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

AGO-172-2015
03-08-2015

RESUMEN EJECUTIVO

El presente estudio se realizó según el Plan Anual Operativo del Área de Auditoría de Gestión Operativa, con el fin de analizar la funcionalidad y utilización de los sistemas de información en uso en el Hospital Dr. Tony Facio Castro.

Como resultado de la evaluación se determinó la existencia de debilidades respecto a la administración de las contraseñas de acceso a los sistemas por parte de los usuarios autorizados; tales como mantenerla escrita y guardarla en lugares de fácil acceso para terceros (gafetes, debajo de teclados o pegada en el escritorio), además de elevar la vulnerabilidad de estos elementos de control al utilizar en su conformación elementos de relativamente fácil acceso a terceros como lo son: combinaciones de nombres de familiares o allegados, fechas relevantes, años de nacimiento de hijos, por ejemplo.

Finalmente, se evidencia la eventual inexistencia de regulaciones definidas respecto a cuales funcionarios pueden acceder a la información en forma de reportes que se generan en los diversos sistemas que se utilizan en las funciones diarias de ese centro de salud.

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

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

AGO-172-2015
03-08-2015

ÁREA GESTIÓN OPERATIVA

EVALUACIÓN REFERENTE A LA FUNCIONALIDAD Y USO DE LOS SISTEMAS DE INFORMACIÓN HOSPITALARIOS HOSPITAL DR. TONY FACIO CASTRO U.E 2601

ORIGEN

El presente estudio se realizó en atención al Plan Anual Operativo del Área Gestión Operativa para el año 2015.

OBJETIVO GENERAL

Analizar la funcionalidad y utilización de los sistemas de información en uso en el Hospital Dr. Tony Facio Castro.

OBJETIVOS ESPECÍFICOS

- Verificar que la funcionalidad del software implementado se ajuste a los requerimientos de los usuarios.

- Analizar la frecuencia de incidencias y problemas en la aplicación.

- Verificar la utilidad de la información que se incluye en los Sistemas Hospitalarios.

ALCANCE

El presente estudio comprende la evaluación sobre la funcionalidad y utilización de los sistemas:

- TASK (Control de marcar de entrada y salida de funcionarios)
- SIPAP (Control de Biopsias, Servicio de Patología)
- ADIM (Registro de Disponibilidades Médicas)
- SIGES (Pedidos Electrónicos)
- SIIS (Sistema Integrado de Servicios de Salud)

La evaluación se realizó entre el 26 de marzo 2015 y el 17 de abril 2015, en el Hospital Dr. Tony Facio Castro.

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

METODOLOGÍA

Para la realización del presente estudio se aplicaron los siguientes procedimientos metodológicos:

Entrevista directa a un total de 31 funcionarios, que se distribuyen de la siguiente manera: SIPAT 2, ADIM 4, TASK 4, SIIS 13, SIGES 10 (ver detalle en anexo 1).

MARCO NORMATIVO

- Ley General de Control Interno, 8292. Julio, 2002.
- Normas Técnicas para la Gestión y Control de las Tecnologías de Información, Contraloría General de la Republica.
- Normas Institucionales de Seguridad Informática TIC-ASC-SEG-002.

DISPOSICIONES RELATIVAS A 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 y 38 de la Ley 8292 en lo referente al trámite de nuestras evaluaciones; al igual que sobre las posibles responsabilidades que pueden generarse ,por incurrir en las causales previstas en el artículo 39 del mismo cuerpo normativo, el cual indica en su párrafo primero:

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

HALLAZGOS

1. Sobre las medidas de seguridad en el acceso a los Sistemas Hospitalarios

De conformidad con los resultados de 31 entrevistas aplicas a los usuarios de 5 sistemas en uso en el hospital Dr. Tony Facio Castro, se determinó que al menos 9 usuarios utilizan contraseñas o ejecutan prácticas de administración de la mismas, que debilitan el esquema de seguridad en el acceso a los sistemas institucionales, tales como: combinaciones de iniciales de familiares cercanos (hijos, conyugues, padres), combinaciones de números representativos para el funcionario (edad de familiares, año de nacimiento propia o de familiares), además al menos dos funcionarios tienen su contraseña escrita y guardada en lugares de fácil acceso (porta gafete, listado de contraseñas al costado del teclado) como se muestra en la siguiente tabla:

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

Tabla 1
Uso de Contraseñas Inseguras
Hospital Dr. Tony Facio Castro
Abril 2014

Nombre de Sistema	Proceso que Automatiza	Cantidad de usuarios con contraseñas vulnerables	Observaciones
SIGES	Control de inventarios en bodegas de proveeduría, control de despacho de insumos o consumibles, para departamentos del Hospital, control de bodega de nutrición.	4	En un caso fue generada por el usuario, usa 4 letras iniciales del nombre. Al menos un usuario usa la contraseña anotada en una hoja debajo del teclado, usa iniciales de nombres de familiares. Un usuario utiliza su nombre como contraseña de acceso. Un usuario tiene la contraseña anotada en un papel que resguarda en el porta gafete, además usa las iniciales de familiares.
SIIS	Procesa las actividades del servicio de Consulta Externa, incluyen formación relacionada con agendas médicas, pacientes, diagnostico, entre otras.	5	El usuario la ingresa de forma directa en el sistema. Un usuario indicó que la contraseña de acceso de la asignaron telefónicamente, dos usuarios indicaron que la contraseña les fue asignada verbalmente. Al menos cinco usuarios utilizan actualmente como contraseña nombres y fechas relacionadas a familiares cercanos tales como: el nombre y año de nacimiento de un hijo.

Fuente: *entrevista a usuario de sistema hospitalarios, Hospital Dr. Tony Facio Castro.*

Al respecto las Normas Institucionales de Seguridad Informática TIC-ASC-SEG-002, en su norma 6. Normas para la Política del Control de Acceso a los Recursos Institucionales, indica:

"6.1. Normas para la política correcto uso de contraseñas de parte de los usuarios de red y aplicaciones

ALCANCE

Esta norma aplica a todos los funcionarios de la Institución, que posean cuentas de red y aplicaciones, para el cumplimiento de sus respectivas funciones.

RESPONSABILIDAD

Será responsabilidad de todos los usuarios de la red y aplicaciones de la Institución acatar las normas establecidas en este documento.

NORMA

Todo funcionario de la red institucional y de aplicaciones, que posea una o varias cuentas creadas a su nombre, deberá cumplir con las siguientes normas, que constituyen las mejores prácticas para la manipulación de las contraseñas personales y lo protegerán del hurto y modificación de la información institucional que administra.

(…)

2. La contraseña no deberá compartirse, sin excepción con ninguna otra persona (aunque se trate de la jefatura, un soportista, o compañeros de trabajo), ya que el dueño de la cuenta será el responsable por el uso que se le dé a la misma.

3. El usuario no debe dejar contraseñas escritas en medios o lugares donde puedan ser accesados por terceros (por ejemplo, en una carpeta del escritorio, en la pantalla del equipo, debajo del teclado u otros).
(…)

6. Las contraseñas generadas por los usuarios para su uso en los servicios de red y aplicaciones, deben contener caracteres de al menos (tres) 3 de las siguientes (cuatro) 4 clases:

Clase	Descripción de la clase
Letras mayúsculas A, B, C, . . . Z.	Letras mayúsculas A, B, C, . . . Z.
Letras minúsculas a, b, c, . . . z.	Letras minúsculas a, b, c, . . . z.
Números 0, 1, 2,. . . 9.	Números 0, 1, 2,. . . 9.
Caracteres especiales: Por ejemplo: Símbolos puntuación ú	Caracteres especiales Por ejemplo: Símbolos puntuación ú
Otros como % & ¡ @ ( ) .	Otros como % & ¡ @ ( ) .

Adicionalmente en el apartado de recomendaciones de la norma citada supra, señala:

" **Paso 7: No Utilice Palabras de Diccionarios, Nombres propios o Palabras Extranjeras**

Como ya se ha mencionado, las herramientas de craqueo de contraseñas son muy efectivas procesando grandes cantidades de letras y combinaciones de números hasta que se halla una contraseña que corresponde, por lo que los usuarios deben evitar usar palabras convencionales como contraseñas. Por la misma razón, también deben evitar palabras regulares con números en el final y palabras convencionales que simplemente son escritas al revés, tal como "nimda", en lugar de "admin". Aunque éstos resultarían difíciles de resolver para las personas, no son ningún reto para las herramientas de ataque de fuerza bruta.

Paso 8: No Utilice Ninguna Información Personal

Uno de las cosas más frustrantes acerca de las contraseñas es que necesitan ser fáciles de recordar para los usuarios. Naturalmente, esto lleva a muchos usuarios a incorporar información personal en sus contraseñas. Sin embargo, es preocupante la facilidad que tienen los "hackers" para obtener información personal acerca de probables objetivos. Por lo que se recomienda fuertemente que los usuarios no incluyan tal información en sus contraseñas. Esto significa que la contraseña no debe incluir nada remotamente relacionado al nombre del usuario, apodo, o el nombre de un familiar o mascota.

También, la contraseña no debe contener cualquier número fácilmente reconocible como números de teléfono o direcciones u otra información que alguien podría suponer viendo su correo.

Paso 9: No escriba la contraseña

Nunca apunte su contraseña; alguien más podría verla.

La utilización de contraseñas donde se utilicen elementos como iniciales o fechas de nacimiento de familiares, letras consecutivas, o nombres de los usuarios, tiene como causa fundamental el desconocimiento y la falta de sensibilización sobre aspectos de seguridad en el acceso a la información que se almacena en los sistemas y bases de datos institucionales.

Entre los aspectos mencionados por los funcionarios del Hospital Dr. Tony Facio Castro, destacan: “Son muchas contraseñas las que hay que recordar”, “como hay que cambiarlas constantemente se me olvida cual es”, “uso mi nombre para recordarlo más fácilmente”, “el nombre de mis hijos no se me olvida”, entre otras.

La situación descrita facilita la eventual intromisión de agentes externos o de accesos no autorizados, a los sistemas institucionales elevando el riesgo que información protegida se vea expuesta de manera irregular.

Aunado a lo anterior se debe mencionar que en la actualidad las organizaciones que se dedican a la sustracción de datos cuentan con herramientas capaces de descifrar contraseñas en pocos segundos, lo que expone a la institución a una eventual sustracción de un activo que se debe considerar de alto valor como es la información que compone sus bases de datos de atención a los asegurados.

Dentro del panorama descrito, la utilización por parte de los usuarios de contraseñas donde se incluyan elementos como su nombre, nombre o iniciales de los hijos o familiares, fechas de nacimiento, números consecutivos, fechas relevantes, o su anotación en hojas que se resguardan en el escritorio o dentro del porta gafetes, son condiciones que deben erradicarse, a efectos de asegurar la seguridad e integridad de los datos que se incluyen o consultan en los sistemas institucionales.

2. Sobre la utilidad de la información incluida en los sistemas hospitalarios.

Como resultado de las entrevistas realizadas a 31 funcionarios con acceso a 5 sistemas de información en uso en el hospital Dr. Tony Facio Castro, se evidenció que para al menos uno de esos sistemas se desconoce la utilidad de la información que se almacena en las bases de datos respectivas, así como de los reportes o informes que se pueden generar. Según se muestra en la siguiente tabla:

Tabla 2
Utilidad de los reportes que generan los sistemas de información
Hospital Dr. Tony Facio Castro
Abril 2014

Sistema	Proceso que automatiza	Reportes que Emite	Uso de los Reportes
TASK (Sistema de control de marcas)	Marcas de entrada y salida de funcionarios.	Listado de marcas de entrada y salida de funcionarios.	Las jefaturas reportan a recursos humanos si existen inconsistencias en las marcas y se procede a los rebajos que correspondan. Además se usa para el pago de tiempos extraordinarios

SIPAP (Sistema de patología)	Permite llevar el control de las biopsias que se realizan en el servicio de patología.	Resultados de biopsias, cantidad de biopsias realizadas por mes por unidad de referencia.	Los resultados de las biopsias son entregadas de forma personal al asegurado. Los reportes de cantidades son enviadas a estadísticas, la administradora del sistema indicó desconocer que uso le dan en esa unidad.
ADIM (Sistema de Disponibilidades Médicas)	Registro de las disponibilidades de los médicos, incluye la información del médico que solicita, quien hace la llamada y del médico que atiende el llamado.	Los usuarios del hospital desconocen la utilidad de la información que se incluye en este sistema, así como los reportes que se emiten.	
SIGES (Pedidos Electrónicos)	Inventarios de suministros y bienes que son adquiridos a nivel local o enviados por el almacén central. Se incluye la solicitud electrónica y los inventarios de bodegas a cargo del servicio de proveeduría.	Existencias de inventario, bodegas con varios rangos. Actas de recepción, vales de entrada, reportes mensuales, costo de almacenables, inventarios. Consumos, entre otros.	Control de inventarios.
SIIS	Agendas médicas en consulta Externa y emergencias	Genera reportes de: cantidad de emergencias atendidas, datos de vigilancia epidemiológica, estadísticas de consulta externa.	Se utiliza como base del boletín estadístico mensual.

Fuente: *Entrevista a usuario de sistema hospitalarios, Hospital Dr. Tony Facio Castro.*

De la información anterior se debe resaltar que aun cuando los sistemas institucionales permiten el acceso una serie de reportes que contienen información relevante respecto a diversos procesos del centro médico, la misma no es analizada sistemáticamente por las jefaturas correspondientes. Merece atención especial el desconocimiento por parte de la Dirección Médica de los alcances del sistema de Disponibilidades (ADIM), el cual eventualmente le permitiría conocer aspectos tales como rendimiento, tiempos de atención de la llamada, entre otros.

Adicionalmente, se desconoce el fin que se da a la información relacionada a reportes estadísticos de áreas como patología, agendas médicas, inventarios, así como de los procesos que permitan asegurar que dicha información es correcta y corresponde efectivamente a lo producido durante el período reportado.

Aunado a lo anterior, se determinó la ausencia de regulaciones respecto a quienes tienen acceso a los reportes que se generan en cada uno de los sistemas evaluados.

Al respecto las Normas Técnicas para la Gestión y Control de las Tecnologías de Información emitidas por la Contraloría General de la Republica, en su capítulo 1 Normas de Aplicación General, señala:

"1.4.4 Seguridad en las Operaciones y Comunicaciones

La organización debe implementar las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información.

Para ello debe:
(…)

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."

Además, en el apartado 14.5 Control de acceso, establece:

"La organización debe proteger la información de accesos no autorizados.

Para dicho propósito debe:
(…)

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

Al respecto del uso de los reportes que se generan en el ADIM (registro de disponibilidades médicas) el Dr. Ho Sai Acón Chan, Director Médico del Hospital Dr. Tony Facio Castro, indicó que desconoce en todos sus extremos el sistema. Además, los usuarios administradores de los sistemas SIGES, Lic. Antonio Gibson Gibson, Jefe de Proveeduría, SIIS, Sra. Marta Salazar Alfaro, Supervisora de Consulta Externa, SIPAT, Sra. Mardley Bustos González, Asistente Administrativa del Servicio de Patología, indicaron desconocer la existencia de regulaciones respecto a quiénes pueden tener acceso a los reportes que se generan en los respectivos programas.

Se debe señalar la información es uno de los activos intangibles más importantes con que cuenta una organización, ciertamente en el caso del Hospital Dr. Tony Facio Castro, no se han establecido al momento de realizar la presente evaluación, los mecanismos de control que permitan regular el acceso a la información que se incluye en los reportes que emiten los sistemas que están en uso en esa unidad, esta situación eleva el riesgo de manipulación inadecuada o ilegal de los datos tanto de los asegurados como de la Institución.

CONCLUSIONES

La contraseña de acceso a un sistema se concibe como un elemento fundamental de la seguridad informática al intentar asegurar por medio de un elemento único e irrepetible que los datos van a ser manipulados por un funcionario que tenga responsabilidades plenamente identificadas respecto al uso y divulgación que se le dará a esa información.

De forma tal que al utilizar contraseñas vulnerables en las que se incluyan por ejemplo: nombre de pila de los usuarios, combinaciones de letras del nombre de los hijos de los usuarios, fechas relevantes, años de nacimiento, entre otros, debilita el control sobre este activo y expone a la institución a eventuales sustracciones o modificaciones no autorizadas de datos.

Ciertamente, la sensibilización y educación de los usuarios en este tema, es un proceso constante que involucra de forma necesaria a los centros de gestión informática locales, así como a los administradores de los sistemas, se debe considerar el establecimiento de un proceso que permita disminuir el riesgo de acceso no autorizados que se produzcan por la utilización de contraseñas con un nivel bajo de seguridad, así como por la utilización de prácticas tales como anotarla en una hoja que se resguarda en el escritorio del funcionario y en el porta gafete.

Aunado a lo anterior, la inexistencia de regulaciones respecto a quiénes pueden acceder a los reportes que generan los diversos sistemas en uso en ese centro médico, permitiría eventuales sustracciones o perdidas de la información que permite establecer entre otros elementos administrativos: niveles de inventarios, agendas médicas, resultados de biopsias, estadísticas de servicios.

RECOMENDACIONES

AL CENTRO DE GESTIÓN INFORMÁTICA DEL HOSPITAL DR. TONY FACIO CASTRO

1. En coordinación con los administradores de los sistemas en uso en ese centro médico proceda a la elaboración y aplicación de un programa de capacitación y sensibilización respecto al uso de contraseñas seguras. Plazo de cumplimiento 1 mes.

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

2. En coordinación con los administradores de los sistemas en uso en ese centro médico proceda a la elaboración y aplicación de los mecanismos de control necesarios para asegurar que los reportes que se generan sean acosados únicamente por aquellos funcionarios que los requieran como parte de sus funciones. Plazo de cumplimiento 3 meses.

COMENTARIO DEL INFORME

De conformidad con lo establecido en el artículo 45 del Reglamento de Organización y Funcionamiento de la Auditoría Interna, los resultados del presente informe se comentaron con la Ing. Ana Vallenas Agüero, Jefe del Centro de Gestión Informática del Hospital Dr. Tony Facio Castro, quien indicó respecto a la recomendación 1: "A los usuarios se las ha dado capacitación constante en ese tema, sin embargo continuaremos con lo recomendado.", y sobre la recomendación 2: " Los administradores son los que tiene el control de los perfiles que se asignan para consulta, pero cumpliremos con lo recomendado".

Adicionalmente se acordó un plazo de cumplimiento de un mes para la recomendación 1 y de tres meses para la recomendación 3.

ÁREA GESTIÓN OPERATIVA

JOSE RAMON HERNANDEZ CORDERO (FIRMA)

Firmado digitalmente por JOSE RAMON HERNANDEZ CORDERO (FIRMA)
Nombre de reconocimiento (DN): serialNumber=CPF-01-0417-1432, sn=HERNANDEZ CORDERO, givenName=JOSE RAMON, c=CR, o=PERSONA FISICA, ou=CIUDADANO, cn=JOSE RAMON HERNANDEZ CORDERO (FIRMA)
Fecha: 2015.08.11 09:41:03 -06'00'

ALEXANDER ARAYA MORA (FIRMA)
2015.08.10 10:21:31 -06'00'

Br. Alexander Araya Mora
ASISTENTE DE AUDITORÍA

Lic. Ramón Hernández Cordero
JEFE DE SUBÁREA

Lic. Edgar Avendaño Marchena
JEFE DE ÁREA

EAM/RHC/AAM/lbc

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

ANEXO 1
FUNCIONARIOS ENTREVISTADOS
POR SISTEMA

SISTEMA	FUNCIONARIO
SIPAT	Sra. Mardley Bustos González, Administradora del Sistema. Sr. Douglas Barrantes, Asistente Técnico en Salud.
ADIM	Sra. Aracelly Pereira Cordero, Jefe Bioestadísticas. Sra. Mishell Arburola Omier, Secretaría de Especialidades Médicas. Sra. Karen Reyes Zamora, Asistente Registros Médicos. Dr. Ho Sai Acón Chan, Directo Médico.
TASK	Licda. Anabell Barrantes Elizondo, Jefe Recursos Humanos. Sra. Roxana Prendigan Prendigan, Secretaria Enfermería. Sra. Katerine Lewis Bolton, Secretaria Enfermería. Sra. Katerine Céspedes Córdoba, Asistente de Gestión, Recursos Humanos.
SIIS	Lic. Teofanis Arceyuth Hernández, Jefe Registros Médicos. Dra. Danisha Sterling Smith, Médico de Apoyo Jefatura Consulta Externa. Sra. Marta Salazar Alfaro, Administradora de Sistema, REDES. Sra. Andrea Gutiérrez Naranjo, Asistente de Redes. Sra. Xinia Jiménez Gaburdi, Asistente de Redes. Sra. Kenly Anderson Cambell, Asistente de Redes. Sra. Yeimi Chávez Joseph, Asistente de Redes. Sra. Lidiett Picado Ramos, Asistente de Redes. Sra. Maylin Portugués Chávez, Asistente de Redes. Sra. Karol Rodríguez Londoño, Asistente de Redes. Sr. Randall Valverde Picado, Asistente de Redes. Sra. Karla Corrales Madrigal, Asistente de Redes. Sra. Irene Amador, Asistente de Redes.
SIGES	Lic. Antonio Gibson Gibson, Jefe Proveeduría. Sr. Jhonny Hernández Vargas, Digitador. Sr. Alexis Gómez Solís, Bodeguero. Sra. Mayela Rodríguez Bolaños, Asistente Nutrición. Sra. Karol Bennet Villiers, Oficinista. Sr. Kevin Rodríguez Gonzales, Bodeguero. Sra. Raquel Rodríguez Ruiz, Secretaria. Sra. Karen Duran Esquivel, Secretaria. Sr. Geovanny Herrera Sanabria, Jefe Proveeduría Farmacia. Sr. Alfredo Ramírez Ramírez, Asistente Técnico.