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

ATIC-274-2015
02-10-2015

RESUMEN EJECUTIVO

El presente estudio se realizó según el programa de Actividades contemplado en 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 (TIC) en la Sucursal de Guápiles"*.

Los resultados del estudio han permitido evidenciar que el cuarto donde se albergan los servidores y el switch de comunicaciones presenta condiciones inadecuadas de espacio físico para el resguardo de los mismos, situación que podría afectar la continuidad en la prestación de los servicios que brinda la Sucursal.

Respecto a la red de comunicaciones de área local, se evidenciaron debilidades en el cableado estructurado, lo anterior debido a que el mismo entro en operación aproximadamente hace 20 años y carece de los lineamientos que deben ser observados durante el proceso de adquisición, desarrollo y mantenimiento de las comunicaciones y redes informáticas en la CCSS y que son de acatamiento obligatorio por parte de las unidades de trabajo de la Institución.

Por otra parte, referente a los equipos informáticos que funcionan como servidores de archivos y bases de datos, se detectó que uno de ellos fue adquirido hace 14 años y por ende se encuentra 100% depreciado en su valor contable, asimismo, se evidenció obsolescencia respecto al sistema operativo y del motor gestor de base de datos que tiene instalado ya que los mismos fueron descontinuados por el fabricante. Aunado a esto, se evidenció que en año 2008 ingresó un servidor con mayores capacidades técnicas al mencionado anteriormente, sin embargo, no se ha realizado el traslado de las bases de datos del Sistema Plataforma de Cajas Institucional (SPIC) y el Sistema Integrado de Control de Presupuesto (SICP) a este equipo informático, situación que podría estar provocando una sub utilización de ese equipo considerando las necesidades y los niveles de criticidad de las aplicaciones con las que dispone la sucursal.

En ese mismo orden de ideas, respecto a los sistemas de alimentación ininterrumpida, se evidenciaron debilidades referentes a la obsolescencia tecnológica, su funcionamiento y su estado físico, asimismo, se detectaron debilidades en los niveles de seguridad utilizados para acceder desde la red de datos a la información digital almacenada en los equipos de cómputo y servidores de la Sucursal.

Finalmente, se determinaron oportunidades de mejora en el plan de mantenimiento preventivo, lo anterior referente al respaldo documental y el registro de las tareas y procedimientos a realizar, así como los responsables de su ejecución.

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

ATIC-274-2015
02-10-2015

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN INTEGRAL GERENCIAL DE LA SUCURSAL DE GUÁPILES
TEMA: GESTIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

ORIGEN DEL ESTUDIO

El presente estudio se efectuó en atención al Plan Anual Operativo del 2015 para el Área de Tecnologías de Información y Comunicaciones.

OBJETIVO GENERAL

Evaluar la gestión de Tecnologías de Información y Comunicaciones de la Sucursal de Guápiles.

OBJETIVOS ESPECÍFICOS

- Revisar los mecanismos de control efectuados por el Centro de Gestión Informática (CGI) de la Dirección Regional de Sucursales Huetar Atlántica y el encargado de informática de la Sucursal de Guápiles para la administración de las Tecnologías de Información y Comunicaciones (TIC).

- Verificar la obsolescencia tecnológica de los equipos TIC, sistemas operativos y gestores de bases de la Sucursal de Guápiles.

- Determinar el cumplimiento de las normas y políticas vigentes en materia de seguridad física y lógica de la Sucursal de Guápiles.

- Revisar la administración del inventario de tecnologías de información y comunicaciones de la Sucursal de Guápiles.

- Revisar la gestión de mantenimiento preventivo y correctivo de los equipos de cómputo del encargado de informática de la Sucursal de Guápiles.

ALCANCE

El estudio comprende la revisión de las actividades sustantivas en materia de TIC realizadas por el encargado de informática de la Sucursal de Guápiles en coordinación con el CGI de la Dirección Regional de Sucursales Huetar Atlántica. El período de la evaluación corresponde de Enero 2014 a Junio 2015, ampliándose en aquellos aspectos que se consideró necesario. Aunado a esto, es importante mencionar que este estudio contempló los siguientes temas:

- Seguridad física y lógica de los equipos TIC.

- Obsolescencia tecnológica de los equipos TIC, sistemas operativos y motores gestores de bases de datos.

- Red de comunicaciones de área local.

- Plan de mantenimiento preventivo y correctivo de los equipos de cómputo.

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

Con el propósito de alcanzar los objetivos propuestos, se desarrollaron los siguientes procedimientos metodológicos:

- Aplicar entrevistas a los siguientes funcionarios:

  - ✓ Sr. Oscar Morera Jiménez, Encargado de Informática de la Sucursal de Guápiles.

  - ✓ Maxie Barthley Martin, Jefe Área Gestión Informática de la Dirección Regional de Sucursales Huetar Atlántica.

- Revisión de documentación remitida por el Sr. Oscar Morera Jiménez, encargado de TIC de la Sucursal de Guápiles y el Lic. Maxie Barthley Martin, Jefe Área Gestión Informática de la Dirección Regional de Sucursales Huetar Atlántica.

- Análisis de la base de datos del Sistema Control Bienes y Muebles (SCBM), mediante ejecución de consultas para determinar el inventario de activos de TIC de la Sucursal de Guápiles.

- Análisis de la base de datos de SICERE, mediante ejecución de consultas para determinar el inventario de activos de TIC de la Sucursal de Guápiles.

- Inspección física de las instalaciones de la Sucursal de Guápiles.

MARCO NORMATIVO

- Ley N°. 8292 – Ley General de Control Interno, CR.
- Normas Técnicas para la Gestión y Control de Tecnologías de Información, CGR.
- Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) Nº R-CO-9-2009.

- Normas Institucionales de Seguridad Informática.
- Normas Institucionales de Tecnologías de Información y Comunicaciones.
- Políticas de Seguridad Informática, CCSS.
- Lineamientos generales de inventario TIC.

ASPECTOS RELACIONADOS CON LA LEY GENERAL DE CONTROL INTERNO

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, 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 (…)".*

ANTECEDENTES

La Sucursal de Guápiles es una unidad administrativa financiera, ubicada en el cantón de Pococí de la provincia de Limón y adscrita a la Dirección Regional de Sucursales Huetar Atlántica, misma que está adscrita a la Gerencia Financiera del a Caja Costarricense de Seguro Social (CCSS). En ese sentido, esta unidad administrativa financiera es de categoría tipo tres y se encuentra ubicada 100 metros al oeste de la Estación de Bomberos en Guápiles, en un terreno de aproximadamente 700 mtrs^2, de los cuales 550 mtrs^2 corresponden a construcción.

Aunado a esto, realiza funciones como la administración del efectivo, gestión de la cobranza, trámites de pensiones, servicio de inspección, trabajo social y servicios de apoyo como el fondo rotatorio, presupuesto, compras, transportes, entre otros y se encuentra conformada por 23 funcionarios distribuidos de la siguiente manera:

Cuadro No. 1
Distribución de trabajadores por puesto Sucursal de Guápiles
Junio 2015

Puesto	Total
Administrador de Sucursal 3	1
Asistente Técnico en Administración 2	1
Asistente Técnico en Administración 3	2
Cajero 2	1
Chofer 1	2
Guarda	1
Inspector de Leyes y Reglamentos 1	1
Inspector de Leyes y Reglamentos 3	3
Operador en Tic	1
Secretaria 3	1
Trabajador Social 3, Lic.	2
Trabajador de Servicios Generales	1
Técnico en Administración 1	5
Técnico en Administración 3	1
Total General	23

Fuente: *Sistema de Información Estadística de Recursos Humanos, creado el 08 de julio del 2015.*

Gestión Informática de la Sucursal de Guápiles

La Sucursal de Guápiles no dispone de un Centro de Gestión Informática, sin embargo, el soporte de las tecnologías de información y comunicaciones es realizada por un funcionario en una plaza con perfil de operador en TIC, realizando labores como: soporte técnico de hardware y software, mantenimiento preventivo y correctivo de los equipos de cómputo e impresoras, elaboración del plan de continuidad en TIC, administración de perfiles y usuarios del Sistema Centralizado de Recaudación (SICERE), Sistema Plataforma de Cajas Institucional (SPIC), Sistema Integrado de Pagos (SIPA), entre otros. Aunado a esto, ejecuta los procesos de cargar en el SICERE los archivos de nómina para los patronos que utilizan el Sistema de Grandes Clientes y Medios Magnéticos como medios de presentación de planilla.

En ese sentido, de acuerdo con el Plan de Continuidad en TIC esta unidad dispone de los siguientes equipos informáticos:

- 26 computadoras.
- 23 Monitores
- 10 impresoras.
- 5 equipos de comunicaciones.
- 2 servidores.
- Entre otros.

Por otra parte, es importante mencionar que el operador supra citado recibe apoyo por parte del CGI de la Dirección Regional de Sucursales Huetar Atlántica en procesos como la gestión de compra de equipos TIC, proyectos informáticos, administración del directorio activo, criterios de baja para las estaciones de trabajo e impresoras, entre otros.

HALLAZGOS

1. SOBRE LA RED DE COMUNICACIONES DE AREA LOCAL.

Se evidenció que la red de comunicaciones de área local presenta debilidades en cuanto al cableado estructurado, a continuación el detalle de lo mencionado:

- El cableado de la red de área local de la sucursal entró en operación desde el año 1995, a la fecha de la presente evaluación suma aproximadamente 20 años desde su implementación.

- Ausencia de etiquetados en los cables de red, tanto en los extremos del panel de conexiones y el switch, situación que impide identificar la ubicación del cableado estructurado dentro del edificio.

- Cables de red expuestos y sin canaleta en diferentes oficinas.

- El switch de comunicaciones ya no dispone de puertos libres para conectar equipos informáticos.

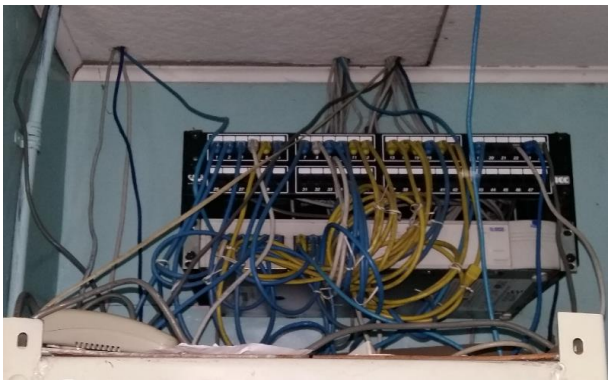
- Respecto a los Conmutadores de red (hubs), uno se encuentra suspendido en el aire sostenido por cables de red y el otro está ubicado en el suelo en estado de deterioro y envuelto en cinta adhesiva.

- Ausencia de puntos de red, todos los equipos de cómputo e impresoras se conectan directamente al switch.

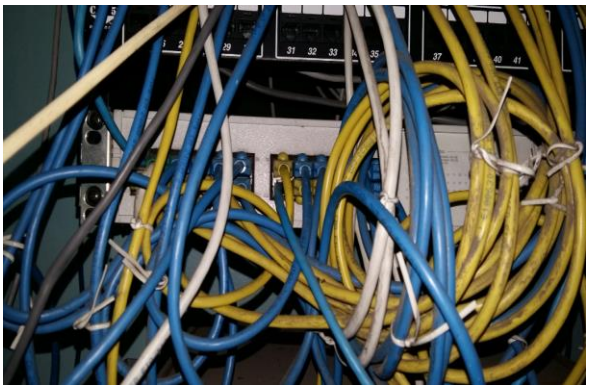
- La categoría del cableado es inferior a 6.

Las siguientes imágenes muestran lo indicado por esta Auditoría:

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



Fotografía 1: Cables de red del cuarto principal de telecomunicaciones



Fotografía 2: Switch de comunicaciones sin puertos disponibles para nuevas conexiones.

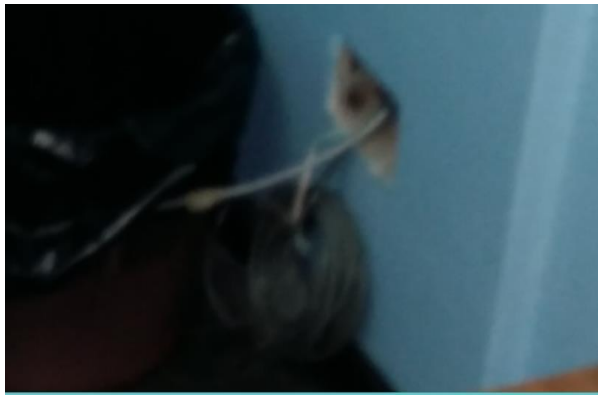
Fotografía 3: Conmutador de red ubicado en el suelo y sellado con cinta adhesiva.

Fotografía 4: Conmutador de red del cuarto de comunicaciones sin puertos disponibles para nuevas conexiones.

Fotografía 5: Cables de red suspendido en el aire y atravesando oficina.

Fotografía 6: Cables de red expuestos y sin canaleta.

Fotografía 7: Hub del cuarto de servidores.



Fotografía 8: Ausencia de puntos de red.

Fuente: *Auditoría Interna. Elaboración propia con base en inspección física realizada el 14 de julio del 2015.*

Por otro lado, según consta en los registros del Área de Comunicaciones y Redes Informáticas a julio del 2014, dicha sucursal dispone de un enlace de comunicación de 6 Mbps.

Cabe señalar, que esta Auditoría corroboró que actualmente el Centro de Gestión Informática (CGI) de la Gerencia Financiera, lidera una iniciativa para agrupar en una compra, las necesidades de cableado de las sucursales a nivel institucional. En ese sentido, se constató que la Sucursal de Guápiles está incluida en dicha iniciativa. No obstante, no se pudo confirmar la aprobación y oficialización de la misma, y se indicó que se trabaja en ajustes para adaptarla a un presupuesto, basados en priorizaciones y criticidad de las condiciones de esas unidades.

Las Normas Técnicas para la Gestión de las Tecnologías de Información de la CGR, en al apartado 1.4.3 de seguridad física y ambiental, indica 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:*
> *(…)*
> *f. La continuidad, seguridad y control del suministro de energía eléctrica,* ***del cableado de datos*** *y de las comunicaciones inalámbricas." (el formato negrita no corresponde al original).*

La Plantilla para la Construcción de cableados de red y centrales telefónicas, en el apartado 4. Cableado horizontal, establece:

> *"Todo lo utilizado para efectuar el cableado horizontal debe cumplir con lo normado para categoría 6a, esto incluye cable par trenzado CAT 6a CMR sin blindar, 4 pares (23 AWG), que cumpla con el estándar IEEE 802.3 y la norma ANSI/TIA-568-B, garantizando frecuencias de hasta 550MHz, conectores RJ45 6a, patch panel´s 6a, patch cord´s 6a, etc".*

El estándar de etiquetado de la Dirección de Tecnologías de Información y Comunicaciones, indica en su punto 1 especificaciones generales sobre uso de etiquetas, lo siguiente:

"El etiquetado se realizará según Norma ANSI/TIA 606A, la cual contiene especificaciones sobre el uso de etiquetas.

Todas las etiquetas a utilizar deben estar diseñadas para cumplir con los estándares internacionales y para sobrevivir a ambientes extremos (humedad, polvo, luz, grasa, temperaturas extremas, etc.).

Cada etiqueta debe estar impresa de acuerdo a los requerimientos particulares, de modo que se pueda adaptar a los tamaños y calibres de los diferentes cables.

Tanto los paneles como las rosetas deben contar con algún tipo de sistema que permita colocar las etiquetas. Estas deben ser de lectura clara y no podrán ser impresas de forma manual.

Para el etiquetado a las estaciones de trabajo, deben quedar al menos cuatro etiquetas por cada conexión, según Figura No. 1, de la siguiente manera:

1. *Una en la caja de pared del cubículo del usuario.*
2. *En la parte frontal de patch panel*
3. *En el extremo del patch cord conectado al patch panel*
4. *En el extremo del patch cord conectado al switch*

1.1 Etiquetado en cables y tomas

- *Los productos de cableado por etiquetar deben facilitar el cambio de etiquetado. Es preferible emplear productos que permitan extraer la etiqueta para ser sustituida en caso de cambiar el identificador o si se ha deteriorado y resulta ilegible.*
- *Emplear etiquetas con el tamaño adecuado al producto por etiquetar.*

(…)

1.2 Etiquetado en Bastidores y Armarios

- *La etiqueta deberá situarse en la parte superior para mejorar la visibilidad, en el centro para evitar ser tapado por los cables.*
- *Para una rápida identificación, la etiqueta debe ser fácil de leer desde cualquier punto del distribuidor.*
- *Cuando se emplean racks de montaje en pared, se deberá elegir el patch-panel que permita etiquetar.*
- *El etiquetado se realiza en el patch-panel, para una rápida identificación de las regletas existentes.*

1.3 Etiquetado en Regletas, Patch-Panels y Patch-Cords

- *Cada regleta o panel debería etiquetarse según el esquema que se indica en este documento.*
- *Las etiquetas deben colocarse de forma que no sean tapadas por cables o patch cords.*
- *Las etiquetas de los puertos individuales deben colocarse de forma que sean visibles, al realizar las interconexiones o cambiar algún patch-cord.*
- *Con las regletas y paneles, se deberán facilitar etiquetas para sustituir cualquier etiquetado de fábrica, y configurar el panel a gusto del cliente o instalador.*
- *Las etiquetas deberán instalarse de forma que se tape el etiquetado de fábrica y así evitar cualquier confusión."*

El Lic. Maxie Barthley Martin, Jefe Área Gestión Informática de la Dirección Regional de Sucursales Huetar Atlántica consultado al respecto, indicó que:

> *"En cuanto a este punto si tiene razón de esas debilidades, de hecho ya se han hecho gestiones de años atrás para cambiar dicho cableado de red, pero por situaciones de presupuestarias nunca se consiguió los recursos para la misma. Dado esa situación ya se está coordinando con la gente Subárea Ingeniería y Mantenimiento de Redes con Master Carlos Madrigal Madrigal, actualmente están en la Dirección Regional y para la otra semana van para otra Sucursal.*
>
> *En cuanto el etiquetado considero eso sí está debería estar, me extraña sobremanera que no haya ninguna información sobre eso."*

Al respecto, el señor Oscar Morera Jiménez, encargado de informática de la Sucursal de Guápiles, manifestó lo siguiente:

> *"La red de comunicaciones de la Sucursal se implementó en el año 1995 que fue cuando se remodeló el edificio y el cable es categoría 5."*
>
> *"El cableado estructurado en su momento se realizó empíricamente ya que no existían proveedores en la zona que realizaran este tipo de cableado de manera certificada, inclusive en primera instancia el cableado de la sucursal era de tipo coaxial, sin embargo mi persona efectuó el cambio tecnología de cable coaxial a cable tipo UTP aproximadamente hace 16 años."*
>
> *"La presencia de cables expuestos se debe a que en primera instancia es una red muy antigua y además la sucursal no cuenta con los recursos para realizar las mejoras cuando es evidente que se debe realizar un cambio total de la infraestructura de cableado por lo que no sería conveniente una inversión en la misma."*

Lo evidenciado por esta Auditoría en relación a las condiciones actuales del cableado estructurado, limita el esquema de administración uniforme de la red de comunicaciones de área local y podría originar problemas de conectividad, además, se podrían materializar riesgos correspondientes a la disponibilidad de los sistemas y procesos críticos de la sucursal, aumento de los costos para la gestión de la continuidad e interrupciones constantes y prolongadas que interfieran con la prestación de los servicios a los usuarios.

2. SOBRE LAS CONDICIONES DEL ESPACIO FÍSICO ASIGNADO PARA LOS SERVIDORES Y EL SWITCH[1] DE COMUNCIACIONES.

En recorrido efectuado por esta Auditoría se pudo constatar que el cuarto donde se albergan los servidores y el switch de comunicaciones presenta condiciones inadecuadas para el resguardo de los mismos, entre los aspectos detectados se encuentran:

- Limitaciones de espacio físico debido a que se encuentra un mueble de madera con puertas de vidrio donde se resguardan papeles, documentos, cajas de cartón, discos compactos, repuestos y artefactos electrónicos, además, encima del mismo fue colocado un servidor.

- Presencia de equipos informáticos en desuso como impresoras, computadoras, monitores, teclados, entre otros.

- El servidor de base de datos y las unidades de potencia ininterrumpida se encuentran sobre un anaquel de metal con una base de madera.

- El switch de comunicaciones presenta un orden inadecuado de los cables de red conectados al mismo.

A continuación se presentan fotografías donde se observa la situación mencionada:

[1] El switch se utiliza para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina.
Fuente: http://www.cisco.com/web/LA/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf

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

FIGURA NO. 1
FOTOGRAFÍAS DEL CUARTO DE SERVIDORES Y SWITCH DE COMUNICACIONES - SUCURSAL DE GUÁPILES

Fuente: *Fotografías capturadas en recorrido a la Sucursal de Guápiles el 08 de julio del 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.*
> *g. 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 Guía de Usuario Final de buenas prácticas en el uso de las TIC DTI-I-SI-0010, en el punto 5 Buenas prácticas para el uso de las estaciones de trabajo, señala lo siguiente:

> *" 5. No utilice el equipo de cómputo sobre ningún tipo de base inestable, como cajas, o mesas en mal estado, de modo que la probabilidad de caer se minimice. "*

El Sr. Oscar Morera Jimenez, encargado de informática de la Sucursal de Guápiles indicó lo siguiente:

> "*La situación se presenta debido al hacinamiento que existe a nivel general en la sucursal, por lo que aprovechamos los espacios existentes para resguardar los equipos, documentos, entre otros."*

No disponer de un espacio físico con las condiciones adecuadas para el resguardo de los servidores y los equipos de comunicaciones podría afectar la continuidad en la prestación de los servicios que brinda la Sucursal, los cuales son necesarios para la ejecución eficaz y eficiente de las funciones encomendadas a esta unidad administrativa financiera, destacándose los procesos de recaudación y facturación de cuotas obrero patronales, así como el trámite y pago de pensiones, la gestión de inspección y cobros, entre otros, los cuales se verían afectados en caso de presentarse alguna falla en esos equipos informáticos.

3. SOBRE LOS EQUIPOS INFORMÁTICOS QUE FUNCIONAN COMO SERVIDORES.

En relación con los equipos informáticos que funcionan como servidores de archivos y bases de datos se detectaron las siguientes debilidades:

3.1 Sobre la obsolescencia tecnológica del servidor placa # 555906

Mediante revisión efectuada en el Sistema Contable de Bienes y Muebles (SCBM), se determinó que el servidor marca Fujitsu con número de placa 555906, se encuentra 100% depreciado en su valor contable y por ende, ha cumplido su ciclo de vida útil.

Aunado a esto, se evidenció que dicho servidor tiene instalado el sistema operativo Microsoft Windows Server 2000 y el motor gestor de base de datos Microsoft SQL 2000, versiones que ya fueron descontinuadas por su fabricante Microsoft.

En ese sentido, es importante mencionar que este activo fue adquirido hace 14 años, sin embargo, en la actualidad es utilizado para almacenar las bases de datos de sistemas de información como el SICP y el SPIC y se encuentra registrado en el Plan de Continuidad en TIC de la Sucursal como un equipo de nivel crítico alto.

3.2 Sobre la utilización del servidor placa # 799896

Se constató que esta unidad administrativa financiera además del equipo informático mencionado en el punto 3.1 de este informe, dispone de otro servidor que según indica el SCBM tiene fecha de ingresó a la unidad en el año 2008, y es utilizado en la actualidad para respaldo de documentos de los funcionarios, cabe señalar que dicho activo se presenta con un nivel de criticidad bajo en el Plan de Continuidad en TIC. A continuación se presenta un cuadro comparativo entre ambos activos:

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

Cuadro No. 2
Cuadro Comparativo de Servidores
Sucursal de Guápiles

Datos	Servidor marca FUJITSU	Servidor marca H. P.
N° Placa	555906	799896
Fecha ingreso	28/03/2001	17/10/2008
Valor inicial	₡4,451,604.00	₡3,026,540.60
Valor Depreciación Acumulada	₡4,451,604.00	₡2,101,165.66
% vida útil	0	31
Sistema Operativo	Windows Server 2000	Windows Server 2008
Cantidad memoria ram	512 Mb	8 GB
Modelo de Arquitectura	32 bits	64 bits
Procesador	2 Intel Xeon 550	Quad Core Xenon
Velocidad del Procesador	1.0 Ghz	2.0 Ghz
Funciones	Almacena bases de datos del SPIC, SICP y cobros	Respaldo de documentos de los funcionarios

Fuente: *Sistema Control de Bienes y Muebles y Plan de Continuidad en TIC, Julio 2015.*

Con base en el cuadro anterior, de acuerdo con el nivel de obsolescencia del servidor 555906, se torna inviable una modernización del sistema operativo y del motor gestor de bases de datos, debido a que no cumple los requisitos mínimos para migrar a versiones superiores de Microsoft como Windows Server y SQL 2008 y 2012, caso contrario al servidor 799896, el cual según sus especificaciones técnicas posee una versión actualizada del sistema operativo, así como mayor cantidad de memoria ram, modelo y velocidad del procesador, entre otros.

En ese sentido, preocupa a esta Auditoría que han transcurrido cinco años desde que ingresó un servidor con las capacidades técnicas necesarias para sustituir el activo de mayor antigüedad, sin embargo, a la fecha no ha sido realizado el traslado de las bases de datos del SPIC y el SICP a este equipo, lo cual permitiría eventualmente disminuir el riesgo respecto a la continuidad de los servicios que presta la Sucursal.

En virtud de lo anterior, puede haberse presentado una sub utilización de ese equipo considerando las necesidades y los niveles de criticidad de las aplicaciones que utiliza la Sucursal, dado que desde el año 2008 dicho activo funciona únicamente como un servidor de respaldo de documentos y no como un equipo que almacena bases de datos de carácter crítico para esta unidad administrativa financiera.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el capítulo 3, punto 3.3 sobre Implementación de infraestructura tecnológica, indican lo siguiente:

"La organización debe adquirir, instalar y actualizar la infraestructura necesaria para soportar el software de conformidad con los modelos de arquitectura de información e infraestructura tecnológica y demás criterios establecidos. Como parte de ello debe considerar lo que resulte aplicable de la norma 3.1 anterior y los ajustes necesarios a la infraestructura actual."

Asimismo, estas normas técnicas en el apartado 4.2 Administración y operación de la plataforma tecnológica señalan que:

"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe: (…)

c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas.

d. Controlar la composición y cambios de la plataforma y mantener un registro actualizado de sus componentes (hardware y software), custodiar adecuadamente las licencias de software y realizar verificaciones físicas periódicas. (…)"

El señor Oscar Morera Jiménez, encargado de informática de la Sucursal de Guápiles, indicó que:

"*El traslado y migración no se ha realizado debido a la carencia de servidores en la región, estamos conscientes de esta problemática y nos encontramos en proceso de realizar el cambio pero se ha ido postergando por razones de disponibilidad del CGI de la Dirección Regional, además, se carece de una UPS para mantener trabajando ese servidor nuevo, ya que la existente está prácticamente obsoleta y no hemos realizado las pruebas para ver si resiste al menos los 2 minutos que generalmente entra a funcionar la planta eléctrica."*

"Es evidente que el servidor es un activo muy antiguo, pero estamos en proceso con el CGI Regional de trasladar las bases de datos y la información contenida en el mismo al otro servidor de la Sucursal, el cual presenta mayores capacidades técnicas".

El uso de software sin soporte implica no recibir actualizaciones de seguridad y parches críticos de resolución de incidencias por parte de la empresa fabricante, provocando vulnerabilidades de seguridad en el sistema operativo que puedan comprometer la confidencialidad, disponibilidad e integridad de los datos procesados y almacenados en los equipos, sistemas gestores de bases de datos y sus aplicaciones

Aunado a lo anterior, la inadecuada gestión para el aprovechamiento adecuado de las inversiones en Tecnologías de Información y Comunicaciones realizadas, puede materializar riesgos referentes a la continuidad en la prestación de los servicios brinda la Sucursal.

4. SOBRE LOS SISTEMAS DE ALIMENTACIÓN ININTERRUMPIDA (UPS POR SUS SIGLAS EN INGLÉS).

En relación con los sistemas de alimentación ininterrumpida, se evidenciaron debilidades referentes a la obsolescencia tecnológica, su funcionamiento y el estado físico de los equipos. A continuación, el detalle de lo mencionado:

4.1 Sobre la vida útil de los sistemas de alimentación ininterrumpida.

De acuerdo con revisión en el SCBM, el 100% de los sistemas de alimentación ininterrumpida (correspondiente a cinco UPS), se encuentran depreciados en su valor contable y por ende, finalizaron su ciclo de vida útil. A continuación se presenta un cuadro con el detalle de lo mencionado:

Cuadro No. 3
UPS Depreciados
Sucursal de Guápiles

N° Placa	Activo	Fecha Ingreso Unidad
502774	UPS 750 W Full Power C/Regulador	10/12/1999
502775	UPS 750 W Full Power C/Regulador	10/12/1999
286075	U.P.S. Unidad Potencia Inint.	24/07/1991
572986	U.P.S. Tripp-Lite 500 VA.	26/12/2001
355037	U.P.S. American Power	02/12/1994

Fuente: *Sistema Contable de Bienes y Muebles, julio 2015.*

Como se puede observar en el cuadro anterior, estos equipos en promedio fueron adquiridos hace 18 años y si bien se encuentran en funcionamiento en la actualidad, representan un riesgo debido a su antigüedad y obsolescencia, lo que contraviene con la normativa establecida respecto a la adquisición de infraestructura acorde a las tendencias tecnológicas actuales.

4.2 Sobre el estado físico y las reparaciones de los sistemas de alimentación ininterrumpida con potencia no mayor a 350 VA.

En recorrido efectuado por esta Auditoría el día 15 de julio del 2015, se constató que de 15 sistemas de alimentación ininterrumpida con potencia no mayor a 350 VA, cuatro de ellos no funcionan y por ende impide que los equipos de cómputo, monitores e impresoras dispongan de protección contra fallos eléctricos o alteraciones en el voltaje, cortos en la energía eléctrica, entre otros. A continuación, el detalle de lo mencionado anteriormente:

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

Cuadro No. 4
UPS Depreciados
Sucursal de Guápiles

N°	Lugar	Funciona Actualmente	Fecha de Compra	Cantidad de Reparaciones
1	Fondo Rotatorio	SI	10/2001	3
2	Jefatura	SI	01/2005	3
3	Central Telefónica	NO	10/2005	2
4	Cobros	SI	10/2005	2
5	Inspección	SI	10/2005	2
6	Inspección	NO	10/2005	4
7	Inspección	NO	10/2005	3
8	Pensiones RNC	SI	10/2005	3
9	Presupuesto	SI	12/2005	3
10	Plataforma	SI	01/2010	3
11	Plataforma	SI	01/2010	3
12	Plataforma	SI	01/2010	2
13	Secretaria	SI	01/2010	2
14	Auditorio	NO	N/A	2
15	Pensiones IVM	SI	N/A	1

Fuente: *Recorrido efectuado por esta Auditoría el día 15 de julio del 2015, además fecha de compra y cantidad de reparaciones fue suministrada por el encargado de informática de la Sucursal de Guápiles.*

Con base en el cuadro anterior, 11 UPS son funcionales y 4 se encuentran en mal estado, además, se puede observar que los equipos han sufrido múltiples reparaciones, situación que podría considerarse como equipos potencialmente aptos para ser sometidos a una evaluación de su nivel de reemplazo. Aunado a esto, se puede constatar que la adquisición de los equipos fue aproximadamente hace 5 y 10 años.

Del mismo modo, se puede evidenciar que diversas UPS se encuentran selladas con cinta adhesiva, generando una imagen de deterioro de los equipos. A continuación una fotografía con la situación señalada:

Fotografía N° 9
Ups Sellada con Cinta Adhesiva
Sucursal de Guápiles

Fuente: *Fotografía capturada por esta Auditoría el día 09 de julio del 2015.*

Las Normas de Control Interno para el Sector Público en el capítulo 4 en el apartado 4.3.1, inciso E, indica lo siguiente:

> *"El jerarca y los titulares subordinados, según sus competencias, deben establecer, actualizar y comunicar las regulaciones pertinentes con respecto al uso, conservación y custodia de los activos pertenecientes a la institución. Deben considerarse al menos los siguientes asuntos:*
>
> *b. La asignación de responsables por el uso, control y mantenimiento de los activos, incluyendo la definición de los deberes, las funciones y las líneas de autoridad y responsabilidad pertinentes."*

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el capítulo 4.2 Administración y operación de la Plataforma tecnológica, indican lo siguiente:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
>
> *a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
> *b. Vigilar de manera constante la disponibilidad, capacidad, desempeño y uso de la plataforma, asegurar su correcta operación y mantener un registro de sus eventuales fallas.*
> *c. Identificar eventuales requerimientos presentes y futuros, establecer planes para su satisfacción y garantizar la oportuna adquisición de recursos de TI requeridos tomando en cuenta la obsolescencia de la plataforma, contingencias, cargas de trabajo y tendencias tecnológicas."*

Los lineamientos generales de inventario TIC en su apartado 7 Diagnóstico de la plataforma tecnológica, indica lo siguiente:

"(…)7.2 El encargado del Centro de Gestión Informática debe brindar a la administración de la unidad de trabajo un reporte con el diagnóstico realizado, señalando los recursos de TIC candidatas al remplazo, mejora, reparación o declaratoria de obsolescencia.

7.4 Corresponde al encargado del CGI realizar revisiones periódicas de todos los recursos de TI, mediante la ***Guía para el Remplazo de Activos TIC****.*

7.5 Entre los parámetros a considerar en el diagnóstico de remplazo de los recursos de TIC prevalecerá:

a) En cuanto a repuestos e insumos;

- *Cantidad en existencia de repuestos en el Centro Médico*
- *Existencia de repuestos en el Mercado*
- *Si existe disponibilidad en el mercado por parte del Fabricante*

b) En cuanto al historial de mantenimiento:

- *Cantidad de veces que se ha reparado el equipo anualmente*
- *Cantidad de componentes internos reemplazados*
- *Cantidad de problemas más frecuentes (Software y Hardware)*

c) En cuanto a tendencias tecnológicas:

- *Requerimientos Institucionales e Internos.*
- *Equipo actual en el Centro Médico.*
-

d) En cuanto al nivel de utilización:

- *Disponibilidad de equipo según área a la que sirve.*
- *Cantidad de horas/día en funcionamiento.*
- *Ambiente de operación.*
- *Uso adecuado del equipo por parte del usuario.*
- *Funciones del usuario del equipo.*

Esos mismos lineamientos en su apartado 8 Responsabilidad sobre la reparación, mejora o remplazo de los recursos TIC indica lo siguiente:

> *"Es responsabilidad de la autoridad del centro de trabajo, con base en el Informe de Remplazo, planificar conforme las regulaciones institucionales la reparación, mejora o remplazo de los recursos de TI, girando las instrucciones pertinentes a los encargados de los distintos procesos relacionados con la gestión solicitada."*

La Guía para la Evaluación del Reemplazo sobre Activos de TIC, en su apartado 3.2.1 Inventario de TIC actual señala que:

> *"Debe efectuarse la selección de los activos de TIC considerados potencialmente aptos para ser sometidos a una evaluación de su nivel de reemplazo. Los siguientes criterios deben ser valorados al efectuar dicha selección:*
>
> *d. Unidad de Potencia Ininterrumpida*
> - *Equipos con mayor antigüedad de uso.*
> - *Equipos con baja capacidad de carga según la necesidad existente.*
> - *Equipos expuestos a un alto nivel de disponibilidad según su ubicación física.*
> - ***Equipos que superen su vida útil (5 años)**" (Lo Subrayado no corresponde al original)*

El 07 de enero del 2015, el Ing. Maxie Barthley Martin, Jefe del Área de Gestión Informática de la Dirección Regional de Sucursales Huetar Atlántica, mediante oficio DRSHA_CGI_0031_01_2015, remite al Lic. Efraín Mata Ríos, Administrador de la Sucursal de Guápiles, *"Informe Técnico de visita a la Sucursal de Guápiles el día 30 12 2014 en revisión a UPS"*, indicando lo siguiente:

> *"(…) Después de realizada la revisión y diagnostico se determinó que los casos que están **Estado UPS "reparar "**se pueden confeccionar el expediente para enviarlos a reparar.*
>
> *Los casos de UPS en **Estado UPS " Comprar** " se va programar para comprar las mismas al menos dos para este año 2015 para lo que es Área del FRO y Cajero , y para los periodos del 2016 y 2017 programar las demás compras.*
>
> *Se dará seguimiento a los casos que se tienen que reparar si efectivamente se pudo reparar para si programar las compras a futuro(…)".*

El día 27 de enero del 2015, el Lic. Efraín Mata Ríos, Administrador de la Sucursal de Guápiles, mediante oficio SSG-1506-054-2015, remite información sobre justificación de compra de UPS a la Licda. Xiomara Poyser Watson, Directora a.i. Regional de Sucursales Huetar Atlántica, indicando lo siguiente:

"Justificación:

(…)Las actuales no funcionan cuando falla el fluido eléctrico, todas las máquinas se apagan hasta que arranque la planta eléctrica.

Estos picos de voltaje sumados a las frecuentes tormentas eléctricas que afectan esta región y los múltiples apagonazos provocan que los trabajos que los funcionarios estén haciendo se pierdan si no se van guardando a cada instante.

Por ser estos activos los principales componentes de trabajo para atender usuarios internos y externos, presenciales o por la vía telefónica, provocan el malestar de las personas porque hay que encender de nuevo las máquinas y abrir los programas que se requieren para la debida atención.

Además por trámites de casos tales como inspección, gestores de cobros, cálculos de pensiones, pagos SFRO, pago de incapacidades, cobro de seguros, claves a patronos, entre otros.

La central telefónica también se apaga bruscamente, así como todos los equipos de cómputo en general. (…)"

El 18 de marzo del 2015, mediante oficio DRSHA_CGI_0788_03_2015, el Ing. Maxie Barthley Martin, Jefe del Área de Gestión Informática de la Dirección Regional de Sucursales Huetar Atlántica, remite información sobre solicitud de compra para implementos tecnológicos a sucursales a la Licda. Gina Galeano Ledezma, Jefe Subárea a.i Gestión Administrativa y Logística de esa misma Dirección, indicando lo siguiente:

"UNIDAD DE POTENCIA ININTERRUMPIDA 800 A 1000VA

El caso de la Sucursal de Guápiles es preferible que se envíen a reparar los actuales para disminuir el costo de comprar UPS nuevas, ya que en su mayoría solo requiere cambio de baterías internas de 12 V 7 A."

El 06 de mayo del 2015, mediante oficio DRSHA-1291-05-2015, la Licda. Xiomara Poyser Watson, Directora Regional a.i de Dirección Regional de Sucursales Huetar Atlántica, remite información sobre autorización de reparación de UPS al Lic. Efraín Mata Ríos, Administrador de la Sucursal de Guápiles, indicando lo siguiente:

"Mediante oficio DRSHA_CGI_0788_03_2015 de fecha 18 de marzo 2015, suscrito por el Ing. Maxie Barthley Martin, brinda informe técnico sobre solicitud planteada en oficio SSG-1506-054-2015, dicho informe recomienda la reparación de las 26 Unidades de Potencia Ininterrumpida (UPS) de la Sucursal de Guápiles"

El Lic. Maxie Barthley Martin, Jefe Área Gestión Informática de la Dirección Regional de Sucursales Huetar Atlántica consultado al respecto, indicó que:

"(…)yo había realizado un informe DRSHA_CGI_0031_01-2015 en visita a la Sucursal 30 12 2014, se envió al Jefe Lic. Efraín Mata Ríos Administrador de la Sucursal, el Área de Compras de la Dirección Regional sobre los casos que se pueden reparar y programar para los años 2015, 2016 y 2017 las que se debía de comprar."

Además, respecto al estado físico de las UPS, el Lic. Barthley indicó:

"Son situaciones que vi y pero como siempre uno no deja las cosas por escrita, pero a partir de ahora todas esas situaciones los voy documentar."

Esa es otra UPS que si esta para comprar por cuanto su estética no se puede cambiar y reparar."

El señor Oscar Morera Jiménez, encargado de informática de la Sucursal de Guápiles, mencionó lo siguiente:

"No se me solicitó por parte de la Dirección Regional de Sucursales un estudio o criterio respecto sobre el estado de las UPS de la sucursal de Guápiles."

"Esta situación se presenta debido a que la Dirección Regional de Sucursales Huetar Atlántica no ha dotado a esta sucursal de equipos nuevos, y dado las limitaciones con los recursos que tenemos es que algunas se encuentran en estas condiciones, es importante señalar que aunque su mayoría se encuentran en estado de obsolescencia estas continúan funcionando."

Utilizar unidades de potencia ininterrumpida que ya agotaron su vida útil puede comprometer la continuidad en la prestación de los servicios de tecnologías de información y comunicaciones, lo anterior debido a fallas eléctricas que se pueden presentar a causa de su obsolescencia y que eventualmente aumenta el riesgo de un fallo en su funcionamiento, desprotegiendo los demás equipos que están conectados (computadoras, monitores, impresoras, entre otros).

Del mismo modo, disponer de UPS que se encuentran en estado de deterioro y selladas con cinta adhesiva, podría provocar una afectación a la imagen institucional referente a la gestión que realizan los funcionarios en TIC para la adquisición, reparación y mantenimiento de la infraestructura tecnológica de la CCSS.

5. SOBRE LOS NIVELES DE SEGURIDAD DE LA INFORMACIÓN DIGITAL ALMACENADA EN LOS EQUIPOS DE CÓMPUTO Y SERVIDORES.

Se detectó debilidades en los niveles de seguridad utilizados para acceder desde la red de datos a la información digital almacenada en los equipos de cómputo y servidores de la Sucursal de Guápiles.

En ese sentido, en la prueba realizada por esta Auditoría con una cuenta de red de dominio diferente a GFINAN, se evidenció que 27% de las estaciones de trabajo correspondiente a 6 equipos informáticos, tiene acceso a carpetas con información de las operaciones que realizan los diferentes departamentos que componen la unidad administrativa financiera, entre los cuales se encuentran archivos de facturas pendientes de pago, asientos de diario, archivos de cuentas 326, conciliaciones, minutas de reuniones, informes mensuales del régimen no contributivo de pensiones, entre otros. Las imágenes que evidencia la situación descrita se muestran en el Anexo 1 de este informe.

En ese sentido, preocupa a esta auditoría que el acceso a los archivos supra citados no es solamente en modo de lectura sino también con la posibilidad de escritura y control total, esto quiere decir que los documentos y carpetas indicadas en este hallazgo permiten agregar, modificar e inclusive borrar información.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en el Capítulo 1 Normas de aplicación general, apartado 1.4 Gestión de la Seguridad de la Información, indican 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."*

Esas mismas normas en el apartado 1.4.2 sobre compromiso del personal con la seguridad de la información señalan que:

> *"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 igual manera, estas normas en el apartado 1.4.5 sobre control de accesos, inciso D, indican que la organización debe:

> *"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."*

Las Políticas Institucionales de Seguridad Informática en el punto 9.3 establecen:

> *"Con el fin de prevenir el acceso no autorizado a los datos de las estaciones de trabajo propiedad de la CCSS, la cuenta de administrador local de cada una de las estaciones de trabajo propiedad de la institución, debe administrarse y configurarse de manera segura, ya que de ello depende minimizar el riesgo de que terceros puedan accesar la información almacenada en las mismas.*
> *La cuenta de administrador local de las estaciones de trabajo, tiene que ser creada y administrada, considerando características de seguridad y robustez iguales a las que se configuran para las cuentas de red y aplicaciones. Los administradores y soportistas de red, deben ser colaboradores activos con los usuarios en el cumplimiento de esta política."*

Consultado sobre el tema, el Señor Morera, encargado de informática de la Sucursal de Guápiles, indicó que:

> *"Si tengo conocimiento de esta situación, en ocasiones se ha producido para compartir documentos en una situación momentánea y talvez no se restringieron los permisos, sin embargo, se debe considerar que efectivamente lo que señala esta Auditoría es un riesgo sobre la seguridad de la información, además, creo que también se presenta debido a que se limita un poco porque existe software que necesita permisos de administrador para ejecutarlos y por ende tienen acceso a este perfil."*

La ausencia de mecanismos de control y seguimiento para garantizar el cumplimiento de las disposiciones Institucionales de seguridad informática, compromete la disponibilidad de la información que utilizan los funcionarios de la Sucursal para el desempeño de sus labores, es importante mencionar que la tecnología usada en los sistemas operativos para compartir carpetas es una práctica realizada por los usuarios para utilizar archivos y documentos de acuerdo con los permisos correspondientes, aprobando leerlos o modificarlos, sin embargo, el uso de esta práctica lo vuelve susceptible al riesgo de ataques tales como infecciones, exposición de información Institucional, así como la eliminación de archivos sin poder definir responsabilidades.

En ese mismo orden de ideas, el acceso sin niveles de seguridad sobre información de actividades administrativas y de carácter contable financiero, eleva el riesgo de que usuarios no autorizados obtengan datos confidenciales que puedan ser utilizados para fines ilícitos o de cualquier otros factor disfuncional y que además puede conllevar a la Institución a procesos judiciales por divulgación no autorizada, daños y pérdida de la información médica, además de afectar la imagen Institucional en relación con el resguardo y protección de la información.

6. SOBRE SOFTWARE LIBRE O GRATUITO UTILIZADO EN LOS EQUIPOS DE CÓMPUTO.

Se detectó el uso de la aplicación informática gratuita llamada VNC, la cual no se encuentra en el listado oficial de software libre y gratuito autorizado por la CCSS V 1.3. En ese sentido, la herramienta supra citada es programa que permite tomar el control de un equipo de cómputo remotamente a través de un ordenador cliente, también es llamado software de escritorio remoto.

Cabe mencionar que esta Auditoría en revisión efectuada de la lista supra citada, detectó una solución de escritorio remoto que tiene el aval de la Dirección de Tecnologías de Información y Comunicaciones (DTIC) llamada Team Viewer, la cual tiene una funcionalidad similar a la herramienta que se utiliza en esta Sucursal. Del mismo modo, existe la funcionalidad de escritorio remoto que trae por defecto los sistemas operativos de Microsoft Windows.

Las Normas Institucionales de Seguridad Informática en el punto 7.3. Normas para la política uso adecuado de estaciones de trabajo cita:

> *"Los soportistas de los Centros de Gestión Informática, deberán velar porque los equipos de cómputo, cuenten con:*
>
> *• Software autorizado por la Institución o bien licencias adquiridas por la Unidad."*

La Guía para la Configuración Segura de Equipos en su apartado 1.16. Instalación de software señala que:

> *(…) ¿Cómo controlar la instalación de software? Establezca una política que haga referencia a la instalación de software con los parámetros mínimos que aseguren la plataforma, detalle un procedimiento para la gestión de instalación identificando los responsables de cada una de las actividades inherentes a la instalación de software.*
> *Limitar los permisos de administrador a los usuarios finales a efectos de que el Sistema Operativo les limite la instalación de dispositivos y software (…).*

El Estándar técnico contra software malicioso y virus en sus diferentes variantes V 2.0 (2015), señala que:

"No se debe instalar barras en los navegadores de Internet, así como otros programas que no estén incluidos en la "Lista Oficial de Software Autorizado en la CCSS".

"Evitar la utilización del software que no sea avalado institucionalmente (consultar la "Lista Oficial de Software Autorizado en la CCSS)".

*Desinstalar cualquier programa de screensaver o cualquier programa que no sea institucional (consultar la **"Lista Oficial de Software Autorizado en la CCSS**)", ya que en la mayoría de los casos permiten el ingreso de spyware y malware.*

El señor Oscar Morera Jiménez, encargado de informática de la Sucursal de Guápiles, mencionó lo siguiente:

"Se utiliza debido a que es un software muy amigable y permite interactuar con el usuario directamente, pero si existe una solución similar en el listado oficial sería importante considerarse, el escritorio remoto de Windows no se utiliza debido a que cierra la sesión e impide que el usuario observe el soporte que recibe."

Utilizar aplicaciones que no se encuentren en el listado oficial de software libre y gratuito autorizado por la CCSS, indica que la herramienta no ha sido evaluada por la Comisión Institucional de Seguridad Informática, por ende, podría representar un riesgo de seguridad de la información ya que no se ha determinado si la aplicación presenta vulnerabilidades que afecten la disponibilidad de los datos que administra.

7. SOBRE EL PLAN DE MANTENIMIENTO PREVENTIVO-CORRECTIVO DE LOS EQUIPOS DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.

Se determinaron oportunidades de mejora en relación con el plan de mantenimiento preventivo y correctivo de la Sucursal de Guápiles. En ese sentido, si bien se dispone de un documento con las fechas en que se va realizar dicho mantenimiento, el mismo no indica un registro de las tareas y procedimientos a realizar, así como los responsables de su ejecución. Del mismo modo, se evidenció que los mantenimientos efectuados durante el primer semestre del año 2015 carecen de un respaldo documental que permita determinar que efectivamente fueron realizados.

Las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información, en el artículo 1.4.6 indican lo siguiente:

"La organización debe mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica…

Para ello debe: Contar con procedimientos claramente definidos para el mantenimiento y puesta en producción del software e infraestructura..."

La citada norma dispone en el apartado 4.2 referente a la Administración y operación de la plataforma tecnológica, señala:

> *"La organización debe mantener la plataforma tecnológica en óptimas condiciones y minimizar su riesgo de fallas. Para ello debe:*
>
> *a. Establecer y documentar los procedimientos y las responsabilidades asociados con la operación de la plataforma.*
>
> *e. Controlar la ejecución de los trabajos mediante su programación, supervisión y registro."*

El Modelo de Organización de los Centros de Gestión Informática, en el apartado de Gestión Técnica señala que el área de Gestión Informática debe:

> *"Programar en forma periódica el mantenimiento preventivo para el hardware, el software y las comunicaciones, con base en las políticas y normas institucionales vigentes, con el fin de lograr la eficiencia, la eficacia y la productividad de la gestión."*

El señor Oscar Morera Jiménez, Encargado de Informática de la Sucursal de Guápiles, señalo que:

> *"Se realizaron algunas boletas sobre los trabajos realizados, sin embargo no se efectuaron en su totalidad, es importante mencionar que generalmente se elabora una boleta donde inclusive el funcionario al que se le realizó el servicio firma así como el Jefe de la Sucursal, pero en ocasiones por ser labores operativas no se documenta en su totalidad."*

La ausencia de un programa de mantenimiento preventivo y correctivo donde se establezca la calendarización, servicios que se deben atender, responsables, procedimientos ejecutados y actividades específicas a realizar para brindar el mantenimiento a los recursos existentes, disminuye la posibilidad de tener mecanismos de control que permitan determinar las condiciones reales de los equipos TIC así como garantizar la ejecución de tareas periódicas de reparación, limpieza y configuración de los mismos.

Aunado a esto, la inadecuada política para el mantenimiento preventivo de los recursos TIC, puede permitir la materialización de riesgos referentes a períodos amplios de acumulación de polvo y suciedad que se adhiere a las piezas internas generando posibles daños y fallos en los componentes de los equipos informáticos.

CONCLUSIONES

Las tecnologías de información representan una de las herramientas primordiales para la consecución de los objetivos sustantivos planteados por las unidades administrativas financieras de la CCSS. En ese sentido, a través de este estudio, la Auditoría determinó oportunidades de mejora referentes a la gestión de las TIC en la sucursal de Guápiles, las cuales tienen el objetivo de contribuir con la administración activa para mejorar la continuidad en la prestación de los servicios que brinda esta unidad.

En primera instancia, se evidenció que el cuarto donde se albergan los servidores y el switch de comunicaciones presenta condiciones inadecuadas de espacio físico para el resguardo de los mismos, situación que podría afectar la continuidad en la prestación de los servicios que brinda la Sucursal, los cuales son necesarios para la ejecución eficaz y eficiente de las funciones encomendadas a esta unidad administrativa financiera.

Respecto a la red de comunicaciones de área local se evidenciaron debilidades en el cableado estructurado, situación que eventualmente podría originar problemas de conectividad, además, se podrían materializar riesgos correspondientes a la disponibilidad de los sistemas y procesos críticos de la sucursal.

Por otra parte, en relación con los equipos informáticos que funcionan como servidores de archivos y bases de datos, se detectó que uno de ellos fue adquirido hace 14 años y por ende se encuentra 100% depreciado en su valor contable, asimismo, se evidenció obsolescencia respecto al sistema operativo y del motor gestor de base de datos que tiene instalado ya que los mismos fueron descontinuados por el fabricante, pese a esto, el activo sigue siendo utilizado para almacenar las bases de datos de aplicaciones críticas como el SPIC. La situación descrita puede provocar vulnerabilidades de seguridad en el sistema operativo que puedan comprometer la confidencialidad, disponibilidad e integridad de los datos procesados y almacenados en los equipos, sistemas gestores de bases de datos y sus aplicaciones.

En ese mismo orden de ideas, se evidenció que desde hace cinco años ingresó un servidor con mayores capacidades técnicas al mencionado anteriormente, sin embargo, no se ha realizado el traslado de las bases de datos del SPIC y el SICP a este equipo informático, situación que podría estar provocando una sub utilización de ese equipo considerando las necesidades y los niveles de criticidad de las aplicaciones con las que dispone la sucursal, en ese sentido, dicho activo funciona únicamente como un servidor de respaldo de documentos y no como un equipo que almacena bases de datos de carácter crítico para esta unidad administrativa financiera. Lo anterior puede materializar riesgos referentes al adecuado aprovechamiento de las inversiones en Tecnologías de Información y Comunicaciones realizadas por esta Sucursal.

En relación con los sistemas de alimentación ininterrumpida, se evidenciaron debilidades referentes a la obsolescencia tecnológica, su funcionamiento y su estado físico. La situación detectada puede comprometer la continuidad en la prestación de los servicios de tecnologías de información y comunicaciones, lo anterior debido a fallas eléctricas que se pueden presentar a causa de su obsolescencia y que eventualmente aumenta el riesgo de un fallo en su funcionamiento, desprotegiendo los demás equipos informáticos que están conectados.

Además, se detectaron debilidades en los niveles de seguridad utilizados para acceder desde la red de datos a la información digital almacenada en los equipos de cómputo y servidores de la Sucursal de Guápiles, lo cual compromete la disponibilidad de la información que utilizan los funcionarios para el desempeño de sus labores volviendo susceptible el riesgo de ataques tales como: infecciones, exposición de información Institucional o la eliminación de archivos sin poder definir responsabilidades.

Finalmente, se determinaron oportunidades de mejora en el plan de mantenimiento preventivo, lo anterior referente al respaldo documental y el registro de las tareas y procedimientos a realizar, así como los responsables de su ejecución. En ese sentido, lo detectado disminuye la posibilidad de tener mecanismos de control que permitan comprobar las condiciones reales de los equipos TIC, así como garantizar la ejecución de tareas periódicas de reparación, limpieza y configuración de estaciones de trabajo u otros activos informáticos.

En síntesis, esta Auditoría propone una serie de recomendaciones a la administración activa, con el fin de solventar las oportunidades de mejora identificadas en la evaluación integral gerencial de la Sucursal de Guápiles, específicamente en la gestión de tecnologías de información y comunicaciones.

RECOMENDACIONES

A LA GERENCIA FINANCIERA

1. Considerando que la recomendación 1 del informe ATIC-208-2015 realizado en la Sucursal de San Ramón, referente al tema sobre red de comunicaciones de área local y que se aborda en la presente evaluación, ya se emitió a esa Gerencia, integrar dentro de la planificación y estrategia establecida en atención a la misma, las acciones que correspondan con el fin de dotar a la Sucursal de Guápiles de una infraestructura adecuada para las telecomunicaciones, valorando que se contemplen aspectos como la telefonía IP considerando los beneficios de este tipo de tecnología, los costos y las tendencias de la institución en esa materia. **Plazo de la recomendación: 9 meses.**

A LA DIRECCIÓN REGIONAL DE SUCURSALES HUETAR ATLANTICA

2. Basado en los criterios de remplazo establecidos en el documento Institucional Guía para la Evaluación del Reemplazo sobre Activos de TIC y acorde a las posibilidades presupuestarias de la Sucursal de Guápiles, gestionar la adquisición de sistemas de alimentación ininterrumpida (UPS) que permitan sustituir los equipos que ya cumplieron su vida útil, presentando condiciones de deterioro y que por su obsolescencia podrían ocasionar fallos que comprometan la continuidad de los servicios. En ese sentido, se debe establecer un plan donde se identifiquen las prioridades y los niveles de criticidad de los equipos que necesitan ser sustituidos, lo anterior en caso que el proceso deba ser realizado en forma paulatina. **Plazo de la recomendación: 6 meses.**

A LA JEFATURA DE LA SUCURSAL DE GUÁPILES

3. En virtud del hallazgo 2 del presente informe, efectuar las gestiones necesarias y acorde a las posibilidades presupuestarias de esta unidad administrativa financiera, para subsanar los siguientes aspectos:

3.1 Resolver el traslado del mueble de madera con puertas de vidrio que almacena papeles, documentos, cajas de cartón, discos compactos, artefactos electrónicos, entre otros, así como los equipos informáticos en desuso que se encuentran en el cuarto de servidores.

3.2 Dotar de un rack[2] para el montaje de los servidores y el switch de comunicaciones que posee la sucursal y que permita realizar una adecuada distribución del espacio físico asignado.

Lo anterior, con las coordinaciones que sea necesario establecer con la Dirección Regional de Sucursales Huetar Atlántica.**Plazo de la recomendación: 6 meses.**

4. En coordinación con el encargado de informática de la Sucursal de Guápiles y el CGI de la Dirección Regional de Sucursales, establecer un plan con plazos, responsables y actividades, orientados a migrar las bases de datos a versiones superiores, así como trasladar los respaldos y demás información que almacena el activo número 555906 al servidor con la placa 799896, el cual de acuerdo con lo evidenciado en el hallazgo 3.2 de este informe, dispone de las especificaciones técnicas requeridas para almacenar bases de datos, respaldos de información y documentos digitales. En ese sentido, posterior a la migración se debe actualizar el Plan de Continuidad en TIC con el fin de indicar que el activo donde se resguardan las bases de datos es un equipo informático con nivel de criticidad alta, además, lo correspondiente en la parte de inventario de equipos, los procedimientos y estrategias de recuperación de hardware, ensayos u otros aspectos que sean necesarios modificar. Lo anterior de acuerdo a lo evidenciado en el hallazgo 3 de este informe. **Plazo de la recomendación: 3 meses.**

5. En coordinación con el encargado de informática de la Sucursal de Guápiles, planificar la ejecución en las estaciones de trabajo que así lo ameriten, las restricciones adecuadas de seguridad en cuanto acceso al sistema operativo y la información que en ellos se almacena, sean carpetas compartidas u otro tipo de recurso disponible en la red de datos, esto atendiendo el punto 5 de este informe y con el fin de cumplir con las mejores prácticas de uso y protección de los equipos de cómputo, así como la información contenida en el mismo, aunado a esto, brindar una capacitación sobre la importancia de aplicar las Políticas y Normas Institucionales de Seguridad Informática de la Institución, dicha capacitación debe documentarse indicando los puntos tratados así como los funcionarios participantes. Lo anterior debe realizarse a los usuarios de la Sucursal que utilicen recursos informáticos en sus labores diarias.**Plazo de la recomendación: 1 mes.**

6. En coordinación con el encargado de informática de la Sucursal de Guápiles, realizar la desinstalación del software gratuito VNC en las estaciones de trabajo que así lo ameriten, y valorar la sustitución del mismo acorde con las herramientas informáticas de control remoto disponibles el listado oficial de software libre y gratuito autorizado por la CCSS V 1.3 o en su defecto utilizar la herramienta de escritorio remoto que disponen los sistemas operativos de Microsoft Windows.**Plazo de la recomendación: 1 mes.**

7. En coordinación con el encargado de informática de la Sucursal de Guápiles, establecer en el plan de mantenimiento preventivo de los equipos informáticos, las actividades a desarrollar, la frecuencia, los usuarios que reciben el servicio, así como la programación y calendarización

[2] Soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones

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

pertinente de acuerdo con la cantidad de estaciones de trabajo y las posibilidades operativos del funcionario responsable de ejecutarlo. Aunado a esto y finalizada la parte técnica del mantenimiento, implementar bitácoras o informes de trabajo sobre los resultados obtenidos durante el proceso de cada mantenimiento realizado, así como las recomendaciones u oportunidades de mejora que sea pertinente señalar a los funcionarios en caso de detectar un inadecuado uso de las estaciones de trabajo.

Del mismo modo, establecer mecanismos de control que permitan verificar la ejecución del plan de mantenimiento preventivo en los equipos informáticos de la Sucursal. **Plazo de la recomendación: 3 meses.**

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, se procedió a comentar los resultados del informe el día 25 de setiembre del 2015 con la el Lic. Efraín Ríos Mata, Jefe de la Sucursal de Guápiles, Sr. Oscar Morera Jiménez, Operador en TIC de la Sucursal de Guápiles y el Ing. Maxie Barthley Martin, CGI de la Dirección Regional de Sucursales Huetar Atlántica. Así mismo, el día 30 de setiembre del 2015, se comentó con el Lic. Danilo Rodas Chaverri, Jefe de la Sub Área de Gestión Administrativa y Logística y el Msc. Alexander Solís Abarca, Jefe del CGI, ambos funcionarios de la Gerencia Financiera.

ÁREA TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIONES

ESTEBAN ZAMORA CHAVES (FIRMA)
Firmado digitalmente por ESTEBAN ZAMORA CHAVES (FIRMA)
Nombre de reconocimiento (DN): serialNumber=CPF-01-1159-0397, sn=ZAMORA CHAVES, givenName=ESTEBAN, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=ESTEBAN ZAMORA CHAVES (FIRMA)
Fecha: 2015.10.07 16:15:25 -06'00'

Lic. Esteban Zamora Chaves
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2015.10.07 16:29:09 -06'00'

Lic. Rafael Herrera Mora
JEFE ÁREA

RAHM/EZCh/lbc

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

ANEXO 1

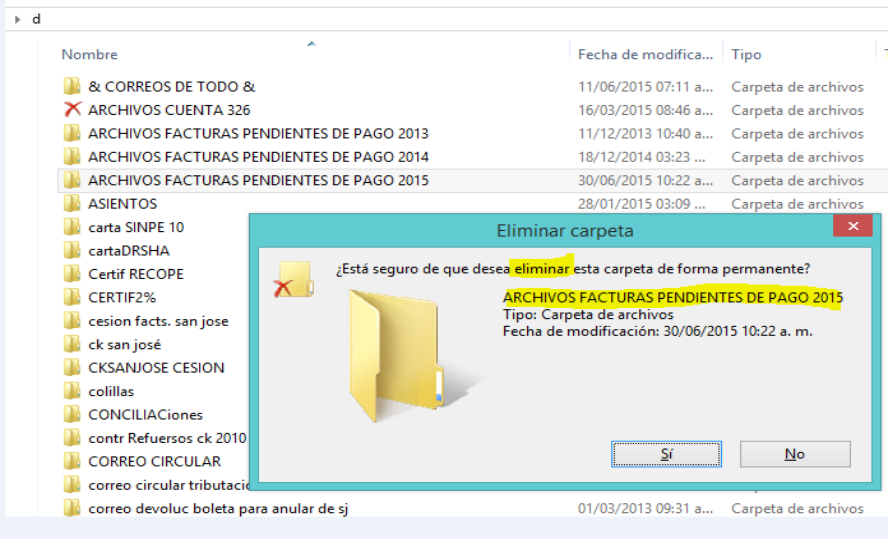
CUADRO N° 5
DEBILIDADES DE SEGURIDAD LÓGICA EN EQUIPOS DE CÓMPUTO
SUCURSAL DE GUÁPILES

Nombre	IP	Presenta debilidades de seguridad Lógica
FINHUADC08	10.12.8.10	SI
FINHUAAPP08	10.12.8.11	SI
1506_345170	10.12.8.32	NO
1506_994192	10.12.8.34	NO
1506_945563	10.12.8.35	SI
1506_785569	10.12.8.38	NO
1506_921811	10.12.8.39	SI
1506_785537	10.12.8.41	NO
1506_837846	10.12.8.42	NO
1506_837858	10.12.8.43	SI
1506_921878	10.12.8.44	NO
1506_667793	10.12.8.45	NO
1506_994155	10.12.8.46	NO
1506_921897	10.12.8.47	NO
1506_921814	10.12.8.49	NO
1506_720777	10.12.8.52	NO
1506_921815	10.12.8.55	SI
1506_994122	10.12.8.56	NO
1506_921896	10.12.8.58	NO
1506_945562	10.12.8.59	NO
1506_921898	10.12.8.60	NO
1506_799853	10.12.8.66	NO

Fuente: *Revisión efectuada por esta Auditoría el 07 de julio del 2015.*

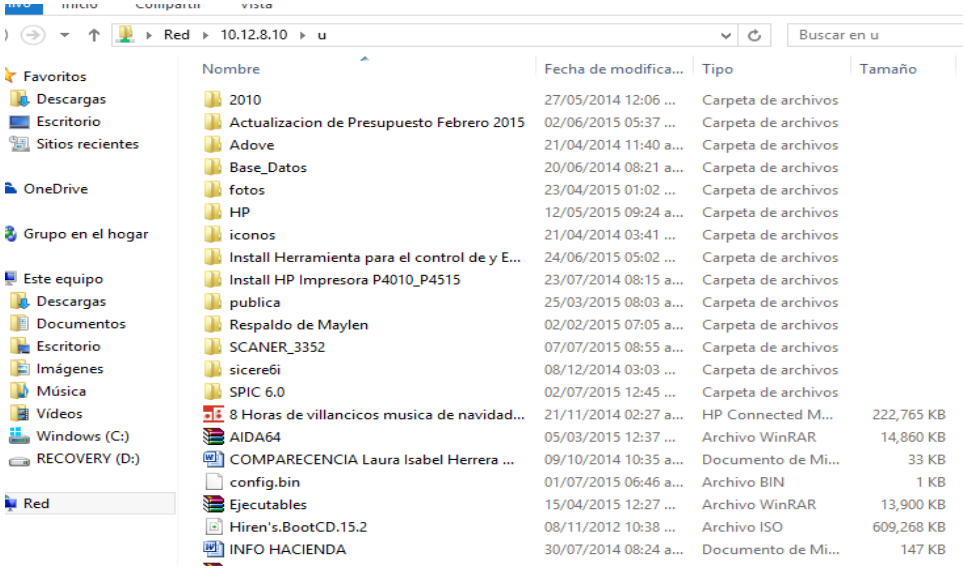
CAJA COSTARRICENSE DE SEGURO SOCIAL
AUDITORIA INTERNA
Tel.: 2539-0821 - Fax.: 2539-0888
Apdo.: 10105

IMAGEN N° 1
POSIBILIDAD DE BORRAR ARCHIVOS EN FORMA MÚLTIPLE.
SUCURSAL DE GUÁPILES



Fuente: *Revisión efectuada por esta Auditoría el 07 de julio del 2015.*

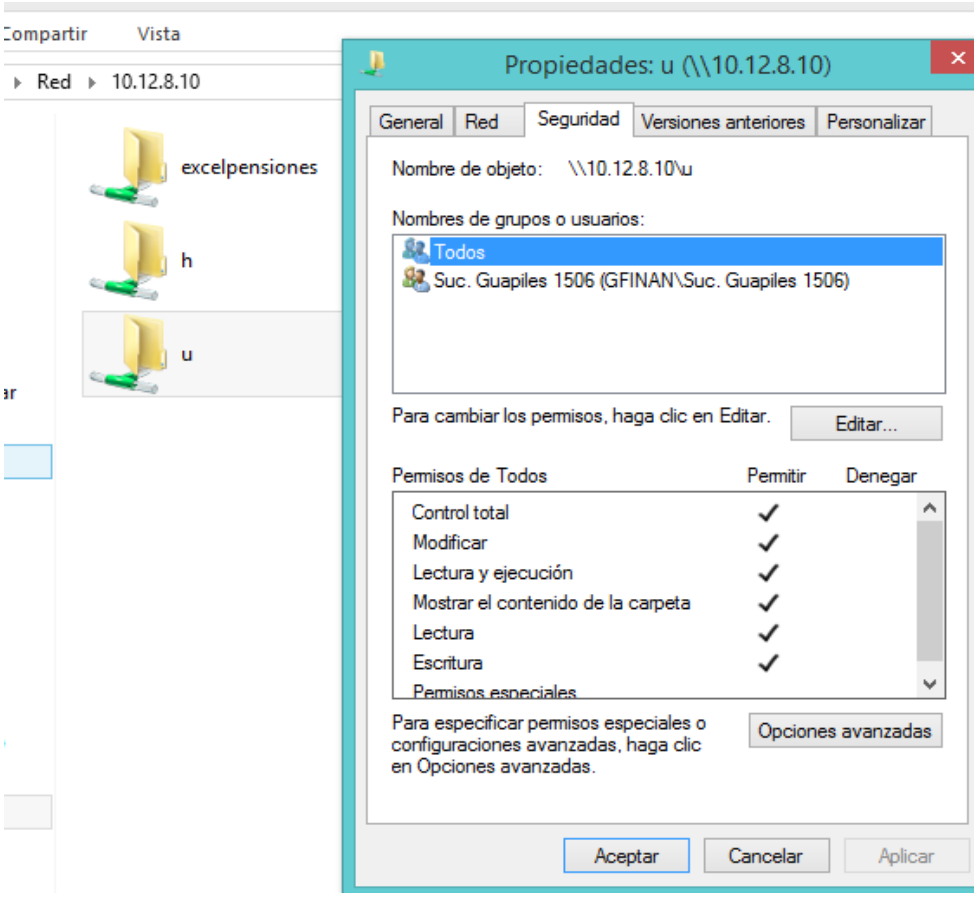
IMAGEN N°2
ACCESO A INFORMACIÓN EN MODO LECTURA Y ESCRITURA
SUCURSAL DE GUÁPILES



Fuente: *Revisión efectuada por esta Auditoría el 07 de julio del 2015.*

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

IMAGEN N°3
NIVEL DE SEGURIDAD "TODOS"
SUCURSAL DE GUÁPILES



***Fuente**: Revisión efectuada por esta Auditoría el 07 de julio del 2015.*