



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ATIC-158-2015
28-07-2015

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo 2015 del Área de Tecnologías de Información y Comunicaciones de la Auditoría Interna, con el fin de evaluar la gestión de las tecnologías de información y comunicaciones en la Sucursal de Alajuela.

Los resultados del estudio han permitido evidenciar oportunidades de mejora en la administración de las TIC de esa Sucursal, como son: la documentación de procedimientos inherentes a la función informática, la implementación de controles para garantizar una seguridad física y lógica (información) suficiente, el registro y control de los activos en TIC otorgados a ese establecimiento, entre otros elementos de relevancia dentro de la disciplina informática.

De manera que, la situación descrita reafirma la necesidad de fortalecer los procesos de gestión de las tecnologías de información y comunicaciones en ese establecimiento, a fin de garantizar que los principales servicios y/o actividades que son responsabilidad del servicio de informática alcancen los objetivos, propósitos y metas para los cuales fueron creados.

En virtud de lo expuesto, este Órgano de Fiscalización institucional ha solicitado a la Jefatura de la Sucursal de Alajuela, adopten acciones concretas para la atención de las recomendaciones insertas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable.



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ATIC-158-2015
28-07-2015

ÁREA TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN INTEGRAL GERENCIAL DE LA SUCURSAL DE ALAJUELA TEMA: TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ORIGEN DEL ESTUDIO

El estudio se efectuó en cumplimiento del Plan Anual Operativo de la Auditoría Interna 2015.

OBJETIVO GENERAL

Evaluar la gestión de las tecnologías de información y comunicaciones en la Sucursal de Alajuela.

OBJETIVOS ESPECÍFICOS

1. Verificar el cumplimiento por parte de la Sucursal de Alajuela respecto de las funciones sustantivas asociadas a la administración de la calidad, servicios continuos y gestión de riesgos en TIC.
2. Constatar la implementación de medidas de seguridad física para la protección de activos en TIC.
3. Verificar la definición y aplicación de controles vinculados con la seguridad lógica y uso de cuentas del directorio activo y sistemas de información institucionales.

ALCANCE

El estudio comprende las acciones realizadas por la Sucursal de Alajuela en su gestión de las tecnologías de información y comunicaciones, durante el período enero 2015 y junio 2015, ampliándose en aquellos casos que se consideró pertinente.

La presente evaluación se realizó conforme a las disposiciones señaladas en las Normas Generales de Auditoría para el Sector Público, emitido por la Contraloría General de la República.

METODOLOGÍA

Para lograr el cumplimiento de los objetivos indicados se ejecutaron los siguientes procedimientos metodológicos:



CAJA COSTARRICENSE DE SEGURO SOCIAL

AUDITORIA INTERNA

Tel.: 2539-0821 - Fax.: 2539-0888

Apdo.: 10105

- Análisis de la información suministrada por la Administración Activa vía correo electrónico y en formato físico, sobre las acciones desarrolladas para dar cumplimiento a actividades sustantivas consignadas en el Modelo de Organización de los CGI.
- Inspección física de las oficinas de la Sucursal de Alajuela.
- Verificación de activos en TIC instalados en diversos servicios de ese establecimiento.
- Consulta a las bases de datos de sistemas de información institucionales como el Sistema Contable Bienes Muebles (SCBM), Portal de Recursos Humanos y registros del directorio activo institucional.
- Entrevista con: MBA. Luis Diego Zamora Benavides, Jefatura de la Sucursal de Alajuela; Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; Srita. Jacqueline Alfaro López, encargada de presupuesto y activos en la Sucursal de Alajuela; Ing. Shirley Sánchez Ramírez, funcionaria del Área de Soporte Técnico de la Dirección de Tecnologías de Información y Comunicaciones; y el Ing. Guillermo Rojas Zapata, Jefatura del Centro de Gestión Informática de la Dirección Regional de Sucursales Huetar Norte.

MARCO NORMATIVO

- Ley General de Control Interno, 8292.
- Manual de Normas de Control Interno para el Sector Público, 2009.
- Normas Técnicas para la Gestión de las Tecnologías de la Información (CGR), 2007.
- Normas Institucionales de TIC, 2012.
- Normas Institucionales de Seguridad Informática, 2008.
- Modelo de Organización de los Centros de Gestión Informática, 2013.
- Guía de Mejores Prácticas en la Gestión de Centros de Producción de Datos, 2008.
- Manual de normas y procedimientos contables y control de activos, mayo 2011.

ASPECTOS NORMATIVOS A CONSIDERAR

Esta Auditoría, informa y previene al Jerarca y a los titulares subordinados, acerca de los deberes que les corresponden, respecto a lo establecido en el artículo 6 de la Ley General de Control Interno, así como sobre las formalidades y los plazos que deben observarse en razón de lo preceptuado en los numerales 36, 37 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

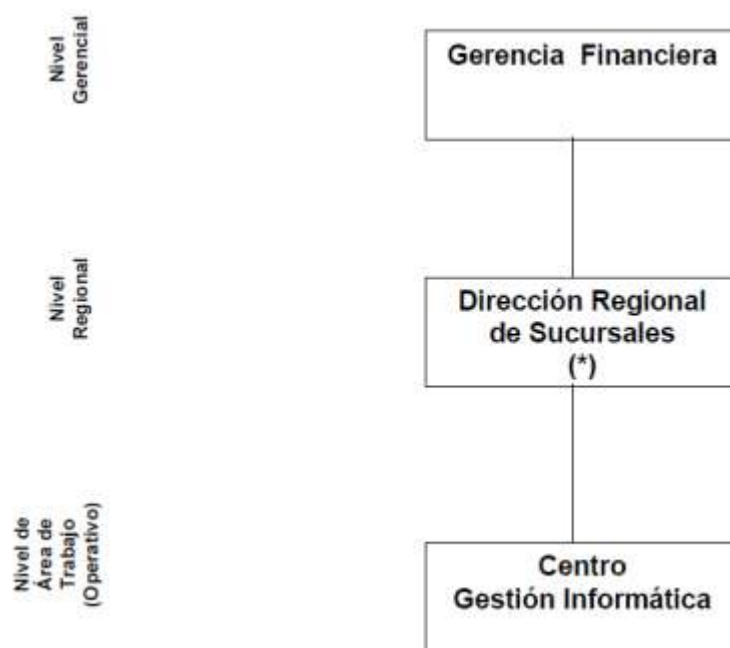
“Artículo 39.- Causales de responsabilidad administrativa. El jerarca y los titulares subordinados incurrirán en responsabilidad administrativa y civil, cuando corresponda, si incumplen injustificadamente los deberes asignados en esta Ley, sin perjuicio de otras causales previstas en el régimen aplicable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

ANTECEDENTE

La estructura orgánica y funcional aplicable a la Sucursal de Alajuela se encuentra establecida en el Modelo de Organización de los CGI (octubre 2013) en cuanto a la gestión de las tecnologías de información, mismo cuyas modificaciones fueron aprobadas por la Junta Directiva en el artículo No. 44 de la sesión No. 8555 del 26 de enero de 2012 y artículo No. 32 de la sesión No. 8658 del 29 de agosto de 2013.

De acuerdo con dicho modelo de organización, esa sucursal deberá recibir soporte técnico del Centro de Gestión Informática de la Dirección Regional de Sucursales Huetar Norte, y su estructura orgánica se ilustra en la Figura 1.

Figura 1: Estructura Orgánica para CGI Tipo B.



Fuente: Modelo de Organización de los CGI (octubre 2013; p.76).



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

En el mismo Modelo de Organización de los CGI se menciona al respecto del nivel de responsabilidad de los establecimientos Tipo B (p.51-52) lo siguiente:

“Es responsable de mantener (en su ámbito de competencia), en óptimo funcionamiento las bases de datos, de administrar información operativa y asesorar técnicamente a las unidades de trabajo. Para cumplir con lo anterior, es fundamental que mantenga interrelaciones constantes con el Centro de Gestión Informática Gerencial y con el Consejo Institucional de Centros de Gestión Informática. Es responsable de la adecuada utilización del equipo de cómputo, de los materiales y suministros necesarios para ejercer sus labores y del cumplimiento efectivo de los procesos y subprocesos para la problemática operativa que se genera en su ámbito de acción. El desarrollo de las actividades debe responder a criterios de eficiencia, eficacia y economía, con el objeto de que se traduzcan en una mejora sustancial de la gestión de los servicios en su ámbito de acción.”

En cuanto a su estructura por procesos (p.52-53), para esos CGI se definen dos subprocesos de trabajo: Gestión Técnica y Soporte Administrativo.

En cuanto al recurso presupuestario asignado, a esa sucursal le fue otorgado para el período 2015 un total de ₡7.000.000,00 (siete millones de colones exactos) en partidas asociadas a las tecnologías de información y comunicaciones (TIC); cuyo desglose se muestra en el Cuadro 1.

Cuadro 1: Presupuesto asignado a la Sucursal de Alajuela en partidas asociadas a las TIC, período 2015.

Partida	Asignación	Gasto
2122 TELECOMUNICACIONES	₡2,120,000.00	₡157,955.00
2159 MANT. REP. EQUIP. CÓMPUTO Y SIST. INFORM	₡4,880,000.00	₡0.00

Fuente: Consulta efectuada al Sistema Integrado de Presupuesto el 05 de mayo de 2015.

Acerca de los riesgos detectados, la Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en esa Sucursal; le proporcionó a esta Auditoría copia digital del Plan de Continuidad aprobado para ese establecimiento, en la cual se incluye la descripción e impacto asociado a 15 riesgos en TIC. Cabe señalar que en el documento se consigna como última versión la 3.2 de abril 2015.

Sobre el recurso humano disponible para el cumplimiento de las funciones asociadas a la gestión de las TIC, vía correo electrónico del 29 de abril de 2015 se informó que esa sucursal únicamente dispone de la Ing. Carmen Anay Hidalgo Arguedas, en una plaza de Analista de Sistemas 4.



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

HALLAZGOS

1. Documentación de procedimientos de trabajo asociados a las TIC

Se evidenciaron oportunidades de mejora en torno a la documentación de los procedimientos de trabajo ejecutados en ese CGI, dado que no se incluyen datos como: fechas de realización, actualización, responsables, autorización, entre otros, que permitan el control sobre las versiones del documento, limitando el poder constatar si los mismos son sometidos a procesos de revisión periódica. Excepción de lo anterior son los documentos:

- Instalación y Configuración Windows 2008 Server R2 - PowerEdge 2900).doc
- Instalación y Configuración SQL 2008 R2 en Servidor.doc

Lo anterior producto de la revisión de los documentos proporcionados por la Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; en respuesta a la solicitud de información sobre la documentación de sus actividades sustantivas.

La Ley General de Control Interno 8292 en su artículo 15, Actividades de Control, establece como deber del jerarca y de los titulares subordinados lo siguiente:

"[...] Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:

- La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.*
- La protección y conservación de todos los activos institucionales.*
- 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.*
- La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.*
- 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 Normas de control interno para el sector público establecen como requisito para las actividades de control (inciso 4.2) lo siguiente:



CAJA COSTARRICENSE DE SEGURO SOCIAL

AUDITORIA INTERNA

Tel.: 2539-0821 - Fax.: 2539-0888

Apdo.: 10105

"[...] 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".

La Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; señaló:

"Protocolos de instalación de sistemas, aplicaciones, bases de datos. Esos protocolos fueron hechos en conjunto con las demás Direcciones Regionales de Sucursales. Se estuvieron revisando a inicios de año, igualmente en forma conjunta con las Direcciones Regionales de Sucursales. Todos los protocolos son remitidos vía correo electrónico a los diferentes compañeros encargados de informática."

La inclusión de información sobre las versiones de los procedimientos documentados y utilizados por esa Sucursal, así como su estandarización en cuanto al formato empleado, eventualmente facilitarían el control y supervisión sobre la actualidad y pertinencia de los mismos, además de garantizar su ajuste y eficacia de su contenido, el cual es fundamental para la atención de diferentes actividades sustantivas en TIC en ese establecimiento.

2. Registro y control de incidencias en TIC

Se evidenció que a lo interno de la Sucursal de Alajuela no se han implementado mecanismos de control a través de los cuales se documenten las incidencias reportadas por los usuarios de ese establecimiento, en torno a problemas o averías en sus equipos tecnológicos (TIC).

La Ley General de Control Interno 8292 en su artículo 15, Actividades de Control, establece como deber del jerarca y de los titulares subordinados lo siguiente:

"[...] Documentar, mantener actualizados y divulgar internamente tanto las políticas como los procedimientos que definan claramente, entre otros asuntos, los siguientes:

- i. La autoridad y responsabilidad de los funcionarios encargados de autorizar y aprobar las operaciones de la institución.*
- ii. La protección y conservación de todos los activos institucionales.*
- iii. 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.*



CAJA COSTARRICENSE DE SEGURO SOCIAL

AUDITORIA INTERNA

Tel.: 2539-0821 - Fax.: 2539-0888

Apdo.: 10105

iv. La conciliación periódica de registros, para verificar su exactitud y determinar y enmendar errores u omisiones que puedan haberse cometido.

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 Normas de control interno para el sector público establecen como requisito para las actividades de control (inciso 4.2) lo siguiente:

“[...] 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 MBA. Luis Diego Zamora Benavides, Jefatura de la Sucursal de Alajuela; indicó:

“No se documentan las incidencias reportadas y atendidas principalmente por el factor de tiempo, dadas las cargas de trabajo, dado que en muchos de los puestos la prioridad es la atención al usuario, por tanto se reporta directamente con la Ing. Carmen Hidalgo para su solución. Lo que podría hacerse es definir una estrategia más ágil que el llenado de un formulario, por ejemplo vía correo electrónico.”

La Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; señaló:

“... En esta Sucursal yo me encargo de brindar mantenimiento correctivo a los equipos de cómputo con la limitante de que no se dispone de presupuesto para la adquisición de repuestos, los cuales al ser necesarios se gestionan con la Dirección Regional directamente...”

De mi parte, colaboro con toda la Dirección Regional para la atención de incidentes. Igual por la Dirección Regional surgió la instrucción de llenar un formulario para la solicitud de soporte, sin embargo en la sucursal los usuarios no han querido utilizar dichos formularios. En la actualidad se atienden los reportes hechos por correo electrónico, mensajería interna y por teléfono...”

Las debilidades en los mecanismos de control establecidos para el registro de las incidencias reportadas en torno a problemas en el funcionamiento y rendimiento de los equipos en tecnologías de información y comunicaciones podrían comprometer la planificación de actividades en el corto plazo, así como el oportuno y pertinente dimensionamiento de las necesidades en cuanto a recursos humanos, presupuestarios y de otra índole suficientes para garantizar la adecuada prestación de los servicios.



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

3. Seguridad física del cuarto de servidores

Se evidenciaron oportunidades de mejora en torno a la ubicación e instalaciones proporcionadas para el cuarto de servidores en la Sucursal de Alajuela, a saber:

- Aun cuando se observaron extintores cercanos al cuarto de servidores, los mismos mostraban vencida su carga de químico interno.
- Los controles de acceso para el cuarto de servidores y telecomunicaciones se limitan al uso de cerraduras con llave convencional, sistemas que no permiten el registro automático de las entradas y salidas a sitios sensibles como ese.
- El cuarto de servidores no dispone de: piso falso, sistemas internos de monitoreo y alarma para la humedad, temperatura y contra robos, bitácora para el registro de entradas y salidas.

Las Normas de Control Interno para el Sector Público, emitidas por la Contraloría General de la República, señalan en su apartado 1 "Normas Generales", lo siguiente:

"El SCI de cada organización debe coadyuvar al cumplimiento de los siguientes objetivos:

a. Proteger y conservar el patrimonio público contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal. El SCI debe brindar a la organización una seguridad razonable de que su patrimonio se dedica al destino para el cual le fue suministrado, y de que se establezcan, apliquen y fortalezcan acciones específicas para prevenir su sustracción, desvío, desperdicio o menoscabo."

La Guía de Mejores Prácticas en la Gestión de Centros de Producción de Datos, emitidas en marzo del 2008, establece lo siguiente:

"Los procedimientos aquí documentados deben ser revisados por todas aquellas Unidades Ejecutoras y funcionarios que estén involucrados directa o indirectamente con la administración de Centros de Producción (conocidos como Centros de Cómputo) en la Institución y valorar si es aplicable en su Unidad."

De igual forma esa guía establece como acciones previas para el control del fuego (10.6.8) las siguientes:

*"... Verifique sus extintores
... Instale detectores de humo en áreas de alto riesgo o muy cerradas
... Revise las baterías de sus detectores de humo una vez al año..."*



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

El MBA. Luis Diego Zamora Benavides, Jefatura de la Sucursal de Alajuela; indicó:

“Las recargas a los extintores ya se encuentran programadas, para la Sucursal de Alajuela toda dicha labor el próximo 29 de junio... Todas estas compras se encuentran centralizadas en la Dirección Regional, por lo cual de nuestra parte dependemos de sus gestiones a fin de poder contar con servicios como el de la recarga de extintores.

... En el caso particular de los aspectos en tecnologías de información y comunicaciones el responsable de la recepción conforme fue el Ing. Rohanny Vindas Umaña. Vía correo electrónico voy a consultarle a ese compañero, por qué no se consideraron la totalidad de elementos incluidos en la normativa en tecnologías de información y comunicaciones acerca de los mecanismos para garantizar la seguridad física del cuarto de servidores (controles de acceso, monitoreo, entre otros).”

Sin embargo, al momento de elaborado el presente informe no se obtuvo respuesta por parte del MBA. Zamora Benavides ni de los representantes de la Dirección de Arquitectura e Ingeniería. Por su parte la Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; señaló:

“Considero que si se encuentran en un lugar seguro dado que el Área de Logística donde está ubicado, es un área con puerta de seguridad y acceso restringido, y hay un área específica para este equipo que se mantiene bajo llave.”

La falta de mecanismos de seguridad en el cuarto de servidores podría comprometer la integridad de los equipos informáticos, situación que expone no solamente el patrimonio institucional, sino además la prestación de servicios a la población costarricense, afectando tanto los intereses institucionales como asistenciales de la CCSS.

4. Control y registro de activos en tecnologías de información y comunicaciones

Se evidenciaron inconsistencias en el inventario de activos en TIC disponibles para la Sucursal de Alajuela, a saber:

- El activo con placa #744554 registrado en el Sistema Contable Bienes Muebles (SCBM) para la unidad 1302 Sucursal de Alajuela como “EN USO” dispone de una recomendación para darse de baja, documentada mediante oficio SA-2563-2014 del 13 de noviembre de 2014.
- El activo con placa #751204 registrado en el SCBM para la unidad 1302 Sucursal de Alajuela como “EN USO” dispone de un comprobante de traslado de activos #46-4613020001314 del 8 de agosto de 2014 con destino a la unidad 2104 Hospital México.



CAJA COSTARRICENSE DE SEGURO SOCIAL

AUDITORIA INTERNA

Tel.: 2539-0821 - Fax.: 2539-0888

Apdo.: 10105

- El activo con placa #751205 registrado en el SCBM para la unidad 1302 Sucursal de Alajuela como "EN USO" dispone de una recomendación para darse de baja, documentada mediante oficio SA-0937-2015 del 15 de abril de 2015.
- El activo con placa #959841 registrado en el SCBM para la unidad 1301 Dirección Regional de Sucursales Huetar Norte como "EN USO", fue incluido como parte del inventario de equipo de cómputo de la Sucursal de Alajuela, mismo que a su vez fue localizado en la inspección de activos efectuada por esta Auditoría el 02 de junio de 2015.
- Fue localizado en los registros del SCBM 2015 únicamente un switch vinculado con la unidad 1302 Sucursal de Alajuela, placa #490609 cuyo estado actual es "RETIRADO". Los números de placa registradas en el inventario de switch llevado a cabo por la Ing. Carmen Anay Hidalgo Arguedas (998942, 998943, 998944) no se encuentran asociadas con ningún activo en el SCBM.

Así mismo, en consulta efectuada a la Jefatura de la Sucursal y a la encargada de informática no se tuvo claridad sobre los períodos de garantía aplicables a dichos equipos de comunicaciones, así como la eventual documentación asociada a la ejecución contractual de mantenimientos.

- 4 activos no disponen de placas metálicas que los identifiquen como bienes institucionales (846138, 846151, 846182, 846184), sino de marcas confeccionadas con marcadores y relieves de anteriores rotulaciones (ver Anexo 1).

Las Normas Técnicas para el Control y Gestión de las TI, emitidas por la Contraloría General de la Republica el 21 junio del 2007, señalan lo siguiente:

"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."

El Manual de normas y procedimientos contables y control de activos establece en su artículo 55 *Identificación o plaqueo de los bienes*, establece:

"Todo bien mueble que la Institución adquiera debe ser identificado en forma inmediata mediante placa de metal, la que debe ser anotada doblemente mediante el uso de marcadores, pintura, grabado o cinta adhesiva; con el fin de que si la placa de metal se desprende, pueda identificarse por cualquiera de los medios anotados..."



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

El MBA. Luis Diego Zamora Benavides, Jefatura de la Sucursal de Alajuela; indicó:

“Esos temas los manejan los compañeros de la Dirección de Arquitectura e Ingeniería, quienes son aquellos que dieron seguimiento a la definición de especificaciones y ejecución de obras para la remodelación de la sucursal. En casos como los aires acondicionados no se contrató como parte de la remodelación los servicios de mantenimiento, situación que al día de hoy nos genera problemas puesto que esos equipos permanecen encendidos todo el día, con el desgaste normal por uso que puedan tener.”

En el caso particular de los aspectos en tecnologías de información y comunicaciones el responsable de la recepción conforme fue el Ing. Rohanny Vindas Umaña. Vía correo electrónico voy a consultarle a ese compañero lo correspondiente a la garantía y mantenimiento de los switch; en cuanto tenga una respuesta se la hare de conocimiento a la Auditoría.”

Sin embargo, al momento de elaborado el presente informe no se obtuvo respuesta por parte del MBA. Zamora Benavides ni de los representantes de la Dirección de Arquitectura e Ingeniería. Por su parte la Srita. Jacqueline Alfaro López, encargada de presupuesto y activos en la Sucursal de Alajuela; señaló:

“... El problema que tenemos con las placas metálicas se debe a que el pegamento proporcionado por la Institución una vez seco no permite que la placa se sostenga por mucho tiempo adherida al equipo donde fue instalado. Cuando las placas se caen o bien me las facilitan a mi persona, o las guardan los mismos compañeros que utilizan el equipo. Se nos ha sugerido emplear calibradores u otras herramientas que permitan marcar la superficie del activo, sin embargo no se ha autorizado su adquisición. Lo que se ha optado es por escribir el número de placa con marcadores.”

... [Sobre los switch] Esos equipos aún están pendientes de ser ingresados en el sistema, paso previo para colocar sus placas correspondientes. En cuanto al acceso al sistema he tenido problemas para la gestión del ingreso al mismo, Además no se podían hacer cambios en el SCBM hasta abril 2015 debido al proceso de inventario institucional. Sin embargo espero en los próximos días estar atendiendo esa labor e instalando las placas en los activos...”

Las debilidades señaladas en el presente hallazgo en cuanto a la gestión de activos en TIC asignados a esa Sucursal podría comprometer la toma de decisiones por parte de las autoridades del establecimiento y demás instancias superiores en cuanto a la planificación y gestión de la adquisición de equipos tecnológicos, además de limitar la eventual detección de posibles pérdidas o sustracciones de activos, comprometiendo así el resguardo y utilización de los mismos, así como afectando el patrimonio institucional.



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

5. Seguridad lógica de los equipos de cómputo de la sucursal

Se detectaron oportunidades de mejora sobre la seguridad lógica en los equipos inspeccionados en la Sucursal de Alajuela, a saber:

- 2 activos presentaban definiciones del antivirus sin actualizar (744561, 959841).
- 1 activo tenía los escudos de protección del antivirus desactivado (744556).
- 1 activo tenía problemas de conexión con el servidor del antivirus (959998). Sobre este particular cabe señalar que el equipo se utiliza como servidor de aplicaciones.
- 1 activo presentaba problemas de inicio de Windows al momento de la inspección, por lo cual no fue posible verificar los datos del mismo.
- Todos los equipos de la sucursal tienen instalado el software de mensajería instantánea "SPARK", el cual no se encuentra incluido como parte del listado oficial de software libre o gratuito autorizado en la CCSS.

Las Normas Técnicas para el Control y Gestión de las TI, emitidas por la Contraloría General de la Republica el 21 junio del 2007, señalan lo siguiente:

"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."

Las Normas Institucionales de TIC, emitidas en abril del 2012, establecen lo siguiente:

"La Dirección de Tecnologías de Información y Comunicaciones a través del Área de Seguridad Informática será la encargada de emitir las Políticas Institucionales de Seguridad Informática y Normas Institucionales de Seguridad Informática, las cuales son de acatamiento obligatorio de todas las unidades de trabajo. A la vez, es la encargada de brindar la asesoría en cualquiera de los temas de seguridad informática."

Las Normas Institucionales de Seguridad Informática, emitidas en abril del 2008, establecen lo siguiente:

"Las normas (conjunto de reglas) aquí documentados deben ser de implementación obligatoria para todas aquellas Unidades Ejecutoras y funcionarios que estén involucrados directa o indirectamente con el uso de tecnologías de información y comunicaciones."



CAJA COSTARRICENSE DE SEGURO SOCIAL

AUDITORIA INTERNA

Tel.: 2539-0821 - Fax.: 2539-0888

Apdo.: 10105

Cabe responsabilidad para aquel funcionario que incumpla las normas de Seguridad Informática establecidas en este documento, de conformidad con el régimen disciplinario vigente en la CCSS."

La Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; indicó: "... en cuanto los equipos con el antivirus desactualizado, si es por ser equipos de apoyo que a veces pasan varios días sin ser usados. El equipo placa 959841, si debe tener algún problema, voy a revisarlo.". Asimismo, fue consultado el Ing. Guillermo Rojas Zapata, Jefatura del Centro de Gestión Informática de la Dirección Regional de Sucursales Huetar Norte; sobre la solicitud de aprobación de la herramienta "SPARK", sin embargo al momento de efectuado el presente informe no se había recibido respuesta.

Las vulnerabilidades en los equipos informáticos, como las señaladas en el presente hallazgo, podría comprometer su funcionamiento, rendimiento e integridad; así como propiciar ambientes poco seguros para el almacenamiento y trasiego de información institucional y de los usuarios de los servicios brindados por esa sucursal financiera.

6. Administración de cuentas de usuario configuradas para acceder a los sistemas de información y Directorio Activo Institucional¹

Se evidenciaron oportunidades de mejora respecto a la administración de cuentas para funcionarios de la Sucursal de Alajuela en los sistemas de información habilitados y el directorio activo institucional, a saber:

- 3 de los funcionarios a quienes les han habilitado cuentas en los sistemas institucionales SIGI, SICO, SICERE y/o RCPI no fueron incluidos dentro de la planilla de la primera y segunda catorcena de mayo 2015 para la unidad 1302 Sucursal de Alajuela (ver Anexo 2 y Cuadro 2).
- 2 cuentas de usuario configuradas en el directorio activo institucional, vinculadas a la Sucursal de Alajuela, no corresponden a funcionarios incluidos dentro de la planilla de la primera y segunda catorcena de mayo 2015 para la unidad 1302 Sucursal de Alajuela, a saber:
 - o Dylana Álvarez Jiménez.
 - o Sofía Solís Solís.

Cuadro 2: Unidad ejecutora con la que aparecen vinculados los funcionarios con cuentas de usuario para los sistemas SIGI, SICO, SICERE y/o RCPI que no fueron incluidos dentro de la planilla de la primera y segunda catorcena de mayo 2015 para la unidad 1302 Sucursal de Alajuela.

¹ En las Políticas de Seguridad Informática institucionales se define al Directorio Activo como: "...un servicio de red utilizado por Microsoft Windows que almacena información acerca de los recursos existentes en la red y controla el acceso de los usuarios y las aplicaciones a dichos recursos. De esta forma, se convierte en un medio de organizar, administrar y controlar centralizadamente el acceso a los recursos de la red."



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

Identificación	Nombre y Apellidos	Unidad(es) Ejecutora(s)
109950411	ARRIETA JIMENEZ MARIELA VANESSA	1301
503150401	AMADOR ARAUZ ELMER	1301 1313
601680978	PASOS GUIDO WILLIAM	1301

Fuente: Base de datos del Portal de Recursos Humanos e información proporcionada por la Ing. Hidalgo Arguedas.

Las Normas Técnicas de Gestión de las TIC (CGR, 2007) establecen en su apartado 1.4 *Gestión de la Seguridad de la Información*, lo siguiente:

“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.” (El subrayado no corresponde con el original).



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

Las inconsistencias supra citadas en torno a las cuentas para el acceso a sistemas de información habilitados en la Sucursal, así como vinculadas al directorio activo institucional; obedecen a debilidades en el control ejercido por la Administración para su gestión, dado que no son informadas apropiada y oportunamente las actualizaciones pertinentes a los responsables de su aplicación en las herramientas correspondientes.

La Ing. Carmen Anay Hidalgo Arguedas, encargada de informática en la Sucursal de Alajuela; vía correo electrónico y mensajería instantánea (Lync) del 16 de junio de 2015, proporcionó el listado de funcionarios con cuentas creadas para acceso a sistemas de información en la Sucursal de Alajuela, que no laboran para ese establecimiento.

La existencia de cuentas habilitadas a funcionarios que no laboran en la Sucursal de Alajuela compromete la adecuada y pertinente asignación de permisos, situación que podría generar eventuales vulnerabilidades en el esquema de seguridad institucional por un uso impropio de los mismos.

CONCLUSIÓN

Las tecnologías de información y comunicaciones representan para el mundo moderno una herramienta de cambio, la cual ha permitido mejorar la prestación de servicios a través de técnicas automatizadas que permiten la minimización del error humano. Por ello, su adecuada administración e implementación son fundamentales a fin de brindar un valor agregado a los procesos institucionales.

Considerando lo anterior, a través del presente estudio se evidenciaron oportunidades de mejora en la administración de las TIC de esa Sucursal, como son: la documentación de procedimientos inherentes a la función informática, la implementación de controles para garantizar una seguridad física y lógica (información) suficiente, el registro y control de los activos en TIC otorgados a ese establecimiento, entre otros elementos de relevancia dentro de la disciplina informática.

Por lo tanto, este órgano fiscalizador ha generado las siguientes recomendaciones en aras de abordar y subsanar los aspectos evidenciados en el presente informe.

RECOMENDACIONES

A LA SUCURSAL DE ALAJUELA

1. Implemente mecanismos de control a través de los cuales se documenten los diferentes cambios en versiones efectuados a los documentos técnicos utilizados por la encargada de brindar servicios en tecnologías de información y comunicaciones, considerando además lo señalado en el Hallazgo 1 del presente informe.

Plazo establecido para su cumplimiento: 3 meses.



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

2. Defina, divulgue e implemente un mecanismo de control a través del cual se estandarice el reporte y documentación de las incidencias reportadas en torno a problemas y/o averías en los equipos de tecnologías de información y comunicaciones disponibles en esa sucursal.

Plazo establecido para su cumplimiento: 3 meses.

3. Elabore, documente e implemente, en conjunto con la Dirección Regional de Sucursales Huetar Norte, una estrategia que permita atender las necesidades de infraestructura y equipamiento señaladas en el hallazgo 3 del presente informe, mismas que garanticen la integridad física de los equipos informáticos custodiados en el cuarto de servidores en el corto o mediano plazo.

Plazo establecido para su cumplimiento: 6 meses.

4. Realice las gestiones pertinentes para que la Dirección de Tecnologías de Información y Comunicaciones valore la inclusión del software de mensajería instantánea "SPARK" dentro de la lista oficial de software libre o gratuito autorizado en la CCSS; o bien que dicha instancia en cumplimiento de sus funciones de asesoría establecidas en su Manual de Organización le indique a la Sucursal la herramienta institucional que puede emplear para suplir esa necesidad tecnológica particular.

Plazo establecido para su cumplimiento: 6 meses.

5. Realizar una revisión y depuración de los registros almacenados en el inventario de equipo de cómputo para esa Sucursal, con el propósito de garantizar que los mismos se ajustan a la realidad actual del establecimiento, en lo que respecta al control de los activos institucionales.

Una vez realizado lo anterior, y en coordinación con los funcionarios responsables del control de activos, se deberá efectuar una revisión a fin de determinar las causas que han generado las diferencias de inventarios señaladas por esta Auditoría en el hallazgo 4 del presente informe, mismas que deberán ser subsanadas.

Plazo establecido para su cumplimiento: 3 meses.

6. Implemente las acciones necesarias para subsanar las debilidades señaladas en el Hallazgo 5 del presente informe en cuanto a la administración de las cuentas para funcionarios de esa Sucursal tanto en el Directorio Activo como para acceder los sistemas de información institucionales habilitados para ese establecimiento. De ser necesario, gestione con la Dirección de Tecnologías de Información y Comunicaciones la realización de los ajustes pertinentes a esos registros.

Plazo establecido para su cumplimiento: 1 mes.



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente estudio fueron comentados el 16 de julio de 2015, reunión a la cual asistieron: MSc. Luis Diego Zamora Benavides, Jefatura de la Sucursal de Alajuela; Ing. Carmen Anay Hidalgo Arguedas, encargada de informática de la Sucursal de Alajuela; y el Ing. Bryan Barquero Fallas, asistente de Auditoría.

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Lic. Rafael Ángel Herrera Mora
JEFE

Ing. Bryan Barquero Fallas
ASISTENTE DE AUDITORÍA

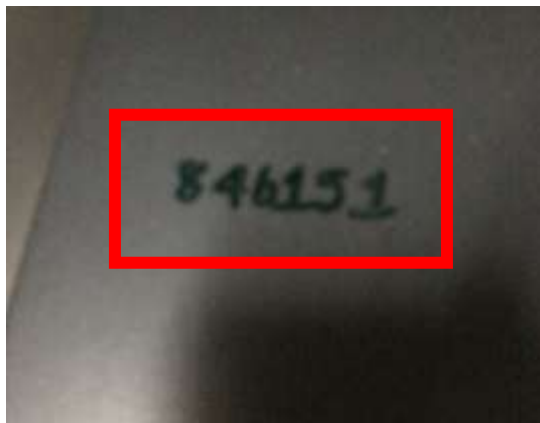
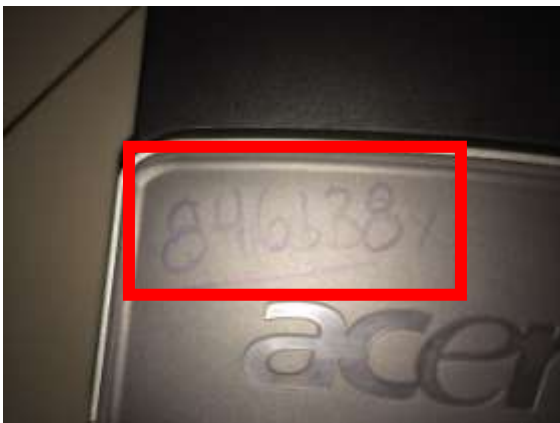
RAHM/BABF/lba



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

ANEXO 1

Equipos sin placa encontrados durante la inspección física efectuada el 02 de junio de 2015 en la Sucursal de Alajuela.



Fuente: Fotografías tomadas durante la inspección física efectuada el 02 de junio de 2015 en la Sucursal de Alajuela U.E. 1302.



CAJA COSTARRICENSE DE SEGURO SOCIAL
 AUDITORIA INTERNA
 Tel.: 2539-0821 - Fax.: 2539-0888
 Apdo.: 10105

ANEXO 2

Funcionarios con cuentas de usuario en los sistemas institucionales SIGI, SICO, SICERE y/o RCPI que no fueron incluidos dentro de la planilla de la primera y segunda catorcena de mayo 2015 para la unidad 1302 Sucursal de Alajuela

Aplicación	Cedula	Nombre y Apellidos			Usuario	Estado	Código de Perfil	Descripción de Perfil	Fecha Caducidad Clave
SICERE	109950411	VANESSA	ARRIETA	JIMENEZ	VARRIETA	ACTIVO	COB_OPE_CO	OPERADOR ADMINISTRATIVO COBRO	25-ago-15
SICERE	109950411	VANESSA	ARRIETA	JIMENEZ	VARRIETA	ACTIVO	GES_CO_AD	GESTOR DE ADMINISTRATIVO COBRO	25-ago-15
SICERE	109950411	VANESSA	ARRIETA	JIMENEZ	VARRIETA	ACTIVO	GE_COB_SUC	GESTOR DE COBROS SUCURSALES	25-ago-15
SICERE	109950411	VANESSA	ARRIETA	JIMENEZ	VARRIETA	ACTIVO	OPE_FACT	OPERADOR DE FACTURACION	25-ago-15
SICERE	109950411	VANESSA	ARRIETA	JIMENEZ	VARRIETA	ACTIVO	OP_COB_SUC	OPERADOR DE COBROS SUCURSALES	25-ago-15
SICERE	503150401	ELMER	AMADOR	ARAUZ	EAMADOR-SICE	ACTIVO	INS_SIC	INSPECTOR LEYES Y REGLAMENTOS CCSS - SICERE	16-ago-15
SICERE	503150401	ELMER	AMADOR	ARAUZ	EAMADOR-SICE	ACTIVO	OPE_CTA_PR	USUARIO OPERADOR CUENTA PROPIA	16-ago-15
SICERE	601680978	WILLIAM GERARDO	PASOS	GUIDO	WPASOSG01	ACTIVO	ADM_GRAL_U	ADMINISTRADOR GENERAL DE USUARIOS	28-jun-15
SICERE	601680978	WILLIAM GERARDO	PASOS	GUIDO	WPASOSG01	ACTIVO	GES_SCR	GESTION DE INCIDENCIAS EN EL SICERE (MODIFICAR)	28-jun-15
SICERE	601680978	WILLIAM GERARDO	PASOS	GUIDO	WPASOSG01	ACTIVO	GES_SCR_CO	GESTIÓN DE INCIDENCIAS EN EL SICERE (CONSULTA)	28-jun-15
SICERE	601680978	WILLIAM GERARDO	PASOS	GUIDO	WPASOSG01	ACTIVO	GES_SCR_EL	GESTION DE INCIDENCIAS EN EL SICERE (ELIMINAR)	28-jun-15
SICERE	601680978	WILLIAM GERARDO	PASOS	GUIDO	WPASOSG01	ACTIVO	INS_APO_IN	APOYO A LA LABOR DE INSPECCION	28-jun-15
SICERE	601680978	WILLIAM GERARDO	PASOS	GUIDO	WPASOSG01	ACTIVO	INS_SIC	INSPECTOR LEYES Y REGLAMENTOS CCSS - SICERE	28-jun-15



CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

Aplicación	Cedula	Nombre y Apellidos		Usuario	Estado	Código de Perfil	Descripción de Perfil			Fecha Caducidad Clave
SICERE	601680978	WILLIAM GERARDO	PASOS GUIDO	WPASOSG01	ACTIVO	OPE_CTA_PR	USUARIO PROPIA	OPERADOR	CUENTA	28-jun-15

Fuente: Base de datos del Portal de Recursos Humanos y listado de usuarios remitido vía correo electrónico del 01 de junio de 2015 y conversación por Lync del 16 de junio de 2015, ambos con la Ing. Carmen Anay H