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

ATIC-218-2015
27-08-2015

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 Golfito.

En la presente evaluación se determinó oportunidades de mejora en la gestión de usuarios de los sistemas de información que se utilizan en la sucursal, asimismo, es importante indicar que estas herramientas tecnológicas son importantes para la Institución por el tipo de información que manejan, almacenan y las transacciones que se puede realizar, por ende la administración de usuarios debe poseer controles exhaustivos que brinden seguridad razonable evitando una inadecuada utilización de la información.

En relación con la administración de usuarios, es importante disponer de mecanismos de control de acceso eficientes y oportunos, los cuales deben ser complementados con la asignación a funcionarios competentes y con perfiles relacionados con la función, ya que este es el único mecanismo que permite asegurar que las transacciones realizadas en la aplicación son reales e integras.

De igual forma se comprobó que el rack donde se encuentran los servidores y equipos de telecomunicaciones se ubica en un espacio físico que no dispone de las condiciones ambientales y de seguridad física establecidas en la normativa aplicable para su debida operación.

Así mismo, contar con inventarios confiables y actualizados certifica no solo la adecuada administración del patrimonio público, sino además proporciona información necesaria para las etapas de planificación de las adquisiciones, siempre con el objetivo de garantizar la prestación del servicio de forma eficiente, eficaz y oportuna. Sin embargo, inconsistencias en el mismo comprometen los servicios financieros brindados a los usuarios internos y externos del Centro.

Un análisis del riesgo, donde se indiquen el impacto y los puntos críticos, además de la documentación de los procesos asociados a Tecnologías de Información y Comunicaciones, permite la elaboración de un plan de continuidad que garantice la operación de los servicios aun cuando se presenten interrupciones mayores. Este Plan de Continuidad debe adaptarse a la realidad de la sucursal, actualizarse de forma periódica y comunicarse a los funcionarios que utilizan los servicios involucrados. Su desatención pone en peligro el funcionamiento de los equipos y la integridad, disponibilidad y confidencialidad de la información.

Por último, es importante la realización de pruebas o simulacros que permitan comprobar la efectividad del plan de continuidad ante un suceso que pueda interrumpir la continuidad de los servicios tecnológicos.

San José, Costa Rica. Ave. 2da, calles 5 y 7. Teléfono 2539-0821, Fax 2539-0888

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

ATIC-218-2015
27-08-2015

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN INTEGRAL GERENCIAL DE LA SUCURSAL DE GOLFITO
TEMA: TECNOLOGIAS DE INFORMACION Y COMUNICACIONES
UNIDAD PROGRAMÁTICA: 1632

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 Golfito, considerando la disposición de recursos existentes y su control, la normativa, políticas y lineamientos aplicables y la relación de sus actividades con los objetivos institucionales en esta materia.

OBJETIVOS ESPECÍFICOS

- Determinar aspectos relevantes de la plataforma tecnológica (hardware, software y telecomunicaciones) y gestión de recursos financieros respecto a Tecnologías de Información y Comunicaciones de la Sucursal de Golfito, de manera que respondan a las necesidades actuales de dicha sucursal y se ajustan a las políticas institucionales.

- Evaluar la suficiencia y oportunidad de la gestión y planificación en Tecnologías de la Información y Comunicaciones de la Sucursal de Golfito, en aspectos como gestión de actividades, administración de riesgos, respaldo de la información, mantenimiento y reparación de equipos.

- Verificar que la asignación de los usuarios y perfiles a los funcionarios de la Sucursal de Golfito se encuentren acordes a las labores desempeñadas por estos.

ALCANCE

El estudio comprende el análisis de la gestión de las tecnologías de información y comunicaciones en la Sucursal de Golfito, El período de la evaluación corresponde de enero 2014 a junio 2015, ampliándose en aquellos aspectos que se consideró necesario.

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

METODOLOGÍA

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

- Estudio de la plataforma tecnológica existente en la sucursal (equipo de cómputo y comunicaciones, respaldos, licencias, entre otros).
- Análisis de la documentación emitida respecto al cumplimiento de las normas técnicas y políticas institucionales en materia de tecnologías de información y comunicaciones.
- Aplicación de entrevistas a la Licda. Isabel Garbanzo León, Administradora de la sucursal, concerniente a Información General, Gestión y Operatividad de los Servicios Continuos en TIC, Seguridad y Adquisición de Bienes y Servicios.
- Inspección física de las instalaciones que comprenden la sucursal.
- Inspección física mediante muestreo de los inventarios de activos de la sucursal.

MARCO NORMATIVO

- Ley General de Control Interno 8292, julio 2002.
- Normas de Control Interno para el sector público, febrero 2009.
- Modelo de organización de los Centros de Gestión Informática, enero 2013.
- Normas Técnicas para la gestión y el control de las Tecnologías de Información, junio 2007.
- Políticas Institucionales de Seguridad Informática, octubre 2007.
- Políticas Institucionales de Seguridad Informática, abril 2008.
- Manual de Normas y Procedimientos para la Administración y Control de Bienes Muebles, octubre 2002.

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

ASPECTOS NORMATIVOS A CONSIDERAR

Esta Auditoria, 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:

> *"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. (…)"*

ASPECTOS GENERALES

Descripción del Modelo de Organización de los Centros de Gestión Informática

La Caja Costarricense de Seguro Social (CCSS), estableció un Modelo de Organización para sus Centros de Gestión Informática, con el fin de ordenar el crecimiento de los sistemas de información institucional.

El 29 de agosto del 2013, la Junta Directiva, mediante artículo 32º de la sesión Nº 8658 aprobó la actualización de dicho documento. La Figura Nº 1 refiere el esquema de coordinación establecido según el tipo de Centro y su ámbito de competencia, según el Modelo Tipo A (Centros de Gestión Informática Gerenciales) o Tipo B (Centros de Gestión Informática Regionales y Locales).

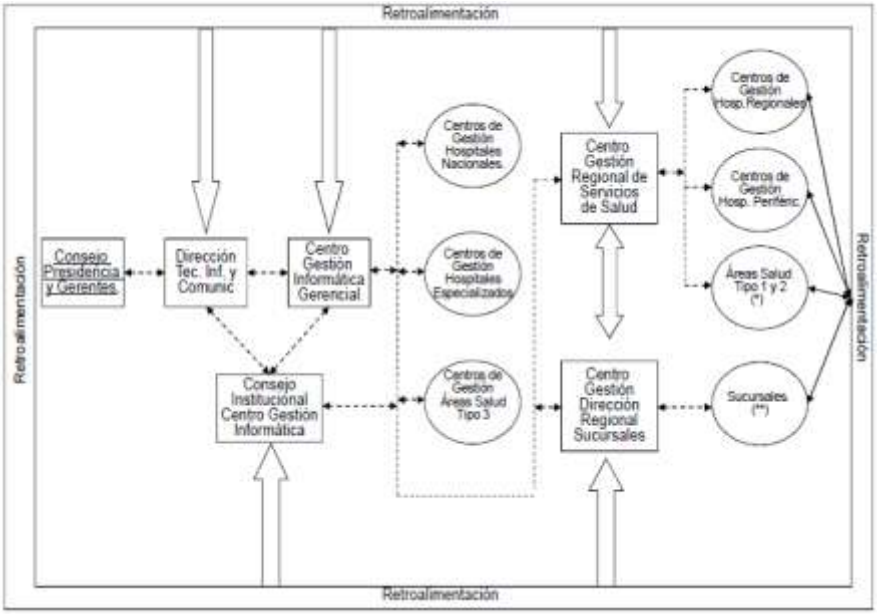


Figura 1. Esquema de Coordinación Centros de Gestión Informática
Fuente: Modelo de Organización Centros de Gestión Informática.

Este modelo permite a los niveles locales de los CGI empoderarse, pero asumiendo la responsabilidad por los proyectos que desarrolle.

Se pretende que los CGI administren en forma autónoma el establecimiento de compras de programas y equipos de cómputo y desarrollen sistemas de información, de acuerdo con las necesidades particulares de cada área, pero siguiendo los lineamientos institucionales y en un marco de un uso eficiente de los recursos institucionales.

El Modelo de Organización de los Centros de Gestión Informática señala que estos Centros deben:

- Analizar y planificar las necesidades de automatización de sistemas y los requerimientos del hardware y software, administrar proyectos operativos específicos, realizar los estudios preliminares, de factibilidad, diseñar aplicaciones específicas y evaluar la gestión informática en su ámbito de acción.
- Su desarrollo implica la amplia participación del nivel usuario, como estrategia fundamental para cumplir con las expectativas y satisfacer las necesidades reales de los establecimientos de salud.
- Desarrolla e implementa sistemas de información y aplicaciones locales, con el fin de automatizar procesos operativos específicos, es responsable del mantenimiento preventivo y correctivo del hardware, del software interno y define acciones que permitan mejorar la gestión en beneficio de los usuarios.

- Otorga la capacitación y la asesoría para solución de problemas operativos, que se presentan a los usuarios finales en la utilización de tecnología de información.
- Coordina acciones con el Centro de Gestión Informática de nivel gerencial respectivo, el Consejo Institucional de Centros de Gestión Informática y cuando se considere necesario con la Dirección de Tecnologías de Información y Comunicaciones (DTIC).

HALLAZGOS

1. **REFERENTE A LA GESTIÓN DE USUARIOS DE LOS SISTEMAS DE INFORMACIÓN EN LA SUCURSAL.**

Esta Auditoría evidenció la existencia de usuarios activos en los sistemas de información que se utilizan en la sucursal, los cuales presentan los siguientes casos:

a. Usuarios activos cuya fecha de vencimiento de la clave ya expiro.

Se identificaron seis usuarios activos de diferentes sistemas de información, cuya fecha de vencimiento de la clave ya expiro, tal y como se muestra a continuación:

Cuadro 1. Usuarios cuya fecha de vencimiento ya expiro

Nombre	Login	Sistema	Perfiles asignados	Fecha Caducidad Clave	Puesto que desempeña actualmente
ISABEL GARBANZO LEON	IGARBANZO	SICERE	ADMINISTRADOR DE SUCURSAL	14/06/2015	Administrador de Sucursal 2
ROGER GUTIERREZ MONTIEL	RGUTIERREZ01	PEAS	INSPECTOR LEYES Y REGLAMENTOS C.C.S.S.	15/03/2012	Inspector de Leyes y Reglamentos 3
MARITZA CHAVES SERRANO	601190187	RCPI	COORDINADOR DE PAGO DIRECTO	14/11/2010	Asistente Técnico en Administración 4
MARITZA CHAVES SERRANO	MCHAVES-SCEI	Sistema Compras Exentas Impuesto	DIGITADOR COMPRAS EXENTAS DE IMPUESTO	04/12/2009	Asistente Técnico en Administración 4
MARIBEL GARCIA JIMENEZ	MGARCIA-SCEI	Sistema Compras Exentas Impuesto	DIGITADOR COMPRAS EXENTAS DE IMPUESTO	04/12/2009	Asistente Administrativo de Agencia
KENIA VILLAGRA QUIROS	603360281	RCPI	ENCARGADO DE REALIZAR PAGOS	23/04/2011	Cajero 1
			AFILIACION TRABAJADORES (OV)		
YENDRY CALVO VENEGAS	SIGI_YPCALVO	SIGI	PLATAFORMISTA SIGI	06/04/2015	Asistente Técnico en Administración 4

Fuente: Sistema Centralizado de Recaudación (SICERE), fecha de la consulta 23 de junio del 2015.

Actualmente la fecha de expiración funciona como un mecanismo de seguridad implementado en los sistemas de información y su propósito consiste en bloquear al usuario una vez alcanzada dicha fecha, posteriormente los encargados del sistema en la sucursal deberían analizar la conveniencia de mantener el usuario activo, o bien, proceder con la respectiva inactivación.

b. Usuarios activos que pertenecen a personas que no laboran en la sucursal.

Se evidenciaron 12 usuarios activos pertenecientes a personas que actualmente no laboran para la Sucursal de Golfito, tal y como se muestra en el siguiente cuadro:

Cuadro 2. Usuarios que pertenecen a personas que no laboran en la sucursal

Nombre	Login	Sistema	Perfiles asignados
YENDRY ESQUIVEL GONZALEZ	SIGI_YESQUIVEL	SIGI	INSPECTOR PRECIN
MARIA EDITH SALAS CASTILLO	603380233	RCPI	ENCARGADO DE REALIZAR PAGOS
			AFILIACION TRABAJADORES (OV)
MARIA EDITH SALAS CASTILLO	MESALAS-SICE	SICERE	SUPERVISOR DE FACTURACION
			OPERADOR DE FACTURACION
			USUARIO OPERADOR CUENTA PROPIA
MARIA JOSE REYES NIETO	603420937	RCPI	USUARIO DE CONSULTA
MERYHELLEN MAYELA MONTERO RIVAS	603640782	RCPI	COORDINADOR DE PAGO DIRECTO
			ENCARGADO DE REGISTRAR Y TRAMITAR COMPROBANTES
			ENCARGADO DE REALIZAR PAGOS
MERYHELLEN MAYELA MONTERO RIVAS	MMONTEROR-SICE	SICERE	USUARIO OPERADOR CUENTA PROPIA
			OPERADOR DE FACTURACION
MERYHELLEN MAYELA MONTERO RIVAS	MMONTEROR-SICO	SICO	PERFIL PARA CONSULTA DE COMPROBANTES EN SICO
CARLOS ALBERTO GUTIERREZ MONTIEL	CGUTIERRM-SICE	SICERE	APOYO A LA LABOR DE INSPECCION
			USUARIO OPERADOR CUENTA PROPIA
			OPERADOR DE FACTURACION
CARLOS ALBERTO GUTIERREZ MONTIEL	CGUTIERRM-SICO	SICO	PERFIL PARA CONSULTA DE COMPROBANTES EN SICO
			PLATAFORMISTA SISTEMA INTEGRADO DE COMPROBANTES
CARLOS ALBERTO GUTIERREZ MONTIEL	SIGI_CGUTIERRM	SIGI	APOYO A INSPECCION
			PLATAFORMISTA SIGI
STEFANY DE LOS ANGELES RUIZ GOMEZ	SRUIZG-SICE	SICERE	OPERADOR DE FACTURACION
			USUARIO OPERADOR CUENTA PROPIA
STEFANY DE LOS ANGELES RUIZ GOMEZ	SRUIZG-SICO	SICO	PLATAFORMISTA SISTEMA INTEGRADO DE COMPROBANTES
			PERFIL PARA CONSULTA DE COMPROBANTES EN SICO

Fuente: Sistema Centralizado de Recaudación (SICERE), fecha de la consulta 23 de junio del 2015.

Las Normas Técnicas para la Gestión y el Control de Tecnologías de Información de la Contraloría General de la República, en el apartado 1.4.5 Control de Acceso, se indica:

> *"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."*

Referente a la gestión realizada para la inactivación de los usuarios y las razones por las cuales estos usuarios todavía se encuentran activos, la Licda. Isabel Garbanzo León, Administradora de la Sucursal de Golfito, mencionó lo siguiente:

> *"Recuerdo que a principios del año pasado (2014) el CGI de la Dirección Regional había remitido un listado con usuarios que se encontraban activos en ese momento, cuyo propósito consistía en revisar la conveniencia de mantenerlos activos o proceder con su inactivación, sin embargo, es importante indicar que en ese entonces yo no era la administradora de la sucursal, por tanto desconozco las acciones que realizó el administrador de ese momento.*
>
> *Así mismo, estos usuarios pertenecen a personas que no estaban laborando cuando ingrese a esta sucursal como administradora (ingrese en diciembre del 2014). No obstante, con el paso del tiempo se ha ido depurando esta lista de usuarios.*
>
> *Vamos a realizar una revisión de usuarios, para proceder a inactivar aquellos que sean necesarios, para esto ya hay un procedimiento de inactivación de usuarios, el cual se ejecuta en coordinación con el Centro de Gestión Informática de la Dirección Regional."*

El hecho de que existan usuarios activos pertenecientes a personas que no laboran en la sucursal podría generar una brecha en la seguridad lógica del sistema informático, lo anterior debido a que los usuarios lograrían ingresar a un módulo en los cuales puedan realizar modificaciones, eliminaciones o utilización de datos no autorizados, situación que podría ser aprovechada por alguna persona para obtener beneficios de las irregularidades antes señaladas.

2. SOBRE LA UBICACIÓN DE LOS SERVIDORES Y EQUIPOS DE COMUNICACIÓN.

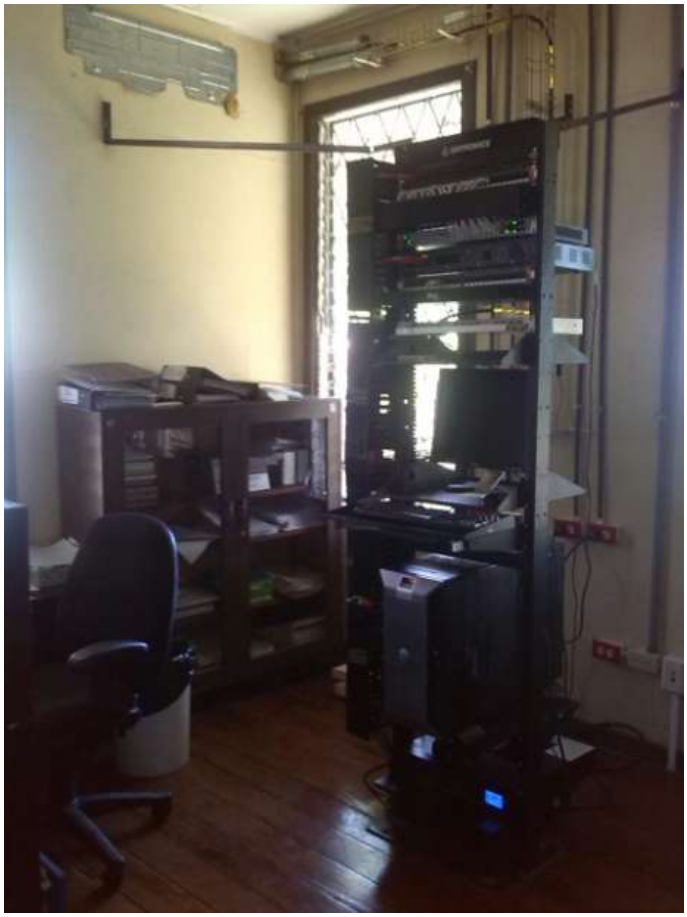
Esta Auditoría comprobó que el rack donde se encuentran los servidores y equipos de telecomunicaciones que brindan soporte tecnológico a la sucursal, se ubica en un espacio físico que no dispone de las condiciones ambientales y de seguridad física establecidas en la normativa aplicable para su debida operación, entre ellos:

- Controles de acceso (Puertas, bitácoras de ingreso, entre otros)
- Controles de humedad y temperatura.
- Detectores de humo.
- Extintores.
- Aire acondicionado dedicado.

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

A continuación, se presenta una imagen que muestra la situación mencionada anteriormente:

Imagen No. 1
Fotografías capturadas de los servidores y equipos de comunicaciones.
Sucursal de Golfito.



Fuente: Elaboración propia con base en inspección física a las instalaciones de la Sucursal de Golfito, Junio 2015.

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, establecen en su artículo 1.4.3 que:

> *"La organización debe proteger los recursos de TI estableciendo un ambiente físico seguro y controlado con medidas de protección suficientemente fundamentadas en políticas vigentes y análisis de riesgos.*
>
> *Como parte de esa protección debe considerar:*

a. Los controles de acceso a las instalaciones: seguridad perimetral, mecanismos de control de acceso a recintos o áreas de trabajo, protección de oficinas, separación adecuada de áreas.
b. La ubicación física segura de los recursos de TI.
c. El ingreso y salida de equipos de la organización. (…)
g. El acceso de terceros. (…)
h. Los riesgos asociados con el ambiente."

Asimismo, el artículo 1.4.6 de dichas normas, establece:

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

Las Políticas Institucionales de Seguridad Informática TIC-Seguridad-001, en su artículo 10.11 PSI-UAR-011 "Política para la Administración del Espacio físico en los Centros de Cómputo" establece que:

"Los equipos en los cuales se almacenan y procesan datos críticos que colaboran con el cumplimiento de los servicios informáticos, debe estar ubicados en un espacio especial que cumpla con condiciones básicas de seguridad para la protección de los datos que contienen y del equipo en sí. Dichas condiciones entre otras son: protección contra humedad y/o polvo, espacio solo accesible por los administradores, uso de cables de corriente alterna debidamente aterrizados, uso de aire acondicionado."

La Licda. Isabela Garbanzo León, Administradora de la Sucursal de Golfito, indico lo siguiente:

"El problema principal de la ubicación del servidor se encuentra en la infraestructura de la sucursal (actualmente se encuentra muy obsoleta).

En el 2014, diseñe un proyecto de remodelación, en el cual se le informaba a los niveles superiores sobre el estado actual de la sucursal y todas sus debilidades (en ellas se incluyo el aspecto de la ubicación de los servidores, los cuales no disponen de una ubicación apropiada).

No obstante, a través de una visita realizada por los ingenieros de la Dirección Regional indicaron que no era factible realizar la remodelación de la sucursal, y más bien recomendaron la construcción de una nueva sucursal.

Actualmente, estamos trabajando en otro proyecto en paralelo que consiste en el alquiler de un edificio para instalar la sucursal.

De igual forma, se han gestionado otros proyectos para tratar de mitigar el impacto de estos riesgos, tal es el caso de la compra de aires acondicionados, el año pasado no hubo el presupuesto suficiente para realizar dicha compra, razón por la cual volvimos a incluir la solicitud para este año y esperamos que se pueda llevar a cabo."

La ausencia de un espacio físico dedicado para el resguardo de los servidores y el rack de comunicaciones podría ocasionar la interrupción en la prestación de los servicios que brinda la Sucursal, debido al deterioro de los equipos tecnológicos, hurtos, robos, fraudes, sabotaje y otros factores ambientales artificiales asociados, situación que impactaría negativamente las finanzas institucionales.

3. REFERENTE A LA GESTIÓN DE ACTIVOS RELACIONADOS CON TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Esta Auditoría evidenció debilidades en la gestión de activos relacionados con tecnologías de información y comunicaciones, las cuales se detallan a continuación:

a. Activos que han sido dados de baja

Se evidenció que ocho activos no se ubicaron físicamente en la Sucursal de Golfito, tal y como se muestra a continuación:

N° Placa	Descripción	Ubicación según SCBM	Estado actual según SCBM
756327	Impresora matriz para computo	Bodega n°1	En Uso
842978	Monitor plano 17" lcd para microcomputadora	Cubículo de cajas Puerto Jimenez	En Uso
756493	Monitor plano para microcomputador ldc 17"	Departamento cobros Golfito	En Uso
756356	Monitor plano para computo	Oficina egresos Golfito	En Uso
773599	Impresora matriz carro angosto	Oficina fondo rotatorio Golfito	En Uso
773594	Impresora láser para microcomputadora	Ingresos-egresos Golfito	En Uso
747632	Fotocopiadora trabajo normal	Oficina fondo rotatorio Golfito	En Uso
756492	Microcomputador estación trabajo	Bodega n°2	En Uso

Fuente: Elaboración propia basada en la Inspección física realizada el 23 de junio del 2015.

Según lo indicado por la Administración, la razón por la cual no se pudieron ubicar estos activos se debe a que ya han sido dados de baja (mediante revisión efectuada por esta Auditoría se corroboro que estos activos disponen de la recomendación de baja del activo), sin embargo, en el Sistema Contable de Bienes y Muebles (SCBM) se indica que el activo todavía se encuentra en uso.

b. Activos con diferentes ubicaciones.

Se evidenció que cuatro activos presentan diferencias en la ubicación con respecto a lo indicado por le SCBM, tal y como se muestra a continuación:

Cuadro 3. Activos con diferente ubicación

N° Placa	Descripción	Ubicación Física	Ubicación según SCBM
756344	Microcomputadora	Ingresos y Egresos	Inspección
756343	Microcomputadora	Ingresos y Egresos Puerto Jiménez	Jefatura
666073	Microcomputadora	Ingresos y Egresos	Asistente de Sucursal
756494	Microcomputadora	Jefatura	Ingresos y Egresos

Fuente: Elaboración propia basada en la Inspección física realizada el 23 de junio del 2015.

Como se observa en el cuadro anterior, se evidencian diferencias en la ubicación de los activos, con respecto a lo indicado por el Sistema Contable de Bienes y Muebles y la inspección física realizada por esta Auditoría.

El Manual de Normas y Procedimientos para la administración y control de Bienes Muebles en su artículo 49 indica:

> *"Todo Jefe de Unidad de Trabajo responderá ante la CAJA por el faltante detectado en su inventario.*
> *Los faltantes serán analizados por la jefatura superior, quien determinará si hubo responsabilidad del funcionario encargado de la custodia del bien. Si existiere responsabilidad de algún funcionario se procederá conforme lo establece el Instructivo que Regula Los Faltantes y Sobrantes de Inventario Físico de Activos, Artículos Varios, Dinero En Efectivo, Valores y Otros, así como lo establecido en el artículo N° 18 de la Normas que regulan Las Relaciones Laborales de la Caja y las Normas y Políticas Institucionales en materia de sanciones disciplinarias."*

En el punto 7.3. Normas para la política uso adecuado de estaciones de trabajo cita:

> *"Cada Centro de Gestión Informática, en coordinación con el respectivo encargado de activos, deberá contar con un inventario actualizado de las estaciones de trabajo, correspondiente a todas las estaciones de trabajo adscritas al Centro de Gestión Informática"*

Al respecto, la Licda. Isabela Garbanzo León, Administradora de la Sucursal de Golfito, mencionó lo siguiente:

> *"En el caso de la ubicación de los equipos, se debe a que en ocasiones se daña algún componente del equipo de cómputo y necesitamos reemplazarlo, la solución más viable para este tipo de casos consiste en utilizar algún otro equipo que se encuentra en otra oficina. Hay servicios prioritarios y no pueden esperar a que el encargado del CGI venga para revisarlo.*

Así mismo, es relevante indicar que la encargada de los activos es actualmente la cajera de la sucursal, por tanto, no se dedica a tiempo completo a la gestión de los activos. Asimismo, el recurso humano en la sucursal es muy limitado.

En cuanto a los activos que no se encuentran físicamente, la mayoría se deben a que son equipos que fueron desechados, sin embargo, la gestión para inactivarlos en el SCBM es muy lenta, de ahí surgen las diferencias.

Ejemplo de ello es el activo N° 756492 el cual ya fue desechado, inclusive funcionarios del CGI nos ayudaron con la destrucción del equipo.

Esta ha sido una ardua labor, ya que cuando recibí la sucursal, la bodega estaba llena de equipos de cómputo dañados, razón por la cual se empezaron todos los trámites para darlos de baja y posteriormente con su respectiva destrucción."

El no llevar a cabo una adecuada gestión de activos, además de una posible afectación al patrimonio institucional, podría causar una interrupción en la prestación de los servicios, o bien, comprometer la garantía de un adecuado uso del recurso público, además contraviene la normativa en materia de administración y control de bienes muebles.

4**. SOBRE EL PLAN DE CONTINUIDAD EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.**

Se constató que la Sucursal de Golfito dispone de un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicaciones, sin embargo, dicho documento no está aprobado por la Subárea de Continuidad de la Gestión en TIC. Asimismo, se evidenció que no se han realizado pruebas o simulacros que permitan comprobar la efectividad del plan ante un suceso que pueda interrumpir la continuidad de los servicios tecnológicos.

Las Políticas Institucionales de Seguridad Informática, en su artículo 10.14 PSI-UAR-014 Política para la elaboración de Planes de Continuidad de la gestión contempla que:

"Cada Unidad y Área de la CCSS, deberá elaborar los respectivos Planes de Continuidad de la Gestión Informática, según lo establece la guía, además velar por su correcta aplicación y realización de pruebas periódicas(…) deberá actualizar los Planes de Continuidad de la Gestión, mínimo cada año y cuando se den cambios tecnológicos que impliquen mejoras a los planes."

Dentro del Plan de Continuidad se debe de elaborar un análisis de riesgos y documentación de procesos, para lo cual la política institucional establece que para el 2012 se deben haber levantado y documentado todos los procesos sustantivos de las unidades, así como tener identificados los riesgos utilizando la metodología del SEVRI y además que se cuente con los planes de tratamiento de los riesgos (plan de acción y de contingencia para cada riesgo identificado).

El Manual de Normas de Control Interno para el Sector Público en el Capítulo 3.2, sobre sistema específico de valoración de riesgo institucional, establece que:

> *"(…) El jerarca y los titulares subordinados, según sus competencias, deben establecer y poner en funcionamiento un sistema especifico de valoración de riesgo institucional (SEVRI)*
>
> *El SEVRI debe presentar las características e incluir los componentes y las actividades que define la normativa específica aplicable. Asimismo debe someterse a las verificaciones y revisiones que correspondan a fin de corroborar su efectividad continua y promover su perfeccionamiento (…)"*

Referente a la razón por la cual no se ha actualizado el Plan de Continuidad, el Licda. Isabela Garbanzo León, Administradora de la Sucursal de Golfito, indicó lo siguiente:

> *"El plan de continuidad es un documento que se elabora en conjunto con el Centro de Gestión Informática de la Dirección Regional. Hace poco tiempo asistí a una capacitación para la elaboración de dicho documento, en ese momento aprovechamos para actualizar el mismo.*
>
> *En el caso de los ensayos, como lo indica la plantilla PTC010 del plan de continuidad, se encuentran programados para efectuarse en el mes de julio y agosto del 2015, dichos ensayos se realizaran en coordinación con el CGI."*

El no contar con un Plan de Continuidad actualizado para la gestión en Tecnologías de la Información provoca que la sucursal se encuentre vulnerable ante interrupciones mayores de sus actividades sustantivas, generando un desaprovechamiento de los recursos actuales, un desbalance entre las variables de costo, beneficio y riesgo y hasta la incapacidad de respuesta ante un riesgo materializado, desembocando en la interrupción parcial o total de los servicios prestados a los pacientes y funcionarios del Centro.

CONCLUSIONES

En la presente evaluación se determinó oportunidades de mejora en la gestión de usuarios de los sistemas de información que se utilizan en la sucursal, asimismo, es importante indicar que estas herramientas tecnológicas son importantes para la Institución por el tipo de información que manejan, almacenan y las transacciones que se puede realizar, por ende la administración de usuarios debe poseer controles exhaustivos que brinden seguridad razonable evitando una inadecuada utilización de la información.

En relación con la administración de usuarios, es importante disponer de mecanismos de control de acceso eficientes y oportunos, los cuales deben ser complementados con la asignación a funcionarios competentes y con perfiles relacionados con la función, ya que este es el único mecanismo que permite asegurar que las transacciones realizadas en la aplicación son reales e integras.

De igual forma se comprobó que el rack donde se encuentran los servidores y equipos de telecomunicaciones se ubica en un espacio físico que no dispone de las condiciones ambientales y de seguridad física establecidas en la normativa aplicable para su debida operación.

Así mismo, contar con inventarios confiables y actualizados certifica no solo la adecuada administración del patrimonio público, sino además proporciona información necesaria para las etapas de planificación de las adquisiciones, siempre con el objetivo de garantizar la prestación del servicio de forma eficiente, eficaz y oportuna. Sin embargo, inconsistencias en el mismo comprometen los servicios financieros brindados a los usuarios internos y externos del Centro.

Un análisis del riesgo, donde se indiquen el impacto y los puntos críticos, además de la documentación de los procesos asociados a Tecnologías de Información y Comunicaciones, permite la elaboración de un plan de continuidad que garantice la operación de los servicios aun cuando se presenten interrupciones mayores. Este Plan de Continuidad debe adaptarse a la realidad de la sucursal, actualizarse de forma periódica y comunicarse a los funcionarios que utilizan los servicios involucrados. Su desatención pone en peligro el funcionamiento de los equipos y la integridad, disponibilidad y confidencialidad de la información.

Adicionalmente, es importante la realización de pruebas o simulacros que permitan comprobar la efectividad del plan de continuidad ante un suceso que pueda interrumpir la continuidad de los servicios tecnológicos.

RECOMENDACIONES

A LA ADMINISTRACIÓN DE LA SUCURSAL DE GOLFITO

1. De acuerdo con la factibilidad económica y operativa de la Sucursal de Golfito, valorar la posibilidad de brindarle al rack de servidores y telecomunicaciones un área física exclusiva que disponga de las condiciones ambientales y de seguridad requeridas para su debida operación de acuerdo con lo establecido en la normativa institucional relacionada con el tema de seguridad informática. **Plazo de cumplimiento: 5 meses.**

2. Realizar una revisión de los usuarios y privilegios asignados a los funcionarios de la Sucursal de Golfito, con el fin de identificar la conveniencia de mantener los usuarios con sus privilegios, o en su defecto, informar a la dependencia encargada del sistema de información para que procedan con la inactivación de los mismos. De igual manera, se le deberá solicitar a esa dependencia la eliminación de los privilegios.

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

Se debe dejar evidencia documental de la revisión realizada y las acciones tomadas. Además, esta revisión se ejecutara con la periodicidad que esta administración considere prudente.

Plazo de cumplimiento: 3 meses.

3. En coordinación con el encargado de activos, ejecutar las acciones correspondientes con el propósito de solventar las debilidades mencionadas en el hallazgo 3 del presente informe. De igual forma, se debe realizar las modificaciones correspondientes en el Sistema Contable de Bienes y Muebles, en el cual se deben registrar los activos que han sido desechadas, incluir la ubicación y responsables de la custodia, entre otros. **Realizar en un plazo de tres meses.**

AL CENTRO DE GESTIÓN INFORMÁTICA DE LA DIRECCIÓN REGIONAL DE SUCURSALES BRUNCA

4. En coordinación con la Administración de la Sucursal de Golfito, actualizar el Plan de Continuidad de las operaciones en el Centro de Gestión Informática acorde con las necesidades reales del mismo, el cual cumpla con lo establecido en el Manual para Elaborar un Plan de Continuidad de la Gestión en Tecnologías de Información y Comunicación. Previo a su revisión y aprobación por la Sub-Área de Continuidad de la Gestión de TIC, realizar y documentar las pruebas de viabilidad del mismo. **Se establece un plazo de 3 meses para su cumplimiento.**

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 13 de agosto del 2015, con la Licda. Isabel Garbanzo León, Administradora de la Sucursal de Golfito; asimismo, se comentó el 20 de agosto del 2015 con el Ing. Roberto Fonseca Padilla, funcionario del Centro de Gestión Informática de la Dirección Regional de Sucursales Brunca.

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

Firmado digitalmente por RANDALL ARAYA LUNA (FIRMA)
Fecha: 2015.09.16 17:05:32 -06'00'

Lic. Randall Araya Luna
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Digitally signed by RAFAEL ANGEL HERRERA MORA (FIRMA)
DN: serialNumber=CPF-01-1216-0002, sn=HERRERA MORA, givenName=RAFAEL ANGEL, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=RAFAEL ANGEL HERRERA MORA (FIRMA)
Date: 2015.09.17 11:11:45 -06'00'

Lic. Rafael Herrera Mora
JEFE

Firmado digitalmente por: MUHAMMAD CARLOS HERRERA BERMUDEZ (FIRMA)
Motivo: ASISTENTE DE AUDITORIA COSEM
Localización: Costa Rica
Fecha y hora: 16.09.2015 15:34:36

Lic. Muhammad Herrera Bermúdez
ASISTENTE DE AUDITORÍA

OSC/RAL/MHB/lba