funcional del sistema, en lo correspondiente a la creación de usuarios, perfiles, objetos fue desarrollado hace más de 20 años, con la herramienta conocida como Developer versión 6, lenguaje de programación que a la fecha no es compatible con los sistemas operativos con los cuales trabaja el sistema OPEN, conllevando a que se tuviera que configurar un servidor virtual con una versión windows compatible con la versión del software, que permitiera el que el sistema pudiese ejecutarse, este módulo.

A esta limitación se debe adicionar problemas con la versión de Oracle que mantiene la base de datos, de ahí que se hable de que el sistema presumiblemente obsoleto con deficiencias en su operación. Ahora bien, a la pregunta si se habían realizado gestiones de compra de las nuevas versiones del lenguaje de programación, se obtuvo la respuesta que desde hace muchos años se habla del cambio tecnológico de la plataforma y el sistema, razón por la cual no se pensó en que fuese necesario el ir escalando en las versiones requeridas, además de la incidencia que implica la versión de ORACLE con que se cuenta. Se debe indicar que, a pesar de lo determinado en el estudio, en la actualidad se está en pruebas una nueva versión del módulo de administración y seguridad, que será puesta en operación con la fase intermedia de cambio de tecnología.

Por otra parte, también se tiene que como parte de nuevos componentes del sistema open (por ejemplo, SIGOS), se han realizado cargas iniciales de datos de usuarios, los cuales fueron ejecutados por personal externo al AYA. Con respecto a esta carga de datos se solicitaron las bitácoras, reportes o controles establecidos para el registro de transacciones, sin embargo se nos refirió a un modelo de gestión de mejoras el cual almacena el requerimiento y autorización de la puesta en operación, sin contarse con el detalle completo de registro que se procedieron a poner en operación y los datos que fueron cargados y sus pistas de auditoraje, indicándose que si se quería saber lo actuado por ese funcionario estaban las pistas de auditoría que mantiene cada tabla en sus registros.

Como lo establecen las diferentes normas citadas, esta es una de las situaciones no deseadas en una adecuada administración funcional de un sistema, en especial a la

separación de funciones, en forma adicional a que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.

En este sentido, queda claro que, para la revisión general realizada a los perfiles y sus privilegios, no existen los controles apropiados para evitar acciones dolosas. A mayor abundamiento, el hecho de la existencia de usuarios con ID genéricas como DBA, AyA, System, lo cual no permite identificar en forma precisa quien realizó el registro o modificación de datos.

El efecto más delicado, lo es la imposibilidad de determinar acciones dolosas realizadas por terceros o funcionarios de la Institución en la manipulación de datos en la base de datos del sistema comercial, sin poderse acreditar o identificar la persona que los causa.

2.6. Perfiles que no se encuentran definidos en el manual de perfiles 2020

Se logró determinar que se registran en el sistema OPEN, en específico en la tabla perfiles un número mayor de perfiles que los que se describen en el manual de perfiles 2020, algunos de los perfiles que no existen en el manual, pero si en la base de datos, son:

- Perfil en blanco sin nombre.
- ACT_REMESAS Actualizador de remesas desarrollo
- ADM_ADMINISTRADOR Administración administrador
- ADM_LECT_ANAL Administración lecturas responsable
- ADM_LECT_RESP Administración lecturas analista
- ADM_SOP_USO_RESP Administración soporte usuarios responsable
- AGENTE_RECAUD Agente recaudadores externos
- ANA_CNTRO TEC_CATST Analista de centro técnico y catastro
- ANA_PERFIL Centro técnico analista
- ANAL DESA PROY Administración proyectos
- ANAL_GOB Facturación de gobierno responsable
- ANALISTA_ATCLI_1 Analista de atención al cliente
- ANALISTA_GOB Facturación de gobierno responsable
- CL_ANALISTA Centro de lecturas analista
- COB_OFI_RESPONSABLE Cobros oficina responsable
- COBRO_ADMI Analista de cobro administrativo
- COM_MARGINALES Comunidades marginales
- CONSULTA_BDG_TOTAL Todas las consultas + BDG
- CONSULTA _BDG_ZONA Consulta de una zona + BDG

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

- CT_RESPONSABLE Centro técnico responsable
- DESARROLLO PROYECTOS HAY DOS PERFILES_ Administración proyectos
- DESARROLLO1 Desarrollo pruebas
- JEFE OFI COM.2 jefe de oficina comercial. Realiza atención directa al público
- NUEVO PERFIL Perfil prueba
- OPE_IMPRESION Operación impresión masiva
- PERFIL_SUB_REG Perfil subregión
- PRU_PERFIL Prueba perfil
- PRU2_PERFIL Prueba perfil
- PRUEBAPERFIL Prueba perfil
- RECAUDADOR Agente recaudador banco solidario

La Ley General de Control Interno, norma en el componente de actividades de control, específicamente en el artículo 5, que la Junta Directiva y los titulares subordinados de AyA; deben documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:

> *"v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación"*.
>
> *"**ARTÍCULO 16.- Sistemas de información** Deberá contarse con sistemas de información que permitan a la administración activa tener una gestión documental institucional, entendiendo esta como el conjunto de actividades realizadas con el fin de controlar, almacenar y, posteriormente, recuperar de modo adecuado la información producida o recibida en la organización, en el desarrollo de sus actividades, con el fin de prevenir cualquier desvío en los objetivos trazados.*
>
> *Dicha gestión documental deberá estar estrechamente relacionada con la gestión de la información, en la que deberán contemplarse las bases de datos corporativas y las demás aplicaciones informáticas, las cuales se constituyen en importantes fuentes de la información registrada.*
>
> *En cuanto a la información y comunicación, serán deberes del jerarca y de los titulares subordinados, como responsables del buen funcionamiento del sistema de información, entre otros, los siguientes:*
>
> ***a)** Contar con procesos que permitan identificar y registrar información confiable, relevante, pertinente y oportuna; asimismo, que la información sea comunicada a la administración activa que la necesite, en la forma y dentro del plazo requeridos para el cumplimiento adecuado de sus responsabilidades, incluidas las de control interno.*
> ***b)** Armonizar los sistemas de información con los objetivos institucionales y verificar que sean adecuados para el cuido y manejos eficientes de los*

recursos públicos.
***c)** Establecer las políticas, los procedimientos y recursos para disponer de un archivo institucional, de conformidad con lo señalado en el ordenamiento jurídico y técnico".*

Al igual que otros aspectos que se han determinado en este informe la falta de documentación apropiada y necesaria, se debe en principio a que el personal que mantiene esta área no sea suficiente para las funciones que fueron dispuestas al área Comercial Nacional en su totalidad, por el grado de especialización, conocimiento del sistema además del proceso comercial y la rotación de personal. Estos aspectos, permitieron el que se realizaran acciones de creación de perfiles, para resolver situaciones particulares, sin que estas decisiones hayan sido estudiadas y analizadas según una adecuada administración.

Un aspecto que complicó este hecho, lo fue el que en las regiones exista la polifuncionalidad, mientras que en el área metropolitana se dé la especialización en temas o procesos específicos, elemento que hizo que se generen una cantidad de perfiles con características y asignación de funciones más amplios para las regiones, los cuales resolvieron situaciones particulares y no nacionales. Ahora bien, para cualquiera que sea el caso no se justifica el hecho de que se creen perfiles sin la documentación necesaria y pertinente, por cuanto esta condición aumenta el riesgo de funcionamiento y administración del sistema.

La existencia de una cantidad mayor de perfiles a los que se conocen o documentan, imposibilita el ejercer una adecuada fiscalización y control a los usuarios de perfiles que no se conoce a que módulos y acciones puede acceder a modificar, actualizar o borrar registros, etc.
De igual forma, el no conocer a plenitud a que tiene derecho o responsabilidad cada usuario con su perfil, imposibilita el poderse imputársele al usuario alguna responsabilidad por los actos y hechos a los cuales no se le informó de sus competencias.

2.7 Usuarios activos en el sistema, con desactivación o modificación justificada por el encargado Regional.

Se determinó, que con memorando GSP-RA-2019-00668 del 10 de abril de 2019, el responsable comercial de la Región Huetar Atlántica comunica al Director Comercial Nacional:

"(…) En razón de mantener actualizada la información de las cuentas de usuario de acceso al Sistema Comercial Integrado OPENSCI, le remito adjunto los formularios respectivos para eliminar las cuentas de los usuarios: Lowell McLean Grant y Orlando Stephen Brenes. Ambos funcionarios laboran en la Cantonal de Limón y actualmente no utilizan el sistema citado" (…).

Ahora bien, de lo comunicado se tiene al 1 de setiembre de 2021, la tabla usuarios muestra para el usuario Orlando Stephen Brenes en los campos COD_UNICOM y COD_CENTEC los valores 4111 en ambos campos. De importancia el resaltar que existen dos usuarios con nombre Orlando Stephen Brenes, uno activo y otro inactivo, el AYA02036 (activo) con 0 sesiones permitidas sin perfil asociado lo cual evidencia una falta de integridad de datos y AYAC02036 sin cod_UNICOM ni cod_centec.

En este mismo sentido tenemos que, con correo del 17 de agosto 2021 el Director Comercial de la Región Chorotega comunica a la responsable de la actualización de registro de administración del OPEN en cuanto a la actualización de modificación de perfiles, entre los cuales hace ver que para el funcionario Arrieta Jimenez Odie se debe eliminar el perfil por cuanto ya no usa el OPEN, al 20 de setiembre se mantiene el perfil y el usuario activo, tablas usuarios, usuarios_perfiles.

De igual forma para el funcionario Baltodano Leon Hernán a la misma fecha se mantiene activo en el sistema OPEN, en igual circunstancia los funcionarios AYA21224 Castro Miranda Manuel, AYA21575 Julio Castro Vindas, Luis Felipe Loaiza Solano usuario AyA00242, German Obando Diaz usuario AYA63060, Luis Palma Vargas usuario AYA63784, Gary Rodriguez Moreira usuario AYA73216, Zúñiga Leal Monge S. usuario AYA95956.

A pesar de lo anterior, se tiene que el responsable de la actualización de registros de usuarios de la administración funcional le comunica al Director Comercial de la Región Chorotega, el 3 de septiembre de 2021 que la solicitud había sido resuelta, tal y como lo solicitó, los usuarios quedaron excluidos del sistema.

Por otra parte, mediante boleta de términos y condiciones de uso de claves y perfiles del OPEN solicita el director regional comercial de la Región Brunca, para el usuario Allan Avendaño Guido usuario AYA08924, se le cambie el perfil Jefe_ofi_com2 por Jefe_ofi_com4, con rige a partir 1 de setiembre del 2021, sin embargo al 20 de setiembre se identifica en la tabla usuario_perfil para este usuario el perfil Jefe_ofi_com2.

Así mismo, con boleta de términos y condiciones de uso de claves y perfiles del OPEN, el 9 de setiembre del 2021, se solicita el cambio de perfil de la funcionaria Damaris Fonseca Hernandez usuario AYA34010 perfil jefe_ofi_com3 a jefe_ofi_com2, al 20 de setiembre muestra la tabla usuario_perfil para este usuario jefe_ofi_com3.

Al igual con boleta de términos y condiciones de uso de claves y perfiles del OPEN solicita el director regional comercial de la Región Brunca, para el funcionario Jacob Esquivel Alfaro usuario AYA31488, se le cambie el perfil Jefe_ofi_com por Jefe_ofi_com1, con rige a partir 6 de setiembre del 2021, sin embargo al 20 de setiembre se identifica en la tabla usuario_perfil para este usuario el perfil Jefe_ofi_com.

En igualdad de condición el funcionario Juan José medina Ruiz usuario AYA51597 de

jefe_ofi_com2 a jefe_ofi_cam1. Solicitud de eliminación de usuario AYA05573 Alvaro Araya Garcia y se encuentra activo en el sistema.

Con memorando No.SG-GSP-RC-2021-00015 del 14 de enero del 2021, el Director comercial de la Región Central Oeste comunica al director comercial Nacional en referencia a la actualización de perfiles OPEN:

- El usuario AYA52248 funcionario Martín Mendez Fallas, está pensionado, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a este usuario.
- El usuario AYA64834 funcionario Javier Perez Jimenez, está pensionado, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a este usuario.
- La usuaria AYA10385 funcionario Daniela Barquero Bolaños, no labora para la institución, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a esta usuaria.
- La usuaria AYA01253 funcionario Giovana Segura Gonzalez, no labora para la Región, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a esta usuaria.
- La usuaria AYAC9625 funcionario Glady Badilla Brenes, no utiliza el OPEN para sus labores, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a esta usuaria.
- El usuario AYA20657 funcionario Helberth Castro Alfaro, no utiliza el OPEN para sus labores, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a este usuario.
- El usuario AYA4374 y AYA04374 funcionario Jorge Chaves Campos, no utiliza el OPEN para sus labores, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activo al 20 de setiembre del 2021, a este usuario. Valga indicar que este funcionario mantiene dos usuarios con diferente perfil (CT_AVERIAS y JEFE_OFI_COM1).
- La usuaria AYA01607 funcionario Liseth Hernandez Cordero, no labora para la institución, a pesar de lo indicado por el Lic. Calderon Brenes la tabla usuarios y usuarios_perfiles muestra activa al 20 de setiembre del 2021, a esta usuaria.

El reporte de actualización de perfiles de usuarios o eliminación de usuarios del Director Comercial de la Región central oeste, mantiene más indicaciones de eliminación o modificación, sin embargo se analizan estos casos a efectos de evidenciar que lo requerido por el procedimiento de actualizar el estado dé cada uno de los usuarios del sistema OPEN cada seis meses no se atiende como corresponde por parte de la Dirección Comercial Nacional.

Con memorando No.UEN-SC-GAM-2021-00254 del 26 de agosto del 2021, la directora de la UEN servicio al cliente GAM, comunica a la administradora funcional del sistema comercial en referencia a los usuarios:

- El usuario AYA67956 Quesada Sanabria Marco JEFE_OFI_COMERCIAL, no usa el

sistema.

- El usuario AYA68029 Quesada Trejos Rodolfo JEFE_OFI_COM 4, no usa el sistema.
- El usuario AYA68355 Juan Diego Quiros Gonzalez JEFE OFI_COM_1, no usa el sistema.
- El usuario AYA69002 Fabio Ramirez Brenes JEFE OFI_COM_1, no usa el sistema.
- AYA69405 Sylvia Ramirez Jara JEFE OFI_COM_1, no usa el sistema.
- El usuario AYA70609 Reyes Castro Alfredo JEFE_OFI_COMERCIAL, no usa el sistema.
- El usuario AYA74563 Rojas Jimenez Yessenia ADM_FACT_RESP, no usa el sistema.
- El usuario AYA76656 Cesar Alonso Sanchez Ramirez CT_ANALISTA, no usa el sistema.
- El usuario AYA80149 GILBERTH SANCHEZ JIMENEZ CT_ANALISTA, no utiliza el sistema.

Y así sucesivamente Directora de la UEN de servicio al cliente de AM, informa de más de cuarenta usuarios que ya no laboran o no usan el sistema, sin embrago se pudo evidenciar que los usuarios trascritos mantienen su usuario activo al 20 de setiembre del 2021, en el sistema según se acredita en las tablas de usuarios, usuarios_perfil.

Otro aspecto que se pudo evidenciar fue el hecho que se solicitó a la Dirección de Capital Humano el que se emitiera un reporte de funcionarios que se habían jubilado, renunciado o despedido de la Institución para los últimos 3 años, reporte que se cruzó con los registros existentes de la tabla de usuarios y se obtuvo el siguiente resultado:

Tabla 2

Tabla de usuarios activos en el sistema que no laboran para el AyA

CODIGO DE USUARIO	NOMBRE DEL FUNCIONARIO	MOTIVO	CODIGO CENTRO TÉCNICO	CODIGO DE OFICINA	NUMERO DE SESIONES	FECHA EN LA CUAL SE DA LA CONDICIÓN	NOM_PERFIL
AYA2026	ANGULO RODRIGUEZ ADRIANA	RENUNCIA	1110	1111	9	04/05/2020	ANALISTA ATCLI
AYA64834	PEREZ JIMENEZ JAVIER	JUBILADO	2111	2111	9	01/12/2020	ANALISTA ATCLI_1
AYA03118	ALPIZAR MORALES LEANDRO	JUBILADO	1111	1111	9	01/11/2019	AT_CLI_ANALISTA
AYA79632	SANCHEZ PEREZ JOSE AURELIO	JUBILADO	1111	1111	7	01/02/2019	CT_ANALISTA
AYAC0041	OBALDIA GARCIA JAVIER	DESPIDO SIN RESP.	1110	1110	5	26/07/2021	CT_ANALISTA
AYA52388	MENDEZ SOLANO JUAN LUIS	JUBILADO	2111	2111	9	01/05/2019	CT_RESPONSABLE_REG
AYAC1053	PANE SANCHEZ FRANCISCO	JUBILADO	1111	1111	8	01/03/2019	JEFE OFI_COM_1
AYA21336	CASTRO PACHECO WILLIAM	JUBILADO	1111	1111	5	01/01/2019	JEFE_OFI_COM 2
AYA67954	QUESADA SALAZAR MARIO	JUBILADO	3111	3111	9	11/08/2020	JEFE_OFI_COM 2
AYA89208	VARGAS ALFARO YAMILETH	JUBILADO	2411	2411	9	01/06/2021	JEFE_OFI_COM 2
AYA52248	MENDEZ FALLAS MARTIN	JUBILADO	2111	2111	5	01/02/2019	JEFE_OFI_COM 3
AYA07742	ARIAS SOLANO RODRIGO	JUBILADO	1111	1111	9	01/03/2019	JEFE_OFI_COM 4
AYA82670	SOLANO FERNANDEZ YORLENE	JUBILADO	1111	1111	10	01/06/2020	JEFE_OFI_COM 4
AYA83419	SOLANO VALVERDE FABIO	JUBILADO	1111	1111	5	01/04/2019	JEFE_OFI_COMERCIAL
AYA90412	VARGAS LEON RAFAEL	JUBILADO	1111	1111	5	01/08/2019	JEFE_OFI_COMERCIAL
AYA93240	VILLALOBOS ESPINOZA MARVIN	JUBILADO	1111	1111	5	01/02/2020	JEFE_OFI_COMERCIAL

Como se puede evidenciar de la tabla anterior existen varios funcionarios que mantienen su estatus de jubilado o renuncia por un periodo mayor a dos años, sin que muestren las acciones administrativas de desactivación en el sistema Comercial OPEN.

En cuanto a lo que dispone el procedimiento de Perfiles de Usuarios al Sistema Comercial Integrado, se tiene que:

> *"Dirección DEL sistema Comercial integrado, debe:*
>
> *Recomendar las políticas o instrucciones a utilizar, por parte de los usuarios en la administración adecuada de las claves de acceso.*
> *Aprobar, diseñar la creación de nuevos perfiles, así como la modificación, exclusión, de acuerdo a las solicitudes de las Subgerencias técnicas de la Gran Area Metropolitana y los Sistemas Periféricos.*
> *Asignar el perfil de usuario solicitado por las jefaturas correspondientes.*
> *Informar al responsable comercial el resultado de la solicitud.*
> *Realizar monitoreos periódicos a los accesos asignados para garantizar la seguridad del sistema.*
> ***Deshabilitar a usuarios que tienen acceso al SCI, Datamart Comercial, Archivo Histórico y Sigos, a solicitud de las jefaturas comerciales.***
> ***Enviar informes periódicos a las jefaturas comerciales, de los usuarios con perfiles asignados, para la revisión y actualización de los mismos***". (El resaltado no pertenece al original)

Ahora bien, con respecto a la deshabilitación de un usuario en el sistema OPEN, el Licenciado Armando Rodríguez Angulo con memorando No.GG-SCI-2021-00593, informa:

> *"(…) El procedimiento para seguir es el siguiente:*
> *a) Encargado de área solicita la exclusión de un usuario ya sea por: pensión, traslado, permiso, cese de contrato o muerte; a través de la boleta de Términos y condiciones para el uso de claves y perfiles.*
> *b) El encargado de área envía boleta vía correo electrónico o por memorando solicitando la exclusión.*
> *c) Se recibe el documento y se procede a ingresar al Sistema de Seguridad, ingresando el número de empleado y se procede con la desactivación quitando la oficina comercial y centro técnico, indicando la observación correspondiente.*
> *d) Una vez inactivado el usuario se ingresa en la ventana: Asignación de Perfiles a Usuarios, se ingresa el código de usuario y se quita el perfil asignado, anotando una observación. (…)"*

Aun cuando existe el procedimiento de solicitar la actualización y revisión de perfiles cada seis meses a las diferentes áreas comerciales involucradas de administrar y controlar la asignación de accesos y que en el particular dispone:

- Velar por que cada funcionario del área correspondiente cuente con el perfil adecuado y actualizado para operar el Sistema Comercial Integrado, Datamart Comercial, Archivo Histórico y Sigos.
- El perfil de acceso debe de ser asignado de acuerdo con las funciones asignadas a cada funcionario. Es importante qué a la hora de otorgarse los permisos de acceso, se determine que el funcionario tenga una clara separación de funciones.
- Informar al usuario de los alcances y responsabilidades del perfil asignado.
- Verificar que cuando un funcionario reciba un permiso de acceso al SCI, Datamart Comercial, Archivo Histórico y Sigos, lea y firme el documento que estipula los derechos y obligaciones adquiridas para el uso y cuidado de la clave asignada.
- Solicitar de forma inmediata deshabilitar la clave de acceso asignada al usuario que deja de laborar para el Área Comercial.
- Revisar y actualizar periódicamente la lista de perfiles de los usuarios asignados al Área Comercial de cada Región.
- Los privilegios concedidos a los usuarios deben ser ratificados cada 6 meses.
- Velar por el buen uso de los accesos al SCI, Datamar Comercial, Archivo Histórico, Sigos.

En este sentido establece el Acuerdo de Junta Directiva N. 2019-470: en lo que respecta a las "Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados"

> *"**Política 6.2: Administración de accesos de usuarios***
>
> *(…) Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.*
> *Cancelar inmediatamente los derechos de acceso de los usuarios que*

cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del AyA o sufrieron la pérdida/robo de sus credenciales de acceso. (…)"

El Acuerdo de Junta Directiva N. 2019-469: en el cual se establecen las Políticas estratégicas para la gestión de las tecnologías de información y de Comunicaciones – TIC's – del Instituto Costarricense de Acueductos y Alcantarillados (CODIGO: AyA_DSI_PoEstTI) disponen:

7.6.4) La Dirección de TI es garante de la confidencialidad, disponibilidad, respaldo y recuperación de los datos de las áreas que alberga TI.
7.6.5) Los usuarios que administran funcionalmente sus sistemas, son responsables por la calidad de los datos que se incluyen en los aplicativos.
7.9.5) Cada funcionario es responsable de la información a la que puede acceder y producir, reconociendo que es parte del activo institucional, y por tanto debe firmar un contrato de responsabilidad, confidencialidad y propiedad intelectual.
7.9.6) Cada funcionario debe conocer qué tan sensible es la información que administra y almacena, basándose en la normativa aplicable y la clasificación de información emitida por la Unidad de Control Interno, haciéndose responsable por su custodia y respaldo.
7.9.7) La Dirección de TI establece las regulaciones para los accesos físico y lógico a sistemas, datos e instalaciones incluyendo la red de comunicaciones, para regular el intercambio de información y los accesos no autorizados.
7.9.8) Las claves de acceso a redes y servicios se asignan en forma centralizada en la Dirección de TI, de acuerdo con el perfil de cada funcionario.
7.9.9) La solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados se harán efectivos por el administrador de cuentas de usuario de manera inmediata, una vez que se reciba la notificación por parte de la Dirección de Gestión de Capital Humano u otra área competente.
7.9.10) El desarrollo y mantenimiento de sistemas de aplicación debe incorporar controles de validación de datos de entrada, procesamiento interno y salida de datos.

Por su parte las NTGCTI disponen:

*"**1.4.5 Control de acceso** La organización debe proteger la información de accesos no autorizados. 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".*

Como causa del porque se da esta situación, se tiene que la falta de personal y la multiplicidad de tareas del área hace que este tema no sea atendido como corresponda.

Sin embargo, en conversación sostenida con la administradora funcional nacional (Dirección del Sistema Comercial Integrado) del open, se indicó que iba a revisar el asunto por cuanto en apariencia estaba sucediendo lo enunciado en este resultado por falta de cuidado del responsable.

Es claro que este tipo de desatenciones debilitan el sistema de control interno y hacen que los sistemas sean vulnerables a transacciones que no deben permitirse por usuarios que ya no deben interactuar con el sistema.

2.8 Falta de documentación apropiada para la administración, control y capacitación de usuarios y el perfil asignado.

Se encontró de la revisión realizada a la tabla objetos que existen definidos en el sistema más de 28,000 registros de tipos de objetos los cuales se pueden asignar a cada perfil.

En virtud del número significativo de objetos se pidió la documentación soporte en la cual se especifique a que derechos o inhabilitaciones hace referencia cada objeto como lo indicó el Manual Usuario del Sistema de Seguridad de la aplicación SGC Código: ADM-93-03-M02: *"el o los objetos definidos en el módulo de seguridad son los privilegios asignados a los perfiles en el nivel de pantallas, reportes, botones, entre otros; los cuales deben tener su acceso controlado, en si se puede resumir que este programa de aplicación define a que realmente tiene acceso un perfil en el nivel de módulo, submódulo, ventana y ícono en el nivel más bajo, en pocas palabras a que tiene acceso un perfil en cuanto a modificar, incluir, borrar o grabar"* , a lo cual se tuvo las siguientes respuestas:

El director Comercial Nacional, administrador del sistema OPEN informó:

> *"Se debe informar si existe un manual descriptivo de los privilegios asignados a cada uno de los perfiles que existen en el sistema comercial, entendiéndose como privilegio a la prerrogativa asignada al perfil para cada módulo o pantalla el derecho a insertar, modificar, eliminar, grabar o actualizar un registro en una función cualquiera de un módulo, ventana o criterio que pueda existir. En este aspecto la Auditoria a investigado que en la tabla objetos y perfiles objetos existen más de 28,00 objetos creados.*
>
> Respuesta de la Dirección Sistema Comercial Integrado:
>
> *Se cuenta con un manual de perfiles de acceso al OPEN SCI, en el cual se indica a las operativas a que tiene acceso cada uno de los perfiles.*
>
> *El OPEN SCI, cuando fue implementado en el año 1998, contaba con una cantidad importante de objetos propios del sistema y que posteriormente con los desarrollos se fueron agregando otros. Adicionalmente, muchos de estos objetos son imágenes que funcionan como objetos de consultas.*

> *La documentación de los objetos es una función del área técnica a cargo de la Dirección de Sistemas de Información".* (El resaltado no pertenece al original)

Así las cosas y lo informado en cuanto a que la documentación de lo que pueda autorizar cada objeto es de resorte de la Dirección de Sistemas de Información, se preguntó a esta área funcional de la documentación de respaldo y descripción para cada objeto que existe en el sistema con memorando AU-2021-00779, a lo que se obtuvo respuesta en memorando No.GG-DSI-2021-00789 en el cual se indica:

> *"(…) En cuanto al perfil de aplicación, éstos son definidos por la administración funcional, según sean los requerimientos del negocio, los cuales son asignados, modificados y eliminados por la aplicación anteriormente mencionada. Específicamente para la eliminación de usuarios, la aplicación elimina el usuario de base de datos y le desasigna el perfil de aplicación de la tabla de asociación, usuario_perfil. Para las actividades de inserción o modificación se ingresan los datos de usuario en la tabla de usuario y en la tabla asociación de usuario_perfil la información de cada funcionario y el perfil solicitado.*
>
> *La asignación de los perfiles de usuarios para poder visualizar los objetos que componen la aplicación, se realiza por medio de la tabla de objetos (tabla recursiva de herencia de objetos para la asignación) y la tabla de asociación perfil_objeto.*
>
> *Es importante mencionar que la tabla de objetos y perfiles de objetos son propias y dedicadas a la gestión de la seguridad del sistema y no de documentación.*
>
> *En cuanto a la documentación de los objetos desconocemos de la existencia de esta, lo que puede existir es una confusión sobre la función de la tabla objetos, ya que esta, como se mencionó anteriormente, es una tabla que utiliza el sistema de seguridad del SCI para habilitar o deshabilitar el acceso un objeto, (ventana, botón, check, etc) dentro del sistema comercial.* (El resaltado no pertenece al original)

El Manual Usuario del Sistema de Seguridad de la aplicación SGC Código: ADM-93-03-M02, dispone:

> *"(…) El Sistema de seguridad es una solución informática que permite administrar de forma centralizada la seguridad del Sistema Comercial Integrado.*
> *Con este sistema se tienen entre otros los siguientes beneficios:*
>
> *Centralización de la administración de la seguridad.*
>
> *Mantener de forma ordenada los diferentes perfiles existentes y facilitar la creación de nuevos permisos para los usuarios.*

Mantener un inventario de objetos de la aplicación SGC.

Este manual pretende ser la guía de consulta para los usuarios que de una u otra forma tienen que interactuar con el sistema de Seguridad. En él se describen las ventanas, procesos y reportes que componen la aplicación, de tal forma que esta sea una herramienta efectiva de consulta para los interesados en conocer el sistema.

El Sistema de seguridad define permisos para que los usuarios puedan realizar ciertas funcionalidades de la aplicación SGC, por ejemplo, por medio de la creación de perfiles se puede definir un grupo de usuarios asociados a un perfil especifico que puede realizar un conjunto seleccionado de tareas, como consultar, insertar, modificar cierta información del sistema.

Asimismo, se define un usuario que tenga acceso al Sistema de seguridad, y sean los encargados de la administración usuarios, perfiles, permisos y monitoreo.

Para lograr el objetivo de integración con las diferentes áreas funcionales que con las cuales interactúa directamente el sistema de seguridad, debe de existir una comunicación en línea con los módulos o sistemas que afectan cada área involucrada.

Objetivo

Una guía de consulta para los usuarios de Sistema de Comercial que de una u otra forma tienen que interactuar con el sistema de Seguridad. En él se describen las ventanas, procesos y reportes que componen la aplicación, de tal forma que esta es una herramienta efectiva de consulta para los interesados en conocer la operativa del sistema.

Módulo de mantenimientos

Objetivos generales

Los objetivos del módulo de mantenimiento son:

- *Registro y mantenimiento de información de los usuarios.*
- *Registro y mantenimiento de información de los perfiles.*
- *Registro y mantenimiento de información de los objetos.*

9.1.5 Mantenimiento de objetos

Figura 5.1.5 (1) Pantalla de mantenimiento de objetos

<u>Descripción y funcionalidad</u>

Esta opción es una pantalla que sirve para ingresar todos los objetos que se desarrollan para la aplicación SGC. Este mantenimiento lo utiliza el departamento de informática

En esta pantalla (figura 5.1.4.1) se hace el mantenimiento de todos los objetos del sistema, como pantallas, reportes, botones, entre otros; los cuales deben tener su acceso controlado.

Los datos que se muestran en la ventana son los siguientes:

- *Aplicación.*
- *Ventana.*
- *Objeto.*
- *Fecha de registro.*
- *Estado*
- *Fecha última operación.*
- *Usuario última operación*
- *Programa última operación.*

Como lo establece el procedimiento el o los objetos definidos en el módulo de seguridad son los privilegios asignados a los perfiles en el nivel de pantallas, reportes, botones, entre otros; los cuales deben tener su acceso controlado, en si se puede resumir que este programa de aplicación define a que realmente tiene acceso un perfil en el nivel de módulo, submódulo, ventana y ícono en el nivel más bajo, en pocas palabras a que tiene acceso un perfil en cuanto a modificar, incluir, borrar o grabar. (El resaltado no pertenece al original)

9.2.4 Asignar objetos a perfil

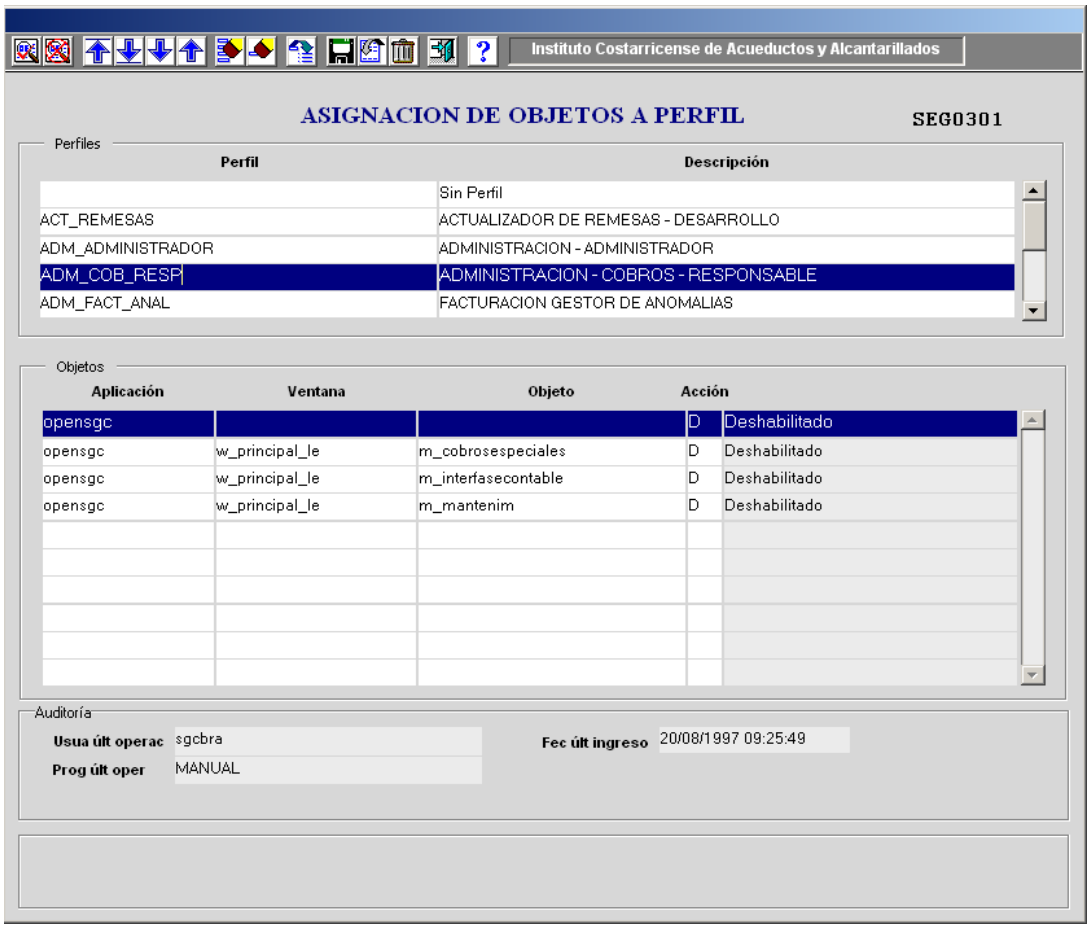


Figura 5.2.4 (1) Pantalla de Asignación de objetos a perfiles

<u>Descripción y funcionalidad</u>

Esta ventana es para asignar los objetos a los perfiles. Una vez que se han ingresado los objetos en el sistema, estos deben de ser asignados a los perfiles que corresponda. Esta agrupación de objetos bajo un mismo perfil es la que permite delimitar los accesos al sistema SGC para por usuario.

Los datos que se muestran en la ventana son los siguientes:

- *Perfil.*
  - *Código de perfil.*
  - *Descripción del perfil.*
- *Objetos.*
  - *Aplicación.*
  - *Ventana.*
  - *Objeto.*
  - *Acción.*
  - *Fecha última operación.*
  - *Usuario última operación.*
- *Programa última operación.*

La ventana permite relacionar los objetos creados con los perfiles. Los

> *campos de color gris corresponden a información de sólo consulta que no puede ser modificada por el usuario. La ventana está compuesta por dos tablas de datos, la tabla superior de la ventana corresponde a la información de los perfiles y la otra tabla corresponde a información de los objetos del sistema. En esta ventana se puede consultar, agregar, modificar y eliminar relaciones objetos a un determinado perfil".*

Con respecto a este tema se tiene que la Ley General de Control Interno N. 8292 dispone los objetivos del sistema de control interno en su artículo 8°, en el 16° lo correspondiente a los sistemas de información y en el artículo 15°, la responsabilidad de la Junta Directiva y los titulares en cuanto a:

> *"a) Documentar, mantener actualizados y divulgar internamente, las políticas, las normas y los procedimientos de control que garanticen el cumplimiento del sistema de control interno institucional y la prevención de todo aspecto que conlleve a desviar los objetivos y las metas trazados por la institución en el desempeño de sus funciones.*
>
> *b) Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:*
>
> *(…)*
> *di. El diseño y uso de documentos y registros que coadyuven en la anotación adecuada de las transacciones y los hechos significativos que se realicen en la institución. Los documentos y registros deberán ser administrados y mantenidos apropiadamente.*
> *(…)*
> *v. Los controles generales comunes a todos los sistemas de información computarizados y los controles de aplicación específicos para el procesamiento de datos con software de aplicación".*

Así mismo, las NCISP, disponen:

> *"(…)*
> ***4.2 Requisitos de las actividades de control***
> *Las actividades de control deben reunir los siguientes requisitos:*
> *e. Documentación. Las actividades de control deben documentarse mediante su incorporación en los manuales de procedimientos, en las descripciones de puestos y procesos, o en documentos de naturaleza similar. Esa documentación debe estar disponible, en forma ordenada conforme a criterios previamente establecidos, para su uso, consulta y evaluación".*

El Acuerdo de Junta Directiva N. 2019-470en el cual: la junta directiva aprueba el documento denominado "Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados", en el cual se dispone:

> ***"Política 2: Clasificación y Control de Activos Generalidades***

El AyA debe tener el control sobre los activos de información que posee como parte importante de la administración de riesgos. Algunos ejemplos de activos son:

a. Recursos de información: bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad, información archivada, etc".

*"**Política 5.1: Procedimientos y responsabilidades operativas Documentación de los procedimientos operativos***

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta política y sus cambios serán autorizados por el Oficial de Seguridad de la Información.

Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:

a. Procesamiento y manejo de la información.
b. Requerimientos de programación de procesos, interdependencias con otros sistemas, tiempos de inicio de las primeras tareas y tiempos de terminación de las últimas tareas.
c. Instrucciones para el manejo de errores u otras condiciones excepcionales que puedan surgir durante la ejecución de tareas.
d. Restricciones en el uso de utilitarios del sistema.
e. Personas de soporte a contactar en caso de dificultades operativas o técnicas imprevistas.
f. Instrucciones especiales para el manejo de "salidas", como el uso de papelería especial o la administración de salidas confidenciales, incluyendo procedimientos para la eliminación segura de salidas fallidas de tareas.
g. Reinicio del sistema y procedimientos de recuperación en caso de producirse fallas en el sistema".

*"**Política 7.5: Seguridad de los procesos de desarrollo y soporte***

Esta política provee seguridad al software y a la información del sistema de aplicación, por lo tanto, se controlarán los entornos y el soporte dado a los mismos.

Procedimiento de control de cambios

A fin de minimizar los riesgos de alteración de los sistemas de información, se implementarán controles estrictos durante la implementación de cambios imponiendo el cumplimiento de procedimientos formales. Éstos garantizarán que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Para ello se establecerá un procedimiento que incluya las siguientes

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

consideraciones:

a. Verificar que los cambios sean propuestos por usuarios autorizados y respete los términos y condiciones que surjan de la licencia de uso.
b. Mantener un registro de los niveles de autorización acordados.
c. Solicitar la autorización del propietario de la información, en caso de tratarse de cambios a sistemas de procesamiento de la misma.
d. Identificar todos los elementos que requieren modificaciones (software, bases de datos, hardware).
e. Revisar los controles y los procedimientos de integridad para garantizar que no serán comprometidos por los cambios.
f. Obtener aprobación formal por parte del responsable del área informática para las tareas detalladas, antes que comiencen las tareas.
g. Solicitar la revisión del Oficial de Seguridad de la Información para garantizar que no se violen los requerimientos de seguridad que debe cumplir el software.
h. Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
i. Obtener la aprobación por parte del usuario autorizado y del área de pruebas mediante pruebas en el ambiente correspondiente.
j. Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
k. Mantener un control de versiones para todas las actualizaciones de software.
l. Garantizar que la implementación se llevará a cabo minimizando la discontinuidad de las actividades y sin alterar los procesos involucrados.
m. Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.
n. Garantizar que sea el implementador quien efectúe el pasaje de los objetos modificados al ambiente operativo, de acuerdo con lo establecido en "Control del Software Operativo".

La falta de un adecuado ordenamiento de funciones, deberes y responsabilidades de las áreas involucradas en la administración, gestión y mantenimiento del sistema OPEN, hace que actividades esenciales como lo pueda ser la documentación descriptiva de los procesos automatizados, se vea comprometido por la falta de esta.

Este ordenamiento de labores ha afectado desde la puesta en producción el sistema y así se enuncia según lo indicado por los responsables al mencionar que desde la misma puesta en operación existieron debilidades en la exigencia al personal responsable de la implantación del sistema de los documentos necesarios para una adecuada administración.

El documentar los sistemas es un proceso que en muchas de las ocasiones es deficiente, por cultura de los informáticos, en este sentido es importante el pensar el mantener a profesionales especialistas en documentación de sistemas en cualquier proyecto de automatización de procesos.

Uno de los efectos más perjudiciales, que mantiene este tipo de inconsistencias de documentación, lo es la creación de relaciones personales para el mantenimiento de

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

sistemas, toda vez que el conocimiento del cómo se procesa la información, o el cómo se deben modificar los sistemas, se condicionan a una o muy pocas personas, creando una dependencia de que solo él o ellos puedan conocer cuál es el esfuerzo necesario para poder realizar las adecuaciones necesarias.

2.9 Estructura de datos y registro de datos complejos de depurar y consolidar para transferencia entre sistemas. Falta de integridad de la base de datos.

La estructura y funcionabilidad de las tablas de datos del sistema comercial OPEN, se encuentran comprometidas en su lógica funcional, como efecto de una inadecuada definición de relación de datos. Si vemos las relaciones que deban existir entre los datos, y las estructuras que las soportan(tablas) deben responder a la integridad, seguridad y eficiencia del procesamiento de datos. En este sentido cuando las estructuras muestran redundancia de datos, registros en blanco, y campos de información que no muestran datos comprometen la conversión o depuración de estos.

En este sentido veamos lo determinado:

1. Se comprueba que la tabla de perfiles_objetos mantiene un registro en blanco para cada tipo de perfil, como se presenta:

ic0001	17/12/1998 12:10:06	manual	opensgc	w_principal_le	m_interfasecontable	D	ACT_REMESAS
ic0001	17/12/1998 12:10:14	manual	opensgc	w_principal_le	m_informes	D	ACT_REMESAS
AYA77504	17/02/2011 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_proyectosurbanisticos	D	ACT_REMESAS
ic0001	17/12/1998 12:10:24	manual	opensgc	w_principal_le	m_bdg	D	ACT_REMESAS
ic0001	17/12/1998 12:10:37	manual	opensgc	w_principal_le	m_impresindescentralizada	D	ACT_REMESAS
AYA95402	21/03/2007 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_lecturas	E	ACT_REMESAS
AYA95402	21/03/2007 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_gestindecheques	E	ACT_REMESAS
ic0001	17/12/1998 00:00:00	manual	opensgc			D	ACT_REMESAS
AYA77504	17/02/2011 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_proyectosurbanisticos0	D	ACT_REMESAS
ic0001	17/12/1998 11:48:58	manual	opensgc	w_principal_le	m_facturacin	D	ACT_REMESAS
ic0001	17/12/1998 11:48:31	manual	opensgc	w_principal_le	m_atalcliente	D	ACT_REMESAS
ic0001	17/12/1998 11:49:26	manual	opensgc	w_principal_le	m_cobrosespeciales1	D	ACT_REMESAS
AYA77504	17/02/2011 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_proyectosurbanisticos0	D	ADM_ADMINISTRADOR
ib0150	19/08/1998 20:44:11	manual	opensgc	w_principal_le	m_alta2	N	ADM_ADMINISTRADOR
ib0150	19/08/1998 20:44:14	manual	opensgc	w_principal_le	m_alta3	N	ADM_ADMINISTRADOR
sgcbra	20/08/1997 09:26:05	manual	opensgc			D	ADM_ADMINISTRADOR
prodcion	15/02/1999 14:13:49	manual	opensgc	w_principal_le	m_mantenim	D	ADM_ADMINISTRADOR
aya42616	06/09/2000 08:31:13	manual	opensgc	w_principal_le	m_cobrosespeciales	D	ADM_ADMINISTRADOR
AYA77504	17/02/2011 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_proyectosurbanisticos	D	ADM_ADMINISTRADOR
ib0150	19/08/1998 20:41:42	manual	opensgc	w_principal_le	m_baja1	N	ADM_ADMINISTRADOR
JLEIVA	23/12/2020 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_anomaliasnodetectables	D	ADM_AUDITORIA
AYA95402	23/02/2016 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_mantenim	D	ADM_AUDITORIA
AYA95402	23/02/2016 00:00:00	SEGURIDAD SGC	opensgc			D	ADM_AUDITORIA
aya42616	06/09/2000 08:31:35	manual	opensgc	w_principal_le	m_cobrosespeciales	D	ADM_COB_RESP
AYA77504	17/02/2011 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_proyectosurbanisticos	D	ADM_COB_RESP
AYA77504	17/02/2011 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_proyectosurbanisticos0	D	ADM_COB_RESP
sgcbra	20/08/1997 09:25:49	manual	opensgc			D	ADM_COB_RESP
prodcion	15/02/1999 14:14:47	manual	opensgc	w_principal_le	m_mantenim	D	ADM_COB_RESP
AYA95402	09/11/2010 00:00:00	SEGURIDAD SGC	opensgc	w_principal_le	m_archivo	D	ADM_COB_RESP
aya42616	27/09/2000 03:47:11	manual	opensgc	w_principal_le	m_interfasecontable	D	ADM_COB_RESP
ANDREA	08/08/1998 00:00:00	manual	opensgc	w_principal_le	m_parametrosdeinterfase	D	ADM_FACT_ANAL
ANDREA	08/08/1998 00:00:00	manual	opensgc	w_principal_le	m_activacinmdulos	D	ADM_FACT_ANAL
sgcbra	20/08/1997 09:25:45	manual	opensgc			D	ADM_FACT_ANAL
prodcion	05/08/1999 08:43:15	manual	opensgc	w_principal_le	m_cobroon-line	D	ADM_FACT_ANAL
prodcion	15/02/1999 14:15:11	manual	opensgc	w_principal_le	m_mantenim	D	ADM_FACT_ANAL
prodcion	05/08/1999 08:43:19	manual	opensgc	w_principal_le	m_cobroanticipado	D	ADM_FACT_ANAL
prodcion	05/08/1999 08:43:28	manual	opensgc	w_principal_le	m_anulacindecobros	D	ADM_FACT_ANAL

A raíz de la determinación de la existencia de un registro en blanco en todos los tipos de perfiles y los objetos asociados, se preguntó a dos funcionarios de la Dirección de Sistemas de Información del porqué de la existencia de esta condición, a lo que se obtuvo el siguiente comentario: “que no se sabía el porqué de la condición, sin embargo, se reconoce que esta condición debe existir para que el programa de seguridad funcione sin saberse la razón”.

Se determina la existencia de usuarios con igual nombre y diferente ID identificador de usuario, esta condición compromete la integridad y seguridad del sistema y las estructuras, en este sentido algunos de los registros muestran la siguiente condición:

Acuna Rojas Gabriela	SLD00160
Acuna Rojas Gabriela	AYA00831
Aguero Cespedes Carlos	E1297008
Aguero Cespedes Carlos	BCA00017
Aguilar Leiva Marvin	AYA22232
Aguilar Leiva Marvin	AYA01701
Alejandro Araya Quesada	AYAC0102
Alejandro Araya Quesada	AYA01029
Alexandra Vargas Fallas	JO1446
Alexandra Vargas Fallas	AYA1446
Alfaro Rodriguez Denia	AYA02715
Alfaro Rodriguez Denia	AYAC2003
Alfaro Sanchez Zaida	AYA02786
Alfaro Sanchez Zaida	A2A1286
Alfaro Sanchez Zaida	AYA01286
Alfaro Sanchez Zaida	AYA1286
Alvarado Aguilar Luis Manuel	AYAC1088
Alvarado Aguilar Luis Manuel	AYA03208
Alvarado Gonzalez Hermes	AYA81214
Alvarado Gonzalez Hermes	AYA03640
Alvarado Jimenez Nefertty	AYAC107
Alvarado Jimenez Nefertty	AYA4501
Alvarez Alfaro Rudy	AYAC2034
Alvarez Alfaro Rudy	AYA04121
Ana Cerdas Rojas	AYAC2060
Ana Cerdas Rojas	AYA22074
Andres Andrade Arce	DCM0166
Andres Andrade Arce	DCM0088
Andres Mora Quiros	CDM0867
Andres Mora Quiros	DCM0867
Arce Gamboa Rafael	AYA06158
Arce Gamboa Rafael	AYA06258
Arias Aguilar Victoria	AYAC0122
Arias Aguilar Victoria	AYA07203
Arroyo Espinoza Nancy	AYAC1045
Arroyo Espinoza Nancy	AYAC2005
Aviles Dominguez Joel	AYA9114
Aviles Dominguez Joel	AYA09114
Calderon Serrano Francisco	E1297009
Calderon Serrano Francisco	BCA00018
Camacho Ibarra Leidy	AYA1667
Camacho Ibarra Leidy	AYA16667
Campos Abarca Jouseth	AYA17040
Campos Abarca Jouseth	AYAC0019
Campos Barquero Kathia	AYA17313
Campos Barquero Kathia	AYAC1093
Campos Campos Yahaira	AYA17363
Campos Campos Yahaira	AYA17373
Campos Chavarria Rosibel	A2AC1004
Campos Chavarria Rosibel	AYAC1004
Cantillano Lopez Maureen	AYAC108
Cantillano Lopez Maureen	AYA4502
Cantillano Lopez Maureen	AYAC0074
Castro Vargas Xinia	AYAC0089
Castro Vargas Xinia	AYAC0070

De la condición encontrada se debe aclarar que, en el nivel de datos, cada uno de estos registros puede tener una eliminación de uso lógica pero no física del registro, por cuanto el sistema OPEN es un sistema histórico de transacciones que se han ejecutado como parte del ejercicio comercial en cuanto a: modificación de recibos, ajuste de facturas, cargos varios, generación de ordenes de campo, atención de clientes, inclusión de nuevos clientes, etc.

Cada uno de estos registros corresponden en principio a la acción de un usuario definido en el sistema, el eliminar un registro de un funcionario que tuvo su participación en el sistema implica que la estructura de base de datos se comprometa y pierda su funcionabilidad relacional e histórica transaccional, de ahí la imposibilidad de eliminar un registro de usuario físicamente. Además, por aspectos legales se debe mantener el registro de quien, cuando y como se realizaron los ajustes o cambios en el sistema.

De forma adicional el haber creado diferentes ID (nomenclatura de acceso) para un

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

mismo usuario, como efecto de desempeñar varios roles en el sistema por ejemplo (notificador, lector, personal de campo para la resolución de ordenes de servicio, etc.) al igual que, cuando un usuario deba desempeñar su función comercial en varias oficinas comerciales o centros técnicos, se deba crearse diferentes ID, se considera que la decisión y lógica utilizada no es la adecuada para mantener la integridad de la base de datos y afecta en forma directa la conversión de datos para ser implementados en nuevas estructuras o nuevos sistemas, conllevando lo anterior a esfuerzos de mayor costo en la depuración de datos.

O en el peor de los casos tener que mantener la misma lógica funcional en nuevos desarrollos, aspecto que no responde a una adecuada normalización de tablas en las bases de datos relacionales.

Otro aspecto que compromete la integridad y la razón de ser de la estructura de base de datos, lo es la falta de registros de información de más de mil registros de creación o eliminación de usuarios, sin la debida información de quien solicita la condición del usuario, campo de importancia dentro de la definición establecida como requisito en el procedimiento de administración de perfiles, el cual dispone:

> ***"(…) LINEAMIENTO PARA ASIGNAR PERFILES***
>
> *La Dirección Sistema Comercial Integrado administrador del Sistema Comercial SCI, es la dependencia encargada de incluir en el sistema la clave de acceso a las diferentes categorías de perfiles, a aquellos usuarios autorizados por las Jefaturas y que realizan funciones comerciales en los diferentes módulos que conforman el sistema a saber:*
>
> - *Atención al Cliente*
> - *Ordenes de Servicio*
> - *Lecturas*
> - *Cobros*
> - *Facturación*
> - *Contratación*
> - *Gestión de Averías*
> - *Datamart Comercial*
> - *Archivo Histórico*
> - *Signos*
>
> *La asignación de los privilegios a los perfiles la realizará por escrito el jefe cantonal de cada oficina, con el visto bueno del responsable Comercial de Región y con base en esta solicitud la Dirección Sistema Comercial Integrado dará el acceso respectivo.*
>
> *En este documento se indicará de acuerdo con el listado que tiene cada región lo siguiente:*

Nombre y Apellidos del funcionario
No. de Empleado
Correo Electrónico
No. de Cédula
Perfil Solicitado.

Razón o justificación para otorgar el acceso: Esto rige para el ingreso a las herramientas del Datamart Comercial, Archivo Histórico, Sigos

No se podrá asignar más de una categoría de perfil a los usuarios. Los mismos son asignados por funciones.

Cuando el funcionario deja de laborar para la Institución es responsabilidad de la jefatura correspondiente (Jefe cantona/ Regional/ o de Agencia o Jefe del área Comercial), solicitar de inmediato la suspensión del acceso al Open, Datamart Comercial, Archivo Histórico, Sigos.

Por su parte establece el Manual Usuario del Sistema de Seguridad de la aplicación SGC Código: ADM-93-03-M02 dispone en la opción de Creación de usuarios:

"Los usuarios creados deben al menos poder conectarse al SGC con los permisos mínimos de navegación en el sistema. ***Debe de registrarse la información del usuario que autoriza la creación.*** *Si un usuario no está creado en la base de datos, el sistema le asigna el estado eliminado, se puede volver a crear por medio del botón*  *"*(El resaltado no pertenece al original)

el registro de quien autoriza se registra en el campo de obs (Observaciones)

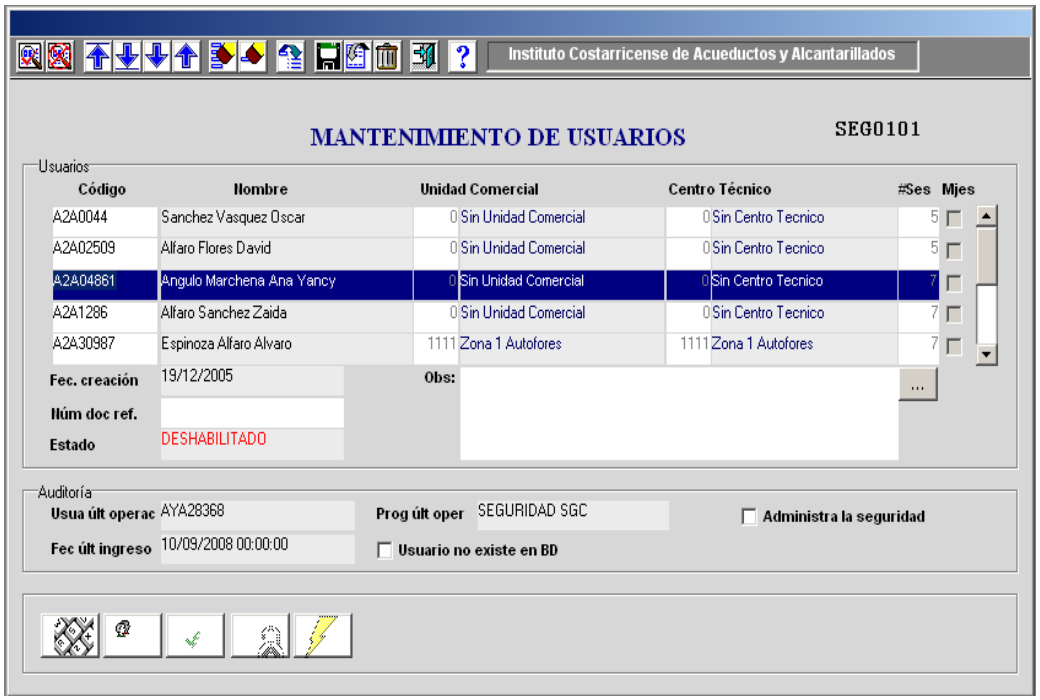
"(…)

RESPONSABILIDADES JEFATURA DE AREA

• Solicitar la creación de nuevos privilegios de acceso (Nuevos perfiles), modificación, exclusión, según las necesidades de cada región, así como otorgar el acceso de visitante a las herramientas del Datamart Comercial y Archivo Histórico.

• Serán los funcionarios competentes autorizados a solicitar un perfil de usuario, de los funcionarios a su cargo.

(…)"



La tabla usuarios muestra para la creación de usuarios en el campo columna DSC_Observaciones, campo donde se debe incluir el nombre del responsable que solicita la creación del usuario, para más de 1000 casos, el registro en blanco o null, más aún el usuario que genera el registro o creación del usuario, es un funcionario de la empresa ATESA empresa encargada del mantenimiento del sistema usuario AYAD0002, aspecto que permite concluir que no existió una adecuada fiscalización y control de la carga de datos que se realizó por parte de terceros. Ej.

NOM_USR	DESC_USR	DSC_OBSERVACIONES
AYA70609	Reyes Castro Alfredo	null
AYA77238	Salas Murillo Wilson	null
AYA81690	Sequeira Pacheco Alejandro	null
AYA07742	Arias Solano Rodrigo	null
AYA04357	Alvarez Mora Mario	null
BCA00016	Castro Vega Randall	null
AYA00924	Agamiz Castillo Ma. Eugenia	null
AYAC0013	Barahona Ronald	null
AYA58249	Morales Pringle Roberto	null
AYA82621	Solano Campo Eduardo	null
AYA10166	Barahona Carvajal Oscar	null
AYA93240	Villalobos Espinoza Marvin	null
AYA90854	Vargas Pineda Danny	null
SLD0080	Vargas Barrientos Karla	null
AYA40379	Contreras Luis Alejandro	null
AYA95845	Zuniga Edgar	null
CSS00006	Bedoya Barrientos Luis	null
AYA86548	Trejos Morales Marco Aurelio	null
AYAC0046	Muriel Cubillo Jorge Alberto	null
AYA972	Usuario de Desarrollo	null
AYA02821	Alfaro Sandoval Yannin	null
AYAC1057	Guevara Herrera Katia	null
AYA15792	Calderon Villalobos Oscar	null
AYA86508	Trejos Avila Sitel	null
AYAC1016	Solano Murillo Patricia	null
AYA37219	Gomez Martinez Max	null
PRODCION	Produccion	null
AYA43812	Guido Hidalgo Vindas	null
AYAC121	Marcela Arce Villarreal	null
AYA20720	Castro Barahona Fernando	null
AYAC1061	Miranda Barahona Luis	null

Ahora bien, el concepto de Integridad de datos, se refiere a la precisión, la coherencia y la integralidad de los datos de una organización. La integridad de un dato alude a un atributo o cualidad inherente a la información que se considera exacta, completa, homogénea, sólida, coherente y confiable, con base en la intención de los creadores de las bases de datos.

Cuando es segura, los datos estarán a prueba de fuerzas externas, las bases de datos son completas, precisas y fiables durante el tiempo, independiente del número de veces que sean accedidas. Esta cualidad, va ligada al propio dato y no al lugar donde se almacena.

El concepto de “integridad en base de datos “garantiza que todos los datos de una base de datos pueden ser rastreados mediante técnicas de trazabilidad, así como conectarse a otros datos. De esta forma se asegura que todo se puede buscar y recuperar. Tener un sistema de integridad en base de datos único, bien definido y controlado aumenta la estabilidad, el rendimiento, la reutilización y facilita el mantenimiento.

Con respecto a este tema el CÓDIGO NACIONAL DE TECNOLOGÍAS DIGITALES MICITT 2020, dispone:

- *Confidencialidad: Esto significa que la información solo está siendo vista o utilizada por personas que están autorizadas para acceder a ella, por tanto, se debe de suscribir el respectivo acuerdo de servicio donde se establezcan claramente las condiciones de las partes, que garanticen la confidencialidad de cualquier tipo de información que se gestione.*
- ***Disponibilidad:** Esto significa que la información es accesible cuando los usuarios autorizados la necesitan.*
- ***No repudio:** Prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibe (no repudio en destino). El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje, para entender mejor corresponde a la irrenunciabilidad, es un servicio de seguridad estrechamente relacionado con la autenticación y que permite probar la participación de las partes en una comunicación.*
- ***Integridad**: esto significa que cualquier cambio en la información por parte de un usuario no autorizado es imposible (o al menos detectado), y se realiza un seguimiento de los cambios realizados por usuarios autorizados; garantizando la exactitud, completitud de la información y los métodos de procesamiento".*

Por su parte, como se ha indicado las NTGCTI, en la norma 1.4 Gestión de la seguridad de la información, establece que el AyA "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". Y en la norma 1.4.4:

> ***"1.4.4 Seguridad en las operaciones y comunicaciones***
>
> *La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.*
>
> *Para ello debe:*
>
> *Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información".*

La falta de políticas de creación y modificación de estructuras de base de datos, además de la falta de documentación suficiente y necesaria de la base de datos del sistema comercial, hacen que las decisiones que se toman en la adecuación de programas o módulos de administración funcional como requerimientos de la funcionabilidad operativa, no respondan en forma adecuada a la integridad que deba tener la base de datos de gestión y administración.

El querer resolver situaciones particulares como crear usuarios para que puedan ejercer varias funciones en el campo o en diferentes oficinas, conllevo a que se

tuviera como medida alterna y no apropiada, el crear para un mismo funcionario diferentes ID.

Este tipo de acciones y soluciones alternas causa como efecto el que:

1. Sea de complejidad el poder dar trazabilidad a las acciones realizadas por un usuario con varias cuentas de usuario.
2. Redundancia de registros de usuarios.
3. La eficiencia del rendimiento de la base de datos se ve comprometida.
4. Incumplimiento de lo que disponen las disposiciones reglamentarias.

2.10 Funciones incompatibles

Mediante informe de la Empresa despacho Auditores Carvajal y Colegiados Contadores públicos autorizados, para el 10 de abril del 2015 con INFORME DE CUMPLIMIENTO Y CONTROL INTERNO DE TECNOLOGÍAS DE INFORMACIÓN, informaron

HALLAZGO 11: PERSONAL DE MANTENIMIENTO DEL SISTEMA OPEN CON ACCESOS AL AMBIENTE DE PRODUCCIÓN.RIESGO MEDIO.

> ***"(…)***
>
> ***CONDICIÓN:***
>
> *Producto del análisis a los usuarios activos de la base de datos del OPEN, se verificó que la mayor parte del personal que le brinda soporte a este sistema puede acceder al ambiente en producción con el perfil "DESARROLLO", pues en dicha base de datos de usuarios aparecen con ese perfil. Según las buenas prácticas para la implementación de sistemas, el personal de mantenimiento no debería tener acceso al sistema en producción, su acceso debería limitarse únicamente a los ambientes de desarrollo y pruebas.*
>
> ***RECOMENDACIÓN:***
>
> *Limitar el acceso del personal de mantenimiento del Sistema OPEN al sistema en producción. En los casos que sean estrictamente necesarios se debe de documentar la debida justificación y mantener bitácoras de las transacciones realizadas.*
>
> ***COMENTARIO DE LA ADMINISTRACIÓN.***
>
> *Actualmente se cuenta con formularios debidamente acreditados para cualquier cambio que se lleve a cabo; sin embargo, se redactará con mayor formalidad el procedimiento, según lo recomendado".*

Como parte de la revisión al cumplimiento de lo indicado por la administración en cuanto a la redacción con mayor formalidad se solicitó las bitácoras para las

transacciones realizadas por personal de mantenimiento del sistema con perfil en el sistema comercial de desarrollo, a lo cual se recibió respuesta del funcionario de AyA, encargado contraparte del mantenimiento del sistema OPEN, indicando:

En este caso, sería dar acceso al SIGETI, ¿que es donde están registrados todos los requerimientos?

Sobre las bitácoras, no es un proceso que se haga a diario, por lo que no comprendo la solicitud. Ya que la bitácora sería el detalle de los registros con en (sic) el número de requerimiento en la columna programa. Entonces sería una consulta a la BD.

De importancia la recomendación del Grupo Auditor externo Carbajal en lo cual indico en el año 2015: *"En los casos que sean estrictamente necesarios se debe de documentar la debida justificación y mantener bitácoras de las transacciones realizadas"*

Posterior a esta respuesta, se recibe una ampliación a lo indicado, en la cual se manifiesta:

> *"(…) Los accesos del personal de Mantenimiento del Open SCI, a la Base de Datos en Producción, obedecen a la atención de requerimientos ingresados por la Dirección Comercial. Para ello, adjunto alguno de estos requerimientos, que como se puede observar, son solicitudes de actualización masiva de datos, en los cuales se registra en la base de datos el código del usuario que atiende la solicitud. (Ver Requerimientos SIGETI.docx).*
>
> *Sobre el tema de lo indicado por la Administración: Adjunto los formularios de "Firma Acta de Aceptación", "Boleta de autorización de Acceso a la Base de Datos" y "Procedimiento para Atención de Mejoras-Incidencias", que respaldan el cumplimiento de lo indicado en respuesta al informe de la Auditoría Externa.*
>
> *En cuanto a otras mejoras que se han implementado: Desde inicios del mes de octubre 2021, estamos utilizando el aplicativo: "Flujo de Gestión de Tareas", donde se registra toda la labor de atención de incidencias y se adjuntan las evidencias como correos electrónicos, y diferentes archivos en formato Excel, Word, PDF, etc.(…)"*

De la revisión a la inclusión, modificación de registros de la base de datos por parte del personal de mantenimiento de sistemas se logra determina que solo para la tabla de cargos varios muestra la siguiente información de transacciones realizadas por personal de mantenimiento de sistemas en fecha posterior al 15 de abril del 2015:

Tabla 3

Transacciones realizadas por el personal de mantenimiento

USUARIO	Cantidad de registros	Porcentaje de recuento
AYA04830 Enrique Angulo Leiva	11,240	1.94%
AYA38484 Heriberto Gonzalez Loría	2,055	0.36%
AYA42757 Luis Hernández Santana	25,998	4.49%
AYAD0003 Reyner Arguedas Chaves	539,339	93.21%
Totales	578,632	100%

En este sentido, llama la atención que la mayor cantidad de registros incluidos o modificados (539,339 registros) lo muestra el usuario AYAD0003 funcionario de la Empresa ATESA, empresa encargada y contratada para el mantenimiento del sistema. lo cual vuelve más compleja y delicada de controlar las acciones ejecutadas por este personal.

Por otra parte, se determina que los funcionarios internos y externos encargados de dar mantenimiento al sistema se mantienen con perfiles de acceso de desarrollo, incumpliéndose la disposición de separación de funciones.

Tabla 4

Perfiles de acceso de desarrollo

AYA95402	12/06/2007 00:00:00	SEGURIDAD SGC	AYAD0003	DESARROLLO
AYA95402	22/03/2007 00:00:00	SEGURIDAD SGC	AYA74622	DESARROLLO
AYA38878	26/02/2007 08:49:41	SEGURIDAD SGC	AYA42757	DESARROLLO
AYA33024	29/11/2001 15:31:21	SEGURIDAD SGC	AYA04830	DESARROLLO
DBA	13/11/2007 11:00:00	MANUAL	AYA38484	DESARROLLO
DBA	01/10/2006 10:00:00	MANUAL	AYAD0001	DESARROLLO

Con respecto a este tema el CÓDIGO NACIONAL DE TECNOLOGÍAS DIGITALES MICITT, establece:

> *"**Separación de tareas:** un control de fraude clave es la separación de funciones. Ciertos roles tienen diferentes niveles de confianza que los de usuarios normales. En particular, los administradores son diferentes a los usuarios normales. En general, los administradores no deben ser usuarios de la aplicación, entre otras premisas que facilitan de las fases de aprobación, autorización, ejecución, registro y otras sean desarrolladas por distintas personas como parte de la gestión del proyecto".*

Por su parte el Acuerdo de Junta Directiva N. 2019-470: prueba el documento denominado "Políticas de seguridad de la Información del Instituto Costarricense

de Acueductos y Alcantarillados", establece:

> *"**Política 7: Desarrollo y mantenimiento de sistemas***
>
> ***Generalidades***
>
> *El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad. Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación. Adicionalmente, se deberán diseñar controles de validación de datos de entrada, procesamiento interno y salida de datos.*
>
> *Dado que los analistas y programadores tienen el conocimiento total de la lógica de los procesos en los sistemas, se deben implementar controles que eviten maniobras dolosas por parte de estas personas u otras que puedan operar sobre los sistemas, bases de datos y plataformas de software de base (por ejemplo, operadores que puedan manipular los datos y/o atacantes que puedan comprometer / alterar la integridad de las bases de datos) y en el caso de que se lleven a cabo, identificar rápidamente al responsable.*
>
> *Por otro lado, es necesaria una adecuada administración de la infraestructura de base, sistemas operativos y software de base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.*
>
> ***Objetivos***
>
> *a. Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas de información.*
> *b. Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.*
> *c. Definir los métodos de protección de la información crítica o sensible.*
>
> ***Alcance***
> *Esta política se aplica a todos los sistemas informáticos, tanto desarrollo propio o de terceros, y a todos los sistemas operativos y/o software de base que integren cualquiera de los ambientes administrados por el AyA en donde residan los desarrollos mencionados".*

A mayor abundamiento, las NCISP disponen:

> **"*1.5 Responsabilidad de los funcionarios sobre el SCI***
>
> *De conformidad con las responsabilidades que competen a cada puesto de trabajo, los funcionarios de la institución deben, de manera oportuna, efectiva y con observancia a las regulaciones aplicables, realizar las*

acciones pertinentes y atender los requerimientos para el debido diseño, implantación, operación, y fortalecimiento de los distintos componentes funcionales del SCI".

"2.5.2 Autorización y aprobación

La ejecución de los procesos, operaciones y transacciones institucionales debe contar con la autorización y la aprobación respectivas de parte de los funcionarios con potestad para concederlas, que sean necesarias a la luz de los riesgos inherentes, los requerimientos normativos y las disposiciones institucionales".

"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".

"4.5.1 Supervisión constante

El jerarca y los titulares subordinados, según sus competencias, deben ejercer una supervisión constante sobre el desarrollo de la gestión institucional y la observancia de las regulaciones atinentes al SCI, así como emprender las acciones necesarias para la consecución de los objetivos".

Las NTCGTI disponen:

*"**1.4.5 Control de acceso***

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.

b. Clasificar los recursos de TI en forma explícita, formal y uniforme de

acuerdo con términos de sensibilidad.

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

i. Establecer controles de acceso a la información impresa, visible en pantallas o almacenada en medios físicos y proteger adecuadamente dichos medios.

j. Establecer los mecanismos necesarios (pistas de auditoría) que permitan un adecuado y periódico seguimiento al acceso a las TI.

k. Manejar de manera restringida y controlada la información sobre la seguridad de las TI.

1.4.6 Seguridad en la implementación y mantenimiento de software e infraestructura tecnológica

La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información.

Para ello debe:

a. Definir previamente los requerimientos de seguridad que deben ser considerados en la implementación y mantenimiento de software e infraestructura.

b. Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura.

c. Mantener un acceso restringido y los controles necesarios sobre los ambientes de desarrollo, mantenimiento y producción.

d. Controlar el acceso a los programas fuente y a los datos de prueba".

La falta de cumplimiento y atención a lo que disponen las normas que aplican en la separación de funciones, además de la inadecuada documentación del sistema, y la dependencia de personal externo para el mantenimiento del sistema OPEN, en complemento al desconocimiento del quién y cómo se pueda realizar la carga masiva de datos, hace que el sistema deba ser actualizado en sus registros por personal de mantenimiento del sistema, además de falta de personal capacitado para la carga de información de parte de la Dirección Comercial Nacional hace que esta actividad la realice el personal de TI, personal que en principio no debe tener acceso al sistema en producción.

La desatención al cumplimiento de separación de funciones, aumentan el riesgo de encontrarse: falta de autenticidad, la integridad se dificulta y la pérdida de confidencialidad de las transacciones y de transferencia o intercambio de información se ve comprometida, además de que implica el implementar controles para garantizar la veracidad de los registros.

2.11 Perfiles con autorización a realizar transacciones mayores a 2,000,000.00 que el procedimiento no establece.

El nivel de autorización está referido al nivel que le corresponde a cada perfil para poder realizar ajustes a recibos puestos al cobro, en este particular el manual de Perfiles establecido por la Gerencia General y Dirección Comercial Nacional 2020, dispone:

INSTITUTO COSTARRICENSE DE ACUEDUCTOS Y ALCANTARILLADOS

GERENCIA GENERAL - DIRECCIÓN SISTEMA COMERCIAL INTEGRADO

NIVELES DE AUTORIZACIÓN PARA APLICACIÓN DE CARGOS VARIOS

De acuerdo a incremento tarifario aprobado mediante RESOLUCION RE-0005-IA-2019

Rige a partir del 01/01/2020 al 31/12/2020

NIVEL	CATEGORIA M3	HASTA UN IMPORTE EN CUALQUIER TARIFA	PERFIL DE AUTORIZACIÓN
1	Hasta 100m3	₡191,240	Jefe Oficina Comercial 1
2	Hasta 250m3	₡498,710	Jefe Oficina Comercial 2
3	Hasta 500m3	₡1,014,460	Jefe Oficina Comercial 3
4	Hasta 1000m3	₡2,045,960	Jefe Oficina Comercial 4
5	Mayor a 1000m3	₡2,048,023	Jefe Oficina Comercial

Nota: Los niveles de autorización se calculan con la tarifa reproductiva.

A pesar de que este procedimiento establece los montos de autorización según el perfil, las tablas asociadas a la administración funcional en referencia a usuarios y perfiles describe y acredita que en la tabla perfiles existen la siguiente distribución:

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

Figura 2

Distribución de nivel de autorización

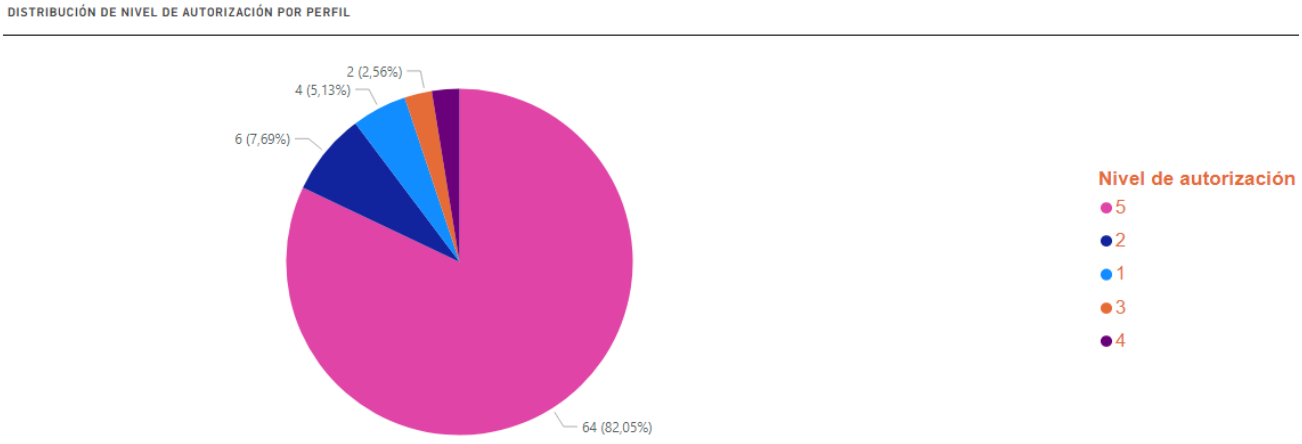


Tabla 5

Distribución por nivel

NIV_AUTORIZ	Recuento de NIV_AUTORIZ
5	64
2	6
1	4
3	2
4	2

Como se puede determinar de las gráficas anteriores 64 perfiles diferentes tienen nivel de autorización 5, 4 perfiles mantienen autorización 1, 6 perfiles nivel 2, 2 perfiles nivel 3 y 2 perfiles nivel 4, así las cosas, se puede concluir que lo dispuesto en el procedimiento no cumple lo establecido por la misma Dirección Comercial, en cuanto al nivel de autorización.

En este punto se debe advertir que en paralelo a lo determinado en cuanto a que existan más perfiles de los dispuestos en el procedimiento al nivel 5, en el nivel de usuario de base de datos existen dos perfiles de privilegios que definen las características que tienen los usuarios del sistema que interactúan con la base de datos del OPEN SCI, según lo informado por el Administrador de base de datos de la Dirección de TI:

> *"(…) Con la idea de conceptualizar la estructura de roles y accesos le comento que existen a nivel de base de datos 2 roles de base de datos principales, los cuales regulan las actividades de los usuarios contra los objetos (tablas, procedimientos, funciones, packages, vistas, etc), estos roles son:*
> *a. CONSULTA_SGC: el cual da acceso a ejecutar o consultar, los datos de los objetos de la base de datos asociados a este rol.*
> *b. USUARIO_SGC: el cual da acceso a ejecutar, insertar, eliminar y actualizar los datos de los objetos de la base de datos asociados a este rol.*
>
> *Estos dos roles son asociados a cualquier usuario que requiera hacer uso del sistema comercial y posteriormente a esto, se le asigna el perfil de aplicación necesario para operar e interactuar con el sistema comercial, esto, según requerido, todo lo anterior por medio de la aplicación de seguridad.*
>
> *En cuanto al perfil de aplicación, estos son los definidos por la administración funcional, según sean los requerimientos del negocio, los cuales son asignados, modificados y eliminados por la aplicación anteriormente mencionada. Específicamente la eliminación de usuarios, la aplicación elimina el usuario de base de datos y le desasigna el perfil de aplicación de la tabla de asociación, usuario y perfil. Para las actividades de inserción o modificación se ingresan los datos de usuario en la tabla de usuario y en la tabla asociación de usuario y perfil la información de cada funcionario y el perfil solicitado.(…)"*

Lo indicado por el Administrador de base de datos de la Dirección de TI lleva a determinar que la asignación real que pueda hacer un usuario del sistema OPEN en el nivel de privilegios (insertar, eliminar, actualizar) se define y acredita en el perfil asignado a ese funcionario y en específico a los objetos que se asignan a ese perfil, pero es de destacar que en el proceso de revisión y análisis de lo que pueda realizar cada perfil, no se puede realizar la actividad de examen, toda vez que no existe documentación que describa el detalle de lo que restrinja cada objeto asociado a cada perfil, en este sentido indica el Director Comercial Nacional en su memorando No.GG-SCI-2021-00593 del 3 de septiembre del 2021:

> ***"(…) Política 6.22: Restricción del acceso a la información***
>
> *El permiso a la información de los funcionarios que tienen acceso a los sistemas de información que administra la Dirección de Sistema Comercial Integrado, es con base a los permisos que se le otorgan o definen a los perfiles de acceso que se asocian a cada uno de los aplicativos".*

Al respecto se preguntó:

> ***"2. Se debe informar si existe un manual descriptivo de los privilegios***

> ***asignados a cada uno de los perfiles que existen en el sistema comercial, entendiéndose como privilegio a la prerrogativa asignada al perfil para cada módulo o pantalla el derecho a insertar, modificar, eliminar, grabar o actualizar un registro en una función cualquiera de un* módulo, ventana o criterio que pueda existir. En este *aspecto la Auditoria a investigado que en la tabla objetos y perfiles objetos existen más de 28,000 objetos creados".***

La respuesta de la Dirección Sistema Comercial Integrado fue:

> *"Se cuenta con un manual de perfiles de acceso al OPEN SCI, en el cual se indica a las operativas a que tiene acceso cada uno de los perfiles.*
>
> *El OPEN SCI, cuando fue implementado en el año 1998, contaba con una cantidad importante de objetos propios del sistema y que posteriormente con los desarrollos se fueron agregando otros. Adicionalmente, muchos de estos objetos son imágenes que funcionan como objetos de consultas.*
>
> *La documentación de los objetos es una función del área técnica a cargo de la Dirección de Sistemas de Información.(…)"*

De lo anterior se concluye que no existe información que permita conocer a qué derechos o funciones restringe un objeto. Toda vez que un perfil como lo indicó el Lic. Luis Fernando Ulate, existe a nivel de base de datos 2 roles de base de datos principales… CONSULTA_SGC: el cual da acceso a ejecutar o consultar, los datos de los objetos de la base de datos asociados a este rol. Además, el USUARIO_SGC: el cual da acceso a ejecutar, insertar, eliminar y actualizar los datos de los objetos de la base de datos asociados a este rol.

En otras palabras, todo usuario nace con los privilegios totales de insertar, modificar, actualizar, eliminar, en el sistema OPEN, estos derechos se le limitan mediante el perfil y los objetos asociados al perfil. En resumen, el hecho de que existan 64 perfiles con nivel de autorización 5, en la medida que no se conozca a que derechos o privilegios mantiene cada perfil y los objetos asociados al perfil, dificulta la administración y control de transacciones que registra cada usuario y crea la dependencia funcional de las personas con conocimiento de lo que pueda autorizar o denegar cada objeto asociado al perfil, en la administración del sistema.

En esta materia como se indicó con antelación el Acuerdo de Junta Directiva N. 2019-470: en documento denominado "Políticas de seguridad de la Información del Instituto Costarricense de Acueductos y Alcantarillados" dispuso en materia de control de accesos, lo que se debe aplicar en los siguientes temas***:***

> ***"Política 6: Control de Accesos***
>
> ***Política 6.2: Administración de accesos de usuarios***
>
> ***Política 6.3: Administración de privilegios***

Las NTGCTI norman

> *"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".*

Y como se ha indicado anteriormente en las NCISP se norma en los Requisitos de las actividades de control, respecto a la documentación.

La falta de un ejercicio propio del control y administración del sistema lleva a que exista esta situación en el nivel de tablas de asignación de perfiles, así mismo como la falta de documentación propias de los sistemas y reportes especializados. En cuanto a reporte especializados se debe hacer la salvedad que el AYA y la Dirección Funcional cuentan con herramientas tecnológicas suficientes para realizar esta labor de control.

Al existir un número tan alto de perfiles con nivel de autorización 5, dificulta y sube el nivel de riesgo de la administración del sistema, por cuanto se debe tener un especial cuidado de un cambio que se le realice a un objeto que esté asociado a cualquiera de los 64 perfiles con nivel 5, por cuanto la autorización está dada y es la de mayor nivel, mientras que el permiso a realizar una transacción válida se define y otorga en el nivel de objeto, en forma complementaria sin que exista documentación apropiada para cada objeto, potencia la posibilidad de cometer errores y facilitar el que, el perfil autorice transacciones que no son competentes para lo que se dispone.

3. CONCLUSIONES

3.1 Se determina que no se implementó la Política de seguridad En específico en cumplir con los acuerdos de Junta Directiva, que mantienen relación directa con el establecimiento, divulgación y capacitación de la política de Seguridad de las TI.

3.2 Los sistemas de información en su ciclo de vida se adecuan y mejoran al contexto de los diferentes requerimientos de la organización, la legislación y demás regulaciones le imponen. Siempre existe una forma mejor de hacer las cosas y de responder a la ciudadanía con los requerimientos tecnológicos que el medio le exige, en ese entorno los sistemas de información son elementos vivos que se transforman a las necesidades que se requieran, estos cambios deben ser acompañados de un adecuado funcionamiento tanto tecnológico como un conocimiento del ser humano que interactúa con los sistemas. De ahí que los programas de adiestramiento son elementos fundamentales para el éxito del sistema y el negocio que se automatiza.

El AyA no cuenta con una estrategia clara, ordenada y coherente para que las labores que se ejecutan en el sistema comercial OPEN por parte de los usuarios respondan

en forma apropiada y coherente con las exigencias que le imponen los cambios tecnológicos (nuevos procedimientos, nuevos módulos, etc.) que se incorporan en el sistema, además de las exigencias que se presentan por parte de los usuarios externos. El conocimiento debe ser integral y particular para la función que se desempeña, entendiendo las consecuencias de las actividades que se ejecutan.

En síntesis, no existe un programa de capacitación adecuado para los usuarios del sistema OPEN, acorde con las exigencias que se requieren por parte de los usuarios externos e internos del AyA.

3.3 El tratar de mejorar el sistema y facilitar funciones nuevas o mejorar las funcionalidades actuales, han implicado el tener que desestimar aspectos propios de control, lo que ha permitido volver un sistema seguro en un sistema vulnerable y complejo de administrar, al punto que personal de mantenimiento y administración de base de datos realicen funciones de administración funcional las cuales son incompatibles entre sí. Conllevando lo anterior a la creación de usuarios para fines específicos de atención de procesos de campo o cantonales, sin importar la redundancia de ID de funcionarios.

3.4 El sistema de Administración funcional se encuentra comprometido en su accionar, toda vez que requiere de personal externo a la dirección comercial nacional, para poder ejecutar las funciones propias de administración. Se evidencia que no existen controles ni documentación apropiada, para las transacciones que se registran en la base de datos por parte del personal de TI y personal contratado para el mantenimiento del sistema.

3.5 Existe incongruencia entre lo que dispone el Manual de perfiles y la realidad de la existencia de perfiles definidos en el sistema, determinándose la existencia de una mayor cantidad de perfiles definidos en el nivel de base de datos, que lo que realmente establece el manual de perfiles del sistema, comprometiéndose la administración funcional del sistema (Dirección del Sistema Comercial Integrado).

3.6 Se evidencian omisiones por parte de los encargados de administrar el sistema de seguridad del sistema comercial OPEN. Al no ejecutar como se deba las acciones necesarias de habilitación, modificación o exclusión de usuarios que comunican los encargados comerciales de las diferentes regiones, como parte de la responsabilidad de estos en su labor de administración descentralizada, conforme la normativa aplicable

3.7 La falta de lineamientos claros en cuanto a quien le corresponde la documentación de descripción de procesos, procedimientos y manuales funcionales, hace que se debilite sistema de control interno y diluye la responsabilidad. Además de que compromete la administración y mantenimiento del sistema en unas pocas personas que conocen el cómo está operativizado los procesos.

3.8 Se determina la existencia de un número excesivo de registros con valor cero o nulo en las tablas que conforman la base de datos, en específico las relacionadas con la administración funcional (Dirección del Sistema Comercial Integrado). Campos como el responsable de la persona que autoriza el perfil y otros campos que se deben considerar esenciales en este proceso.

Lo anterior permite concluir que la base de datos pierde: exactitud, oportunidad, confidencialidad, autenticidad, integridad y disponibilidad.

3.9 Por otra parte, no existe claridad por parte de los encargados de dar mantenimiento a la base de datos, en el poder identificar el porqué de la existencia del requerimiento de un registro en blanco en la tabla de asignación de objetos a perfiles, para cada uno de los perfiles, lo cual demuestra la falta de conocimiento de procesos que fueron implementados desde el año 1998 por la Empresa responsable de la implementación del sistema, que no fueron documentados o en su defecto no existió la transferencia tecnológica necesaria para la adecuada administración y operación del sistema.

3.10 No existe la documentación necesaria ni pistas de auditoría para dar trazabilidad, a las modificaciones de los datos del sistema comercial OPEN que se ejecutan en el ambiente de desarrollo y mantenimiento de sistemas, además de que no existe un control apropiado a las transacciones que se ejecutan por terceros en el sistema, conllevando a un debilitamiento del Control Interno. El hecho de existir un acta de aceptación de que el requerimiento cumple con lo solicitado no garantiza que la afectación de los datos se dé solamente en lo solicitado por la Dirección Comercial Nacional, por cuanto el perfil asignado a este personal permite el acceso completo al sistema. En resumen, la norma establece que esta actividad preferiblemente no se debe dar, y en caso de darse debe estar suficientemente documentada y controlada, aspecto que con la documentación revisada no cumple de forma eficiente la condición de documentación.

3.11 No existe documentación suficiente y necesaria de lo que permite o deniega un objeto asociado a un perfil, esto en conjunto con un gran número de perfiles con nivel de autorización de nivel 5 (autorización a ajustes superiores a ₡ 2,000,000.00), vuelve crítica la actividad de administración, mantenimiento y control de la asignación de perfiles a usuarios y las funciones que deba desarrollar cada usuario en el proceso de comercialización de los servicios que presta el AyA.

3.12 Con el presente informe la Auditoría Interna desea dar un valor agregando con recomendaciones que permite una mejora en las medidas de control, conforme lo normado en la Ley General de Control Interno y las NCISP

4. RECOMENDACIÓN

De conformidad con el artículo 12 inciso c) de la Ley General de Control Interno, No. 8292, se emiten las siguientes recomendaciones a cumplir dentro del plazo conferido

Instituto Costarricense de Acueductos y Alcantarillados
+ 506 2242 5000 * www.aya.go.cr
Pavas, San José, Costa Rica.

para ello. El incumplimiento no justificado constituye causal de responsabilidad.

La Auditoría Interna se reserva la posibilidad de verificar la efectiva implementación de las recomendaciones, y valorar si pudiera existir responsabilidad, en caso de incumplimiento injustificado de estas, según lo normado en el artículo 39 de la Ley General de Control Interno, No. 8292.

Para el cumplimiento de las recomendaciones se deberá cumplir con la remisión de la certificación de cierre o de avance, según lo que fuera solicitado con el oficio AU-2021-083 del 15 de febrero del 2021

Al Máster. Eric Bogantes Cabezas, Gerente General o quien ocupe el cargo:

4.1 Implementar en forma inmediata un comité de TI Institucional, que permita el generar los insumos necesarios para la toma de decisiones en cada uno de los niveles que se requieran, además de velar por el adecuado cumplimiento de lo que en materia regulatoria establezcan las nuevas normas de MICITT y las sanas prácticas. Remitir en a la Auditoría oficio de formalización del Comité Estratégico de TI como asesor del jerarca (Observación 2.1)

4.2 Realizar un diagnóstico de la situación actual de la institución con respecto a aquellos aspectos relevantes referentes a su Marco de Gestión de TI y esfuerzos necesarios para la implementación del Marco Normativo de Gobierno y Gestión de las Tecnologías de Información MICITT 2022, que permita identificar las brechas. Remitir a la Auditoría Interna copia del diagnóstico y del plan de acción para implementación de la normativa del MICITT y actualización de la normativa interna, incluyendo el Marco Orientador del Sistema Específico de Valoración de Riesgos, en cuanto al portafolio de riesgos de TI. (Observación 2.1 y 2.2)

4.3 Asegurar la implementación de las políticas de seguridad aprobadas por Junta Directiva, la cual deberá actualizarse conforme la normativa emitida por el MICITT y cumplir con lo dispuesto por la Junta Directiva en acuerdos Nos 2019-468, 2019-469, 2019-470, 2019-471, para lo cual la Administración Activa deberá asegurarse que ninguna práctica, procedimiento, lineamiento o costumbre administrativa, bajo el criterio de discrecionalidad administrativa, pueda constituirse contraria al ordenamiento jurídico. Remitir a la Auditoria Interna los documentos que acrediten la actualización de la normativa, su debida divulgación y capacitación. (Observación 2.1, 2.2)

4.4 Determinar las áreas deficitarias de capacitación del personal que interactúa con el sistema comercial a efectos de formalizar e implementar el Plan de Capacitación. Remitir a la auditoría interna copia del plan de capacitación, evidencia de la capacitación ejecutada y la evaluación de la misma (Observación 2.3)

4.5 Formalizar el canal oficial de instrucción para los usuarios del sistema, en la comunicación de los cambios, directrices y aplicación de normativa que se disponga,

a efectos de no crear confusiones e interpretaciones erróneas. Remitir a la Auditoría Interna la estrategia definida como canal de comunicación (observación nro. 2.3)

4.6 Instruir de forma inmediata a la Dirección de Sistemas de Información y Dirección comercial nacional para que documenten de forma apropiada la descripción de los objetos que se utilizan para el otorgamiento de privilegios a los perfiles que existen en el sistema. Remitir a la Auditoría Interna una certificación en la cual conste el establecimiento de este requisito de las actividades de control solo para los objetos activos (asignados a los perfiles) en el sistema (observación nro. 2.8)

Al Lic. Armando Rodríguez, director Comercial Nacional o quien ocupe el cargo:

4.7 Formalizar un plan de acción para la implementación de la estrategia que permita resolver el inconveniente de tener que crear diferentes ID's para un mismo funcionario a efectos para que un funcionario pueda desarrollar diferentes actividades de campo o trabajar en varias oficinas comerciales. Remitir a la Auditoría Interna una certificación en la que se incluya el plan de acción para implementar la estrategia y una certificación que asegure el cumplimiento del plan de acción en un plazo razonable para administrar los riesgos (observación nro. 2.4)

4.8 Ejecutar un examen exhaustivo de las transacciones realizadas por personal ajeno a la Dirección Comercial, para el módulo de seguridad y administración, se debe validar las transacciones realizadas por éstos, en caso de que se considere improcedentes. Remitir a la Auditoría Interna una certificación en la que se detalle el examen realizado y las acciones correctivas ejecutadas. (observación nro. 2.5)

4.9 Documentar de forma apropiada el manual de perfiles 2020, con los perfiles existentes en el sistema comercial OPEN, o en su defecto eliminar los perfiles que no son apropiados para la operación del sistema. Remitir a la Auditoría Interna copia de la formalización del manual de perfiles 2020 (observación nro. 2.6)

4.10 Cumplir inmediatamente lo dispuesto en el procedimiento de Perfiles de Usuarios al Sistema Comercial Integrado, en todas sus disposiciones, en específico a la adecuada administración de perfiles "Inclusión, modificación y eliminación de usuarios. Se deberá remitir a la Auditoria Interna un detalle de los cambios realizados y una certificación que indique que se cumplió con lo normado en el procedimiento. (observación nro. 2.7)

4.11 La administración funcional (Dirección del Sistema Comercial Integrado) del sistema comercial en conjunto con la Dirección de Sistemas de información deberá de documentar todos los procesos claves del sistema (programas, estructuras de datos, etc.) que garanticen que el traslado o migración de datos se pueda realizar de forma íntegra y segura, depurándose los datos de la base de datos, evitándose la redundancia de datos y normalizándose las estructuras relacionales. Remitir a la Auditoría Interna una certificación que aseguren el cumplimiento de lo recomendado.

Entendiendo la normalización como “el proceso de organización de datos en una base de datos. Esto incluye crear tablas y establecer relaciones entre dichas tablas de acuerdo con reglas diseñadas tanto para proteger los datos como para que la base de datos sea más flexible al eliminar la redundancia y la dependencia incoherente”. Remitir a la Auditoría Interna una certificación en la que se informe que los procesos claves del OPEN fueron documentados. (observación nro. 2.9)

4.12 Efectuar un muestreo y evaluación de lo actuado en el ambiente de producción por el personal de TI en cuanto a la inclusión, modificación o actualización de datos en la base datos. Además, deberá formalizar y divulgar el procedimiento en el cual se determine como, cuando y en qué condiciones se autoriza la inclusión, modificación de datos por parte el personal de mantenimiento del sistema, documentándose las transacciones ejecutadas. Remitir a la Auditoría Interna una certificación en la que se informe sobre la culminación de la evaluación y la formalización del procedimiento. (observación nro. 2.9)

4.13 Cumplir con la adecuada categorización que deba tener cada perfil según el nivel de autorización asignado en la ejecución de disminución de recibos puestos al cobro según lo establece la disposición de la Gerencia General. Remitir a la Auditoría Interna un reporte del cumplimiento de lo recomendado a la Auditoría Interna. (observación 2.10)

Ing. Luis Fernando Vindas
Encargado

Máster. Marco Espinoza Rosales
Director Área de Tecnología de Información

Máster. Karen Espinoza Vindas
Auditora Interna

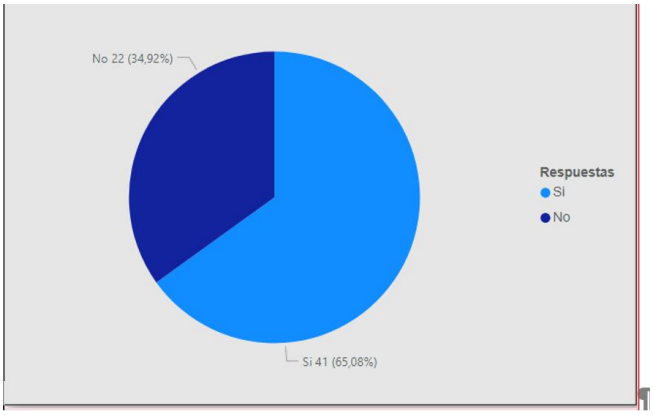
Anexo Nro. 1

1. Conocimiento del perfil con respecto a las funciones desarrolladas, a lo cual el 35% de los funcionarios encuestados manifiesta no conocer las características del perfil asignado para las funciones que realiza.

X

Figura 3

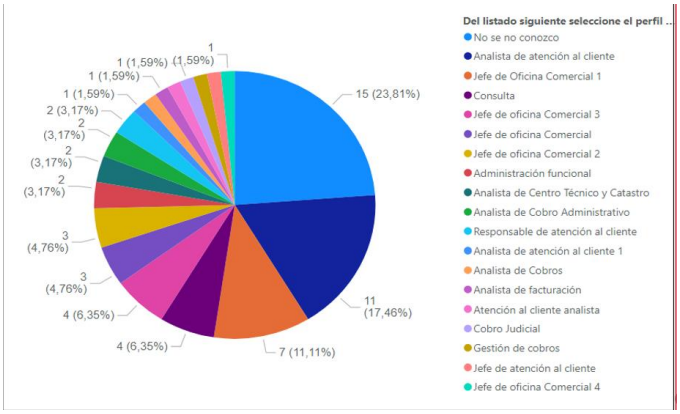
Características del perfil asignado



Nota: El 24%, indica no conocer cuál es el nombre del perfil asignado

Figura 4

Detalle de perfiles

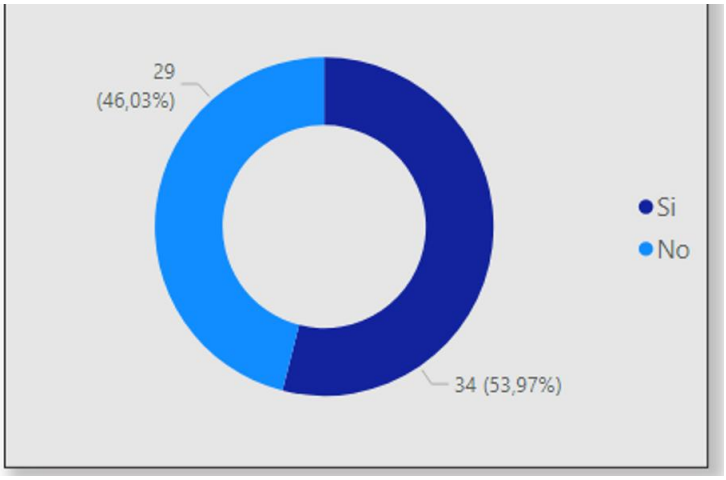


Nota: El 54% de los encuestados no recuerda haber firmado la boleta de TERMINOS Y CONDICIONES PARA EL USO DE CLAVES Y PERFILES, en la cual se establecen aspectos relevantes como: "*La contraseña de acceso, es la prueba irrefutable de que es el USUARIO, quien ingresa OPEN y que todas las operaciones registradas,*

Datamart Comercial, Archivo Histórico y SIGOS, son responsabilidad única y exclusivamente del encargado de la contraseña."

Figura 5

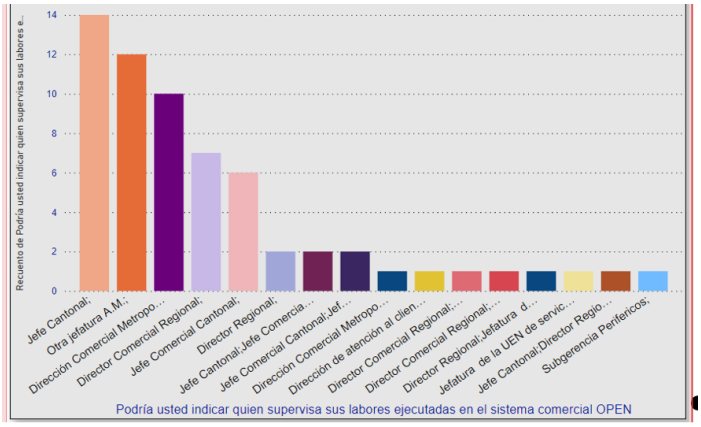
Solicitud para el uso de claves y perfiles de acceso



Nota: Un aspecto importante, lo es el hecho que el 100% de los encuestados, indican que alguien le supervisa su trabajo:

Figura 6

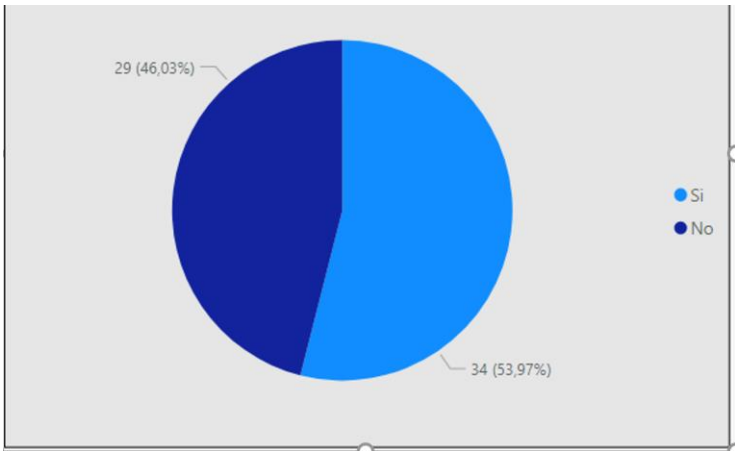
Supervisión en OPEN



Nota: El 46% indica no haber recibido, ni recibir una capacitación adecuada para el uso del sistema comercial OPEN con respecto a las funciones asignadas.

Figura 7

Capacitación recibida



Notas: De especial interés el destacar la estadística que muestra la consulta de capacitación, por cuanto es evidente que, para poder ejercer las funciones de forma apropiada, se debe conocer a plenitud los procesos y procedimientos que se establecen en los diferentes módulos del sistema, así como las directrices, reglamentos y normativa asociada al proceso comercial.

No debe ni puede permitirse que la atención de un reclamo o inquietud de un abonado no sea resuelta de forma apropiada, o en su defecto que la atención sea ambigua o no clara para el cliente, toda vez que el cómo se atienda o resuelva sus inquietudes, reflejará el cómo el abonado visualiza a la Institución.

ANEXO Nro. 2

Este anexo, presenta el detalle para cada usuario del sistema que mantiene más de un ID de usuario y quien o que programa generó el registro.

1. Alvarez Alfaro Rudy AYAC2034, AYA04121, código unicom 4211

Tabla usuarios

SEGURIDAD SGC	AYA2034	Rudy Alvarez Alfaro	4411	4411
MANUAL	AYA04121	Alvarez Alfaro Rudy	4211	4211
SEGURIDAD SGC	AYAC2034	Alvarez Alfaro Rudy	4211	4211

Tabla usuario_perfil

USUARIO	F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
AYA77504	04/04/2011 00:00:00	SEGURIDAD SGC	AYAC2034	JEFE OFI_COM_1	vb

2. Dayana Rodriguez Galeano AYA26011, AYA72602 código unicom 1213 y 1312

Tabla Usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC
MANUAL	AYA72602	DAYANA RODRIGUEZ GALEAN(	1312	1312
MANUAL	AYA26011	DAYANA RODRIGUEZ GALEAN(	1213	1213

3. Edgar Trejos Alvarado AYA6499, AYA499, AYA62999 código unicom 1110, 1200, 1211

Tabla usuarios

23/05/2018 10:57:56	MANUAL	AYA64999	EDGAR TREJOS ALVARADO	1211	1211
23/05/2018 10:57:56	MANUAL	AYA499	EDGAR TREJOS ALVARADO	1200	1200
23/05/2018 10:57:56	MANUAL	AYA6499	EDGAR TREJOS ALVARADO	1110	1110

4. Fabricio Murillo Rojas DCM00165, DCM00190 código unicom 1111

Tabla de usuarios

SEGURIDAD SGC	DCM0889	Fabricio Murillo Rojas	0	0
SEGURIDAD SGC	AYA00165	Fabricio Murillo Rojas	0	0
SEGURIDAD SGC	DCM00190	Fabricio Murillo Rojas	1113	1111
SEGURIDAD SGC	DCM00165	Fabricio Murillo Rojas	1113	1111
SEGURIDAD SGC	DCM0165	Fabricio Nurillo Rojas	1113	1111

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL
30/05/2019 08:47:09	SEGURIDAD SGC	DCM0889	

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL
16/04/2021 13:00:07	SEGURIDAD SGC	AYA00165	

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL
25/06/2021 00:00:00	SEGURIDAD SGC	DCM00190	ANALISTA ATCLI_1

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL
16/04/2021 00:00:00	SEGURIDAD SGC	DCM00165	ANALISTA ATCLI_1

5. Gerardo Noguera Valverde AYA 60942, AYA60904 código unicom 3211

   Tabla Usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC
MANUAL	AYA60904	GERARDO NOGUERA VALVERD	3211	3211
MANUAL	AYA60942	GERARDO NOGUERA VALVERD	3211	3211

6. Gerardo Quiros Ulloa AYA6860, AYA68600 código unicom 1200

   Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC
MANUAL	AYA68600	GERARDO QUIROS ULLOA	1200	1200
MANUAL	AYA6860	GERARDO QUIROS ULLOA	1200	1200

7. José Aniceto Acuña Garro AYA00647, AYA6471, AYA6470, AYA6472, AYA6473, AYA6474 código unicom 1111, 1213, 1313, 1413, 1312, 1111

   Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC
MANUAL	AYA6474	JOSE ANICETO ACU?A GARRO	1111	1111
MANUAL	AYA6473	JOSE ANICETO ACU?A GARRO	1312	1312
MANUAL	AYA6472	JOSE ANICETO ACU?A GARRO	1413	1413
MANUAL	AYA6471	JOSE ANICETO ACU?A GARRO	1213	1213
MANUAL	AYA6470	JOSE ANICETO ACU?A GARRO	1313	1313
SEGURIDAD SGC	AYA00647	Acuna Garro Jose Aniceto	1111	1111

   Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL
05/11/2020 00:00:00	SEGURIDAD SGC	AYA00647	JEFE OFI_COM_1

8. Jairo Stevens Adams AYAC2133, AYA0920 código unicom 4311

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA0920	Jairo Stevens Adams Soto	4311	4311	15
SEGURIDAD SGC	AYAC2133	Jairo Stevens Adams Soto	4311	4311	9

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
22/01/2020 00:00:00	SEGURIDAD SGC	AYA0920	JEFE OFI_COM_1	Jorge Mdrigal

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
16/02/2015 00:00:00	SEGURIDAD SGC	AYAC2133	JEFE_OFI_COM 2	Ana Julia Odio

9. Johnny Arauz Díaz AYA05155, AYA5155 código unicom 3711, 3411

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA5155	Johnny Arauz Diaz	3411	3411	8
SEGURIDAD SGC	AYA05155	Johnny Arauz Diaz	3711	3711	10

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
28/05/2018 00:00:00	SEGURIDAD SGC	AYA5155	ADM_LECT_RESP	Daisy Castro

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
04/11/2014 00:00:00	SEGURIDAD SGC	AYA05155	JEFE OFI_COM_1	Noily Guti□rrez

10. Jonny Badilla Duarte AYA00992, AYA992 código unicom 5112, 5911

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA992	Jonny Badilla Duarte	5911	5911	12
MANUAL	AYA00992	Jonny Badilla Duarte	5112	5112	0

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
11/10/2019 00:00:00	SEGURIDAD SGC	AYA992	JEFE OFI_COM_1	Luis Edo

11. Jorge Chaves Campos AYA04374, AYA4374 código unicom 2411

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA04374	Jorge Chaves Campos	2411	2411	7
SEGURIDAD SGC	AYA4374	Jorge Chaves Campos	2411	2411	5

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
11/10/2016 00:00:00	SEGURIDAD SGC	AYA04374	JEFE OFI_COM_1	Andres Calderon

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
27/08/2015 00:00:00	SEGURIDAD SGC	AYA4374	CT_AVERIAS	Alvaro Araya Alvarez

12. Jorge Rodriguez Zeledon AYA01104, AYA01048 código unicom 1111

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA01048	Jorge Rodriguez Zeledon	1111	1111	7
SEGURIDAD SGC	AYA01104	Jorge Rodriguez Zeledon	1111	1111	7

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
19/06/2017 00:00:00	SEGURIDAD SGC	AYA01048	CT_ANALISTA	VB Hermes Alvarado

13. Julio Ramirez Torres AYAC0246, AYA69978 código unicom 1213, 1110

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA69978	Julio Ramirez Torres	1110	1110	12
SEGURIDAD SGC	AYAC0246	Julio Ramirez Torres	1213	1213	7

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
06/01/2010 00:00:00	SEGURIDAD SGC	AYAC0246	JEFE OFI_COM_1	

14. Luis Granados Solis AYA94880, AYA39488 código unicom 3311

Tabla usuarios

F_ACTUAL	PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
23/05/2018 10:57:56	MANUAL	AYA39488	LUIS GRANADOS SOLIS	3311	3311	0
23/05/2018 10:57:56	MANUAL	AYA94880	LUIS GRANADOS SOLIS	3311	3311	0

15. Luis Paulino Chacon Salas AYA25921, AYA32592, AYA22592 código unicom 1126, 1300, 1200

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
MANUAL	AYA22592	Luis Paulino Chacon Salas	1200	1200	0
MANUAL	AYA32592	Luis Paulino Chacon Salas	1300	1300	0
SEGURIDAD SGC	AYA25291	Luis Paulino Chacon Salas	0	0	0
SEGURIDAD SGC	AYA25921	Luis Paulino Chacon Salas	1126	1126	15

Tabla usuarios_perfiles

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
14/05/2014 17:18:46	SEGURIDAD SGC	AYA25291		

F_ACTUAL	PROGRAMA	NOM_USR	NOM_PERFIL	USUARIO_AUTORIZA
23/03/2021 00:00:00	SEGURIDAD SGC	AYA25921	ANALISTA ATCLI_1	Alejandro Gonzalez Bogan

16. Marco Tulio Cruz Campos AYA24976, AYA24976 código unicom 1400, 1413

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
MANUAL	AYA24976	MARCO TULIO CRUZ CAMPOS	1413	1413	0
MANUAL	AYA24796	MARCO TULIO CRUZ CAMPOS	1400	1400	0

17. Orlando Alvarado Arias AYA3211, AYA2290 código unicom 1111, 1100

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
MANUAL	AYA2290	ORLANDO ALVARADO ARIAS	1100	1100	0
MANUAL	AYA3211	ORLANDO ALVARADO ARIAS	1111	1111	0

18. Rafael Rodriguez Soto AYA73689, AYA73683 código unicom 1126

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
MANUAL	AYA73683	RAFAEL RODRIGUEZ SOTO	1126	1126	0
SEGURIDAD SGC	AYA73689	RAFAEL RODRIGUEZ SOTO	1126	1126	0

19. Rodrigo Meneses Obando AYAAYA52, AYA52697 código unicom 1413

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
SEGURIDAD SGC	AYA52697	Rodrigo Meneses Obando	1413	1413	5
SEGURIDAD SGC	AYAAYA52	Rodrigo Meneses Obando	1413	1413	5

20. Victor Ureña Ureña AYA88032, AYA8032 código unicom 1313, 1110

Tabla usuarios

PROGRAMA	NOM_USR	DESC_USR	COD_UNICOM	COD_CENTEC	MAX_NUM_SESSIONES
MANUAL	AYA8032	VICTOR URE?A URE?A	*1110*	*1110*	*0*
MANUAL	AYA88032	VICTOR URE?A URE?A	*1313*	*1313*	*0*

ANEXO Nro.2

VALORACIÓN DE OBSERVACIONES AL BORRADOR DEL INFORME DE LA AUDITORÍA DE CARÁCTER PARA EVALUAR LA SEGURIDAD DEL SISTEMA COMERCIAL INTEGRADO EN CUANTO A LOS PERFILES

Párrafo	**Recomendaciones**		
RESUMEN (Página 4)	*"En la estructura funcional que da soporte y administra el qué pueda o deba hacer un funcionario dentro del sistema, radica en la asignación de un perfil que designa y define a que opciones, módulos o procesos puede acceder un usuario en un área específica para las funciones asignadas que deba desempeñar".* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Asignación de un perfil que designa? Aquí es importante indicar quien hace la designación, pues es una tarea que corresponde a las áreas usuarias quien al final concretas los roles que se asignan al perfil, el párrafo deja sin claridad el alcance"*		
¿Se acoge?	Si ( )	No ()	Parcial (x)
Argumentos Al	Se debe aclarar los dos procesos básicos que existen en "el de definición y el de asignación de perfiles de usuarios en el sistema Comercial Integrado": La definición y creación de perfiles del sistema OPEN, corresponde al personal de administración funcional (Dirección Comercial Nacional), con base en los diferentes procesos que se ejecutan en las áreas operativas. Ahora bien, la solicitud de asignación la realiza los encargados comerciales con base en la experiencia y conocimiento de las funciones que se desean que sean ejecutadas por parte de los usuarios, en armonía con el conocimiento que se tiene de las prerrogativas (privilegios) asignados a cada perfil que existe en el sistema. En este sentido queda claro que la definición, administración de perfiles es una labor de la administración funcional de la Dirección Comercial Nacional y no de los encargados. De lo indicado se debe aclarar que los encargados de las áreas usuarias si pueden y deben solicitar cual perfil debe tener cada usuario en el sistema, no así cuales son las características propias de cada perfil de usuario por cuanto es una labor propia de la administración función funcional Dirección Comercial Nacional. Si se cambiara a que sean estas áreas usuarias las que definan los privilegios de cada perfil se desvirtuaría la razón de ser de los administradores funcionales y los controles que deban existir en aras de vigilar la labor que se desarrolla en cada uno de los procesos que se ejecutan.		

	En resumen, lo que se dice en el párrafo que comenta el Lic. Armando Rodríguez lleva razón en cuanto a que quien solicita la asignación es el responsable del área comercial, no así quien define y administra las características del perfil es la Dirección Comercial, que es lo que en principio se indica en el comentario del informe. A mayor abundamiento lo que establece el procedimiento de asignación de perfiles de usuarios del sistema OPEN ***DIRECCIÓN SISTEMA COMERCIAL INTEGRADO.*** • Recomendar las políticas o instrucciones a utilizar, por parte de los usuarios en la administración adecuada de las claves de acceso. • Aprobar, diseñar la creación de nuevos perfiles, así como la modificación, exclusión, de acuerdo a las solicitudes de las Subgerencias técnicas de la Gran Area Metropolitana y los Sistemas Periféricos. • Asignar el perfil de usuario solicitado por las jefaturas correspondientes. • Informar al responsable comercial el resultado de la solicitud. • Realizar monitoreos periódicos a los accesos asignados para garantizar la seguridad del sistema.

Párrafo	Recomendaciones
RESUMEN **(Página 4)**	*En este sentido la adecuada administración en creación, modificación y eliminación de usuarios es una actividad importante dentro proceso mismo de comercialización de los servicios, existen premisas importantes que definen cual debe ser las generalidades de creación y asignación de perfiles o derechos de lo que debo o puedo hacer en los sistemas de información como lo puedan ser: "el principio de necesidad de saber o menor privilegio", "Todo debe estar prohibido a menos que se permita expresamente" y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente".* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Error redacción"*

Párrafo	Recomendaciones		
	"Esta premisa es confunsa (SIC), una cosa es lo que establece el principio de legalidad en la que un funcionario público solo puede hacer lo que esta (SIC) expresamente autorizado y otra cosa es el modelo de datos de tienen los diversos sistemas de información y más la base de datos Oracle, en la que el fabricante de tecnologia (SIC) ha definido dentro de la lógica funcional que para crear un usuario en primera instancia se habilita o contiene todos los permisos y luego en la aplicación de seguridad se deshabilitan accesos. En este sentido esta lógica no es aplicable porque las soluciones o modelos provienen del mercado quien dicta las pautas de uso		
¿Se acoge?	Si ( )	No (x)	Parcial ( )
Argumentos Al	Si vemos quien dispone el principio de la necesidad de saber o menor privilegio, "todo debe estar prohibido a menos que se permita expresamente y no sobre la premisa inversa de "Todo está permitido a menos que se prohíba expresamente", aún cuando podría interpretarse como algo legal, no lo es por cuanto es más que claro que el comentario está referido a una sana práctica establecido por la Contraloría General de la República y la Norma ISO 27001, es decir se sugiere que este principio básico sea utilizado en la definición de privilegios asignados a un perfil, el como se pueda implementar el principio en un sistema de información, claro que dependerá de las características propias del software de administración de base de datos y el sistema mismo, y lo que los analistas de sistemas en conjunto con los administradores definan que deba o pueda hacer cada usuario, no existe en cómputo una sola forma de hacer las cosas, lo que establece la norma es que se debe velar porque el acceso a la información y poder realizar modificaciones por parte de los usuarios se tome como principio el hecho de que todo debe estar prohibido a menos que se permita expresamente. De igual forma establece los mismos términos y condiciones establecidas en el documento de asignación de perfiles: Toda operación que se realice quedará registrada en los sistemas de seguridad que poseen: El Open SCI, Datamart Comercial, Archivo Histórico y SIGOS. Este registro electrónico es la prueba ante cualquier instancia administrativa o judicial, de que la operación fue realizada por el usuario asignado. En resumen la observación realizada no mantiene relación con lo que se indica en el informe en específico a como se deban crear o asignar los privilegios a los perfiles.		

Párrafo	Recomendaciones		
RESUMEN (Página 5)	*Con las recomendaciones dadas la Auditoría Interna aporta valor agregado en la mejora de los procesos y subprocesos institucionales y coadyuva con la Administración en el logro de los objetivos institucional del sistema de control interno, específicamente en el componente de sistemas de información. A su vez, se dan recomendaciones mejoran los controles, los procesos de dirección y los riesgos.* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Error en redacción"*		
¿Se acoge?	Si (x)	No ( )	Parcial ( )
Argumentos AI	Se acoge y se adiciona la palabra que quedando de la siguiente forma: A su vez, se dan recomendaciones que mejoran los controles"		

Párrafo	Recomendaciones		
ALCANCE (Página 2)	*"La auditoría abarcó los datos en Open al 30 de junio del 2021 En lo que fuera de interés se amplía el periodo de análisis a efectos de cumplir con el objetivo del estudio"* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"El alcance es hacia atras (SIC) del 30 de junio del 2021. Con la debida consideración el tiempo debe de tener un inicio y fin en virtud que la documentación tiene un plazo de conservación de los documentos por disposición con el GEDI"*		
¿Se acoge?	Si ( )	No (x)	Parcial ( )
Argumentos AI	Cuando se indica que la "auditoría abarco los datos en Open al 30 de junio del 2021", la prosa utilizada es clara al indicar que se refiere a la información almacenada en la base de datos hasta el 30 de junio del 2021, o sea toda aquella información que conste en la base de datos hasta esta la fecha indicada y por lógica anterior al 30 de junio del 2021, ahora bien la discriminación, selección o depuración de los datos que se extraen son propios de los criterios que se definieron en el momento oportuno.		

Párrafo	Recomendaciones		
METODOLOGÍA APLICADA (Página 2)	*"En la estructura funcional que da soporte y administra el qué pueda o deba hacer un funcionario dentro del sistema, radica en la asignación de un perfil que designa y define a que opciones, módulos o procesos puede acceder un usuario en un área específica para las funciones asignadas que deba desempeñar".* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Las encuestas no puede determinar el grado de conocimiento, sino que permiten obtener "la percepción en el grado de conocimiento. La percepción es una apreciación subjetiva que sirve como un criterio, para mejorar esa percepción pero no es un fin en si (SIC) mismo"*		
¿Se acoge?	Si ()	No (X)	Parcial ( )
Argumentos AI	Primero que nada, es oportuno el transcribir la definición dada por la Real Academia Española al término encuesta de la siguiente forma: "Conjunto de preguntas tipificadas dirigidas a una muestra representativa de grupos sociales, para averiguar estados de opinión o conocer otras cuestiones que les afectan." A mayor abundamiento se tiene que: **La encuesta es un instrumento para recoger información cualitativa y/o cuantitativa de una población estadística. Para ello, se elabora un cuestionario, cuyos datos obtenidos será procesados con métodos estadísticos.** Las encuestas son entonces una herramienta para conocer las características de un grupo de personas. Puede tratarse de **variables económicas**, como el nivel de ingresos (cuantitativa), o de otro tipo, como las preferencias políticas (cualitativo). Así las cosas con la encuesta desarrollada se pretendió conocer cuál era el grado de conocimiento que se tiene por parte de los usuarios de los perfiles y las funciones asignadas al igual que el grado de capacitación que se tiene del sistema, entre otras cosas, ahora bien como cualquier método estadístico puede ser sujeto de mejora o de afinar el diagnóstico que se requiera, de ahí que la recomendación		

	dada para este caso sea *"Se deberá determinar las áreas deficitarias de capacitación del personal que interactúa con el sistema comercial a efectos de definir las estrategias que se deban seguir, en capacitación, motivación o cualesquiera otras áreas susceptibles a mejorar*". Como se puede determinar será responsabilidad de la administración el investigar y definir las áreas deficitarias, es decir el análisis se debe realizar con el instrumento o metodología que se quiera utilizar y es propio del área que lo realice y no es la Auditoría quien deba realizarlo o definir como hacer el diagnóstico.

Párrafo	**Recomendaciones**		
CONCLUSIÓN	*"El sistema de Administración funcional se encuentra comprometido en su accionar, toda vez que requiere de personal externo a la dirección comercial nacional, para poder ejecutar las funciones propias de administración. Se evidencia que no existen controles ni documentación apropiada, para las transacciones que se registran en la base de datos por parte del personal de TI y personal contratado para el mantenimiento del sistema".* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *Esto debe aclararse, existe Dirección de Sistema Comercial Integrado que administra una serie de aplicaciones que soportan la gestión comercial y operativa del AyA donde se administra y opera sistemas de acueducto*		
¿Se acoge?	Si ( )	No (x)	Parcial ( )
Argumentos Al	El estudio y todos los comentarios que se desarrollan en el informe están referidos al Sistema Comercial Integrado OPEN, y no a la administración y operación del acueducto metropolitano u la gran cantidad de sistemas que se administran en el resto del país, en este sentido no se tendría ningún argumento válido para que se interprete como administración funcional a la administración operativa de los sistema de abastecimiento o tratamiento de agua que mantiene el AyA en la actualidad, más aún cuando el párrafo en lo subsiguiente conceptualiza y amplia el comentario.		

Párrafo	Recomendaciones		
CONCLUSIÓN	*"Se determina la existencia de un número excesivo de registros con valor cero o nulo en las tablas que conforman la base de datos, en específico las relacionadas con la administración funcional. Campos como el responsable de la persona que autoriza el perfil y otros campos que se deben considerar esenciales en este proceso".* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Aclarar término, esta nomenclatura no existe en el manual de organización"*		
¿Se acoge?	Si (X)	No ( )	Parcial ( )
Argumentos AI	Se aclarará desde el inicio del informe		

Párrafo	Recomendaciones		
RECOMENDACIÓN 4.5	*"Definir el canal oficial de instrucción para los usuarios del sistema, en la comunicación de los cambios, directrices y aplicación de normativa que se disponga, a efectos de no crear confusiones e interpretaciones erróneas. Remitir a la Auditoría Interna la estrategia definida como canal de comunicación (observación nro. 2.3)"* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Esta recomendación no esta (sic) clara, canal es el medio de comunicación que se utiliza formalmente en el AYA para girar ordenes, directrices o divulgar información y se puede interpretar que ese canal es el SDI. ¿O es acaso que se desea recomendar que sea un área de trabajo o dependencia?"*		
¿Se acoge?	Si ( )	No (x)	Parcial ( )
Argumentos AI	Del análisis a la documentación revisada para el estudio se pudo determinar que tanto la Gerencia General, como la Dirección Comercial Nacional y las Direcciones Comerciales Regionales giran instrucciones de acatamiento obligatorio para los usuarios finales del sistema, algunas que por su redacción pueden tender a confundir a los funcionarios, lo que se pretende es que solo exista un medio "canal", que emita estas directrices circulares, disposiciones o comunicaciones a efectos de que no se		

Párrafo	Recomendaciones
	mal interprete las disposiciones y que en caso de duda solo existe una persona o grupo de personas autorizadas en aclarar estas.

Párrafo	Recomendaciones		
RECOMENDACIÓN 4.6	*"La Gerencia General debe instruir de forma inmediata a la Dirección de tecnologías de Información y Dirección comercial nacional para que documenten de forma apropiada la descripción de los objetos que se utilizan para el otorgamiento de privilegios a los perfiles que existen en el sistema. Remitir a la Auditoría Interna una certificación en la cual conste el establecimiento de este requisito de las actividades de control (observación nro. 2.8) Se debe ejecutar solo para los objetos activos (asignados a los perfiles) en el sistema"* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Se recomienda ajustar la recomendación a que la documentación de los objetos asociados a la aplicación Open SCI que vincula en el uso con los perfiles, es una materia técnica que no compete a la Dirección del Sistema Comercial Integrado, por lo que la recomendación sería: La Gerencia General debe instruir de forma inmediata a quien corresponda, para que documenten de forma apropiada la descripción…"*		
¿Se acoge?	Si ( )	No (x)	Parcial ( )
Argumentos AI	El sistema comercial OPEN, tiene como áreas fundamentales en su accionar un componente técnico y otro funcional. No podría conceptualizarse un sistema de información sin la relación fundamental de proceso y automatización, en este sentido el desligar o el pretender que una labor de documentación solo se deba dar en lo técnico o que esta labor sea responsabilidad del área técnica, sería el ver solo el componente técnico sin la visión de administración, si analizamos el cómo se asignan de perfiles a usuarios, se determina que es una labor más de experiencia y conocimiento, que más que una labor que tenga su sostenibilidad en un manual en el cual se establezcan en forma clara que pueda o no pueda ejecutar un perfil en una pantalla, módulo o sistema, de ahí que no sería conveniente que esta recomendación sea solo de ejecución de la parte técnica. Por último, es de importancia el reiterar que esta labor debe ser desarrollada para los 300 objetos que se utilizan en la actualidad.		

Párrafo	Recomendaciones		
RECOMENDACIÓN 4.7	*"Adecuar en el menor tiempo posible la estrategia de como poder resolver el inconveniente de tener que crear diferentes ID's para un mismo funcionario a efectos de poder que un funcionario desarrolle diferentes actividades de campo o trabajar en varias oficinas comerciales. Remitir a la Auditoría Interna una certificación en la que se detalle la estrategia y el plan de implementación de la misma. (observación nro. 2.4)"* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Establecer un plan de trabajo para implementar una estrategia para resolver el inconveniente de teer (SIC) que crear diferentes ID´s para un mismo funcionario a efectos de poder que un funcionario desarrolle diferentes actividades de campo o trabajar en varias oficinas..."*		
¿Se acoge?	Si ( )	No (...)	Parcial (X)
Argumentos AI	La observación no es clara en su contenido, no se indica lo que se pretende o se solicita con la observación. Se mejora la redacción, dejando claro que es responsabilidad de la Administración Activa, el efecto cumplimiento de la estrategia y la razonabilidad de los tiempos del plan, para administrar los riesgos.		

Párrafo	Recomendaciones		
RECOMENDACIÓN 4.12	*"Efectuar un muestreo y evaluación de lo actuado en el ambiente de desarrollo por el personal de TI en cuanto a la inclusión, modificación o actualización de datos en la base datos."* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Esta recomendación desde la perspectiva funcional no tiene sentido, pues en el ambiente de desarrollo es donde se ejecutan los cambios o adecuaciones para mejorar el entorno de producción. Además este ambiente se cambia con cierta períodicidad (SIC) para ajustarlo a las adecuaciones. Los cambios validos (SIC) y ciertos están en el ambiente de producción"*		
¿Se acoge?	Si (x)	No ( )	Parcial ( )
Argumentos AI	Lleva razón el comentario se debe cambiar la palabra de desarrollo por producción.		

Párrafo	Recomendaciones		
RECOMENDACIÓN 4.13	*"Cumplir con la adecuada categorización que deba tener cada perfil según el nivel de autorización asignado en la ejecución de disminución de recibos puestos al cobro según lo establece la disposición de la Gerencia General. Deberá remitirse un reporte del cumplimiento de lo recomendado a la Auditoría Interna (observación 2.10)"* Con el oficio GG-2021-04549 recibido el 2 de diciembre del 2021 se indica por parte de la Gerencia General la siguiente observación: *"Se recomienda adecuar la recomendación. Cumplir con una adecuada categorización que deba tener cada perfil es subjetivo. Se sugiere:* *Establecer una categorización razonable que deba tener cada perfil según el nivel de autorización asignado en la generación de notas de crédito vinculados a la disminución del importe total a pagar en las facturas o recibos puesto a al cobro, según lo establece la disposición de la Gerencia General"* *Es recomendación 2.11 , la recomendación 2.10 se refiere a Funciones incompatibles*		
¿Se acoge?	Si ( )	No (X)	Parcial ( )
Argumentos Al	Sin entrar en polémicas lo sugerido por la observación es exactamente lo que la recomendación establece, en este sentido no se ve la necesidad de cambiar la redacción, más aún tiene muy claro lo que hay que hacer el que redacta la observación, solo en cuanto a razonable no es de recibo por cuanto es una disposición administrativa definida por la Gerencia General en conjunto con la Dirección Nacional Comercial ya lo razonable fue definido con antelación.		