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

ATIC-267-2015
25-09-2015

RESUMEN EJECUTIVO

El presente estudio se realizó según el plan anual operativo 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) del Hospital México"*.

Los resultados han permitido evidenciar que este nosocomio presenta debilidades de control interno en la atención de vulnerabilidades en seguridad lógica y física detectadas en la ejecución del presente estudio, el registro y control de activos y sistemas computacionales.

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

En virtud de lo expuesto, este Órgano de Fiscalización institucional recomienda a la Dirección General, adopten acciones concretas para la atención de las recomendaciones insertas en el presente informe, en congruencia con lo establecido en el marco normativo aplicable.

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

ATIC-267-2015
25-09-2015

ÁREA DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

EVALUACIÓN INTEGRAL GERENCIAL DEL HOSPITAL MÉXICO
TEMA: GESTIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.
HOSPITAL MÉXICO U.P. 2104

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 las tecnologías de información y comunicaciones del Hospital México (CGIHM).

OBJETIVOS ESPECÍFICOS

- Evaluar la suficiencia y oportunidad de la gestión y planificación en Tecnologías de la Información y Comunicaciones del Hospital México, acorde a las actividades sustantivas indicadas en el Modelo de Organización de los Centros de Gestión Informática.

- Evaluar la dependencia de los sistemas de información utilizados en el hospital y las medidas tomadas para garantizar su disponibilidad y continuidad.

- Verificar los controles establecidos por el Centro de Gestión Informática del Hospital México (CGIHM) para la administración del Directorio Activo (AD por sus siglas en ingles)[1]

- Verificar el nivel de obsolescencia tecnológica de los equipos de cómputo, sistemas operativos y gestores de bases de datos del CGIHM.

[1]El Directorio Activo (AD por sus siglas en inglés) es una infraestructura organizada de almacenamiento de datos de usuarios, computadoras, impresoras y otros periféricos y contiene las políticas que definen los derechos que tienen, tanto usuarios como equipos, cuando trabajan en el ámbito del AD.

ALCANCE

El estudio comprende el análisis de las actividades sustantivas del CGI del Hospital México, en concordancia con el Modelo de Organización de los Centros de Gestión Informática, además de otras acciones ejecutadas por el Hospital en materia de Tecnologías de Información y Comunicaciones. El período de la evaluación corresponde de enero 2014 a abril 2015. Aunado a esto, es importante mencionar que este estudio contempló los siguientes temas:

- Seguridad física.
- Seguridad lógica.
- Cumplimiento de las funciones del Modelo de Organización de CGI.
- Revisión del Directorio Activo y consola del System Configuration Manager.
- Obsolescencia tecnológica de los activos de TIC.

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:

- Verificar el apego a las funciones establecidas en el Modelo de Organización de los Centros de Gestión Informática Tipo B.

- Estudio de la plataforma tecnológica existente en el Centro de Gestión Informática (equipo de cómputo y comunicaciones, respaldos, sistemas de información, 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.

- Entrevista y solicitud de información a los funcionarios del Hospital México:

  - ✓ Lic. Adrián Badilla Muñoz, jefe a.i., Unidad de Tecnologías de Información y Comunicaciones.
  - ✓ Licda. Carolina Gallo Chaves, jefe a.i., Oficina Financiero Contable
  - ✓ Lic. Luis Andrey Sánchez Piedra, encargado de activos.
  - ✓ Licda. Vilma Campos Gómez, Directora Administrativa Financiera.
  - ✓ Lic. Reynaldo Mora Araya, jefe, Ingeniería y Mantenimiento.
  - ✓ Ing. Harold Morales Charpantier, Unidad de Tecnologías de Información y Comunicaciones
  - ✓ Ing. Ulises Salazar Bolaños, Unidad de Tecnologías de Información y Comunicaciones

- Revisar muestra de equipos de cómputo y determinar si las carpetas compartidas de los mismos impiden el acceso a usuarios no autorizados.

- Análisis de la base de datos del SCBM (Sistema Control Bienes y Muebles), mediante ejecución de consultas para determinar la vida útil de los equipos de cómputo del Hospital México.

- Revisión y análisis de los usuarios de red, equipos de cómputo y servidores registrados en el directorio activo del Hospital México.

- Inspección física de las instalaciones que comprenden el Centro de Gestión Informática.

- Verificar la vulnerabilidad de los servidores del Hospital México.

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.
- Manual de Organización de Centros de Gestión Informática.
- Lineamientos generales de inventario TIC.
- Estándar técnico contra software malicioso y virus en sus diferentes variantes.
- Guía para la configuración segura de equipos TIC-SEG-004, v.2.0
- Reglamento a la Ley contra la corrupción y el enriquecimiento ilícito en la función pública, Decreto Ejecutivo Nº 32333 del 12 de abril de 2005.

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

El Hospital México fue inaugurado en 1969 (47 años de construido al 2015), dispone de un área de construcción de aproximadamente 21.000 m2; actualmente su categoría es de Hospital Nacional especializado, y está conformado por los Servicios de Medicina General y Especializada, Cirugía, Gineco-Obstetricia y Hemato-Oncología; Servicios de Apoyo (Farmacia, Laboratorio Clínico, Radiología, Trabajo Social, Nutrición, Enfermería, Registro y Estadísticas de Salud) y Servicios Administrativos (Recursos Humanos, Materiales, Financiero Contable, Servicios Generales, Ingeniería y Mantenimiento y Gestión Informática).

Este centro hospitalario está localizado en el distrito de La Uruca, al Oeste de la ciudad de San José, se encuentra entre los principales hospitales del Seguro Social.

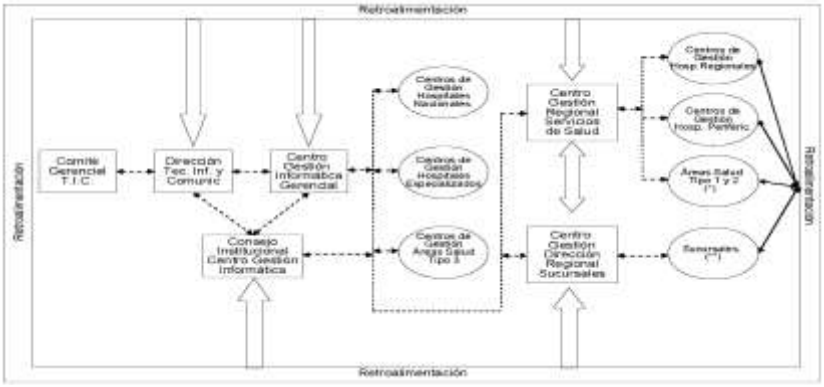
Así mismo, posee todas las Especialidades y Subespecialidades que practican la medicina más avanzada y su estructura física está catalogada como una de las más modernas del área, con un edificio de 7 pisos, donde se ubican todos los Servicios Médicos y Administrativos y una amplia Consulta Externa.

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 31 de enero del 2008, la Junta Directiva, mediante artículo 25º de la sesión Nº 8222 aprobó dicho documento. La Figura Nº 1 refiere el esquema de coordinación establecido según el tipo de Centro y su ámbito de competencia, respecto al Modelo Tipo A (Centros de Gestión Informática Gerenciales) o Tipo B (Centros de Gestión Informática Regionales y Locales). A continuación la figura con el esquema de coordinación de Centros de Gestión Informática:

Figura 1. Esquema de Coordinación Centros de Gestión Informática



Fuente: Modelo de Organización Centros de Gestión Informática, página 80.

Cabe destacar que el Centro de Gestión Informática del Hospital México responde a la estructura organizacional Tipo B.

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 así como el desarrollo de sistemas de información, de acuerdo con las necesidades particulares de cada área, siguiendo los lineamientos establecidos y el 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).

Sobre el Centro de Gestión Informática (CGI).

El Centro de Gestión Informática del Hospital México se encuentra categorizado como un Centro de Gestión Informática Regional y Local Tipo B, por lo que es responsable de mantener en óptimo funcionamiento las bases datos, administrar información operativa, asesorar técnicamente a las unidades de trabajo, mantener una adecuada utilización del equipo de cómputo, materiales y suministros necesarios para ejercer sus labores, del cumplimiento efectivo de los procesos y subprocesos de trabajo que administran la "Gestión Técnica y Soporte Administrativo".

Dentro de su ámbito de acción desarrolla actividades de dirección, planificación, ejecución, coordinación, supervisión y control de actividades profesionales y administrativas en el área de sistemas de información y comunicaciones, y administra proyectos informáticos.

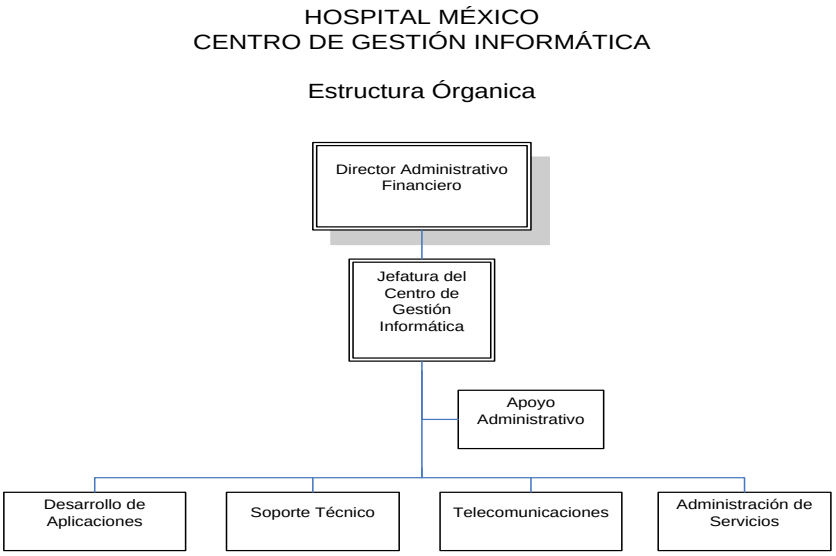
A nivel local se encarga de controlar el cumplimiento efectivo de las políticas, normas y lineamientos establecidos para la operación de los sistemas de información institucionales.

Su objetivo general es brindar un servicio eficiente y oportuno en cuanto a la administración de los sistemas de información y la transmisión de datos, de acuerdo con la tecnología disponible en el centro de trabajo.

- Estructura Orgánica y Funcional

La siguiente figura muestra la Estructura Organizacional y Funcional del Centro de Gestión Informática del Hospital México:

Figura 2. Centro de Gestión Informática



Fuente: Modelo de Organización Centros de Gestión Informática

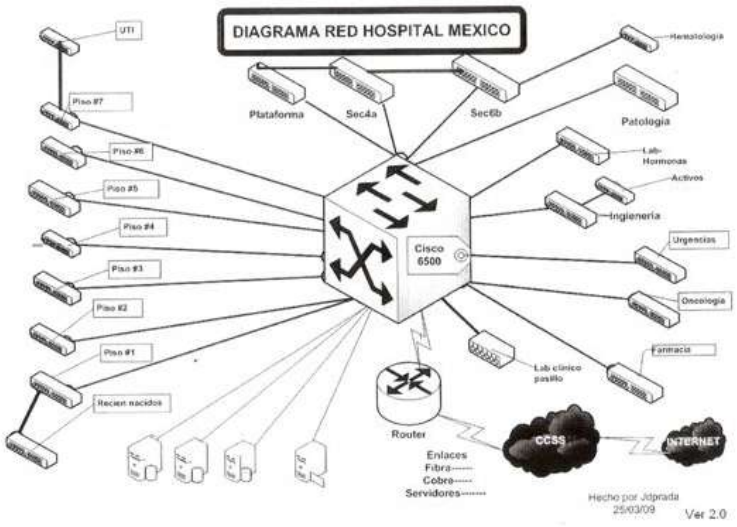
- Recurso Humano

El recurso humano del Centro de Gestión Informática está conformado por un Jefe de Gestión-2 en TIC, cuatro Analistas en Sistemas-2, dos Analistas en Sistemas-1, un Asistente en TIC, dos Técnicos en Mantenimiento-2, cuatro Operadores en TIC y dos Secretarias-2, encargados de la gestión técnica y de soporte administrativo.

- Dotación de equipo

El hospital posee un inventario de 1.729 equipos correspondientes a computadoras, monitores e impresoras. Tiene 663 estaciones de trabajo con un registro de 1.037 usuarios con acceso a la red institucional. La cobertura de conexión se encuentra en un estimado del 98% del total de servicios del hospital. A continuación se presenta el Diagrama de la Red de Conexión del Hospital México:

Ilustración 1 Diagrama de Red Hospital México



Fuente: Centro de Gestión Informática del Hospital México.

HALLAZGOS

1. **EN RELACIÓN A LA SEGURIDAD FÍSICA EN TORNO A LOS CUARTOS DE COMUNICACIONES DEL CGIHM.**

Se constató que el Área de servidores no posee alimentación de corriente eléctrica proveída por dos unidades de corriente ininterrumpida (UPS) las cuales estén en redundancia (si una parte del sistema falla el resto asume el control) una seguida de la otra y a su vez conectada a una planta eléctrica, ofreciendo así disponibilidad principalmente para los equipos de computación de usuarios y servidores.

Así mismo se determinó la inexistencia de cámaras de seguridad controlando el acceso a los equipos de comunicación, además de los siguientes elementos en al menos uno de los cuartos de racks[2] y gabinetes[3]:

- Controles de climatización y humedad.
- Protección eléctrica.

[2] Es un armario, soporte o estructura de metal, en el que se instalan los paneles de parcheo y los equipos activos proveedores de servicios.
[3] Caja de ensamble donde se acomodan todas las partes de la computadora. El gabinete es la parte de un equipo de cómputo que sirve para proteger a todos los componentes internos.

- Protección contra incendios.
- Piso y techo falso.
- Extinguidores de fuego o con revisión periódica desactualizada.

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: (…)*
>
> - *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.*

El Lic. Adrián Badilla Muñoz, Jefe del CGI del Hospital México manifestó lo siguiente:

> *(…) en lo que concierne a la corriente eléctrica del cuarto de servidores es una debilidad que efectivamente tiene que señalarse, nosotros hemos solicitado que se mejore la seguridad en esos aspectos, cabe la aclaración que el CGIHM no es especialista en el tema eléctrico, en ese sentido la solución la debe facilitar un especialista en esa rama, sin embargo, existe una carencia por parte del hospital para mejorar dicha situación, asimismo cabe indicar que a las UPS no se les realiza mantenimiento, lo que podría afectar la prestación del servicio.*
>
> *Respecto a la seguridad si es importante indicar que se poseen controles biométricos de acceso, sin embargo en ocasiones es necesario poseer un sistema de vigilancia y monitoreo 24-7, que permita controlar dentro de la infraestructura el resguardo de la información.*

Que el Centro de Procesamiento de datos o cuarto de racks y gabinetes no posea la seguridad física suficiente lo hace propenso a problemas potenciales de: Infraestructura, electricidad, incendio o inundación, accesos de personas no autorizadas a los cuartos de servidores, entre otros que pueden afectar el adecuado funcionamiento de estos, así como la continuidad del servicio y el deterioro de la imagen pública del hospital.

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

2. SOBRE EL ACCESO A CARPETAS DE ARCHIVOS PERSONALES DE LOS FUNCIONARIOS COMPARTIDAS DEL HOSPITAL MÉXICO.

Esta Auditoría evidenció el acceso mediante la red a carpetas con archivos compartidos sin contraseñas, lo que permite explorar, y manipular su contenido sin dejar evidencia de las acciones realizadas, según se logró determinar en los equipos con las siguientes direcciones IP: 10.81.1.25 / 10.81.1.46 / 10.81.1.176 / 10.81.1.78.

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, señala 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, cita 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:

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

> *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 acceder a 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 Lic. Badilla, expresó lo siguiente:

> *En torno el acceso a carpetas compartidas, se puede revisar, sin embargo con el cambio de dominio a la Gerencia Médica se va a subsanar esta situación, ya que es parte del proceso que se tiene que hacer.*

El acceso mediante la red a carpetas compartidas sin contraseñas permite que usuarios puedan ingresar al equipo remotamente dando la capacidad para copiar, descargar, crear o cargar ficheros nuevos en el equipo, lo que podría originar en desaparición de archivos, fuga de información, carga de virus como troyanos y malware, así como keylogger que dan la posibilidad de almacenar en un archivo las combinaciones de teclas utilizadas por el equipo remoto, y de esta forma obtener acceso a contraseñas e información privada y confidencial.

3. RESPECTO A LA VIGENCIA TECNOLÓGICA DEL SOFTWARE UTILIZADO EN EL HOSPITAL.

Se evidenció que el software utilizado en el Hospital México, específicamente en la gestión de bases de datos y sistemas operativos se encuentra sin soporte técnico por parte de las empresas que los distribuyen, lo cual representa la posible materialización de riesgos relacionados con seguridad informática.

3.1 Sobre el software de gestión de bases de datos SQL Server.

Se determinó que el SQL SERVER en sus versiones 2000, 2005 o 2008 (ver tabla 1), herramienta que es usada para brindar soporte a las bases de datos del hospital, se encuentra en estado de obsolescencia ya que la empresa desarrolladora Microsoft Windows finalizó el soporte a dichas aplicaciones, por lo que no disponen de parches, ni de actualizaciones de seguridad ante las nuevas amenazas informáticas.

Tabla 1. Plataforma Base según servidor

Nombre del equipo	Dirección IP	Plataforma Base	Aplicación
medmexbdd13	10.81.1.33	SQL Server 2000	Sistema Integrado de Farmacia (SIFA)
medmexbdd12	10.81.1.15	SQL Server 2000	Sistema Integrado de Cirugía (SICIR)
medmexbdd12	10.81.1.15	SQL Server 2005 o SQL Server 2008	MEDISYS

Fuente: Planes de Continuidad Hospital México 3 0 (abril, 2012).

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en torno al punto 3.3 Implementación de la infraestructura tecnológica, indica:

> *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.*

El Lic. Badilla, comentó lo siguiente:

> *En lo que respecta al software para la gestión de base de datos obsoleto, tenemos un DBA experto que se encarga de revisar si los sistemas se encuentran actualizados con sus respectivos parches, cabe resaltar que para el sistema SIFA y el SIHOMEX si se tiene una base de datos en SQL 2000 ya que si se actualiza puede presentar problemas de compatibilidad.*

Que el software para la gestión de base de datos a saber SQL SERVER en sus versiones 2000, 2005 o 2008 utilizadas en los servidores del CGIHM se encuentra en estado de obsolescencia, compromete la seguridad de la información de los datos almacenados al no disponer de las últimas actualizaciones que facilita Microsoft, por lo anterior se incrementa el riesgo a incidencias graves en torno a la seguridad.

3.2 Respecto del Sistema Operativo que soporta las aplicaciones del SIFA, SICIR y Medisys.

Se identificó que el sistema operativo utilizado en el cual opera el Sistema Integrado de Farmacia (SIFA), Sistema de Cirugías (SICIR) y el Medisys, es Windows Server 2003, sin embargo su soporte técnico por parte de Microsoft finalizó el 13 de julio de 2010, y además su servicio de asistencia extendida finalizará el 14 de julio de 2015, situación de la cual el CGI del Hospital no ha efectuado acciones concretas para su abordaje.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, respecto al punto 3.3 Implementación de la infraestructura tecnológica, señala:

> *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.*

En ese sentido el Lic. Adrián Badilla, manifestó lo siguiente:

> *Según lo anterior, la situación señalada se presenta con la plataforma Windows Server 2003, esta no se puede actualizar por situaciones de compatibilidad con el sistema SIFA y el sistema de admisión del Medisys, este último se va a corregir en el momento en que se implemente el ARCA.*

Que la plataforma base la cual soporta los servidores del CGIHM, Windows Server 2003 no posea un plan para actualizar o migrar representa un grave riesgo respecto a violaciones en torno a la protección de datos, asimismo que no se pueda actualizar el sistema operativo de los servidores puede denotar en una vulnerabilidad para toda la infraestructura informática del Hospital, además de aumento de costos de mantenimiento, brechas de seguridad y falta de nuevas funcionalidades que ofrezcan confiabilidad, seguridad y disponibilidad al servidor.

4. EN TORNO A LA ADMINISTRACIÓN DEL ACTIVE DIRECTORY

Se determinó que 975 usuarios en el Active Directory, no han efectuado inicio de sesión en la computadora en más de 60 días, además, cabe resaltar las siguientes situaciones:

- 539 usuarios no han hecho inicio de sesión desde que se les creo el usuario.
- 587 usuarios se encuentran laborando en una unidad ejecutora diferente a la 2104.
- 55 usuarios se crearon con cuentas generales, lo que impide identificar al responsable de dicho perfil.

La Ley General de Control Interno N° 8292 del 31 de julio 2002, en su Artículo 8 sobre el Concepto de Sistema de Control Interno en sus incisos c determinan lo siguiente:

> *c) Garantizar eficiencia y eficacia de las operaciones.*

Las Normas Técnicas para la Gestión y Control de las Tecnologías de Información, en su Capítulo 1 Normas de Aplicación General en el apartado 1.4.5 Control de Acceso, establecen:

> *La organización debe garantizar, de manera razonable, la confidencialidad, integridad y disponibilidad de la información, lo que implica protegerla contra uso, divulgación o modificación no autorizados, daño o pérdida u otros factores disfuncionales.*

Para ello debe documentar e implementar una política de seguridad de la información y los procedimientos correspondientes, asignar los recursos necesarios para lograr los niveles de seguridad requeridos (…)

Además, dichas Normas en el apartado 1.4.5 Control de Acceso, señalan:

La organización debe proteger la información de accesos no autorizados.
Para dicho propósito debe:

d. Establecer procedimientos para la definición de perfiles, roles y niveles de privilegio, y para la identificación y autenticación para el acceso a la información, tanto para usuarios como para recursos de TI.

e. Asignar los derechos de acceso a los usuarios de los recursos de TI, de conformidad con las políticas de la organización bajo el principio de necesidad de saber o menor privilegio. Los propietarios de la información son responsables de definir quiénes tienen acceso a la información y con qué limitaciones o restricciones.

En relación a lo anterior, el Lic. Badilla, manifestó lo siguiente:

En relación a las cuentas de usuario en el Active Directory, respectos a los usuarios genéricos se podrían utilizar asociado a algún servicio de los sistemas de información, también es utilizado en los diferentes servicios del hospital en los que el personal no es fijo, esto por cuanto el personal en muchas áreas por lo general rota, asimismo es responsabilidad del jefe de servicio indicar cuando un usuario ya no necesita ingresar a la aplicación, por ejemplo cuando se pensiona, se traslada a otra unidad, pero si es responsabilidad del jefe de servicio hacer la indicación.

La inadecuada gestión de los usuarios de red registrados en el directorio activo debilita la administración y exploración en cuanto al uso de las cuentas de red institucional que utilizan los funcionarios que laboran en este Centro de Salud, aunado a lo anterior, la utilización de usuarios de red sin la responsabilidad directa de un funcionario, puede materializar riesgos de seguridad en cuanto a los controles de acceso y las normas establecidas por la Institución referentes a la seguridad de la Información, integridad, confidencialidad y disponibilidad de la información y recursos informáticos, pudiéndose presentar accesos no autorizados, interrupciones en la continuidad de las operaciones y detrimento en la confiabilidad de los sistemas de apoyo.

5. REFERENTE AL CONTROL DE ACTIVOS EN TIC.

Se evidenció las siguientes inconsistencias en el registro contable de información de los activos TIC del Hospital México realizado en el Sistema para el Control y Gestión de Bienes Muebles (SCBM):

- En revisión del Plan de Continuidad de la Gestión en TIC elaborado por el CGI del Hospital se determinó que los activos indicados en el Anexo 2, se encuentran sin placa.
- De la verificación física efectuada a una muestra de activos TIC de ese centro médico, se comprobó que la computadora placa número 790410, no fue localizada en la ubicación con la que se registró en el SCBM.

Las Normas de Control Interno para el Sector Público, en su punto 4.4.5 sobre las verificaciones y conciliaciones periódicas, estipulan:

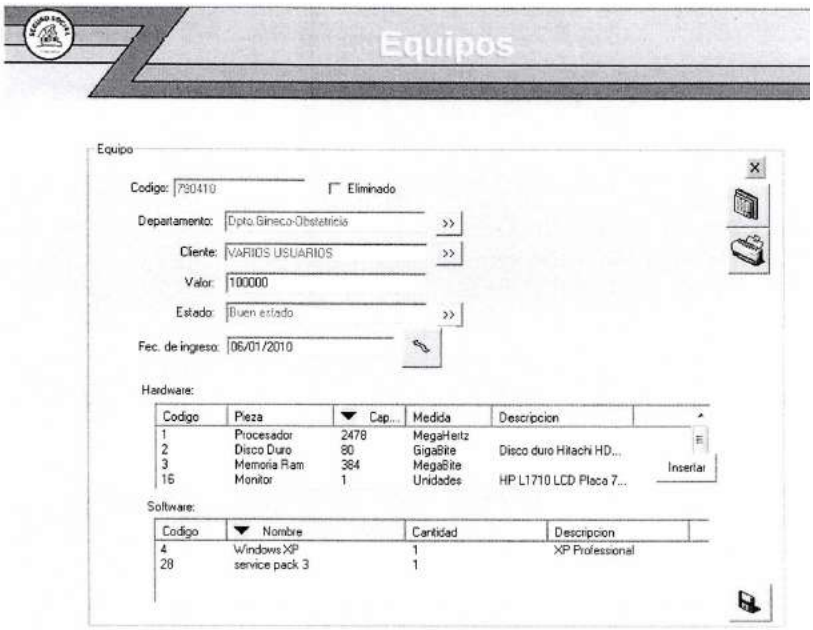
> *La exactitud de los registros sobre activos y pasivos de la institución debe ser comprobada periódicamente mediante las conciliaciones, comprobaciones y otras verificaciones que se definan, incluyendo el cotejo contra documentos fuentes y el recuento físico de activos tales como el mobiliario y equipo, los vehículos, los suministros en bodega u otros, para determinar cualquier diferencia y adoptar las medidas procedentes.*

En ese sentido, el Lic. Badilla Muñoz, señaló lo siguiente:

> *Por lo que refiere al control de activos, en relación a la ausencia de placas es probable que sean equipos de telecomunicaciones antiguos los que presenten esta situación, ya que antes no se les identificaban con una placa, también podría darse que en algún momento se cambió un equipo por garantía o el servicio donó el equipo, sin embargo se tendría que revisar los activos en esa condición, asimismo cabe indicar que el usuario responsable del activo es quien debe velar por su correcto uso y ubicación, según las normas establecidas.*

Al respecto la Dra. Sandra María Vargas responsable del activo placa número 790410, señaló que esté se trasladó para su reparación, sin embargo, en el taller indicaron que se encuentra en el departamento de Gineco-Obstetricia, se adjunta imagen facilitada del Sistema Integrado de Gestión de Bienes y Servicios (SIGBS)

Ilustración 2. Información del sistema SIGBS.



Fuente: *Información Sistema Integrado de Gestión de Bienes y Servicios (SIGBS), mayo 2015.*

La presencia de inconsistencias en el registro de información de los activos del CGIHM en torno a los equipos de computación, dificulta la labor de la administración para asignar responsabilidades en caso de extravío o hurto de algún bien, además, este tipo de omisiones van en detrimento de una adecuada presentación de la información financiera, pues no se cuentan con elementos suficientes para obtener certeza razonable sobre la exactitud de las cifras de activo fijo registradas, ni su depreciación.

6. EN TORNO AL PLAN DE CAPACITACIÓN DEL PERSONAL DEL CENTRO DE GESTIÓN DE INFORMACIÓN DEL HOSPITAL MÉXICO.

Se determinó la ausencia de un plan capacitación o cursos especializados para el personal del Centro de Gestión Informática, en torno a avances tecnológicos, manejo de la información y seguridad en la red que permita incrementar los conocimientos de estos. Aunado a lo anterior, es importante indicar que la última actividad de esta índole en la que participaron los funcionarios de informática fue coordinada en noviembre del 2013.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en su punto 2.4 indican:

El jerarca debe asegurar la independencia de la Función de TI respecto de las áreas usuarias y que ésta mantenga la coordinación y comunicación con las demás dependencias tanto internas y como externas.

Además, debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada, suficiente, competente y a la que se le haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones.

Según lo anterior, el Lic. Badilla Muñoz, señaló lo siguiente:

En torno a la capacitaciones, cabe decir que es un tema realmente limitado, lo que se ha hecho en otras ocasiones cuando se adquiere un equipo es solicitar dentro de la compra un apartado de transferencia tecnológica. Por otra parte, se envió el diagnostico de necesidades de capacitación al CENDEISSS, esta indica las necesidades de capacitación por unidad, las cuales se especificaron, sin embargo a la fecha de la presente evaluación no se ha recibido respuesta por parte de dicha entidad.

Que el personal de TI no posea capacitaciones actualizadas en temas de TIC, incide en el conocimiento respecto a nuevas tecnologías de información, deteriora la imagen del personal a identificarse con los objetivos de la organización, asimismo la productividad y la calidad del trabajo.

7. ACERCA DEL RESGUARDO DE CINTAS MAGNÉTICAS EN UNA UBICACIÓN EXTERNA AL HOSPITAL.

Si bien el Hospital México dispone de almacenamiento externo para el resguardo de la información, el mismo se realiza en forma mensual los primeros lunes de cada mes, lo cual podría afectar en la oportunidad con la que se restablezcan los servicios tecnológicos del hospital ante una eventual catástrofe que afecte el almacenamiento de datos principal.

Las Normas técnicas para la gestión y el control de las Tecnologías de Información en su numeral 1.4.4 Seguridad en las operaciones y comunicaciones citan:

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe: a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.
b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.

c. Establecer medidas preventivas, detectivas y correctivas con respecto a software "malicioso" o virus"

Las Normas Institucionales en Tecnologías de Información y Comunicaciones, en su apartado 4.2 Administración y operación de la plataforma tecnológica, señalan lo siguiente:

Las unidades de trabajo de la CCSS que operan TIC, deben mantener respaldos actualizados de los archivos de datos, de los programas y del software de los sistemas, con el propósito de asegurar la prestación de los servicios a los usuarios internos y externos. Deben definir formalmente y efectuar rutinas de respaldo acorde a la Guía para Elaborar Planes de Continuidad de la Gestión TIC emitido por la Subgerencia de Tecnologías de Información y Comunicaciones.

Los medios de respaldo deben mantenerse en un lugar externo al Centro de Operaciones TIC, que cuente con medidas de acceso restringido y controlado.

Se deben establecer los procedimientos de control para los procesos de restauración de datos

Las Normas Institucionales de Seguridad Informática en su apartado 7.10. Normas para la política de realización de respaldos indican que:

Para el respaldo de sistemas y base de datos:

2. Ejecución del plan de recuperación y respaldo de información y atención de eventualidades.
3. Velar por el correcto y seguro almacenamiento de los dispositivos que contienen los datos generados en los respaldos. Llevar un buen control de la existencia de dichos dispositivos, conforme se vayan necesitando.
4. Realizar pruebas periódicas, para verificar que los respaldos se están ejecutando correctamente.

La Guía para la elaboración de respaldos TIC-GPR-0001, en su apartado I Introducción, lo siguiente:

Recuperación rápida y eficiente: Es necesario probar la confiabilidad del sistema de respaldo en la recuperación de la información. Hay sistemas que aparentemente no tienen ninguna falla al generar el respaldo, pero al recuperar los datos simplemente no funciona. Esto depende de la efectividad y calidad del medio utilizado para almacenar el respaldo. Un sistema de respaldo y recuperación de información tiene que ser probado y debe ser eficiente. El hardware y los dispositivos a utilizar deben ser de una marca reconocida, esto como complemento para tener fiabilidad en los respaldos.

Respecto a lo anterior, el Lic. Badilla señaló lo siguiente:

> *En relación a los respaldos el encargado es el Ing. Ronald Sanchez quien dispone de las políticas de respaldo, en este momento se está haciendo la compra de un equipo que permite resguardar la información en un sitio alterno en tiempo real, sin embargo de momento se hace mediante cinta magnética la cual es custodiada por el Banco Nacional, asimismo preocupados por la necesidad de almacenar la información en tiempo real en un sitio alterno al Hospital, se coordinó junto con los CGI`s de los hospitales nacionales realizar un esfuerzo del cual se le planteó la necesidad al nivel central, en lo que respecta la solución está para desarrollarse a largo plazo.*

El no poseer un centro de procesamiento de datos alterno externo al Hospital México para garantizar la continuidad del negocio, se podría materializar que se dé fuga de información de datos críticos a personas no autorizadas, afectación del servicio y daños a la imagen institucional.

8. EN TORNO A LAS VULNERABILIDADES DETECTADAS EN LOS PUERTOS ABIERTOS DE SERVIDORES DEL CGIHM

Se determinó en 8 servidores ubicados en el Hospital México la cantidad de 237 puertos abiertos informáticos y 23 vulnerabilidades asociados a estos, asimismo cabe indicar que en estos servidores se encuentran alojadas 15 aplicaciones informáticas tales como el Medisys, SICIR, entre otros de uso hospitalario (ver tabla 3).

Tabla 2. Puertos abiertos según dirección IP

IP	FUNCIÓN PRINCIPAL	Número de Aplicaciones	Número de Puertos abiertos	Riesgos detectados
10.81.1.151	Data Protector		40	3
10.81.1.12	Servidor SQL / aplicaciones	1	16	1
10.81.1.194	Clúster máquinas virtuales		20	
10.81.1.81	Domain Controller HM		28	
10.81.1.45	Servicios SQL MAIL		16	2
10.81.1.69	Internet Information Services	1	14	4
10.81.1.75	Windows Server Update Services		15	1
10.81.1.30	Servidor SQL	2	16	5
10.81.1.15	Servidor SQL	5	19	1
10.81.1.33	Servidor SQL	1	10	
10.81.1.34	Servidor SQL / Servidor ORACLE	4	43	6
Totales		**15**	**237**	**23**

Fuente: Elaboración propia, 2015.

Para determinar lo anterior se efectuó una prueba de seguridad mediante la utilización del software Nmap (v. 6.47) herramienta de código abierto para la exploración de redes y auditoría de seguridad con el fin de revisar la información acerca de los puertos abiertos, lo cual puede conllevar al acceso de intrusos en el sistema u otros eventuales riesgos. Asimismo, en la tabla 4 se indican los métodos potencialmente riesgosos que se podrían utilizar según el puerto vulnerable.

Tabla 3. Métodos potencialmente riesgosos según puerto

Dirección IP	Puerto	Métodos Potencialmente Riesgoso
10.81.1.151	80/TCP	TRACE
	2376/TCP	PUT, DELETE
	2386/tcp	PUT, DELETE
10.81.1.12	80/TCP	TRACE
10.81.1.45	80/TCP	TRACE
	8080/tcp	TRACE
10.81.1.69	21/tcp	ftp-anon: Anonymous FTP login allowed (FTP code 230)
	25/tcp	This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT
	80/tcp	Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
	8459/tcp	Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
10.81.1.75	80/tcp	Potentially risky methods: TRACE
10.81.1.30	21/tcp	_ftp-anon: Anonymous FTP login allowed (FTP code 230)
	25/tcp	This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH TURN ETRN BDAT VRFY
	80/tcp	Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
	90/tcp	Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH
	8459/tcp	Potentially risky methods: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH

Fuente: Elaboración propia, 2015.

Al respecto, en el anexo 1 de este documento se definen los principales conceptos relacionados con los métodos potencialmente riesgosos.

Las Normas Técnicas para la Gestión de Tecnologías de Información de la Contraloría General de la República, en relación al punto 1.4 gestión de la seguridad de la información, cita:

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

Según lo anterior el Lic. Badilla, indicó:

> *En relación a los puertos abiertos, se había hecho una revisión de políticas para verificar que estén funcionando de acuerdo a las mejores prácticas recomendadas por Microsoft, sin embargo se podría hacer una revisión, creo que muchos de los puertos abiertos se dan ya que cuando se instala los programas estos habilitan los puertos que requieren para operar correctamente, o bien en el momento en que se configuraron los equipos.*

La existencia de 237 puertos abiertos y 23 vulnerabilidades asociados a estos, puede poner en riesgo la seguridad de la información de los servidores, además de causar trafico indeseado al servidor, abrir puertas para que personas no autorizadas puedan acceder a datos restringidos, obtener privilegios y saturar los servicios.

CONCLUSIONES

La gestión tecnológica es un sistema que determina un dominio de prácticas, pero también es un proceso cuya función es la planeación, la organización, la dirección, la ejecución y el control del desarrollo tecnológico en los sistemas de información.

Respecto a la evaluación integral gerencial del Hospital México, que valoró la gestión de Tecnologias de Información y Comunicaciones, evidenció oportunidades de mejora en torno a la seguridad física de manera que se proteja el equipo de amenazas externas y ambientales, además, se garantice la prevención de incidentes eléctricos para asegurar que la energía fluya de forma continua e ininterrumpida en los equipos de cómputo y cuartos de servidores.

Por lo anterior, es necesario reducir el riesgo de acceso no autorizado a la información y proteger contra perdida o daño, asimismo, se pueden requerir controles especiales para prevenir amenazas físicas (cámaras de vigilancia) y salvaguardar los medios de soporte como el suministro electrónico.

Así mismo, se detectaron debilidades en relación al uso de carpetas compartidas sin contraseñas, en ese sentido los permisos deben ser asignados según el tipo de información que se maneje o según el directorio activo, normalmente se recomienda, según las reglas y políticas decidir cuáles son los privilegios que va a manejar un perfil específico.

Sin embargo, es cada vez más clara la necesidad de que se brinde a los usuarios una mayor protección contra el posible mal uso de la información que le compete, sin que esto implique un intento de limitar o restringir los beneficios que pueden aportar las tecnologías de información.

En cuanto a la plataforma base del servidor y el software para la gestión de base de datos, ambos obsoletos es necesario se considere para su reemplazo una investigación minuciosa, que analice los datos, funciones y eventuales riesgos que se podría incurrir para que estos sean mitigados, además de examinar y evaluar cómo se pueden transferir la información resguardada, asimismo es indispensable documentar los procesos que esos sistemas fomentan y los objetivos que ser quieren alcanzar, a fin de que se satisfagan las necesidades y se propicie oportunidades de mejor al hospital.

Por otra parte, la implementación de un directorio activo (Active Directory, en inglés) permite la administración de los recursos, servicios y usuarios de la red de forma centralizada, de manera que permita optimizar el tiempo de respuesta ante cualquier solicitud de soporte ya sea de hardware o de software por parte de los funcionarios, sin embargo durante la presente evaluación se evidenció vulnerabilidades respecto a compartir carpetas con contenido de índole privada, sin los adecuados niveles de seguridad recomendados, por lo esto supone un riesgo para la institución.

También, cabe señalar la importancia que recae en la administración de activos, debido a que esta Auditoría evidenció equipos con faltante de placas, lo que impide sentar responsabilidades sobre los mismos en caso de hurto o daño a los equipos.

En lo que respecta a las capacitaciones se determinó que la ausencia de estas, hace que el personal informático no pueda asumir la actividad de tareas con tecnología más avanzada a la instaurada en el hospital o las realicen con grandes complicaciones e inversiones de tiempo en el análisis de las mismas.

Por lo que refiere al resguardo de la información de los sistemas de información en sitio alterno externo al hospital se constató que no se posee del mismo, esto pone en riesgo de pérdida de información crítica y vulnerable referente a las operaciones del nosocomio.

Con respecto al análisis de vulnerabilidades realizado a los servidores del Hospital México, se detectó que existen puertos de comunicaciones abiertos lo que permite realizar búsquedas de debilidades en los sistemas, mediante la exploración o envió de un amplio número de paquetes de apariencia legítima, quienes tienen como objetivo reducir la disponibilidad de un determinado activo (servidor).

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 del Hospital México, específicamente en la gestión de Tecnologías de Información y Comunicaciones.

RECOMENDACIONES

A LA DIRECCIÓN GENERAL

1. Elaborar un análisis costo-beneficio con el fin de fortalecer la seguridad física del cuarto de comunicación, servidores y gabinetes según lo evidenciado en el hallazgo número uno del presente informe. Dicho análisis deberá contemplar al menos los siguientes aspectos:

    a. Mecanismos de control de accesos.
    b. Procedimiento para el acceso al ambiente físico, en donde se justifique, autorice y monitoree el ingreso a los cuartos de servidores.
    c. Disponer de un reporte de funcionarios, contratistas y terceras personas que ingresen a estos recintos.
    d. Diseñar e implementar medidas de protección contra factores ambientales (incendio, humedad) instalando dispositivos y equipo especializado para monitorear y controlar el ambiente.

    En caso de que sea factible la implementación de estos mecanismos, se deberá definir un plan con responsables, actividades y plazos que permitan fortalecer dichos aspectos de seguridad física.

Adicionalmente, es importante que esa Dirección establezca los mecanismos de control y seguimiento que garanticen el cumplimiento de las actividades.

Plazo de la recomendación: 4 meses.

2. En coordinación con el Área de Ingeniería y Mantenimiento realizar las mejoras y revisiones necesarias en los sistemas de alimentación ininterrumpida (UPS) del Hospital, con el fin de evitar fallos que afecten los equipos de cómputo.

   Así mismo, efectuar un plan de mantenimiento preventivo y correctivo a las UPS, el cual contemple la frecuencia y pruebas periódicas que permitan verificar el correcto funcionamiento de estos equipos, lo anterior deberá coordinarse con los usuarios para evitar cualquier tipo de incidente y de esta forma garantizar la continuidad de los servicios que brinda el centro hospitalario.

Plazo de la recomendación: 4 meses.

3. Planificar la ejecución en las estaciones de trabajo del Hospital México que así lo ameriten, de las restricciones adecuadas de seguridad en torno al 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, según lo señalado en el punto número dos del presente informe, con el fin de velar por el cumplimiento de las mejores prácticas de uso y protección de los equipos de cómputo.

Plazo de la recomendación: 4 meses.

4. Según lo evidenciado por este Ente Fiscalizador en el hallazgo número tres del presente informe se elabore una estrategia que permita mitigar el rezago tecnológico presente en los servidores de gestión de bases de datos SQL Server y Sistema Operativo Windows Server 2003. Dicho análisis deberá contemplar al menos los siguientes aspectos:

   - Pruebas de funcionamiento.
   - Análisis de riesgos a los cuales se podría incurrir para que estos sean mitigados.
   - Seleccionar la mejor alternativa de solución.
   - Planificar la migración de los datos

Plazo de la recomendación: 3 meses.

5. Establecer un procedimiento documentado que defina los lineamientos generales que deben seguir los Jefes de Servicio de los diferentes servicios que conforman el Hospital, para informar al CGI sobre los funcionarios que ya no laboran en este centro médico, se pensionaron u otra

situación que se considere necesaria para suspender o eliminar cuentas de red. Lo anterior con el objetivo de tener una efectiva comunicación que le permita al Centro de Gestión Informática efectuar una adecuada administración de los usuarios de red. Una vez finalizado el documento, se debe remitir a la Dirección General del Hospital para su respectiva valoración, y de esta manera emitir un comunicado a las Jefaturas de Servicio, donde se informe que dicho procedimiento debe ser de acatamiento obligatorio.

Del mismo modo, efectuar las gestiones necesarias para eliminar las cuentas de red sin responsabilidad directa de algún usuario, de funcionarios que ya no trabajan en este centro médico. Además, verificar los usuarios genéricos si están ligados a algún proceso almacenado, entre otras situación relacionadas al Directorio Activo, al fin de subsanar las inconsistencias indicadas en el hallazgo número cuatro de este informe.

Plazo de la recomendación: 3 meses.

6. Actualizar y mantener un repositorio completo de la configuración de los activos, revisarlos periódicamente para verificar y confirmar la integridad de los datos.

   Con relación al activo placa número 790410, se debe identificar de manera formal al propietario o persona responsable de este y verificar su ubicación.

Plazo de la recomendación: 3 meses.

7. Definir un plan de capacitación con temas que requiere el personal en Tecnologías de Información y Comunicación en relación con las posibilidades presupuestarias del hospital, y permitan disponer de una formación especializada en apoyo a la gestión de Seguridad de la Información.

Plazo de la recomendación: 3 meses.

8. Realizar los estudios técnicos, financieros, de factibilidad y de valoración de riesgos necesarios, que conduzcan a establecer una periodicidad menor respecto al resguardo de la información en el sitio alterno, con el propósito de afrontar contingencias y elaborar estrategias de respaldo y recuperación de la información, para garantizar la continuidad de las operaciones y los procesos críticos de este, ante un eventual desastre natural o provocado por el hombre, lo anterior en relación con lo evidenciado en el hallazgo número siete.

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

Plazo de la recomendación: 3 meses.

9. Analizar e implementar las medidas de seguridad que correspondan con el fin de subsanar lo evidenciado en torno a los puertos abiertos en los servidores en relación con lo indicado en el hallazgo número ocho del presente informe, con el fin de mitigar el escaneo de puertos bloqueando servicios y paquetes en la red.

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 10 de setiembre de 2015 con el Dr. Douglas Montero Chacón, Director General y el Lic. Adrián Badilla Muñoz, jefe del Centro de Gestión Informática, ambos del Hospital México, respecto de la recomendación número siete, el Dr. Montero Chacón indicó:

> *"La misma se remita al Centro de Desarrollo Estratégico e Información en Salud y Seguridad Social y no al Hospital México, debido a que ya se hizo la solicitud de las capacitaciones para su personal y se trasladó a dicha unidad; a razón que no tienen autorizado pagar capacitaciones por las políticas de contención del gasto institucional".*

Sin embargo, por la relevancia e impacto del tema, esta Auditoría considera que la misma debe ser liderada por la Dirección General de ese hospital, y que sea éste quien ejecute a lo interno las acciones que estime pertinente para subsanar el tema de las capacitaciones en el Centro de Gestión Informática de este nosocomio.

ÁREA TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES

HUBERT ALBERTO GARCIA GORDON (FIRMA)
Digitally signed by HUBERT ALBERTO GARCIA GORDON (FIRMA)
Date: 2015.10.07 18:25:13 -06'00'

Ing. Hubert García Gordon
ASISTENTE DE AUDITORÍA

RAFAEL ANGEL HERRERA MORA (FIRMA)
Firmado digitalmente por RAFAEL ANGEL HERRERA MORA (FIRMA)
Fecha: 2015.10.07 13:47:26 -06'00'

Lic. Rafael Ángel Herrera Mora
JEFE

RAHM/HGG/lba

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

ANEXO

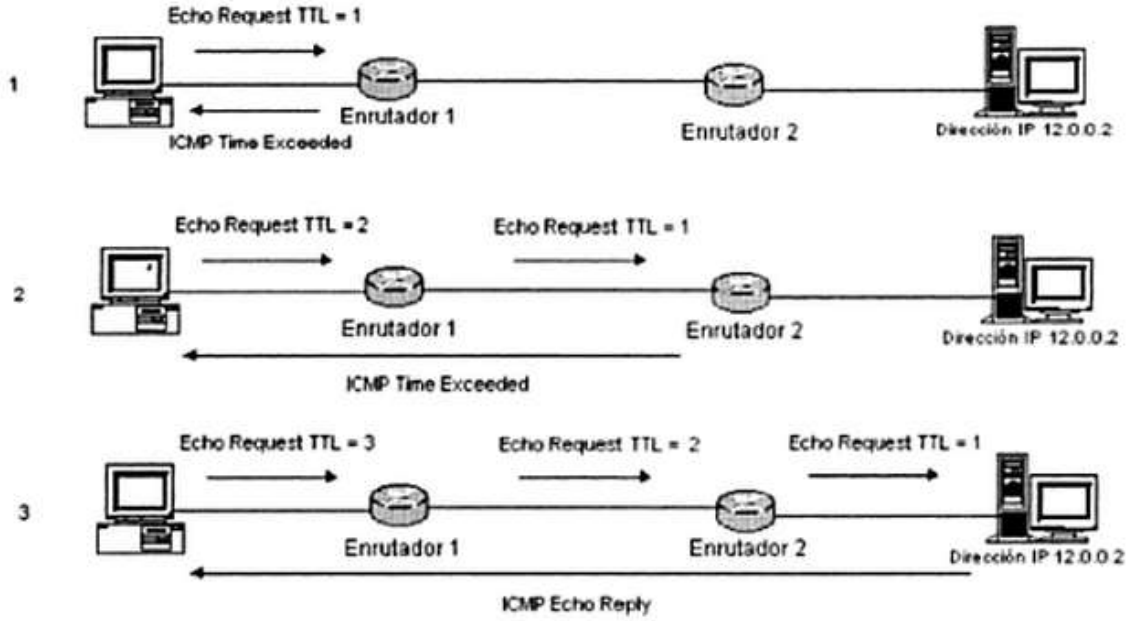
Anexo 1

GLOSARIO

- Método potencialmente riesgoso: TRACE para Philippe Mathon (2004) en su libro *Windows Server 2003. Network infrastructures: preparación para el examen MCSE, MCSA* lo define de la siguiente manera:

Este comando permite indicar la ruta utilizada por los paquetes para lelgar a un destino. El comando tracert envía una sucesión de paquetes ICMP Echo Request con un primer valor de TTL a 1. La estación emisora de los paquetes espera un mensaje ICMP Time exceeded (Tipo 11 código 0 significado TTL=0) para enviar de nuevo un paquete ICMP Request con un TTL valor 2 y así sucesivamente, hasta obtener de la máquina de destino un paquete ICMP Echo Response, según se refleja a continuación.

Ilustración 3. Comando Tracert



Fuente: Windows Server 2003. Network infrastructures: preparación para el examen MCSE, MCSA (2004). Pág. 74

- Método potencialmente riesgoso: PUT, de acuerdo con el Centro de Conocimiento de IBM (IBM Knowledge Center) el presente método se puede definir de la siguiente manera:

  La petición contiene datos y un URL. El servidor proxy almacena los datos en el recurso identificado en el URL. Si el recurso ya existe, PUT lo sustituye con los datos contenidos en la petición. Si el recurso no existe, PUT lo crea y lo llena con los datos contenidos en la petición. Este método se puede manejar a través de conexiones persistentes.

  La habilitación del método PUT permite que los archivos se escriban en Caching Proxy mediante HTTP y FTP. Como PUT permite a los clientes escribir en Caching Proxy, es necesario que utilice las configuraciones de protección de servidor para definir quién puede utilizar PUT y los archivos en los que se puede utilizar PUT.

- Método potencialmente riesgoso: DELETE, asimismo el Centro de Conocimiento de IBM lo define de esta manera:

  El servidor proxy suprime el objeto identificado por el URL. DELETE permite a los clientes borrar los archivos de Caching Proxy. Utilice las configuraciones de protección de servidor para definir quién puede utilizar DELETE y en qué archivos.

- ftp-anon: Anonymous FTP login allowed (FTP code 230): Comprueba si un servidor FTP permite conexiones anónimas. Según Pérez Duran (2012 de la Universidad Francisco de Paula Santander en el Taller de Seguridad Informática[4] indicó que:

  Este servicio FTP permite inicio de sesiones anónimas. Cualquier usuario remoto puede conectarse y autenticarse sin proveer una contraseña o credenciales únicas. Esto permite al usuario acceder a cualquier archivo disponible en el servidor FTP.

- Servidor es compatible con los siguientes comandos: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT.

- Método potencialmente riesgoso: TRACE COPY PROPFIND SEARCH LOCK UNLOCK DELETE PUT MOVE MKCOL PROPPATCH

[4] chrome-extension://gbkeegbaiigmenfmjfclcdgdpimamgkj/views/app.html

Anexo 2

Tabla 4. Tipo de activo por marca y servicio sin número de placa.

Tipo	Marca	Servicio
Análogo	Nortel	Nutrición
Análogo	Nortel	Nutrición
Fax	Samsung	Nutrición
Análogo	Nortel	
Análogo	Nortel	
Análogo	Panasonic	Urgencias
Análogo	Panasonic	Sección 16
Análogo	Siemens	Sección 14
Análogo	LG	Sección 13
Análogo	Panasonic	Sección 13
Análogo	Panasonic	Sección 12
Fax	Sharp	Medicina Nuclear
Análogo	Nortel	Sección 9
Análogo	Panasonic	Jefatura de Sección
Análogo	Sonystar	Recursos Humanos
3800	Nortel	Administración
Mesas Operadoras	Nortel	Administración
	Nortel	Administración
2616	Nortel	Bodega Central Telefónica
Análogo	Siemens	Rayos X
Análogo	Siemens	Rayos X
Fax	Panasonic	Quimica Clinica
Fax	Panasonic	Primer Piso
Análogo	Tatung	Obstetricia
Análogo	Panasonic	Cuarto de residentes
Análogo	General	Sala de operaciones
Análogo	Siemens	Sala de operaciones
Fax	Panasonic	Medicina Interna
Análogo	Panasonic	Cuarto de residentes
Análogo		Cirugía de Tórax
Análogo		Cirugía de Tórax
Fax	Panasonic	Cirugía de Tórax
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Disco	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos

Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
Análogo	Nortel	Cuidados Intensivos
2212	Nortel	Cuidados Intensivos
3903	Nortel	Cuidados Intensivos
3903	Nortel	Cuidados Intensivos
3903	Nortel	Cuidados Intensivos
3903	Nortel	Cuidados Intensivos
3903	Nortel	Cuidados Intensivos
Fax	Panasonic	Clínica del SIDA
Inalámbrico		Laboratorio Serología
Fax	Canon	
Análogo	Panasonic	Dermatología
Fax	Panasonic	Dermatología
Análogo	Panasonic	Dermatología
Fax	Sharp	Biblioteca
Análogo	Panasonic	Ingeniería
Análogo	Panasonic	Banco Oxígeno
Análogo	Nortel	Bodega de Materiales
medmexrac01	Data Protector	Servidor
Apolo	Servidor SQL Servidor Aplicaciones	Servidor
webserver03	Internet Information Services	Servidor
medmexdc02	Domain Controller HM	Servidor
medmexdc01	Domain Controller CCSS	Servidor
webserver02	Internet Information Services	Servidor
Servertess	Cubos OLAP Medisys	Servidor
medmexsql02	Servicios SQLMAIL	Servidor
medmexdc03	Domain Controller HM	Servidor
Webserver	Internet Information Services	Servidor
Medmexwsus	Windows Server Update Services	Servidor
medmexsql01	Servicios SQLMAIL	Servidor
medmexdes01	Servidor de Pruebas	Servidor
medmexdc04	Domain Controller HM	Servidor
medmexbdd13	Servidor SQL	Servidor

medmexbdd14	Servidor SQL Servidor ORACLE	Servidor
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Plataforma
Impresora		Sección 6A
Impresora		Sección 6A
Impresora		Sección 6A
Impresora		Sección 6A
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Impresora		Sección 5
Monitor		Sección 5
Impresora		Farmacia Oncología
Impresora		Farmacia Oncología
Impresora		Sección 4B
Impresora		Sección 4B
Impresora		Sección 4B
Impresora		Sección 4B
Impresora		Sección 4B
Impresora		Sección 4
Impresora		Sección 4
Impresora		Sección 3A
Impresora		Sección 3A
Impresora		Sección 2B
Impresora		Sección 2B
Impresora		Sección 2B
Impresora		Sección 2B
Impresora		Sección 2A
Impresora		Sección 2A
Impresora		Sección 2A

Impresora	Sección 1B
Impresora	Sección 1B
Impresora	Sección 1B
Impresora	Sección 1B
Impresora	Sección 1B
Impresora	Sección 1B
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Sección 1A
Impresora	Neurología
Impresora	Neurología
Impresora	Archivo Clínico
Impresora	Archivo Clínico
Impresora	Archivo Clínico
Impresora	Archivo Clínico
Impresora	Archivo Clínico
Impresora	Archivo Clínico
Impresora	Jefatura de Consulta Externa
Impresora	Jefatura de Consulta Externa
Impresora	Jefatura de Consulta Externa
Impresora	Jefatura de Consulta Externa
Monitor	Jefatura de Consulta Externa
Impresora	Validación de Derechos
Impresora	Contraloría de Servicios

Fuente: Planes de Continuidad Hospital México 3 0 (abril, 2012).