D y A

CONTRALORÍA GENERAL DEL ESTADO

DIRECCIÓN NACIONAL DE AUDITORÍAS INTERNAS

DNAI-AI-0050-2017

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL IESS

INFORME GENERAL

a la confidencialidad del Sistema de Información Médica AS400

TIPO DE EXAMEN : EE **PERIODO DESDE :** 2014-01-01 **HASTA :** 2016-12-31

INSTITUTO ECUATORIANO DE SEGURIDAD SOCIAL

Examen especial a la confidencialidad del Sistema de Información Médica AS400, por el periodo comprendido entre el 1 de enero de 2014 y el 31 de diciembre de 2016

DIRECCIÓN DE AUDITORIA INTERNA

Quito-Ecuador

RELACION DE SIGLAS Y ABREVIATURAS UTILIZADAS

AI	Auditoría Interna
AS/400	El sistema AS/400 es un equipo de IBM de gama media y alta, para todo tipo de empresas y grandes departamentos. Se trata de un sistema multiusuario, con una interfaz controlada mediante menús y comandos CL (Control Language) intuitivos que utiliza terminales y un sistema operativo basado en objetos y bibliotecas, denominado OS/400.
OS/400 V7R1M0	Sistema Operativo del IBM AS/400
CONTRO	Nombre de programa inicial para menú "*Control General de Sistema*"
C.D	Consejo Directivo
CGTH	Coordinación General de Talento Humano
CGTIC	Coordinación General de Tecnología y Comunicaciones
ENABLED	Activo, habilitado del Sistema Operativo
EGSI	Esquema Gubernamental de Seguridad de la Información
DISABLED	Inactivo, Deshabilitado del Sistema Operativo
DNTI	Dirección Nacional de Tecnología de la Información
HCAM	Hospital Carlos Andrade Marín
HJCA	Hospital José Carrasco Arteaga
HTMC	Hospital Teodoro Maldonado Carbo
IESS	Instituto Ecuatoriano de Seguridad Social
INVCL001	Nombre de programa inicial para menú "*Control General del Sistema de Inventarios*"
MIS	Medical Information System
MEDI11	Nombre de programa inicial para menú "*Sistema de Gestión Hospitalaria*"
ISO/IEC 27002	Estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

QINACTITV	Intervalo tiempo espera en minutos, para el cierre de sesión inactiva
QDSCJOBITV	Tiempo antes de finalizar trabajos desconectados
QSECURITY	Nivel de Seguridad General del Sistema OS/400 V7R1M0
QPWDMAXLEN	Longitud máxima de contraseña
QPWDMINLEN	Longitud mínima de contraseña
QPWDLMTCHR	Limitar caracteres en contraseña
QPWDLMTREP	Límite para caracteres repetidos
QPWDLVL	Nivel de contraseña
QPWDPOSDIF	Límite para posiciones de caracteres en contraseña
QPWDRQDDGT	Dígito requerido en contraseña
QUERY	Consulta que se realiza para extraer información de una base de datos
UATH	Unidad Administrativa de Talento Humano
UM	Unidades Medicas
VPN	Una red privada virtual (RPV), en inglés: Virtual Private Network (VPN) es una tecnología de red de computadoras que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet.
SQL	SQL (por sus siglas en inglés Structured Query Language; en español lenguaje de consulta estructurada)
TI	Tecnología de la Información
TIC	Tecnología de la Información y Comunicaciones
TH	Talento Humano

ÍNDICE

IESS

Ref. Informe aprobado el 2017-12-19

Quito, D.M.

Señores
Presidente y Miembros del Consejo Directivo
Instituto Ecuatoriano de Seguridad Social
Presente

De mi consideración:

La Contraloría General del Estado en uso de sus atribuciones constitucionales y legales, por intermedio de la Unidad de Auditoría Interna del Instituto Ecuatoriano de Seguridad Social, efectuó el examen especial a confidencialidad del Sistema de Información Médica AS400, por el período comprendido entre el 1 de enero de 2014 y el 31 de diciembre de 2016.

La acción de control se efectuó de acuerdo con las Normas Ecuatorianas de Auditoría Gubernamental emitidas por la Contraloría General del Estado. Estas normas requieren que el examen sea planificado y ejecutado para obtener certeza razonable de que la información y la documentación examinada no contiene exposiciones erróneas de carácter significativo, igualmente que las operaciones a las cuales corresponden, se hayan ejecutado de conformidad con las disposiciones legales y reglamentarias vigentes, políticas y demás normas aplicables.

Debido a la naturaleza de la acción de control efectuada, los resultados se encuentran expresados en los comentarios, conclusiones y recomendaciones que constan en el presente informe.

De conformidad con lo dispuesto en el artículo 92 de la Ley Orgánica de la Contraloría General del Estado, las recomendaciones deben ser aplicadas de manera inmediata y con el carácter de obligatorio.

Atentamente,
Dios, Patria y Libertad,

Eco. María Cristina Orbe Cajiao
AUDITOR INTERNO DEL IESS

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

Motivo del examen

El examen especial practicado en el Instituto Ecuatoriano de Seguridad Social se realizó de conformidad a la Orden de Trabajo 0010-IESS-AI-2017 de 14 de febrero de 2017 suscrita por la Auditora Interna del IESS y en cumplimiento al Plan Operativo de Control 2017 de la Unidad de Auditoría Interna del IESS, que fue modificada con oficios 12976-DAI y 13367-DAI de 27 de abril y 3 de mayo de 2017.

Objetivos del examen:

- Identificar los procedimientos de confidencialidad implantados en la administración, operación y uso de claves del Sistema de Información Médica AS400.

- Comprobar los procesos establecidos en la solicitud, autorización, otorgamiento, manejo y retiro de claves del Sistema de Información Médica AS400.

- Verificar el cumplimiento de las disposiciones legales, reglamentarias y demás normativa vigente aplicables a la confidencialidad del Sistema de Información Médica AS400.

Alcance del examen

El examen especial se realizó a la confidencialidad del Sistema de Información Médica AS400, por el período comprendido entre el 1 de enero de 2014 y el 31 de diciembre de 2016.

El análisis comprendió los procedimientos de control implementados en los procesos de administración, operación y uso del Sistema de Información Médica MIS AS400; así como la comprobación de las características de seguridad del referido sistema y de los procedimientos establecidos para la solicitud, autorización, creación de perfiles, otorgamiento, manejo; bloqueo retiro de claves, y perfiles de usuarios, a fin de

Das

determinar si ofrecen seguridad razonable a las operaciones realizadas en el sistema, en las Unidades Médicas de Nivel III del IESS: Hospital Carlos Andrade Marín, Hospital Teodoro Maldonado Carbo y Hospital José Carrasco Arteaga, durante el período comprendido entre el 1 de enero de 2014 y el 31 de diciembre de 2016.

Base Legal

Con Decreto Supremo 9, de 23 de junio de 1970, publicado en el Registro Oficial 6, de 29 de junio de 1970, se suprimió el Instituto Nacional de Previsión; y, con Decreto 40, de 2 de julio de 1970, se transformó la Caja Nacional del Seguro Social en el Instituto Ecuatoriano de Seguridad Social, que continúa vigente con la Ley de Seguridad Social, publicada en Suplemento de Registro Oficial 465 de 30 de noviembre de 2001.

El artículo 16 de la Ley de Seguridad Social estableció la naturaleza jurídica del IESS como una entidad pública descentralizada, creada por la Constitución Política de la República, dotada de autonomía normativa, técnica, administrativa, financiera y presupuestaria, con personería jurídica y patrimonio propio, que tiene por objeto indelegable la prestación del Seguro General Obligatorio en todo el territorio nacional.

La Constitución de la República del Ecuador, publicada en el Registro Oficial 449 de 20 de octubre de 2008, en su artículo 370 establece que el Instituto Ecuatoriano de Seguridad Social, es una entidad autónoma regulada por la Ley, que será responsable de la prestación de las contingencias del seguro universal obligatorio a sus afiliados.

El Consejo Directivo del IESS, con Resolución C.D. 457 de 8 de agosto de 2013, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, estableció la nueva estructura organizacional para la Institución, en la que dividió a las dependencias del IESS en áreas que desarrollan procesos operativos y de apoyo administrativos; y, cambió los nombres a varias dependencias, así por ejemplo a la Dirección de Desarrollo Institucional (DDI), la denominó Dirección Nacional de Tecnología de la Información (DNTI), y la ubicó en la estructura organizacional dentro de los Procesos de Apoyo como parte de la Coordinación General de la Gestión Estratégica; la Dirección del Seguro General de Salud Individual y Familiar bajo la Coordinación General de Prestaciones y las Unidades Médicas y Dispensarios bajo la Dirección General del IESS; reformada con las Resoluciones C.D.483, de 6 de mayo de 2015; en donde se suprimen algunas Coordinaciones, entre ellas la Coordinación

TRES27

General de Prestaciones y la Dirección General de Salud Individual y Familiar pasa a depender directamente del Consejo Directivo del IESS; y con C.D 509 de 18 de febrero de 2016; esta Dirección de nuevo se encuentra bajo la Dirección General del IESS.

Por otra parte, el Consejo Directivo emitió la C.D 468 de 30 de mayo de 2014, en donde se emitió el Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS, en donde entre los órganos de gestión se encontró la Coordinación General de Talento Humano y la Coordinación General de Tecnologías de Información y Comunicación dependiendo de la Gerencia General de la Unidad Médica.

Con Resolución C.D. 535 de 8 de septiembre de 2016, el Consejo Directivo del IESS aprobó la reforma integral al Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social y derogó las Resoluciones C.D 457, C.D 483, C.D. 509 mencionadas en párrafos anteriores, conforme memorando IESS-PCD-0134-ME de 8 de mayo de 2017, del Prosecretario del Consejo Directivo al Director Nacional de Gestión Documental, entro en vigencia el 6 de mayo de 2017; considerando la Dirección Nacional de Tecnología de la Información forma parte de los Procesos Adjetivos de Apoyo a cargo de la Gestión Nacional de Tecnologías de la Información y que cuenta con 4 Subdirecciones Nacionales de: Infraestructura de Tecnología de la Información, de Desarrollo Informático, de Arquitectura y Soluciones, Seguridad Informática; así mismo como parte de los Procesos Sustantivos se encontró a la Dirección del Seguro General de Salud Individual y Familiar; y se agregó como parte de los Procesos Adjetivos de Asesoría del Consejo Directivo al Director Nacional de Riesgos Institucionales; en la que se determinaron atribuciones y responsabilidades para estas dependencias, por lo que las recomendaciones que se emiten en el presente informe van dirigidas a su cumplimiento.

Estructura orgánica

En el ámbito nacional

El Consejo Directivo del IESS, con Resolución C.D. 457 de 8 de agosto de 2013, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, estableció la nueva estructura organizacional para el IESS, en los siguientes términos:

Nivel Directivo: 2. Dirección General

Nivel de Apoyo: 2.4. Coordinación General de Gestión Estratégica

...

2.4.3 Dirección Nacional de Tecnología de la Información

2.2 Coordinación General de Prestaciones

2.2.1 Dirección del Seguro General de Salud Individual y Familiar

Conforme la Resolución emitida por Consejo Directivo C.D. 483 de 13 de abril de 2015, la Dirección del Seguro General de Salud Individual y Familiar, pasó de depender de la Dirección General del IESS al Consejo Directivo del Instituto, según consta en el artículo 5.- de este instrumento. Así también se eliminó entre otras, a la Coordinación General de Prestaciones, establecidas en la Resolución C.D. 457.

Con la Resolución C.D. 509 de 18 de febrero de 2016 se realizó la reforma parcial al Estatuto Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, emitido con Resolución C.D. 457 de 8 de agosto de 2013, en lo referente a la estructura de la Dirección del Seguro General de Salud Individual y Familiar, se conformó por las Subdirecciones de: Aseguramiento del Seguro de Salud, Provisión de Servicios, Garantía de la Calidad de los Servicios de Salud, Vigilancia y Gestión de la Información del Seguro de Salud, Financiera del Seguro de Salud y paso a depender de la Dirección General del IESS.

En el ámbito Nacional:

Nivel Directivo: 2. Dirección General

2.1.1 Gestión del Seguro de Salud Individual y Familiar

Dirección del Seguro General de Salud Individual y Familiar

Cinco

En los Hospitales Nivel III:

El Consejo Directivo del IESS, con Resolución C.D. 468 de 30 de mayo de 2014, expidió el Reglamento Interno para la creación de la nueva estructura de las Unidades Médicas de Nivel III del IESS, con los siguientes niveles:

Nivel Directivo: Gerencia General
Nivel de Apoyo: Coordinación General de Tecnologías de la Información y Comunicación.

Monto de recursos examinados

Por la naturaleza del examen especial el monto de los recursos financieros a examinar, no aplica.

Servidores relacionados

Anexo 1
Seis

CAPÍTULO II

RESULTADOS DEL EXAMEN

Seguimiento de recomendaciones

Respecto de la confidencialidad del Sistema de Información Médica MIS AS400, la Auditoría Interna del IESS y la Contraloría General del Estado, emitieron 4 recomendaciones constantes en los informes: DAI-AI-0391-2015, DAI-AI-0109-2016 y DADSySS-0058-2016, aprobados el 21 de abril de 2015, 1 de febrero de 2016 y 17 de junio de 2016, respectivamente, las que se encuentran en estado de no cumplidas, según se detalla a continuación:

Informe: DAI-AI-0391-2015 del examen especial ***"a los procesos precontractual, contractual y de ejecución de las adquisiciones de bienes y servicios y gestión de farmacia en el IESS, Hospital Regional José Carrasco Arteaga";*** por el período comprendido entre el 1 de enero de 2010 y el 31 de diciembre de 2013, aprobado el 21 de abril de 2015 y distribuido con memorandos IESS-AI-2015-1806 y 1807-ME de 22 de diciembre de 2015, del cual una no se encuentra cumplida y que se cita a continuación:

> ***"Comentario: No se han definido las competencias en los niveles de acceso al sistema informático de la gestión de Farmacia.-... Recomendación 7. Al Director del Seguro General de Salud Individual y Familiar.-*** *Dispondrá a los Directores Médicos de la Unidades de Salud establezcan, de acuerdo a los niveles de complejidad de las mismas, los niveles de acceso a las funcionalidades del Sistema AS400, considerando que no existan servidores que desempeñen funciones incompatibles relacionadas con la emisión de recetas, su despacho y registro. De no existir las condiciones apropiadas para esta separación de funciones, se deberán implementar procedimientos de supervisión y control oportunos sobre la veracidad de las mismas...".*

Situación actual: No cumplida

La Analista Administrativa de la Coordinación de la Comisión de Seguimiento de Recomendaciones de la Dirección General puso en conocimiento al Director del Hospital José Carrasco Arteaga el memorando IESS-DG-2016-0053-M de 15 de enero

SIETE 24

de 2016, sobre los resultados de este examen especial, para conocimiento e implementación inmediata.

El Director del Seguro General de Salud Individual y Familiar encargado y titular, en funciones desde el 8 de enero de 2016 hasta el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 hasta el 26 julio de 2016, respectivamente, con memorando IESS-DSGSIF-2016-0370-M de 26 de enero de 2016, dispuso a los Directores Médicos y Gerentes Generales de las Unidades Médicas, el cumplimiento de la recomendación a nivel nacional, en los hospitales de tercer nivel Carlos Andrade Marín, Teodoro Maldonado Carbo y José Carrasco Arteaga, determinándose que en estas unidades médicas efectuaron las siguientes acciones:

- En el Hospital Carlos Andrade Marín: el Gerente General del HCAM, del período comprendido entre el 8 de junio de 2015 y 31 de diciembre de 2016, con memorando IESS-HCAM-GG-2016-0133-M de 2 de febrero 2016, dirigido al Director Técnico, Coordinadora General de Diagnóstico y Tratamiento, encargada, Coordinador General de Talento Humano, encargado y Jefe de la Unidad Farmacia Hospitalaria instruyó sobre el cumplimiento de la recomendación 7; para tal efecto, se modificó el acceso a la opción 2 *"Dispensarios Anexos/Subrogados"* del menú de "Despacho de órdenes de farmacia", que corresponde en el sistema al perfil de grupo *"CFARMA"* y programa *"FARM00"*, el cual, fue restringido, mediante la parametrización de las *"opciones asignadas a usuarios"*, en el programa *"CONTROU"*, por consiguiente, en esta Unidad Médica, para hacer uso de la opción "*Dispensarios Anexos/Subrogados*", es necesario contar con la solicitud y autorización de la Jefa de la Unidad de Farmacia Hospitalaria, conforme constó en memorando IESS-CGDT-UFH-2016-0306-M de 5 de febrero de 2016, remitido al Coordinador General de TICs del HCAM, en cumplimiento de esta recomendación.

- En el Hospital Teodoro Maldonado Carbo: el Gerente General del HTMC, encargado, con período de actuación comprendido entre el 17 de julio de 2015 y el 7 de marzo de 2016, con memorando IESS-HTMC-GG-2016-0228-M de 10 de febrero de 2016, informó al Director del Seguro General de Salud Individual y Familiar, encargado, lo siguiente:

  "... Traslado memorando Nro. IESS-HTMC-CGTINFCOM-381-M, enviado por el... Coordinador General de Tecnologías Información y Comunicación, el OCHO

mismo que dando atención al Memorando IESS-DSGSIF-2016-0370 del 26 de enero de 2016; sobre el cumplimiento de la recomendación N°7...- Los auxiliares de Farmacia poseen en el Sistema AS/400 usuarios para realizar gestiones correspondientes a su área: estos usuarios son: Usuario de despacho... CFARMA FARM000...Usuario de bodega INVBODUM INVCL0002...INVCL004...".

La información trasladada, por el Gerente General del Hospital Teodoro Maldonado Carbo, fue de carácter informativo, sin embargo no se realizó un análisis de los accesos asignados a las opciones asignadas a los usuarios de despacho del hospital, que permita determinar la implementación de controles para el caso de servidores que desempeñen funciones incompatibles relacionadas con la emisión de recetas, su despacho y registro, en el Sistema de Información Médica MIS AS400.

- En el Hospital José Carrasco Arteaga: el Gerente General del HJCA, encargado, con período de actuación comprendido entre el 20 de mayo de 2015 y el 29 de abril de 2016, no remitió respuesta al requerimiento realizado el Director del Seguro General de Salud Individual y Familiar, por lo cual el Coordinador de la Comisión de Seguimiento de Recomendaciones y la Directora General del IESS con memorandos: IESS-DG-2016-1499 y 1550-M de 29 de agosto de 2016 y 8 de septiembre de 2016, solicitaron al Gerente General del HJCA, actuante en el período comprendido entre el 2 de mayo de 2016 y el 27 de octubre de 2016, un informe detallado de las actividades ejecutadas para su cumplimiento con plazo hasta el 14 de septiembre de 2016, mismos que se contestaron con memorandos: IESS-HJCA-GG-2016-1721-M, IESS-HJCA-GG-2016-1933-M y como alcance IESS-HJCA-GG-2016-2070-M de 1, 16 y 27 de septiembre de 2016, en los que adjuntó el memorando IESS-HJCA-DT-2016-2452-M de 27 de junio de 2016 del Director Técnico del hospital, remitido al Coordinador de la Comisión de Seguimiento de la Dirección General, que respecto de la recomendación 7, mencionó:

"... Mediante memorando N° IESS-HJCA-DIRTEC-2016-0316-M, del 1 de febrero de 2016,... para dar cumplimiento a la Recomendación Nro. 7 ya mencionada, recomendamos: 1.- La emisión desde la Dirección Médica como autoridad competente, de la disposición para el bloqueo inmediato del acceso al descargo de fármacos de especialidad en el MIS AS400, a médicos generales, basado en el nivel de prescripción establecido en el CNMB. 2.- La emisión desde la Dirección Médica como autoridad competente, de la disposición escrita a los médicos generales, a los que se les ha asignado la

nueve

función de descargo de la medicación continua, esto, con la finalidad de que su actividad en la institución tenga respaldo legal... 4. La emisión desde la Dirección Médica como autoridad competente, de la disposición a la Coordinación General de Hospitalización y Ambulatorio para que, en trabajo conjunto con la Jefatura de Farmacia o su delegado y el Comité de Farmacoterapia, se estructuren perfiles de prescripción que se autorizarán a las diferentes especialidades en Consulta Externa...".

El Gerente General de HJCA del 2 de mayo de 2016 y el 27 de octubre de 2016, no evidenció la supervisión para la ejecución de acciones recomendadas por el Director Técnico del hospital, en cuanto del bloqueo inmediato del acceso al descargo de fármacos de especialidad y la asignación escrita de las funciones de descargo de medicación continua, a los médicos generales.

Por lo expuesto, las actividades efectuadas en las Unidades Médicas no fueron coordinadas para la implementación de restricciones de acceso a las opciones del Sistema de Información Médica MIS AS400, tampoco se efectuó un análisis, que permita la generación de un plan de acción a nivel nacional, pues en los Hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga; existen 21 y 46 usuarios activos que en el sistema tienen perfiles de grupo *"CFARMA"* y programa *"FARM00"*, asignados a los servidores que realizaron tareas de descargo de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"*, que tuvieron habilitada por defecto la opción 2 *"Dispensarios Anexos/ Subrogados"*, para la generación recetas como dispensarios anexos.

Informe: DAI-AI-0109-2016 del examen *especial* ***"a la contratación y pago de prestadores privados por servicios de salud a los afiliados y pensionistas, en la Dirección Provincial del IESS Chimborazo"***, por el período comprendido entre el 1 de enero de 2011 y el 30 de abril de 2015, aprobado el 1 de febrero de 2016 y distribuido con memorandos IESS-AI-2016- 0924-ME y 0925 de 21 de junio de 2016.

"Comentario:Prestadores privados concedieron citas a su propio establecimiento y/o clínica sin conocimiento de la Unidad Provincial de Prestaciones del Seguro de Salud del Chimborazo.- *...* ***Recomendación 5.- A la Directora del Seguro General de Salud Individual y Familiar.-*** *Dictará los lineamientos y políticas para que la Coordinación General de Tecnología de Información y Comunicación del HCAM, limite el uso y acceso al aplicativo informático que tienen los médicos privados como usuarios de la plataforma AS400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente... .-* ***Recomendación 6.- A la Directora del Seguro General de Salud Individual y Familiar.-*** *Solicitará la revisión inmediata del*

Diez a/

aplicativo informático desarrollado en la plataforma AS400, para delimitar el acceso que tiene los prestadores privados para direccionar consultas hacia otra especialidad diferente a la que fue derivado el paciente, así como a sí mismos...".

Situación actual: No cumplidas

El Coordinador de la Comisión de Seguimiento de Recomendaciones de la Dirección General con memorando IESS-DG-2016-1138-M de 1 de julio de 2016, remitió al Director del Seguro General de Salud Individual y Familiar, del período comprendido entre el 8 de enero de 2016 y el 26 de julio de 2016, las recomendaciones 5 y 6 del informe DAI-AI-0109-2016, disponiendo su implementación inmediata.

El Director del Seguro General de Salud Individual y Familiar encargado y titular, en funciones durante el período comprendido el 8 de enero de 2016 y el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 y el 26 julio de 2016, respectivamente; y los Directores del Seguro General de Salud Individual y Familiar encargados, actuantes de los períodos comprendidos entre el 27 de julio de 2016 y el 27 de septiembre de 2016; y, entre el 28 de septiembre de 2016 y el 31 de diciembre de 2016; no dictaron los lineamientos y políticas para que la Coordinación General de Tecnología de Información y Comunicación del HCAM, limite el uso y acceso al aplicativo informático que tienen los médicos privados como usuarios de la plataforma AS/400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente, ni solicitaron la revisión inmediata del aplicativo informático desarrollado en la plataforma AS/400, para delimitar el acceso que tiene los prestadores privados para direccionar consultas hacia otra especialidad diferente a la que fue derivado el paciente, así como a sí mismos.

Informe: DADSySS-0058-2016 del examen especial **"a la contratación y pago a prestadores privados por servicios de salud para los afiliados y pensionistas de la Provincia de Pichincha en la Dirección del Seguro General de Salud Individual y Familiar IESS"**, por el período comprendido entre el 01 de enero de 2012 al 31 de diciembre de 2014 aprobado el 17 de junio de 2016

"Comentario: Prestadores privados acreditados vía web con informe negativo, no fueron suspendidos.- *...* ***Recomendación 8.- A la Director del Seguro General de Salud Individual y Familiar.-*** *Dispondrá al Subdirector Nacional de Garantía de la Calidad de los Servicios del Seguro de Salud, que* once

conjuntamente con el Subdirector Provincial de Prestaciones del Seguro de Salud, Pichincha, realicen controles sobre las acreditaciones realizadas vía web, con el fin de que estos prestadores culminen con el proceso de acreditación y que se deshabiliten del sistema AS-400 a los prestadores que no cumplan con los requisitos establecidos en la normativa vigente, en conocimiento del Director del Seguro General de Salud Individual y Familiar".

Situación actual: No cumplida

El Coordinador de la Comisión de Seguimiento de Recomendaciones de la Dirección General con memorando IESS-DG-2016-1320-M de 29 de julio de 2016, remitió al Director del Seguro General de Salud Individual y Familiar encargado del período comprendido entre el 27 de julio de 2016 y el 27 de septiembre de 2016, la recomendación 8 del informe DADSySS-0058-2016, disponiendo su implementación inmediata y solicitó se comunique documentadamente su avance.

El Director del Seguro General de Salud Individual y Familiar encargado del período comprendido entre el 27 de julio de 2016 y el 27 de septiembre de 2016, con memorando IESS-DSGIF-2016-2709-M de 3 de agosto de 2016, dispuso a los siguientes servidores: Subdirector Nacional de Garantía de la Calidad de los Servicios de Salud, Subdirector Nacional de Aseguramiento del Seguro de Salud y Subdirectora Provincial de Prestaciones del Seguro de Salud Pichincha, encargada, el cumplimiento de la recomendación 8 y solicitó que en el plazo de 5 días se remita la documentación de su implementación.

Al respecto, la Subdirectora Provincial de Prestaciones del Seguro Salud Pichincha, encargada con período de actuación comprendido entre el 1 de enero de 2016 y el 16 de septiembre de 2016, con memorandos IESS-SDPSSP-2016-8024-M y IESS-SDPSSP-2016-8106 de 4 y 5 de agosto de 2016, remitió al Subdirector Nacional de Garantía de la Calidad de los Servicios del Seguro de Salud con período de actuación comprendido entre el 18 de abril de 2016 y el 6 de octubre de 2016, el listado de Prestadores Externos activos a los cuales se realizó la acreditación vía web.

El Coordinador de la Comisión de Seguimiento de Recomendaciones de la Dirección General con memorando: IESS-DG-2016-2059-M de 8 de noviembre de 2016, insistió al Director del Seguro General de Salud Individual y Familiar del período comprendido entre el 28 de septiembre de 2016 y el 31 de diciembre de 2016, de cumplimiento a la

Doc 6

recomendación 8 del Informe DADSySS-0058-2016, solicitó que se tome en consideración la posible existencia de recomendaciones no aplicables, como por ejemplo al presentarse *"Cambio de Normativa"*, en las que se debía justificar documentadamente la no aplicabilidad, para el respectivo análisis; sin embargo, no se evidenció la respuesta a este pedido ni las acciones adoptadas para realizar la inactivación de los prestadores que no cumplieron los requisitos.

El equipo de auditoría solicitó con memorandos IESS-AI-2017-0411-ME y IESS-AI-2017-0461-ME de 16 y 24 de marzo de 2017, al Subdirector Nacional de Garantía de la Calidad de los Servicios del Seguro Salud, por el período comprendido entre el 13 de octubre de 2016 y el 31 de diciembre de 2016, información al respecto del cumplimiento de la recomendación 8, sin embargo, en las contestaciones realizadas con memorandos IESS-SNGCSSS-2017-0263 y 303-M de 21 de marzo y 3 de abril de 2017, hizo referencia a la existencia de un cambio de normativa con Acuerdo Ministerial 5310 de 15 de diciembre de 2015 del Ministerio de Salud Pública, no obstante, no evidenció las acciones realizadas que permitan la implementación de la recomendación número 8, por lo que las inobservancias persisten; sin que se identifiquen a los prestadores de salud que no cumplieron los requisitos establecidos en la normativa vigente, tampoco su inactivación del Sistema de Información Médica MIS AS400.

El Acuerdo Ministerial 5310 de 15 de diciembre de 2015 del Ministerio de Salud Pública, determinó un cambio en la normativa del IESS y señaló, que la competencia para la calificación de prestadores externos correspondió a la Autoridad Sanitaria Nacional (Ministerio de Salud Pública), sin embargo, los Subdirectores Nacionales de Garantía de la Calidad de los Servicios del Seguro Salud y los Subdirectores Provinciales de Prestaciones del Seguro de Salud Pichincha, no solicitaron los lineamientos a los Directores del Seguro General de Salud Individual y Familiar, en relación a este cambio, para la ejecución de los procesos de acreditación de prestadores externos y su deshabilitación en el Sistema de Información Médica MIS AS400, en caso de no calificarse, tampoco estos últimos supervisaron el cumplimiento de la recomendación 8.

El Director del Seguro General de Salud Individual y Familiar encargado y Director del Seguro General de Salud Individual y Familiar, en funciones desde el 8 de enero de

TRECE

2016 y el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 y el 26 julio de 2016, respectivamente; no emitió lineamientos, ni supervisó la implementación de las recomendaciones 7, 5, 6 de los informes del DAI-AI-0391-2015, DAI-AI-0109-2016, no dispuso la coordinación de actividades para que en las Unidades Médicas se implementen restricciones de acceso a las opciones del Sistema de Información Médica AS400, tampoco efectuó un análisis, que permita la generación de un plan de acción a nivel nacional, pues en los Hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga; existen 21 y 46 usuarios activos que en el sistema tienen perfiles de grupo *"CFARMA"* y programa *"FARM00"*, asignados a los servidores que realizaron tareas de descargo de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"*, que tuvieron habilitada por defecto la opción 2 *"Dispensarios Anexos/ Subrogados"*, para la generación recetas como dispensarios anexos; ni emitió los lineamientos y políticas para que el Coordinador General de Tecnología de Información y Comunicación del HCAM, limite el uso y acceso al aplicativo informático de los prestadores privados como usuarios de la plataforma AS/400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente, ni solicitó la revisión inmediata del sistema; lo que ocasionó que persistan las debilidades identificadas, incrementando el riesgo de ejecución de funciones incompatibles en el Sistema de Información Médica MIS AS400 tanto para el caso de despacho y prescripción de fármacos en los hospitales, como para el caso de la generación de citas realizadas por prestadores privados del servicio de salud.

Los Directores del Seguro General de Salud Individual y Familiar encargados desde el 27 de julio de 2016 y el 27 de septiembre de 2016; del 28 de septiembre de 2016 y el 31 de diciembre de 2016, respectivamente; no emitieron lineamientos, ni supervisaron la implementación de las recomendaciones 7, 5, 6 y 8 de los informes DAI-AI-0391-2015, DAI-AI-0109-2016 y DADSySS-0058-2016, no dispusieron la coordinación de actividades para que en las Unidades Médicas se implementen restricciones de acceso a las opciones del Sistema de Información Médica MIS AS400, tampoco efectuaron un análisis, que permita la generación de un plan de acción a nivel nacional, pues en los Hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga; existieron 21 y 46 usuarios activos que en el sistema tuvieron perfiles de grupo *"CFARMA"* y programa *"FARM00"*, asignados a los servidores que realizaron tareas de descargo de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"*, que tuvieron habilitada por defecto la opción 2 *"Dispensarios Anexos/ Subrogados"*,

CATORCE

para la generación recetas como dispensarios anexos; ni emitieron los lineamientos y políticas para que el Coordinador General de TIC's del HCAM, limite el uso y acceso al aplicativo informático de los prestadores privados como usuarios de la plataforma AS/400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente, ni solicitaron la revisión inmediata del sistema además, no se deshabilitaron los prestadores externos que no cumplieron los requisitos establecidos en la normativa vigente, lo que ocasionó que persistan las debilidades identificadas e incrementó el riesgo de ejecución de funciones incompatibles en el Sistema de Información Médica MIS AS400 tanto para el caso de despacho y prescripción de fármacos en los hospitales, como para el caso de la generación de citas realizadas por prestadores privados del servicio de salud; y, del acceso no autorizado por parte de prestadores externos no calificados y que no fueron deshabilitados del sistema.

Los citados Directores del Seguro General de Salud Individual y Familiar, inobservaron lo establecido en el artículo 92.- Recomendaciones de auditoría de la Ley Orgánica de la Contraloría General del Estado; y, las Normas de Control Interno 401-03 Supervisión y 600-02 Evaluaciones periódicas.

Los Subdirectores Nacionales de Garantía de la Calidad de los Servicios del Seguro de Salud, titular y encargado, que actuaron durante los períodos comprendidos entre el: 18 de abril de 2016 y el 6 de octubre de 2016; 13 de octubre de 2016 y el 31 de diciembre de 2016; y, los Subdirectores Provinciales de Prestaciones del Seguro Salud Pichincha, por los períodos comprendidos entre el: 1 de enero de 2016 y el 16 de septiembre de 2016; y, el 19 de septiembre de 2016 y el 31 de diciembre de 2016, no solicitaron lineamientos al Director del Seguro General de Salud Individual y Familiar, relacionados con el cambio de las competencias respecto de las acreditaciones de prestadores y consultorios privados según lo dispuesto con Acuerdo Ministerial 5310 de 15 de diciembre de 2015 del Ministerio de Salud Pública, lo que ocasionó que no se deshabiliten del Sistema de Información Médica MIS AS400 a los prestadores de salud que no fueron calificados; incumpliendo lo establecido en el artículo 92.- Recomendaciones de auditoría de la Ley Orgánica de la Contraloría General del Estado; e inobservando las Normas de Control Interno 401-03 Supervisión y 600-02 Evaluaciones periódicas.

QUINCE

Los Gerentes Generales del HTMC, encargados, actuantes en los períodos comprendidos entre el: 17 de julio de 2015 y el 7 de marzo de 2016; y, 8 de marzo de 2016 y el 13 de octubre de 2016; ni el Gerente General del HJCA, encargado por los períodos comprendidos entre el: 20 de mayo de 2015 y el 29 de abril de 2016; no supervisaron el cumplimiento de la recomendación 7 en la Unidad Médica a su cargo, ni dispusieron el bloqueo inmediato del acceso de las opciones incompatibles en el perfil de despacho de fármacos, tampoco establecieron los controles y mecanismos de supervisión para la ejecución de estas actividades, lo que ocasionó que no se establezcan los niveles de acceso a las funcionalidades del Sistema de Información Médica MIS AS400; pues existieron usuarios con perfiles de despacho de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"* y habilitada por defecto la opción 2 *"Dispensarios Anexos/Subrogados"*, que permite generar recetas como dispensarios anexos; sin que en el sistema se evidencien la restricción del acceso de la opción 2, ni se definieron los procedimientos para que el personal autorizado supervise y controle los registros de despacho y emisión de recetas realizados en el sistema.

El Gerente General del HJCA en funciones desde el 2 de mayo de 2016 y el 27 de octubre de 2016; no dio seguimiento a la ejecución de lo establecido en memorando IESS-HJCA-DT-2016-2452-M de 27 de junio de 2016; al no disponer que se realice el bloqueo inmediato de las opciones incompatibles en el perfil de despacho de fármacos; lo que ocasionó que no se establecieran los niveles de acceso a las funcionalidades del Sistema de Información Médica MIS AS400; pues existieron usuarios con perfiles de despacho de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"* y habilitada por defecto la opción 2 *"Dispensarios Anexos/Subrogados"*, que permite generar recetas como dispensarios anexos; sin que en el sistema se evidencien la restricción del acceso de la opción 2, ni se establecieron los procedimientos para que el personal autorizado supervise y controle los registros de despacho y emisión de recetas realizados en el sistema.

Los referidos servidores inobservaron lo establecido en el artículo 92.- Recomendaciones de auditoría de la Ley Orgánica de la Contraloría General del Estado; y, las Normas de Control Interno 401-03 Supervisión y 600-02 Evaluaciones periódicas.

Dieciseis

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0074, 0075, 0076, 0077, 0078, 0079, 0080, 0092, 0093, 0095, 0108-0010-IESS-AI-2017 de 9 de mayo de 2017 a los Directores del Seguro General de Salud Individual y Familiar, Subdirectores Nacional de Garantía de la Calidad de los Servicios del Seguro de Salud, a la Subdirectora Provincial de Prestaciones del Seguro Salud de Pichincha, encargada y Subdirector Provincial de Prestaciones del Seguro Salud de Pichincha, y a los Gerentes Generales de los Hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga titulares y encargados, obteniendo las siguientes respuestas:

El Director del Seguro General de Salud Individual y Familiar encargado y Director del Seguro General de Salud Individual y Familiar, en funciones desde el 8 de enero de 2016 y el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 y el 26 julio de 2016, respectivamente, en respuesta al oficio 0074-0010-IESS-AI-2017 de 9 de mayo de 2017; con comunicación de 19 de mayo de 2016, respecto del cumplimiento de las recomendaciones 7, 5, 6; señaló:

> *"... **Recomendación 7** (...) Mediante memorando Nro. IESS-DSGSIF-2016.-1802-M del 14 de junio de 2016, se pone en conocimiento de la... Directora General del Instituto Ecuatoriano de Seguridad Social el Manual de procesos para la Gestión Farmacéutica... **Memorando IESS-DSGIF-2016-1802-M**... toda vez que la Dirección General de Salud Individual y Familiar se encuentra en el proceso de implementación del modelo de gestión en el servicio farmacéutico de los establecimientos de salud. Pongo en su conocimiento el "Manual de Procesos para la Gestión Farmacéutica".- Memorando IESS-**DSGSIF-2016-1816-M...** Se requiere que en el Sistema MIS/AS400, se implemente la opción para registrar el código CIE 10 que viene en la solicitud correspondiente en la pantalla de generación de pedidos de auxiliares de diagnóstico y recetas de farmacia, generados desde los dispensarios Anexos y Establecimientos de Salud de la Red Pública y Complementaria, con la finalidad de que las unidades de pertinencia médica de las Subdirecciones Provinciales de Prestaciones de Salud, puedan verificar la correlación entre los estudios pedidos y los estudios realizados al paciente con diagnósticos presuntivos y diferenciales.- Con respecto... **memorando IESS-DSGSIF-2016-0370-M de 26 de enero de 2016**.- informo que los Hospitales... mencionados generar* (sic) *mediante memorando No. IESS-HCAM-GG-2016-0071-M, IESS-HTMC-GG-2016-0228-M y IESS-CAA304-DM-2016-0032-M respectivamente ... **Recomendación 5 y 6** (...) Mediante memorando IESS-DSGSIF-2016-1352-M del 10 de mayo de 2016, mediante el cual se pone en conocimiento a... la Directora General del Instituto Ecuatoriano de Seguridad Social, el Manual de Procesos de Derivaciones que se orienta a estandarizar los procedimientos para los procesos de derivación, referencia/contra referencia, entre las unidades médicas de salud del IESS.- Con memorando IESS-*
>
> DIECISIETE

DSGSIF-2016-1676-M del 3 de junio de 2016 se socializa el Manual de Procesos de Derivaciones con los Directores Provinciales, Subdirectores Provinciales y Nacionales para el cumplimiento e implementación...".

Lo comentado, por el Director del Seguro General de Salud Individual y Familiar, no modifica el criterio de auditoría, por cuanto las acciones realizadas y reportadas por parte de las Unidades Médicas a nivel nacional, no fueron coordinadas, y no se cumplió con lo dispuesto en la recomendación 7, puesto que no se implementaron los controles en los niveles de acceso a las funcionalidades del Sistema de Información Médica MIS AS400 en los hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga, no obstante se aplicaron los correctivos en la parametrización del sistema, en el Hospital Carlos Andrade Marín; tampoco, pese a la generación del *"Manual de procesos para la Gestión Farmacéutica"*, se evidenció en los hospitales HTMC y HJCA, la implantación de procedimientos de supervisión y control oportunos de las actividades de los servidores autorizados para el despacho de medicamentos y la generación de recetas como dispensarios anexos; al respecto del cumplimiento de la recomendaciones 5 y 6; además de la generación del *"Manual de Procesos de derivación, referencia/contra referencia";* no se evidenció políticas y lineamientos para la implementación de controles para la restricción del acceso para el uso de médicos y prestadores privados al Sistema de Información Médica AS400, para el direccionamiento de consultas.

El Gerente General del HJCA, actuante en período comprendido entre el 2 de mayo de 2016 y el 27 de octubre de 2016, en respuesta al oficio 0108-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 19 de mayo de 2017, señaló:

"... envié el informe solicitado, el cual incluye como anexo el informe de cumplimiento de la recomendación N°7, y se realizaron varias acciones para dar cumplimiento.- a) El anexo que consta el cumplimiento de la recomendación N° 7 y está como memorando Nro. IESS-HJCA-DT-2016-2452-M de fecha 27 de junio de 2016, suscrito por el Dr..., Director Técnico del HJCA.- b) Se coordinaron entre los Gerentes y Coordinadores de TICs de los Hospitales José Carrasco Arteaga y Carlos Andrade Marín para que se capaciten nuestros funcionarios...".

Lo mencionado, no modifica el criterio de auditoría por cuanto, no se evidenciaron las acciones ejecutadas conforme lo expresado el memorando IESS-HJCA-DT-2016-2452-M de fecha 27 de junio de 2016; por lo que no se implementó la recomendación Nro.7 del informe DAI-AI-0391-2015 del examen especial *"a los procesos*

DIECIOCHO

precontractual, contractual y de ejecución de las adquisiciones de bienes y servicios y gestión de farmacia en el IESS, Hospital Regional José Carrasco Arteaga"; por el período comprendido entre el 1 de enero de 2010 y el 31 de diciembre de 2013.

El Subdirector Nacional de Garantía de la Calidad de los Servicios de Salud, actuante por el período comprendido entre el 13 de octubre de 2016 y el 31 de diciembre de 2016; en respuesta al oficio 0078-0010-IESS-AI-2017 de 9 de mayo de 2017, con memorando IESS-SDNGCSSS-2017-0586-M de 17 de mayo de 2017, al respecto del cumplimiento de la recomendación 8.- del informe DADSySS-0058-2016 del examen especial *"a la contratación y pago a prestadores privados por servicios de salud para los afiliados y pensionistas de la Provincia de Pichincha en la Dirección del Seguro General de Salud Individual y Familiar IESS"*, por el período comprendido entre el 1 de enero de 2012 al 31 de diciembre de 2014, señaló:

> *"... Conforme me compete las funciones como Subdirector Nacional de Garantía de la Calidad de los Servicios de salud, desde el 13 de octubre de 2016, al 31 de diciembre del 2016, me ratifico en el contenido del memorando IESS-SNGCSSS-2017-303-M de 3 de abril de 2017, mediante el cual se informa y se adjunta los diferentes requerimientos formulados... al Coordinador Institucional de Calidad, para que gestione el cumplimiento de las recomendación (SIC).- Una vez más mediante memorando IESS-SDNGCSSS-2017-0374-M, requiero el seguimiento de las recomendaciones, a lo cual el Ing... informa lo actuando mediante memorando No. IESS-CCA-2017-0094-M de 27 de abril de 2017, acorde a las competencias de esa Coordinación, en lo que compete a la Recomendación 8...Al respecto, la acreditación a los prestadores y consultorios externos vía web, se realizó a partir de la resolución C.D 378 de 24 de agosto de 2011, y estuvo vigente hasta la emisión del Acuerdo Ministerial 5310 del 15 de diciembre de 2015, emitido por el Ministerio de Salud Publica.- En este sentido, una vez que han transcurrido más de quince meses desde la vigencia del Acuerdo Ministerial 5310, y por consiguiente la suspensión del procedimiento de acreditación realizada vía web, la Coordinación Institucional de Calidad, una vez que el Ministerio de Salud Publica culmine el proceso de calificación de prestadores de salud emitirá los respectivos informes...".*

La Subdirectora Provincial de Prestaciones del Seguro Salud de Pichincha, encargada, actuante durante el período comprendido entre el 1 de enero de 2016 y el 16 de septiembre de 2016, en respuesta al oficio 0079-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 18 de mayo de 2017, al respecto del cumplimiento de la recomendación 8.- del informe DADSySS-0058-2016 del examen especial *"a la contratación y pago a prestadores privados por servicios de salud para los afiliados y pensionistas de la Provincia de Pichincha en la Dirección del Seguro General de Salud*

Diecinueve 27

Individual y Familiar IESS", por el período comprendido entre el 1 de enero de 2012 y el 31 de diciembre de 2014; señaló:

> *"... La recomendación dice que se haga una visita para continuar con el proceso de acreditación, pero este proceso de acreditación ya no es competencia del IESS, desde diciembre de 2015, sino del Ministerio de salud Publica en acuerdo 5310 del MSP, por lo tanto al ser de cumplimiento obligatorio por ser el ente rector, el IESS, no puede hacer el proceso de acreditación para emitir un certificado de acreditación y además porque la misma contraloría realizó observaciones a la CD 020 que es la que mantiene los formatos para Acreditación.- Por lo tanto lo referente a directrices para poder realizar lo requerido por contraloría nunca nos fueron dados de parte de la Direccion General ni de la Subdirección Nacional de Aseguramiento.- En cuanto a que porque no se inactivaron es porque la misma Resolución 378 indica que si no se realizó la visita seis meses posteriores al registro en la web (que es cuando el mismo sistema emitía la acreditación condicionada), se entendería visita realizada..."*.

El Subdirector Nacional de Garantía de la Calidad de los Servicios de Salud, que actuó durante los períodos comprendidos entre el: 18 de abril de 2016 y el 6 de octubre de 2016; en respuesta al oficio 0077-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 25 de mayo de 2017, señaló:

> *"... Conforme el Acuerdo Ministerial N° 00005310, publicado con Registro Oficial Edición Especial 439 de 31-dic.-2015, en el cual establece el* ***NORMA PROCEDIMIENTO EVALUACION Y ADQUISICION DE SERVICIOS DE SALUD.-*** *Art 2.- Disponer que la Norma Técnica denominada "Procedimiento de evaluación, selección, Calificación y adquisición de servicios de salud de la Red Pública Integral de Salud y de la Red Privada Complementaria", sea aplicada a nivel nacional como una normativa del Ministerio de Salud Pública de carácter obligatorio para el Sistema Nacional de Salud...* ***DISPOSICION DEROGATORIA****... En tal virtud, lo expuesto en la resolución del Consejo Directivo CD20 y CD40 quedan derogadas con sus procedimientos de (acreditación) calificación de proveedores.- Ante la recomendación 8 mediante la cual el Director del Seguro de Salud Individual y Familiar del período comprendido entre el 27 de julio del 2016 y el 19 de septiembre de 2016, con memorando* ***IESS-DSGIF-2016-2709-M,*** *del 03 de agosto del 2016 dispuso:... se solicita que en el plazo de 5 días se remita la documentación de su implementación.- La Subdirección de Garantía de Calidad, cumpliendo con la recomendación antes citada ejecutó las siguientes actividades: Con Memorando IESS-SDNGCSSS-2016-0215-M del 03 de agosto del 2016 se solicita a la... Subdirectora Provincial de Prestaciones del Seguro de Salud Pichincha, encargada: remita el Listado de Acreditaciones realizadas vía Web de Prestadores Externos (...).- mediante memorando IESS-SDNGCSSS-2016-0224-M del 05 de Agosto del 2016 se solicita... se analice el listado que remite la Subdirección Provincial de Salud de Pichincha y se verifique si dichos proveedores prestan servicios de salud y mantienen el contrato vigente, y así verificar que los mismos se encuentren activos y verdaderamente estan prestando servicios de salud, caso contrario se eliminen de la base de datos.-*

VEINTE

Esta petición se realiza ya que la Subdirección de Garantía de Calidad no contaba con acceso al AS-400 para evidenciar dicha información y esta era manejada por la Subdirección Aseguramiento.- (...) con Memorando IESS-SDNGCSSS-2016-0225-M de 05 de agosto de 2016, se da a conocer al ... Director del Seguro de Salud, las acciones tomadas frente a la recomendación.- con Memorando IESS-SDNGCSSS-2016-0226-M del 05 de agosto de 2016 se convoca a la II reunión para continuar con la ejecución de lineamientos de calidad para la calificación de prestadores externos... Ante la dificultad del IESS de trazar lineamientos para la calificación de proveedores externos, que vayan en contra de las directrices y normativas dadas por el MSP como Autoridad Sanitaria Nacional, la Coordinación de Articulación de la Red, lleva estas inquietudes al seno de la comisión técnica de la RPIS; para lo cual el MSP socializa la Norma Técnica y sugiere se emita sugerencias de mejoramiento...".

Lo mencionado, por los Subdirectores Nacionales de Garantía de la Calidad de los Servicios de Salud y la Subdirectores Provinciales de Prestaciones del Seguro Salud de Pichincha, no modifica el criterio de auditoría, debido a que con Acuerdo Ministerial 5310 de 15 de diciembre de 2015, se establecieron cambios en la normativa que modificaron los procedimientos establecidos para la acreditación web, sin embargo, no se dictaron lineamientos por parte de los Directores del Seguro General de Salud Individual y Familiar, para el cumplimiento de la recomendación Nro.8, ni los Subdirectores Nacionales de Garantía de la Calidad de los Servicios de Salud y la Subdirectores Provinciales de Prestaciones del Seguro Salud de Pichincha, señalaron la ausencia de estas directrices, por lo que no se establecieron los procedimientos que permitan realizar la inactivación en el Sistema de Información Médica MIS AS400 de los prestadores privados que no mantienen relación con el Instituto Ecuatoriano de Seguridad Social.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

El Subdirector Provincial de Prestaciones del Seguro Salud Pichincha, actuante en el período comprendido entre el: 19 de septiembre de 2016 y el 31 de diciembre de 2016; con comunicación de 25 de mayo de 2017, señaló:

"... La Subdirección de Pichincha es un ente operativo que se rige por las disposiciones que constan en el Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social... En virtud de lo manifestado corresponde a la Dirección Nacional de Salud y a la Subdirección de Aseguramiento emitir las políticas necesarias para realizar los controles que permitan brindar calificar y

VEINTEYUNO 21

acreditar a los prestadores externos de los servicios de salud, con el objeto de contar con un servicio adecuado de salud para los afiliados.- Debo dejar constancia que la Contraloría General del Estado, en las observaciones realizadas dentro del examen especial que motiva esta comunicación, señala que la Resolución CD20, que es el instrumento que permite acreditar a los proveedores externos de los servicios de salud, es una herramienta obsoleta y debe ser actualizada. Esta acción, la de actualización, corresponde, de acuerdo con la Ley y el Estatuto, al Consejo Directivo del IESS, por ser la autoridad competente para emitir las regulaciones en la Institución, y las instancias administrativas debemos cumplir con esas disposiciones. Hasta tanto las direcciones han tenido que trabajar con esta herramienta que no responde a las necesidades actuales del IESS.- Por su parte, es pertinente señalar que el Acuerdo 5310 de diciembre 2015 determina que la competencia para las acreditaciones le corresponde al Ministerio de Salud Pública y que, mediante Memo IESS-SDCSS-2014-0467-M, se prorroga el tiempo de duración de la acreditación de prestadores externos de los servicios de salud, hasta que se emita la nueva normativa...".

Lo comentado por el Subdirector Provincial de Prestaciones del Seguro Salud Pichincha, actuante en el período comprendido entre el: 19 de septiembre de 2016 y el 31 de diciembre de 2016, no modifica el criterio de auditoría, en razón de que no adjuntó, la documentación citada en su punto de vista, ni presentó alternativas para el cumplimiento de la recomendación, tampoco advirtió al Director del Seguro General Individual y Familiar, sobre la afectación de las actividades con relación al cambio de normativa para la acreditación y validación de prestadores externos.

El Director del Seguro General de Salud Individual y Familiar encargado y Director del Seguro General de Salud Individual y Familiar, en funciones desde el 8 de enero de 2016 y el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 y el 26 julio de 2016, respectivamente, con comunicación IPBR-2017-004 de 28 de mayo de 2016, no acotó puntos de vista adicionales a este comentario.

El Director del Seguro General de Salud Individual y Familiar, encargado, actuante en el período comprendido entre el 28 de septiembre de 2016 y el 31 de diciembre de 2016, con memorando IESS-DSGIF-2017-1581-M de 30 de mayo de 2017, señaló:

"... he tomado las siguientes acciones para dar cumplimiento a la normativa reguladora de la confidencialidad de los datos del Sistema Nacional de Salud de la siguiente manera: 1. Mediante Memorando Nro. IESS-DSGSIF-2017-0528-M de 11 de febrero de 2017, el Director del Seguro de Salud Individual y Familiar encargó al Analista Administrativo DSGSIF la función como: "analista funcional del sistema de Gestión Hospitalaria MIS AS-400 (...) siendo la contraparte de la Coordinación Nacional (sic) de Tecnología de la Información del HCAM unidad que se encarga de administrar y desarrollar mejoras en el

VEINTE Y DOS

Sistema del AS400".- 2.Mediante Memorando Nro IESS-DSGSIF-2017-0589-M de 16 de febrero de 2017... puso en conocimiento de los Subdirectores(as) Provinciales de Prestaciones del Seguro de Salud, el Memorando IESS-DSGSIF-2017-0528-M de 11 de febrero de 2017, mediante el cual se designó un funcionario que atenderá los requerimientos funcionales del Sistema AS-400.- 3. Mediante Memorando Nro. IESS-DSGSIF-2017-1135-M de 12 de abril de 2017, el Analista Administrativo designado como contraparte de la DSGSIF... reemitió para su aprobación al Director del Seguro General de Salud Individual y Familiar el instrumento denominado: "Aceptación del Acuerdo de Confidencialidad en el Acceso al Sistema Informático MIS AS400".- 4. Mediante firma inserta de 13 de abril de 2017, (...) el Director del Seguro General de Salud Individual y Familiar aprobó el instrumento antes citado... 5. Mediante comentario de 13 de abril inserto en hoja de ruta del Memorando Nro. IESS-DSGSIF-2017-1135-M de 12 de abril de 2017, el Director del Seguro General de Salud Individual y Familiar autorizó al Analista Funcional del Sistema AS400 el requerimiento realizado, a su vez dispuso "proceder conforme a la normativa legal vigente".- 6. Mediante Memorando Nro. IESS-DSGSIF-2017-1146-M de 13 de abril de 2017, el Analista Funcional del Sistema AS400, remitió el requerimiento al Coordinador General de TIC-HCAM el Requerimiento Funcional...7. Mediante Memorando Nro. IESS-DSGSIF-2017-1146-M de 13 de abril de 2017, el Director del Seguro General de Salud Individual y Familiar Encargado a la fecha, dispuso a los Subdirectores Provinciales de Prestaciones del Seguro de Salud la implementación del instrumento denominado: "Aceptación del Acuerdo de Confidencialidad en el Acceso al Sistema Informático MIS-AS400, mismo que en su parte electrónica entrará en vigencia a partir del lunes 1 de mayo de 2017 8. Mediante Memorando Nro. IESS-DSGSIF-2017-1364-M de 04 de mayo de 2017, el Director del Seguro de Salud Individual y Familiar, solicitó a los Subdirectores Nacionales del Seguro de Salud y Subdirectores Provinciales de Prestaciones del Seguro de Salud la gestión correspondiente para proceder con la actualización de la información de usuarios activos del Sistema MIS-AS400, documento al que adjuntó los formularios actualizados de: "creación de usuarios" y "acuerdos de confidencialidad" 9. Mediante Memorando Nro. IESS-DSGSIF-2017-1576-M de 30 de mayo de 2017, el Director del Seguro General de Salud Individual y Familiar, remitió al Coordinador General de TIC-HCAM, el pedido de validación e inactivación de usuarios del Sistema MIS-AS400, en las dependencias administrativas del Seguro de Salud. 10. Mediante Memorando Nro. IESS-DSGSIF-2017-1580-M de 30 de mayo de 2017, el Director del Seguro de Salud Individual y Familiar, dispuso al Analista Funcional de la DSGSIF y Subdirectores Nacionales de Garantía de la Calidad de los Servicios de Salud, Provisión de Servicios Aseguramiento del Seguro de Salud realicen los lineamientos necesarios para la concesión de acceso a las historias clínicas de los pacientes atendidos en las unidades médicas del IESS, por parte del personal médico y administrativo de las casas de salud.- Los documentos antes mencionados evidencian las acciones ejecutadas por la Dirección del Seguro General de Salud Individual y Familiar emitió los lineamientos y directrices necesarias para la elaboración y suscripción de acuerdos de confidencialidad por parte de los usuarios que tienen acceso al Sistema AS400...".

Lo comentado por el Director del Seguro General de Salud Individual y Familiar, encargado, actuante en el período comprendido entre el 28 de septiembre de 2016 y el 31 de diciembre de 2016, no modifica el comentario de auditoría, debido a que las

VEINTE Y TRES 24

acciones correctivas presentadas, se efectuaron posterior a la fecha de corte del examen especial, esto es, 31 de diciembre de 2016.

El Gerente General del HJCA, actuante en el período comprendido entre el 2 de mayo de 2016 y el 27 de octubre de 2016, con comunicación de 30 de mayo de 2017, acotó:

> *"...a) Desde la Gerencia General del HJCA, se coordinó... para dar cumplimiento al memorando IESS-HJCA-DT-20162452-M* (sic), *y la recomendación 7. Luego de varias reuniones se acordó que los médicos generales que tenían acceso a atender pacientes y recetar en Consulta Externa del Hospital José Carrasco Arteaga, se realice el traspaso de puestos al Centro de Atención Ambulatoria Central de Cuenca. Por ello, se envió el memorando de Gerencia Nro. IESS-HJCA-GG-2016-1784-M, de fecha 07 de septiembre de 2016, al... Director Administrativo del Centro de Atención Ambulatoria para iniciar el traspaso de los médicos.- b) Al mismo tiempo... desde la Coordinación General de Hospitalización y Ambulatorio del HJCA, se solicitó a través de memorando Nro. IESS-HJCA-CGHA-2016-1272-M, de fecha 07 de septiembre de 2016 a la Coordinación General de Tecnologías de la Información y Comunicación(TICs) del HJCA, el cierre de las agendas de los dos médicos generales, para que ya no tengan acceso a la atención y prescripción desde consulta externa.- c) Con memorando Nro. IESS-CE-CC-2016-3209-M, de fecha 12 de septiembre de 2016, suscrito por el... Director Administrativo del Centro de Atención Ambulatoria, se informa al HJCA, que se ha procedido con la consulta de traspaso de puestos a la Dirección de Talento Humano, de los Médicos Generales... d) A través de memorando Nro. IESS-DNGTH-2016-5286-M, de fecha 20 de septiembre de 2016, el Director Nacional de Talento Humano, autoriza el traspaso... al Centro de Atención Ambulatoria Central de Cuenca. Al momento los dos médicos generales, no son parte del Hospital José Carrasco Arteaga... ".*

Lo expuesto, por el Gerente General del HJCA, actuante en el período comprendido entre el 2 de mayo de 2016 y el 27 de octubre de 2016, evidenció las acciones administrativas tomadas, en relación al personal médico que realizó prescripción y despacho de fármacos, sin embargo, el traslado de los médicos generales mencionados, no mitigó el riesgo en el Sistema de Información Médica MIS AS400, debido a la existencia de opciones por defecto habilitadas para el área de farmacia, quienes también hacen uso del menú *"Despacho de órdenes de farmacia"*, con perfil de grupo *"CFARMA"* y programa *"FARM00"*, que continuó con la opción 2 *"Dispensarios Anexos/Subrogados"*, habilitada por defecto, persistiendo el riesgo de la ejecución de funciones incompatibles por parte de los servidores que laboran esta área de servicio.

VEINTE Y CUATRO

Conclusiones

- El Director del Seguro General de Salud Individual y Familiar encargado y titular no emitió lineamientos, ni supervisó la implementación de las recomendaciones 7, 5, 6 de los informes del DAI-AI-0391-2015, DAI-AI-0109-2016, ni dispuso la coordinación de actividades para que en las Unidades Médicas se implementen restricciones de acceso a las opciones del Sistema de Información Médica MIS AS400, tampoco efectuó un análisis, que permita la generación de un plan de acción a nivel nacional, pues en los Hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga; existen 21 y 46 usuarios activos que en el sistema tienen perfiles de grupo *"CFARMA"* y programa *"FARM00"*, asignados a los servidores que realizaron tareas de descargo de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"*, que tuvieron habilitada por defecto la opción 2 *"Dispensarios Anexos/ Subrogados"*, para la generación recetas como dispensarios anexos; tampoco emitió los lineamientos y políticas para que el Coordinador General de Tecnología de Información y Comunicación del HCAM, limite el uso y acceso al aplicativo informático de los prestadores privados como usuarios de la plataforma AS/400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente, ni solicitó la revisión inmediata del sistema; lo que ocasionó que persistan las debilidades identificadas, incrementando el riesgo de ejecución de funciones incompatibles en el Sistema de Información Médica MIS AS400 tanto para el caso de despacho y prescripción de fármacos en los hospitales, como para el caso de la generación de citas realizadas por prestadores privados del servicio de salud.

- Los Directores del Seguro General de Salud Individual y Familiar titulares y encargados, no emitieron lineamientos, ni supervisaron la implementación de las recomendaciones 7, 5, 6 y 8 de los informes DAI-AI-0391-2015, DAI-AI-0109-2016 y DADSySS-0058-2016, ni dispusieron la coordinación de actividades para que en las Unidades Médicas se implementen restricciones de acceso a las opciones del Sistema de Información Médica MIS AS400, tampoco efectuaron un análisis, que permita la generación de un plan de acción a nivel nacional, pues en los Hospitales Teodoro Maldonado Carbo y José Carrasco Arteaga; existieron 21 y 46 usuarios activos que en el sistema tuvieron perfiles de grupo *"CFARMA"* y programa *"FARM00"*, asignados a los servidores que realizaron tareas de descargo de

veinte y cinco

fármacos con acceso al menú de *"Despacho de órdenes de farmacia"*, que tuvieron habilitada por defecto la opción 2 *"Dispensarios Anexos/ Subrogados"*, para la generación recetas como dispensarios anexos; ni emitieron los lineamientos y políticas para que el Coordinador General de TIC's del HCAM, limite el uso y acceso al aplicativo informático de los prestadores privados como usuarios de la plataforma AS/400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente, ni solicitaron la revisión inmediata del sistema además, no se deshabilitaron los prestadores externos que no cumplieron los requisitos establecidos en la normativa vigente, lo que ocasionó que persistan las debilidades identificadas e incrementó el riesgo de ejecución de funciones incompatibles en el Sistema de Información Médica MIS AS400 tanto para el caso de despacho y prescripción de fármacos en los hospitales, como para el caso de la generación de citas realizadas por prestadores privados del servicio de salud; y, del acceso no autorizado por parte de prestadores externos no calificados y que no fueron deshabilitados del sistema.

- Los Subdirectores Nacionales de Garantía de la Calidad de los Servicios del Seguro de Salud, titulares y encargados; y, los Subdirectores Provinciales de Prestaciones del Seguro Salud Pichincha, no solicitaron lineamientos al Director del Seguro General de Salud Individual y Familiar, relacionados con el cambio de las competencias respecto de las acreditaciones de prestadores y consultorios privados según lo dispuesto con Acuerdo Ministerial 5310 de 15 de diciembre de 2015 del Ministerio de Salud Pública, lo que ocasionó que no se deshabiliten del Sistema de Información Médica MIS AS400 a los prestadores de salud que no fueron calificados

- Los Gerentes Generales del HTMC, encargados; ni el Gerente General del HJCA, encargado no supervisaron el cumplimiento de la recomendación 7 en la Unidad Médica a su cargo, ni dispusieron el bloqueo inmediato del acceso de las opciones incompatibles en el perfil de despacho de fármacos, tampoco establecieron los controles y mecanismos de supervisión para la ejecución de estas actividades, lo que ocasionó que no se establezcan los niveles de acceso a las funcionalidades del Sistema de Información Médica MIS AS400; pues existieron usuarios con perfiles de despacho de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"* y habilitada por defecto la opción 2 *"Dispensarios Anexos/Subrogados"*, que permite generar recetas como dispensarios anexos; sin

veinte y seis

que en el sistema se evidencien la restricción del acceso de la opción 2, ni se definieron los procedimientos para que el personal autorizado supervise y controle los registros de despacho y emisión de recetas realizados en el sistema.

- El Gerente General del HJCA no dio seguimiento a la ejecución de lo establecido en memorando IESS-HJCA-DT-2016-2452-M de 27 de junio de 2016; al no disponer que se realice el bloqueo inmediato de las opciones incompatibles en el perfil de despacho de fármacos; lo que ocasionó que no se establecieran los niveles de acceso a las funcionalidades del Sistema de Información Médica MIS AS400; pues existieron usuarios con perfiles de despacho de fármacos con acceso al menú de *"Despacho de órdenes de farmacia"* y habilitada por defecto la opción 2 *"Dispensarios Anexos/Subrogados"*, que permite generar recetas como dispensarios anexos; sin que en el sistema se evidencien la restricción del acceso de la opción 2, ni se establecieron los procedimientos para que el personal autorizado supervise y controle los registros de despacho y emisión de recetas realizados en el sistema.

Recomendaciones

A la Directora General del IESS

1. Dispondrá al Director del Seguro General de Salud Individual y Familiar, responsable de la observancia de las recomendaciones emitidas en los informes de auditoría interna y externa, que una vez comunicadas a la institución, disponga a los servidores responsables de su cumplimiento que éstas deben ser aplicadas de manera inmediata y con el carácter de obligatorio.

Al Director del Seguro General de Salud Individual y Familiar

2. Dispondrá a los Directores Médicos de la Unidades de Salud establezcan, de acuerdo a los niveles de complejidad de las mismas, los niveles de acceso a las funcionalidades del Sistema de Información Médica MIS AS400, considerando que no existan servidores que desempeñen funciones incompatibles relacionadas con la emisión de recetas, su despacho y registro. De no existir las condiciones apropiadas para esta separación de funciones, se deberán implementar

VEINTE Y SIETE

procedimientos de supervisión y control oportunos sobre la veracidad de las mismas.

3. Dispondrá al Coordinador General de Tecnologías de la Información y Comunicaciones del HCAM, coordiné con los administradores de la parametrización del Sistema de Información Médica MIS AS400 de las Unidades Médicas a nivel nacional, el análisis para la implementación de las restricciones de acceso aplicadas en ese hospital, de manera de limitar el acceso a la opción 2 *"Dispensarios Anexos/Subrogados"* del menú *"Despacho de órdenes de farmacia"* para los usuarios con perfil de grupo *"CFARMA"* y programa *"FARM00"*, no obstante, se implementaran los procedimientos para que este acceso sea autorizado y bajo la responsabilidad de los jefes de área requirentes.

4. Dictará los lineamientos y políticas para que la Coordinación General de Tecnología de Información y Comunicación del HCAM, limite el uso y acceso al aplicativo informático que tienen los médicos privados como usuarios de la plataforma AS/400, en los procesos de agendamiento de citas, a pacientes que requieren atención subsecuente.

5. Solicitará la revisión inmediata del aplicativo informático desarrollado en la plataforma AS/400, para delimitar el acceso que tiene los prestadores privados para direccionar consultas hacia otra especialidad diferente a la que fue derivado el paciente, así como a sí mismos.

6. Dispondrá al Subdirector Nacional de Garantía de la Calidad de los Servicios del Seguro de Salud, que conjuntamente con el Coordinador Provincial de Prestaciones del Seguro de Salud, Pichincha, coordinen con los responsables de las Direcciones Nacionales de Riesgos Institucionales y de Tecnologías de la Información emitan lineamientos y procedimientos para que los Administradores del Sistema de Información Médica MIS AS400, que gestionan los accesos de los prestadores externos a nivel nacional, ejecuten la inactivación periódica de aquellos no acreditados y/o calificados para la prestación de sus servicios al Instituto Ecuatoriano de Seguridad Social; además establecerá las instrucciones necesarias para que en la Dirección a su cargo se realice el reporte regular de estos prestadores externos para su deshabilitación del sistema, base legal que será remita al Director General para su aprobación y cumplimiento obligatorio.

VEINTE Y OCHO

No se establecieron procedimientos para la administración de usuarios, configuración de seguridad y parametrización del Sistema de Información Médica MIS AS400

El Sistema de Información Médica MIS AS400, es utilizado por las Unidades Médicas del IESS a nivel nacional, la plataforma e infraestructura relacionada, como equipos servidores y base de datos se encontraron alojados en el Centro de Cómputo ubicado en el Hospital Carlos Andrade Marín. Este sistema estuvo conformado de los siguientes módulos: Admisión Consulta Externa, Admisión Hospitalaria, Manejo de Historia Clínica Médica, Enfermería, Farmacia, Bodegas, Facturación, Agendamiento Contact Center, Administración de Parámetros de la unidad.

Las actividades de administración, configuración, desarrollo y mantenimiento del Sistema de Información MIS AS400 estuvieron a cargo del Coordinador General de TIC's del HCAM; no obstante para la implementación, operación y control del sistema en cada Unidad Médica a nivel nacional, se otorgaron usuarios administradores para realizar actividades de parametrización, gestión de usuarios y soporte del área a la que pertenecieron.

En la base de datos del Sistema de Información Médica MIS AS400, constó que a nivel nacional existieron 581 perfiles de administradores activos, en las Unidades Médicas de estos: 220 correspondieron a Administradores de *"Control General de Sistema"*, 162 tuvieron perfiles de *"Médico Maestro"* con permiso de efectuar la parametrización en el aplicativo de dependencias, agendamientos, salas; y, 199 fueron *"Administradores de Control de Bodegas"*.

A nivel de los hospitales de nivel III, se mantuvieron en general 36 usuarios administradores, asignados al personal que trabajó en el área de TIC's, con los siguientes programas: *"CONTRO"*, *"MEDI11"* e *"INVCL001"*, correspondientes a perfiles de administración: *"Control General del Sistema"*, *"Sistema de Gestión Hospitalaria"* y *"Control General del Sistema de Inventarios"*; con capacidad de creación de usuarios y parametrización de la Unidad Médica, agendamiento, asignación de médicos a dependencias, creación de bodegas, autorización de fármacos, entre otros, que se detallan:

VEINTE Y NUEVE

Hospital	Perfiles de Administración				Total	Observaciones
	Control General del Sistema	Sistema de Gestión Hospitalaria	Control General Sist. Invent.	Súper usuario utilizado HCAM		
HCAM		2		2	4	Los usuarios: MTHOSPIT, ADMIN, BD9999001, no registran el nombre y cédula de ciudadanía
HTMC	6 (*)	2	2		10	
HJCA	9 (*)	8	5		22	Los usuarios con programa CONTRO: AM0103016, AM0103021, no laboran en el área de informática y fueron trasladas a Docencia y Planificación.
TOTAL:					36	

(*) Creados en el Sistema de Información Médica MIS AS400, en la Unidad Médica denominada *"SUPERUSUARIO??"*

En las Unidades Médicas de nivel III, se presentaron las siguientes novedades:

- El proceso de la solicitud, autorización y entrega de claves a los usuarios en las Unidades Médicas de Nivel III, inició con el memorando de pedido realizado por Quipux, documento que no se mantuvo impreso o en medios magnéticos del área de TIC's, además se presentaron formularios de creación de usuarios suscritos por la jefatura de servicios solicitante, el usuario responsable, y el servidor responsable de la entrega de usuario y clave; sin embargo, los datos y documentos solicitados no guardaron consistencia en cada uno de los hospitales, pues, en el caso del HTMC se solicitó copias de la cédula y del contrato de considerarlo necesario; se pidió la situación laboral, funciones, módulos que se requirieron del sistema, perfil de acceso; mientras que el HCAM y HJCA no se los requirió; así también, para la entrega de los usuarios y claves en el HCAM y HJCA se enviaron por correo Institucional y en el HTMC se entregaron con oficio.

- Los administradores de usuarios en los hospitales HCAM, HTMC y HJCA, no documentaron las opciones del sistema con acceso autorizado y asignado a los usuarios, ni las pusieron en conocimiento del Responsable de la Unidad que solicitó y autorizó el acceso; así como las solicitudes de cambio en la parametrización del sistema enviadas por Quipux, ni el estado anterior al cambio ni los resultados en el sistema.

TREINTA

- El archivo de los respaldos de las solicitudes en el HTMC, se encontró organizado y conformado por documentos tales como: solicitud, autorización, entrega de claves y pedido de activación de usuarios bloqueados, a diferencia del HCAM y HJCA que no contaron con documentos completos y organizados de estas actividades.

- En el HCAM, se parametrizó el sistema para que la clave de usuario inicialmente creada se caduque y se solicite su cambio obligatorio en el primer ingreso; no obstante, en el HTMC y HJCA no se realizó este procedimiento, por lo que la clave asignada inicialmente, podía mantenerse activa por 40 días, siendo vulnerable debido a que la primera clave asignada fue el nombre del usuario entregado; lo que incrementó el riesgo de accesos no autorizados.

- En el HCAM, se realizó la administración de seguridad general del Sistema de Información Médica MIS AS400, mediante la configuraciones en el sistema operativo OS/400 V7R1M0 de los valores de sistema, que permitieron controlar, entre otros la complejidad de las contraseñas y los bloqueos automáticos de usuarios, sesiones y claves, el nivel de seguridad general del sistema, configurado en el valor *"QSECURITY"* se estableció en 40; además, para la creación de contraseñas de los usuarios, en el sistema se especificaron los valores para los parámetros: *"QPWDMINLEN", "QPWDLMTCHR", "QPWDLMTREP", "QPWDPOSDIF", "QPWDRQDDGT"*; que admitieron la creación de contraseñas débiles, que presentaron riesgo de ser vulneradas, pues su longitud mínima fue de 4 caracteres, conformadas con solo letras o solo números, claves que permitieron patrones con palabras comunes y con caracteres y dígitos repetidos, según se demuestra a continuación:

TREINTA Y UNO

VALOR DEL SISTEMA	DESCRIPCION	VALOR ASIGNADO	COMPORTAMIENTO
QPWDLVL	Nivel de contraseña	0	Se admiten las contraseñas de usuario con una longitud de 1 a 10 caracteres
QPWDMAXLEN	Longitud máxima de contraseña	10	La contraseña permite hasta 10 dígitos o caracteres
QPWDMINLEN	Longitud mínima de contraseña	4	La contraseña no puede contener menos de 4 dígitos y caracteres.
QPWDLMTCHR	Limitar caracteres en contraseña	*none	Permite que la contraseña contenga todo tipo o patrones de caracteres; palabras comunes como por ejemplo IESS.
QPWDLMTREP	Límite para caracteres repetidos	0	Pueden repetirse
QPWDPOSDIF	Límite para posiciones de caracteres en contraseña	0	No obliga a cambio de posición de los caracteres en la contraseña, permite patrones de contraseña, como por ejemplo: iess1, iess2, iess3.
QPWDRQDDGT	Dígito requerido en contraseña	0	No requerido

Al respecto, el Consejo Directivo del IESS con Resolución C.D. 521 de 28 de abril de 2016, emitió las *"Políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones"*, en los artículos 11 y 12, referentes a Generales y Administración del Título III Contraseñas, estableció:

> *"... **Art.- 11 Generales.-** El cumplimiento de la política de contraseñas por parte de las y los usuarios internos (funcionarios, servidores y trabajadores) del IESS, es extremadamente importante ya que constituyen la primera línea de defensa para garantizar que el acceso a los aplicativos informáticos sólo sea ejecutado por personal autorizado. Tanto equipos, sistemas y datos utilizan mecanismos de contraseñas para controlar acceso, como al inicio de sesión en la computadora, ingreso a la red institucional, para utilizar sistemas internos y externos, etc. No existe ninguna tecnología que pueda prevenir el acceso no autorizado.- **Art.- 12 Administración.-** Se acatará lo siguiente: ... 7.- Las contraseñas de los usuarios deben cumplir con ciertos requerimientos de seguridad los cuales definirá la Dirección Nacional de Tecnología de la Información con el objeto de evitar que los usuarios elijan contraseñas débiles. No se utilizarán contraseñas que resulten obvias, fáciles de adivinar o descubrir, o predecibles para un atacante: (el mismo identificador de usuario, palabras de diccionario, fechas o nombres de personas allegadas, secuencias de números repetidos o consecutivos)...".*

- Los bloqueos automáticos de sesión inactiva del Sistema de Información Médica MIS AS400, que se encontraron configurados en los valores de sistema: TREINTA Y DOS

"QINACTITV" y *"QDSCJOBITV"*, dieron al usuario la posibilidad de mantener abierta la sesión sin actividad por el lapso de 25 minutos.

- Adicionalmente, en la Coordinación de TIC's del HCAM, se desarrolló el programa *"SRRELOJ"*, que se encontró en ambiente de producción a partir de 18 de enero de 2014, este programa fue asignado a los usuarios médicos, la funcionalidad de un reloj denominado *"TEMPORIZADOR ATENCIÓN MÉDICA"*, permitió extender, sin límite, el tiempo de 25 minutos establecido en los valores de sistema *"QINACTITV"* y *"QDSCJOBITV"*, evitando el control de tiempo de bloqueo de sesión inactiva del sistema, pues se mantiene la sesión activa hasta que cualquier usuario lo desactive, incidiendo en el consumo de recursos del servidor de aplicaciones donde se encuentra instalado el sistema, en caso de permanecer activo; sin embargo, no se realizó un análisis por dependencia y especialidad, de los valores establecidos para el tiempo de bloqueo de sesión inactiva en el Sistema de Información Médica MIS AS400; ya que también, este sistema fue utilizado por las áreas administrativas de las Unidades Médicas, tales como: farmacia y bodega.

Al respecto, la Administradora del sistema de la Coordinación General de TIC del HCAM, explicó que esta configuración obedeció al tiempo requerido por el personal médico del hospital, quienes según lo establecido por el IESS, deben realizar el registro médico en el Sistema de Información Médica MIS AS400 y los procedimientos para la atención médica de los pacientes, también mencionó que en el caso de otras especialidades existentes en hospitales de nivel III, como por ejemplo: odontología y sicología requirieron de tiempos mayores al máximo establecido en el sistema de 25 minutos.

Como referencia, citamos el Esquema Gubernamental de Seguridad de la Información EGSI, que constó en el Acuerdo Ministerial 166 publicado en el Suplemento del Registro Oficial 88 de 25 de septiembre de 2013, elaborado en base a la norma NTE INEN-ISO/IEC 27002 *"Código de Práctica para la Gestión de la Seguridad de la Información"*, que establece controles al respecto del tiempo de inactividad de la sesión, en los siguientes términos:

> *"... 7.20. Tiempo de inactividad de la sesión a) Suspender las sesiones inactivas después de un período definido de inactividad sin consideración de lugar*

TREINTA Y TRES

dispositivo de acceso b) Parametrizar el tiempo de inactividad en los sistemas de procesamiento de información para suspender y cerrar sesiones ...".

Además, el Consejo Directivo del IESS con Resolución C.D 521 de 28 de abril de 2016, emitió las *"Políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones"*, en el artículo 33.- Generales, del Título *"Política de Desarrollo de Software"*, estableció:

"... 1.- Toda solicitud de desarrollo, evaluación o modificación de programas informáticos deberá empezar con el pedido formal a la Dirección Nacional de Tecnología de la Información, para su análisis y aprobación...".

Por lo que este desarrollo, no ha sido analizado ni aprobado por la Dirección Nacional de Tecnología de la Información.

- Para el bloqueo automático de usuarios y múltiple sesiones del Sistema de Información Médica MIS AS400, a través del software OS400 contó con los valores de sistema *"USREXPDATE"*, *"USREXPITV"* y *"LMTDEVSSN"*; en los dos primeros no se estableció la fecha e intervalo de caducidad de usuario y en el último no se limitó el número de sesiones de los dispositivos; lo que indicó que no se aplicaron controles de expiración automática de inactivación de usuarios, tal es el caso de los contratos de servicios ocasionales, de médicos practicantes (internado y externado), pasantes, proveedores, entre otros casos en los que se conoció el plazo de finalización de actividades por parte de estos servidores, trabajadores o terceros que prestaron sus servicios a la entidad; así también se establecieron valores entre 1 y 5 sesiones por dispositivo, permitiendo el ingreso múltiple al sistema desde el mismo computador o diferentes computadores, según se describe:

NOMBRE	PARAMETRO	DESCRIPCION
FECHA DE CADUCIDAD DEL USUARIO	USREXPDATE	Especifica la fecha en que el perfil de usuario caduca y se inhabilita automáticamente.
INTERVALO DE CADUCIDAD USUARIO	USREXPITV	Especifica el intervalo de caducidad (en días) que debe transcurrir antes de que el perfil de usuario se inhabilite automáticamente.
LIMITAR SESIONES	LMTDEVSSN	Especifica si el número de sesiones de dispositivo permitidas a un usuario está limitado.

Lo comentado se presentó debido a que los Directores Nacionales de Tecnología de la Información encargados con períodos de actuación comprendidos entre el: 25 de junio

TREINTA Y CUATRO

de 2014 y el 7 de enero de 2015; 18 de mayo de 2015 y el 31 de diciembre de 2016; no emitieron directrices para la elaboración y aplicación de procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médica MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, tampoco dieron lineamientos a los Coordinadores Generales de TIC's del HCAM para la administración de las seguridades a nivel de software; ya que no revisaron las configuraciones realizadas a través del sistema operativo OS/400 V7R1M0, en relación a seguridad de contraseñas y bloqueos automáticos de usuario y sesión.

La Coordinadora de la Unidad Informática del HCAM, encargada; los Coordinadores Generales de TIC's del HCAM titulares y encargados, de los períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 10 de agosto de 2014; 11 de agosto de 2014 y el 16 de diciembre de 2015; 18 de diciembre de 2015 y el 31 de diciembre de 2016; no propusieron, ni solicitaron al Director Nacional de Tecnología de la Información, la elaboración de los estándares y políticas que permitan generar los procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médicas MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, tampoco revisaron las seguridades a nivel de software, ni las configuraciones realizadas a través del sistema operativo OS400 V7R1M0, pues los valores del sistema: *"QPWDMINLEN", "QPWDLMTCHR", "QPWDLMTREP", "QPWDPOSDIF", "QPWDRQDDGT"* permitieron la creación de contraseñas débiles e incrementaron el riesgo de ser vulneradas (fáciles de adivinar), debido a que su longitud mínima fue de 4 caracteres, conformadas por letras o números, que pueden ser palabras comunes, letras o dígitos repetidos, tampoco parametrizaron basados en un análisis de los tiempos establecidos para el bloqueo de sesión inactiva del sistema por dependencia y especialidad, tanto para áreas médicas como administrativas, tales como: farmacia y bodega, pues el reloj denominado *"TEMPORIZADOR ATENCIÓN MÉDICA"*, evitó el control de bloqueo de sesión inactiva, manteniéndola activa hasta que cualquier persona la desactive, incidiendo en el consumo de recursos del servidor de aplicaciones donde se encuentra

TREINTA Y CINCO

instalado el sistema, en caso de mantenerse en ejecución; desarrollo que no fue analizado y aprobado por la DNTI, por lo que no se ajustó a las necesidades de las dependencias de las Unidades Médicas del IESS; ni configuraron los bloqueos automáticos de los usuarios en el caso de accesos temporales de los contratos de servicios ocasionales, de médicos practicantes (internado y externado), pasantes, proveedores, entre otros casos en los que se conoció el plazo de finalización de actividades por parte de estos servidores, trabajadores o terceros que prestaron sus servicios a la entidad a través de la aplicación de los valores del sistema operativo *"USREXPDATE", "USREXPITV"* y *"LMTDEVSSN"*; así también se establecieron valores entre 1 y 5 sesiones por dispositivo, permitiendo el ingreso múltiple al sistema desde el mismo computador o diferentes computadores.

Los Coordinadores Generales de TIC's del HJCA, de los períodos comprendidos entre el: 1 de septiembre de 2014 y el 30 de junio de 2015; y, 1 de julio de 2015 al 31 de diciembre de 2016, no propusieron ni solicitaron al Director Nacional de Tecnología de la Información la elaboración de los estándares y políticas que permitan generar los procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médica MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, entre otros.

Lo mencionado, ocasionó que las actividades de parametrización y administración de usuarios en el Sistema de Información Médica MIS AS400 no cumplan con requisitos estándares de información en el contenido de formularios, documentación de soporte, módulos solicitados, funciones, entre otros; para conceder el acceso a los usuarios, ni se hayan establecido las responsabilidades de los servidores que ejercieron actividades de administración a nivel nacional; que no se mantengan los expedientes completos y organizados del sustento de las autorizaciones de las acciones realizadas por los administradores del sistema en los Hospitales Carlos Andrade Marín y José Carrasco Arteaga; y que la configuración de seguridad aplicada incremente el riesgo de acceso no autorizados al sistema.

Por lo que los citados servidores, incumplieron lo dispuesto en los artículos 22.- Deberes de las o los servidores públicos letras a) y b) de la Ley Orgánica del Servicio

TREINTA Y SEIS

Público; letra e), del número 2.4.3, del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido por el Consejo Directivo del IESS, mediante Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referentes a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información; el artículo 41 números 1 y 7 del Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468 de 30 de mayo de 2014, en referencia a las funciones y perfiles de los órganos de gestión y dependencias que integran las Unidades Médicas de Nivel III; las Normas de Control Interno 200-07 Coordinación de acciones organizaciones; 401-03 Supervisión, 410-04 Políticas, y procedimientos ; y, 410-10 Seguridad de tecnología de información, y, artículos 1 y 2 de las *"Políticas que regulan las actividades relacionadas con el uso de Tecnologías y Comunicaciones"* emitidas con Resolución C.D. 521 de 28 abril de 2016, que establecen:

> *"...***C.D.457**... ***Art. 2.4.3 Dirección Nacional de Tecnología de la Información*** *... será responsable de la planificación, coordinación y dirección de las actividades referentes a los procesos de Gestión de Tecnológica de Información y Comunicaciones y tendrá las siguientes funciones y responsabilidades ... e) Generar lineamientos y directrices para la gestión de infraestructura de la tecnología de información, bases de datos, redes y sistemas, desarrollo y mantenimiento de aplicaciones y soporte técnico a usuarios ...".*
>
> *"...* **CD. 521**... ***Art. 1.- Finalidad.-*** *Las Políticas de Tecnología de la Información y Comunicación tienen como finalidad el proteger la información, a la Institución y buscar un aumento en la seguridad y aprovechamiento de la tecnología, lo que contribuye de manera determinante a aumentar la eficiencia en el trabajo y garantizar la continuidad de las operaciones de la Institución...* ***Art. 2.- Ámbito.-*** *Las Políticas de Tecnología de la información y Comunicación serán aplicadas de manera obligatoria por las y los funcionarios, servidores y trabajadores que integran el IESS a nivel nacional, que utilicen el hardware, software y comunicaciones, para el cumplimiento de sus actividades diarias. La Dirección Nacional de Tecnología de la Información será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su cargo el uso de recursos tecnológicos de forma desconcentrada...".*
>
> *"...* ***CD. 468.... Art. 41.- De la Coordinación General de Tecnología de la Información y Comunicación.-*** *... 1. Proponer las políticas para el acceso, manejo, y procesamiento de la información y de los servicios de red, a través de las herramientas de Tecnología de Información y Comunicación (TIC);... 7.*

TREINTA Y SIETE

Controlar la seguridad, integridad y proteger el carácter institucional de la información manejada por los usuarios...".

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0081, 0082, 0083, 0084, 0085, 0096; y, 0097-0010-IESS-AI-2017 de 9 de mayo de 2017 a los Directores Nacionales de Tecnología de la Información encargados; y, Coordinadores Generales de TIC's de los Hospitales: Carlos Andrade Marín; y, José Carrasco Arteaga, obteniendo las siguientes respuestas:

El Coordinador General de TIC's del HJCA, del período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, en respuesta al oficio 0096-0010-IESS-AI-2017, remitió la comunicación de 17 de mayo de 2017, en la que señaló:

"... Una vez realizada una visión general de la infraestructura informática y procesos que se llevaba dentro del (sic) Coordinación General de TIC's del HJCA emite un documento denominado ***"INFORME EJECUTIVO DE LA SITUACION ACTUAL DE LA COORDINACION DE TICS"****, donde se hace constatar en otros la falta de procesos que estén acordes a la resolución 468 .... y que garanticen el correcto uso y resguardo de la información que se genera en la parte administrativa... se han realizado las acciones necesarias para establecer políticas institucionales que deberían ser emitidas por la DNTI, las cuales como se puede observar no se tenían aprobadas y estandarizadas para las unidades médicas en el período de tiempo en el cual preste mis servicios a la institución ...".*

El Coordinador General de TIC's del HCAM, del período comprendido entre el 11 de agosto de 2014 y el 16 de diciembre de 2015, en respuesta al oficio 0082-0010-IESS-AI-2017, remitió la comunicación de 22 de mayo de 2017, en la que manifestó:

"... Es preciso señalar que, durante mi período de gestión se implementó una "Mesa de Ayuda" oficializada a través de Quipux y correo electrónico; razón por la cual, era de conocimiento y uso de los funcionarios de la Institución, la misma que se encuentra activa hasta la presente fecha, en la que se realizan los tramites que garantizan el cumplimiento de procedimientos y estándares de seguridad en la creación y desactivación de usuarios, lo cual demuestra la gestión efectuada para garantizar el cumplimiento de criterios de seguridad de acceso al Sistema... es preciso señalar que durante mi período de gestión no existió normativa legal o técnica emitida por autoridad competente mediante la cual se establezcan los parámetros o directrices de cumplimiento sobre los controles que deberían ser aplicados.- Por otra parte, debido a la cantidad de funcionarios y el poco número de computadores con los que cuenta la Institución existía la necesidad de que más de un usuario utilice el mismo dispositivo para iniciar su sesión, razón por la cual se establecieron ingresos múltiples por cada equipo conforme se indica en su observación...".

TREINTA Y OCHO

El Coordinador General de TIC's del HJCA, encargado, actuante en el período comprendido entre el 1 de julio de 2015 y el 31 de diciembre de 2016; en respuesta al oficio 0097-0010-IESS-AI-2017, remitió el memorando IESS-HJCA-CGTIC-2017-0148-M de 24 de mayo de 2017, en el que manifestó:

> *"... En base a la resolución CD 468 se establecen las actividades y directrices al personal de TIC incluidas la gestión de usuarios MIS-AS400... puesto que como política local todo el personal de TIC realiza el soporte a cada una de las áreas Médicas y Administrativas de HJCA, por lo que necesitan acceso respectivo al sistema para cumplir esta actividad así como la respectiva capacitación... En la coordinación General de TIC HJCA se dispone de un archivo físico de: Requerimiento de Usuario, Asignación de Clave y formulario de datos... ".*

Lo mencionado por los Coordinadores Generales de TIC's del HCAM y HJCA; no modifica el comentario de auditoría debido a que no propusieron ni coordinaron el establecimiento de procedimientos para la atención de solicitudes, autorización, entrega de claves, inactivación de usuarios, soporte; así como su documentación y archivo; tampoco sobre la implementación de mejores prácticas para la aplicación de controles de seguridad en la construcción de contraseñas, bloqueos automático, control de acceso y sesiones inactivas.

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016; en respuesta al oficio 0085-0010-IESS-AI-2017, remitió el memorando IESS-SDNSI-2017-0004-M de 22 de mayo de 2017, en el que señaló:

> *"... En mi período de gestión... como Director Nacional de Tecnología de la Información a partir de Julio de 2015, se preparó e impulsó una propuesta de políticas hasta llegar a su aprobación por parte del Consejo Directivo, lo que no fue efectuado por administraciones que me precedieron.- La Resolución Nro. C.D. 521 fue difundida por la Dirección Nacional de Gestión Documental, a través del sistema de gestión documental Quipux, para conocimiento y su aplicación a los titulares de las unidades administrativas y médicas del IESS a nivel nacional... según consta en memorando N° IESS-CD-2016-0178-ME de 28 de junio de 2016... Cabe indicar que, las directrices sobre los controles de contraseñas, se encuentran descritas en el Titulo III, artículo 12 de citada Resolución.- Además en razón de la gestión descentralizada del IESS, por seguros especializados, circunscripción territorial o jurisdicción, mediante memorando N° IESS-DNTI-2017-1520-M de 7 de abril de 2017, se solicitó e insistió a los titulares de las unidades administrativas y medicas a nivel*

TREINTA Y NUEVE

nacional, hacer cumplir y aplicar las políticas por parte del personal a su cargo... Esta estructura autónoma que le concedió la Resolución N° C.D. 468 a la Coordinación de Tecnologías de la Información y Comunicación, ha traído contratiempo en la gestión de la Dirección Nacional de Tecnología de la Información – DNTI ... Por lo expuesto, considero que para poder supervisar y controlar mejor manera a la Coordinación de Tecnologías de la Información y Comunicación de los hospitales de nivel III, con el propósito que se alineen a las disposiciones, procedimientos, procesos, directrices y demás lineamientos que señale la DNTI, y no continuar al margen de consolidar las seguridades de la plataforma tecnológica institucional, se debería proceder a la revisión de la Resolución N° C.D. 468 con relación a las responsabilidades de dichas coordinaciones, puesto que deben ser definidas como unidades de apoyo tecnológico... y no con competencias y funciones similares o equivalentes a la Dirección Nacional de Tecnología de la Información... ".

Lo mencionado, por el Director Nacional de Tecnología de la Información, encargado, no modifica lo comentado de auditoría, en razón de que no presentó un proyecto de reforma a la normativa vigente para organizar las actividades, funciones y responsabilidades de las Coordinaciones Generales de Tecnología y Comunicaciones en los hospitales de tercer nivel, tampoco evidenció directrices emitidas para gestión, documentación y actividades de administración de usuarios y parametrización del Sistema de Información Médica AS400, ni dio lineamientos para la aplicación de mejores prácticas para la configuración de seguridad de contraseñas, inactivación de sesiones, bloqueos automáticos entre otros.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, con comunicación de 29 de mayo de 2017, acotó:

"... Existe falta de interpretación en el establecimiento de las funciones del Coordinador de TICs de los Hospitales de Nivel III, lo que conlleva a seguir manteniendo mi postura al decir que es DNTI es la encargada de realizar y difundir políticas del manejo de este sistema ya que las mismas debería ser reflejadas a toda la institución.- Es importante indicar que no se pueden emitir políticas para el manejo de sistemas que no son administrados de manera directa por las unidades médicas ya que no se conoce de manera adecuada el desarrollo del mismo y al emitir documentos diferentes e individuales no se logra solventar de ninguna manera la correcta estandarización de las mismas a

GARANTÍA

nivel institucional, pudiéndose producir vacíos que afecten el uso del sistema...".

Lo comentado por el Coordinador General de TIC's del HJCA; evidenció la falta de procedimientos estándares para la administración del Sistema de Información Médica AS400, gestión de usuarios, seguridad y parametrización.

El Coordinador General de TIC's del HCAM, actuante con período comprendido entre el 18 de diciembre de 2015 y el 31 de diciembre de 2016, en respuesta a lo expresado en la conferencia final de resultados, con memorando IESS-HCAM-CGTIC-2017-1125-M de 5 de junio de 2017, señaló:

"... me permito indicar que ésta Coordinación cuenta con una herramienta de gestión JTRAC, a través de la cual se registra las solicitudes de cambios, de parametrización del sistema la misma que se solicitó de manera formal a la Dirección Nacional de Tecnología de la Información Memorando Nro. IESS-HCAM-CGTIC-2016-0419-M con fecha 23 de marzo de 2016, y fue atenida (sic) mediante Memorando Nro. IESS-DNTI-2016-1329-M. En el cual se lleva la documentación del cambio a implementarse y aprobación de los requerimientos previa la puesta producción.- Mediante Memorando Nro. IESS-DSGSIF-2017-0528-M de fecha 11 de febrero de 2017 la Dirección Nacional de Salud-IESS, nombra un analista funcional del sistema de Gestión Hospitalaria MIS-AS400 que actúa como la contraparte de la Coordinación General de Tecnologías de la Información y Comunicación –HCAM a través del cual se está canalizando los pedidos y se está gestionando la atención de los requerimientos y gestión de cambios en el sistema MIS-AS400.- (...) con el fin de atender, esta observación y que a su vez acatando lo indicado en la Resolución C.D 521 de 28 de abril de 2016, emitió las "Políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones", en los artículos 11 y 12... Se realizó el análisis de la configuración de seguridad del Sistema Operativo OS/400 V7R1M0 el mismo que fue presentado al Director de Dirección Nacional de Tecnología de la Información y mediante acta de reunión adjunta se implementaron mejoras en la seguridad a partir del 01 de junio de 2017, las mismas que contemplan: Se establece tener una clave de 8 a 10 caracteres.- Debe contener dígitos la contraseña.- Cambiar el parámetro para que no repita las últimas 10 contraseñas.- Las mismas que fueron comunicadas mediante la Dirección Nacional de Salud-IESS mediante memorandos IESS-DSGIF-2017-1592-M a nivel nacional.- (...) me permito adjuntar el análisis realizado del uso del temporizador que se encuentra actualmente implementado en el sistema médico AS400, el documento se encuentra en pruebas para enviar a la aprobación de la Dirección Nacional de Salud, una vez aprobado pueda ser implementado en producción y comunicado a nivel nacional a los usuarios del sistema...".

Lo comentado, por el Coordinador General de TIC's del HCAM, encargado, actuante con período comprendido entre el 18 de diciembre de 2015 y el 31 de diciembre de

CUARENTA Y UNO

2016, no modifica el comentario de auditoría, por cuanto, presentó las acciones correctivas realizadas, posteriormente al corte del examen especial, conforme las observaciones determinadas en este comentario, tampoco demostró la supervisión en la ejecución y documentación de los procedimientos realizados para la solicitud, autorización, atención para las actividades de creación, reseteo, inactivación y gestión de usuarios y opciones asignadas en el Sistema de Información Médica MIS AS400, no obstante la implementación de la herramienta JTRAC se refirió a una parte de la atención de cambios en el sistema, como es el desarrollo y mantenimiento del aplicativo.

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, con memorando IESS-SDNSI-2017-0017-M de 2 de junio de 2017, señaló:

> *"...La Subdirección Nacional de Seguridad Informática, en aras del cumplimiento del robustecimiento de las claves de los equipos y sistemas en general de la Institución ha emitido el documento "ADMINISTRACION CONFIDENCIAL Y SEGURA DE CLAVES DE ACCESO.- Directriz" cuyo objetivo es instrumentar la aplicación del numeral 7 del artículo CD 521... y ha entregado en reunión de trabajo a la Coordinación de TICS del HCAM dicho documento para su revisión y análisis de la viabilidad de aplicación sobre el sistema AS400... ".*

Lo comentado, no modifica el comentario de auditoría, por cuanto las acciones correctivas se presentaron posteriores a la fecha de corte del examen especial, ni evidenció propuestas para la revisión de la normativa expresada en la Resolución C.D 468 acerca de las funciones y responsabilidades de la Coordinación General de Tecnología y Comunicaciones de los Hospitales de tercer nivel.

Conclusiones

- Los Directores Nacionales de Tecnología de la Información encargados no emitieron directrices para la elaboración y aplicación de procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médica MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, tampoco dieron lineamientos a los

CUARENTA Y DOS

Coordinadores Generales de TIC's del HCAM para la administración de las seguridades a nivel de software; ya que no revisaron las configuraciones realizadas a través del sistema operativo OS/400 V7R1M0 en relación a seguridad de contraseñas y bloqueos automáticos de usuario y sesión, lo que ocasionó que las actividades de parametrización y administración de usuarios en el Sistema de Información Médica MIS AS400 no cumplan con requisitos estándares de información en el contenido de formularios, documentación de soporte, módulos solicitados, funciones, entre otros; para conceder el acceso a los usuarios, ni se hayan establecido las responsabilidades de los servidores que ejercieron actividades de administración a nivel nacional; qué no se mantengan los expedientes completos y organizados del sustento de las autorizaciones de las acciones realizadas por los administradores del sistema en los Hospitales Carlos Andrade Marín y José Carrasco Arteaga; y que la configuración de seguridad aplicada incremente el riesgo de acceso no autorizados.

- La Coordinadora de la Unidad Informática del HCAM, encargada, los Coordinadores Generales de TIC's del HCAM, encargados, no propusieron, ni solicitaron al Director Nacional de Tecnología de la Información la elaboración de los estándares y políticas que permitan generar los procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médica MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, tampoco revisaron las seguridades a nivel de software, ni las configuraciones realizadas a través del sistema operativo OS/400 V7R1M0, pues los valores del sistema: *"QPWDMINLEN", "QPWDLMTCHR", "QPWDLMTREP", "QPWDPOSDIF", "QPWDRQDDGT"* permitieron la creación de contraseñas débiles e incrementaron el riesgo de ser vulneradas (fáciles de adivinar), debido a que su longitud mínima fue de 4 caracteres, conformadas por letras o números, que pueden ser palabras comunes, letras o dígitos repetidos, tampoco parametrizaron basados en un análisis de los tiempos establecidos para el bloqueo de sesión inactiva del sistema por dependencia y especialidad, tanto para áreas médicas como administrativas, tales como: farmacia y bodega, pues el reloj denominado *"TEMPORIZADOR ATENCIÓN MÉDICA"*, evitó el control de bloqueo de sesión inactiva, manteniéndola activa hasta que cualquier persona la

CUARENTA Y TRES

desactive, incidiendo en el consumo de recursos del servidor de aplicaciones donde se encuentra instalado el sistema, en caso de mantenerse en ejecución; desarrollo que no fue analizado y aprobado por la DNTI, por lo que no se ajustó a las necesidades de las dependencias de las Unidades Médicas del IESS; ni configuraron los bloqueos automáticos de los usuarios en el caso de accesos temporales de los contratos de servicios ocasionales, de médicos practicantes (internado y externado), pasantes, proveedores, entre otros casos en los que se conoció el plazo de finalización de actividades por parte de estos servidores, trabajadores o terceros que prestaron sus servicios a la entidad a través de la aplicación de los valores del sistema operativo *"USREXPDATE", "USREXPITV"* y *"LMTDEVSSN";* así también se establecieron valores entre 1 y 5 sesiones por dispositivo, permitiendo el ingreso múltiple al sistema desde el mismo computador o diferentes computadores, lo que ocasionó que las actividades de parametrización y administración de usuarios en el Sistema de Información Médica MIS AS400 no cumplan con requisitos estándares de información en el contenido de formularios, documentación de soporte, módulos solicitados, funciones, entre otros; para conceder el acceso a los usuarios, ni se hayan establecido las responsabilidades de los servidores que ejercieron actividades de administración a nivel nacional; que no se mantengan los expedientes completos y organizados del sustento de las autorizaciones de las acciones realizadas por los administradores del sistema en el Hospital Carlos Andrade Marín; y que la configuración de seguridad aplicada incremente el riesgo de acceso no autorizados al sistema.

- El Coordinador General de TIC's del HJCA y el Coordinador General de TIC's del HJCA, encargado, no propusieron ni solicitaron al Director Nacional de Tecnología de la Información la elaboración de los estándares y políticas que permitan generar los procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médica MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, entre otros, lo que ocasionó que las actividades de parametrización y administración de usuarios en el Sistema de Información Médica MIS AS400 no cumplan con requisitos estándares de información en el contenido de formularios, documentación de soporte, módulos solicitados, funciones, entre otros; para

COMPARENTES Y CONSTANTE

conceder el acceso a los usuarios, ni se hayan establecido las responsabilidades de los servidores que ejercieron actividades de administración a nivel nacional; que no se mantengan los expedientes completos y organizados del sustento de las autorizaciones de las acciones realizadas por los administradores del sistema en el Hospital José Carrasco Arteaga.

Recomendaciones

Al Director Nacional de Tecnologías de la Información

7. Coordinará con los Directores Nacionales de Procesos y de Riesgos Institucionales, la elaboración de los estándares y políticas que permitan generar los procedimientos para regular las actividades y responsabilidades de los administradores del Sistema de Información Médicas MIS AS400, así como, de los servidores de las áreas requirentes, con respecto de la solicitud, autorización, documentación de soporte, para la creación, usuarios, entrega de claves, asignación de perfiles, reseteo de claves, activación e inactivación de usuarios, entre otros, documentos que serán puestos a consideración del Director General y Director del Seguro de Salud Individual y Familiar, respectivamente, para su respectiva aprobación y difusión a nivel institucional.

8. Coordinará con los Directores Nacionales de Procesos y de Riesgos Institucionales, analizaran la Resolución C.D. 468, en relación a las competencias de la Coordinación General de Tecnologías de la Información y de considerar procedente, elaboran un proyecto de reforma de la misma, que permita regular las actividades en relación, a la propuesta de políticas, actividades de desarrollo y mantenimiento de sistemas, y demás que se contrapongan con lo establecido en la Resolución C.D. 535, a fin de que el marco normativo permita el trabajo coordinado y alineado a las políticas, lineamientos y procedimientos dictados por la DNTI, responsable del sistema informático Institucional, infraestructura y plataformas.

9. En coordinación con la Dirección Nacional de Riesgos Institucionales, establecerán la política institucional de seguridad para la implementación de controles en los sistemas informáticos para la construcción contraseñas seguras, su caducidad y demás controles automáticos para el acceso seguro al Sistema de Información

CUARENTA Y CINCO

Médica MIS AS400, como es el caso de bloqueo de sesiones por inactividad, número permitido de sesiones por usuario, caducidad de usuarios temporales y sin actividad, entre otros.

Al Coordinador General de TIC's del HCAM

10. Implementará y administrara las seguridades del Sistema de Información Médica MIS AS400, revisando las configuraciones realizadas a través del sistema operativo OS400 V7R1M0, a fin de que los parámetros: *"QPWDMINLEN", "QPWDLMTCHR", "QPWDLMTREP", "QPWDPOSDIF", "QPWDRQDDGT"* no permitan la creación de contraseñas débiles y que representan riesgo de ser vulneradas (fáciles de adivinar), sin que se acepten patrones con palabras comunes y con caracteres y dígitos repetidos, así también revisará la configuración de los valores de sistema *"USREXPDATE", "USREXPITV" y "LMTDEVSSN";* a fin de caducar los accesos de usuarios temporales y limitar el número de sesiones por dispositivo para impedir el ingreso múltiple al sistema desde el mismo computador o diferentes computadores.

11. Revisará en conjunto con la Dirección Nacional de Tecnología de la Información, la implementación del programa *"SRRELOJ", "TEMPORIZADOR DE ATENCION MEDICA"* de modo que su uso sea restringido y se asigne de ser el caso únicamente a personal médico, también aplicará modificaciones que permitan limitar el tiempo máximo de uso de este programa conforme los parámetros de tiempo de atención máxima permitidos por especialidad en la Unidad Médica.

No se establecieron procedimientos para el otorgamiento de una identificación única a los usuarios del Sistema de Información Médica MIS AS400

El Coordinador General de TIC's del HCAM, con memorando IESS-HCAM-CGTIC-2017-0462-M de 7 de marzo de 2017, adjuntó, en formato digital los registros correspondientes a los usuarios y autorizaciones a nivel nacional del Sistema de Información Médica MIS AS400, a partir de la cual se tomó una muestra de usuarios con estado activo de los Hospitales de tercer nivel: Carlos Andrade Marín, Teodoro Maldonado Carbo, José Carrasco Arteaga, en la que se observó lo siguiente:

- De 12 usuarios del Hospital Carlos Andrade Marín, 5 del Hospital Teodoro Maldonado Carbo y 13 del Hospital José Carrasco Arteaga, no se registró el

CUARENTA Y SEIS

nombre del servidor autorizado para el ingresó, en su lugar se anotó la descripción de la actividad o uso, tales como: *"terapista ver registro médico", "consultas QRY", "Jhon", "usuario de oftalmología del día",* entre otros, o registran números de cédulas de ciudadanía con errores, según se detalla:

Hospital	Estado	Perfil usuario	Nombre	Cédula	Referencia	Grupo	Programa
Carlos Andrade Marín	A	MTTERAPIA	Terapista Ver Registro Medico		Terapista ver registro medico	CMEDIC	MEDI10
	A	RP1701001	Usuario Repestad HCAM		Usuario de informática	CADMIE	REPES00
	A	AMQUERY	Usuario Para Realización De Qrys		Consultas	CFACTU	CONS01
	A	DCE1701001	Docencia Dr. Izquierdo Cesar		Docencia	CFACTU	*none
	A	CXPAQUETE	Informática Conexión		C1722624226		
	A	MTQUERY	Consultas Qry		Consultas	CMEDIC	CONS01
	A	MT9999003	Consultas Médicos Proyecto Md Research		Consultas médicos proyecto	CMEDIC	CONS01
	A	FT1701043	Disponible 4			CFACTU	CONTROU
	A	MA1701352	Usuario Disponible Ma			CMEDIC	MEDI10
	A	EFJHON1	Jhon	1710307941		CENFER	ENF000
	A	EFOFTAL	Usuario de Oftalmología Del Día	1801786250	Oftalmología ho día	CENFER	ENF000
	A	TL1701003	Usuario patología a nivel nacional		Patología	CSERVI	SERV00
Teodoro Maldonado Carbo	A	AH0902095	Consult. historias clínicas 2		Ventanilla de dosis unitaria-	CADMI	MEDI10
	A	AH0902114	Consult. historias clínicas 6		-Ventanilla de dosis unitaria-	CADMI	MEDI10
	A	AU0902610	****			CENFER	ENF000
	A	EF0903055	Usuario enfermería*	0918713371	ENFERMERIA	CENFERC	ENF000

CUARENTA Y SIETE

Hospital	Estado	Perfil usuario	Nombre	Cédula	Referencia	Grupo	Programa
José Carrasco Arteaga	A	MT0103359	(*)	E226303		CMEDIC	MEDI10
	A	IF0103077	Estudiantes docencia 8			CMEDIC	MEDI10
	A	MR010339	Usuario libres			CMEDIC	MEDI10
	A	MR0103609	Usuario invalido	966		CMEDIC	MEDI10
	A	AX0103018	Disponible ax			CENFER	ENF000
	A	PR0106063	Usuario capacitación (*)			CSERVI	SERV00
	A	EF0103563	Usuario para reportes dtv			CENFER	ENF000
	A	BD0103074	Usuario asignado a Contraloría			INVBODUM	INVCL003
	A	IF0103103	Estudiantes			CMEDIC	MEDI10
	A	EF0103135	(*)	030110601-		CENFER	ENF000
	A	EF0103205	(*)	0104/80759		CENFER	ENF000
	A	PR0103136	(*)	E226303		CSERVI	SERV00
	A	RP0103001	Usuario de reportes			CADMIE	REPES00

(*) Consta el nombre del usuario

- Constaron 1.129; 27 y 576 registros de usuarios de la base de datos del Sistema de Información Médica MIS AS400 en los Hospitales Carlos Andrade Marín, Teodoro Maldonado Carbo y José Carrasco Arteaga, sin ningún dato en el campo de cédula de ciudadanía, según se detalla:

Hospital	Usuarios	Campos de cédula de ciudadanía vacíos	%
Carlos Andrade Marín	4.583	1.129	24,63%
Teodoro Maldonado Carbo	2.276	27	3,70%
José Carrasco Arteaga	1.751	576	32,90%

- En el campo *"NOMBRE_USUARIO_CREA"* donde se debió registrar el nombre del servidor que creó los usuarios en la base de datos del Sistema de Información Médica MIS AS400, constaron: 1.293; 569 y 301 registros para cada caso en los hospitales: HCAM, HTMC y HJCA, en su orden, en los que se ingresaron datos como: *"súper usuario nacional", "usuario del sistema de réplica", "usuario* GARANTÍA VOCHOR

producción bodegas", "administrados de bodegas"; que correspondieron a perfiles de usuarios administradores del sistema sin identificar, según se presenta a continuación:

Nombre de servidores que crearon usuarios	HCAM	HTMC	HJCA
SUPER USUARIO NACIONAL SISTEMA AMBULATORIOS	42		
USUARIO DEL SISTEMA DE REPLICA	1.215	545	301
USUARIO PRODUCCION BODEGAS (SUPERUSUARIO)	36		
ADMINISTRADOR DE BODEGAS HTMC		24	
Total general:	**1.293**	**569**	**301**

Por lo expuesto, los usuarios internos, externos y temporales no fueron identificados a través de cédula y nombre; y, en el caso de usuarios genéricos para conexión de procesos automáticos u otro propósito, que estos sean catalogados de uso exclusivo y el acceso de responsabilidad del área informática.

Lo comentado, se presentó debido a que la Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 10 de agosto de 2014; 11 de agosto de 2014 y el 16 de diciembre de 2015; y, 18 de diciembre de 2015 y el 31 de diciembre de 2016; la Coordinadora Informática del HTMC, encargada, los Coordinadores Generales de TIC's del HTMC encargados y titulares, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014; desde el 13 de agosto de 2014 y el 7 de enero de 2015; desde el 2 de marzo de 2015 y el 10 de abril de 2015, desde el 18 de mayo de 2015 y el 31 de mayo de 2015, 1 de junio de 2015 y el 22 de junio de 2015; y, del 29 de julio de 2015 y el 20 de marzo de 2016; y desde el 21 de marzo de 2016 y el 13 de diciembre de 2016; los Coordinadores Generales de TIC's del HJCA, titular y encargado, actuantes en los períodos comprendidos entre el: 1 de septiembre de 2014 y el 30 de junio de 2015; y 1 de julio de 2015 y el 31 de diciembre de 2016; no establecieron los procedimientos para el otorgamiento de una identificación única a todos los usuarios internos, externos, temporales; y, la elaboración, aprobación y difusión para la creación de usuarios genéricos que interactúan con el Sistema de Información Médica MIS AS400, en casos de excepción, lo que ocasionó la imposibilidad de identificar a las personas

CORRESPONDE

responsables del uso de usuarios y contraseñas en el sistema e incrementando el riesgo de acceso no autorizado al sistema y sus bases de datos.

Los referidos servidores incumplieron lo dispuesto en las letras a) y b) del artículo 22.- Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; números 1 y 7 del artículo 41 de la Coordinación General de Tecnologías de la Información y Comunicación, del Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, referente a las funciones y perfiles de los órganos de gestión y dependencias que integran las Unidades Médicas de Nivel III; y la Norma de Control Interno 410-12 Administración de soporte de tecnología de información.

El Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, establece:

> *"... Art. 41.- De la Coordinación General de Tecnología de la Información y Comunicación.-... 1. Proponer las políticas para el acceso, manejo, y procesamiento de la información y de los servicios de red, a través de las herramientas de Tecnología de Información y Comunicación (TIC);... 7. Controlar la seguridad, integridad y proteger el carácter institucional de la información manejada por los usuarios...".*

Los Directores Nacionales de Tecnología de la Información encargados con períodos de actuación comprendidos entre el: 25 de junio de 2014 y el 7 de enero de 2015; y, 18 de mayo de 2015 y el 31 de diciembre de 2016, no emitieron directrices a los Coordinadores de TIC's de los hospitales HCAM, HTMC y HJCA para la creación de usuarios de manera que todos se encuentren identificados con el nombre del servidor que es responsable de la utilización de la clave de acceso al sistema de Información Médica MIS AS400 y procedimientos de excepción para el manejo de usuarios genéricos, la imposibilidad de establecer responsabilidades y acuerdos sobre el uso y confidencialidad de la información con los usuarios internos, externos y temporales no identificados a través de cédula y nombre; y, en el caso de usuarios genéricos para conexión de procesos automáticos u otro propósito, que estos sean catalogados de uso exclusivo y el acceso de responsabilidad del área informática; lo que ocasionó la imposibilidad de identificar a las personas responsables del uso de usuarios y

cincuenta y

contraseñas en el sistema, incrementando el riesgo de acceso no autorizado al sistema y sus bases de datos.

Los referidos servidores incumplieron lo dispuesto en los artículos 22.- Deberes de las o los servidores públicos, las letras a) y b) de la Ley Orgánica del Servicio Público, la letra e), del número 2.4.3, del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido por el Consejo Directivo del IESS, mediante Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referentes a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información; y, las Normas de Control Interno 200-07 Coordinación de acciones organizacionales, 401-03 Supervisión, 410-04 Políticas, y procedimientos ; y, 410-12 Administración de soporte de tecnología de información.

La Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referente a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información, establece:

> *"...e) Generar lineamientos y directrices para la gestión de infraestructura de la tecnología de información, bases de datos, redes y sistemas, desarrollo y mantenimiento de aplicaciones y soporte técnico a usuarios...".*

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0081, 0082, 0083, 0086, 0087, 0088, 0090, 0096, 0097; 0084 y 0085-0010-IESS-AI-2017 de 9 de mayo de 2017; a los Coordinadores Generales TIC's del HCAM; a los Coordinadores Generales de TIC's del HTMC; a los Coordinadores Generales de TIC's del HJCA; y, los Directores Nacionales de Tecnología de la Información encargados, obteniendo las siguientes respuestas:

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, en respuesta al oficio 0096-0010-IESS-AI-2017, con comunicación de 17 de mayo de 2017, señaló:

> *"... Una vez realizada una visión general de la infraestructura informática y procesos que se llevaba dentro del* (sic) *Coordinación General de TIC's del HJCA se emite un documento denominado* ***"INFORME EJECUTIVO DE LA SITUACION ACTUAL DE LA COORDINACION DE TICS"****, donde se hace*

CINCUENTA Y UNO

constatar en otros la falta de procesos que estén acordes a la resolución 468 y la falta de una plataforma CORE de servidores o software sobre la cual se deben implementar los sistemas o servicios que ayudaran a generar una plataforma estándar y controlada de aplicativos que ayudarían a generar mejores tiempos de respuesta en los trabajos cotidianos que el personal desempeña y que garanticen el correcto uso y resguardo de la información que se genera en la parte administrativa... se han realizado las acciones necesarias para establecer políticas institucionales que deberían ser emitidas por la DNTI, las cuales como se puede observar no se tenían aprobadas y estandarizadas para las unidades médicas en el período de tiempo en el cual preste mis servicios a la institución, es importante indicar que el centralismos que maneja DNTI no permitió implementar una serie de proyectos bases en la plataforma CORE informática del HJCA y que se manejan en otras instituciones públicas del país...".

El Coordinador General de TIC's del HCAM, que actuó en el período comprendido entre el 11 de agosto de 2014 y el 16 de diciembre de 2015, en respuesta al 0082-0010-IESS-AI-2017, con comunicación de 22 de mayo de 2017, señaló:

"... Durante mi período de gestión se implementó una "Mesa de ayuda", la misma que se encuentra activa hasta la presente fecha, con el objetivo de estandarizar procedimientos que garanticen el cumplimiento de estándares de seguridad en la creación y desactivación de usuarios...".

Lo mencionado por los Coordinadores Generales de TIC's del HCAM y HJCA, no modifica el comentario de auditoría debido a que no informaron los motivos por los cuales se crearon usuarios que no identificaron a los servidores y/o responsables de su uso en el Sistema de Información Médica MIS AS400.

El Coordinador General de TIC's del HCAM, que actuó en el período comprendido entre el 21 de marzo de 2016 y el 13 de diciembre de 2016, en respuesta al 0090-0010-IESS-AI-2017, con comunicación de 22 de mayo de 2017, señaló:

"... puedo indicar que durante los 9 meses que estuve como Coordinador de TIC del HTMC, no se recibió directriz alguna por Quipux sobre creación de usuarios de parte de la Dirección Nacional de Tecnologías de la Información del IESS, ni del Hospital Carlos Andrade Marín de la ciudad de Quito, los cuales son los que administran el Sistema de Información Médica AS400 a nivel nacional, es decir no era exigido ingresar el número de cédula de los usuarios que se creaban en el sistema, pero como medida de control y seguridad informática se implementó en mi Coordinación un formulario físico para la creación del usuario el cual era llenado por la persona, adjuntando su copia de cédula y su copia de contrato o acción de personal.- Si la persona que ingresaba a la institución era un médico o enfermera debían anexar el Quipux o memorando por parte del Jefe del Servicio, indicando las dependencias y los

CINCUENTA Y DOS

procedimientos médicos que debían estar activados en el sistema, así como el horario en el que iban a laborar.- Es por eso que apenas constan 27 usuarios creados sin número de cédula de un total de 2.276. En cuanto a los dos usuarios AH0902095 y AH0902114 asignados a Ventanillas de dosis unitaria, fue solicitada su creación por parte de la Jefe de Farmacia del HTMC... con permiso en el sistema para consultar la historia clínica de los pacientes con la finalidad de elaborar la dosis unitaria de medicamentos adecuada recetada por los médicos... Estos dos usuarios podía (sic) *ser utilizados por todo el personal que laboraba en el área de dosis unitaria de farmacia, es por esto que en el sistema no se registró el número de cédula ni nombre de usuario. De la misma manera ocurrió con los dos usuarios de enfermería AU0902610 y EF0903055 los cuales fueron creados para ser utilizados en los aplicativos desarrollados y colgados en la Intranet del HTMC para censo de camas y dietas de pacientes hospitalizados por lo cual no eran usados por un usuario especifico...".*

Lo mencionado por el Coordinador General de TIC's del HCAM, no modifica el criterio de auditoría, en razón de que no evidenció procedimientos y lineamientos en relación al uso y responsabilidad del acceso de usuarios genéricos, y de conexión para aplicativos.

El Director Nacional de Tecnología de la Información, encargado con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016; en respuesta al oficio 0085-0010-IESS-AI-2017, con memorando IESS-SDNSI-2017-0004-M de 22 de mayo de 2017, señaló:

"... la DNTI el 28 de enero de 2016, elaboró el Procedimiento de Acceso a la Base de Datos Stand By, en el cual entre otros aspectos, se regula la creación de usuarios genéricos, con el objetivo de controlar los accesos a la base con criterios de seguridad informática, por lo tanto, la creación de usuarios genéricos es a solicitud del negocio, previa autorización de su titular, su control es netamente administrativo en coordinación con la unidad de Talento Humano.- Cabe indicar que el referido procedimiento no se puso en conocimiento de la dependencias administrativas y medicas a nivel nacional, toda vez que sobre la base de las funciones establecidas en la Resolución C.D 457, la DNTI es la única dependencia habilitada para efectuar desarrollos de sistemas; empero, (...) la Resolución C.D. 468 le dio potestad a la Coordinación de Tecnologías de la Información y Comunicaciones de los hospitales de nivel III, de desarrollar programas o software para las unidades médicas, sin que estas se hayan previamente coordinado con esta dirección, por lo tanto, los usuarios genéricos creados en el sistema AS400 son de exclusiva responsabilidad de quienes los ejecutaron y de la autoridad que dispuso crearlos, más aún cuando la base de datos del sistema médico AS400 está bajo la custodia y administración del HCAM...".

Lo comentado, por el Director Nacional de Tecnología de la Información, no modifica el comentario de auditoría, puesto que no emitió directrices relacionadas con la

identificación de los usuarios y creación de usuarios genéricos en las bases de datos de los Sistemas de Información del Instituto, entre ellos, el Sistema de Información Médica MIS AS400.

La Coordinadora Informática del HTMC, encargada y Coordinadora General de TIC's del HTMC, encargada; que actuó en el período comprendido entre el 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014; en respuesta al oficio 0086-0010-IESS-AI-2017, con oficio JRI-2017-001 de 23 de mayo de 2017, señaló:

> *"... En el cuadro adjunto del presente oficio extraído de la base de datos de los usuarios entregados por el HCAM constan 4 pertenecientes al Hospital Teodoro Maldonado Carbo los cuales revisando la base de datos fueron creados en el año 2015 y 2016 años que no corresponde a mi período de gestión como Coordinadora General de Tecnología de Información.- En el caso de los usuarios mencionados el Sistema permitió crearlos de esa manera porque en la fecha de creación no estaba implementado el control con la base de datos del registro civil la cual fue puesta en producción el 18 de noviembre de 2016(...).- Referente a los campos de cédula de ciudadanía, debo indicar que no constan ingresados ningún dato en el caso del HTMC = 27 campos vacíos de cédulas de ciudadanía, debo indicar... la implementación del control con la base de datos del registro civil fue implementada el 18 de noviembre de 2016 por el HCAM año que no corresponde a mi período de gestión(...) Es necesario recalcar que los 27 usuarios faltantes no se encontraron en la base de datos de afiliados la cual se tomó como universo para actualizar el universo de usuarios del HTMC.- Al respecto del campo donde debió registrar el nombre del servidor que creó los usuarios para el Sistema de Información Médica AS400, contaron 569 del HTMC; debo indicar a usted que el registro de quien creó un usuario es transparente para el Administrador del Sistema que maneja funciones básicas ya que es un proceso interno del Sistema AS400 que lo administra el HCAM.- El 9 de octubre del año 2013 envié por escrito las funciones al personal que estaba a mi cargo detallando cada una de las actividades de las cuales estaban responsables...Además cabe recalcar que durante mi gestión nunca se establecieron procedimientos y/o funciones que se debían cumplir por parte de la Dirección Nacional de Tecnología de la Información...".*

Lo mencionado por la Coordinadora Informática del HTMC, encargada, no modifica el comentario de auditoría, por cuanto, en conocimiento de la ausencia de control para la identificación de los usuarios creados en el sistema informático, no presentó sus observaciones al respecto a los administradores del Sistema de Información Médica MIS AS400 en el Hospital Carlos Andrade Marín, responsables de la aplicación de mejoras y cambios en el citado aplicativo.

CINCUENTA Y CUATRO

El Coordinador General de TIC's del HJCA, encargado, actuante en el período comprendido entre el 1 de julio de 2015 al 31 de diciembre de 2016; en respuesta al oficio 0097-0010-IESS-AI-2017, con memorando IESS-HJCA-CGTIC-2017-0148-M de 24 de mayo de 2017, señaló:

> *"... En lo referente a 13 usuarios con incoherencias en HJCA se detalla: En el caso de los usuarios que no fueron creados con la cédula de ciudadanía en la referencia, es debido a que eran funcionarios extranjeros y su número de identidad no se encuentra registrado para los casos MT010335* (sic) *y PR0103136.- Para los usuarios que registran una descripción en lugar del nombre, fueron creados en gestiones anteriores, al momento se encuentran inactivos.- Se ha restringido la creación de usuarios para reportes y estadísticas, debido a que la información que muchas veces se requiere, se remite al Departamento de Planificación y Estadística, quienes tienen los usuarios con los perfiles correspondientes para ese manejo de la información , y los usuarios mencionados ya no son utilizados.- El usuario asignado BD0103563*(sic) *fue solicitado para un examen especial por la Contraloría.- Los usuarios EF0103135, EF0103136* (sic) *se encuentran laborando y activos en el sistema según el rol que desempeñan en el MIS-AS400 (...).- En base a lo establecido en la resolución 468, articulo 41... y en base a la asignación al cargo de Coordinador de TIC HJCA a la fecha se ha realizado las siguientes acciones: Se asignó un persona para la gestión y depuración de usuarios en el Área de TIC.- Todo requerimiento para creación para creación de usuarios en MIS-AS400 se recibe y gestiona por Quipux, se registra: pedido, formulario de datos y asignación de clave... se establecen las actividades y directrices al Personal de Tic incluidas la gestión de usuarios MIS-AS400... No se recibió archivo ni documentación relacionada por funcionarios anteriores en la Coordinación General HJCA...".*

Lo mencionado por el Coordinador General de TIC's del HJCA, encargado, no modifica el comentario de auditoría, en razón que no realizó la supervisión de las actividades realizadas por el personal encargado de la gestión de usuarios del Sistema de Información Médica MIS AS400; ni adjuntó la documentación de soporte para la creación de estos usuarios, por lo que no evidenció la responsabilidad sobre su uso; ni justificó la falta de identificación de los mismos, manifestando la falta de procedimientos para identificación y entrega de usuarios en el referido sistema.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

CINCUENTA Y CINCO

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, con comunicación de 29 de mayo de 2017, acotó:

> *"... se solicitó a DNTI normas y políticas para el correcto manejo de los recursos informáticos, sin embargo, se puede apreciar... que las mismas estaban en proceso de aprobación y estandarizadas para las unidades médicas.- Para la entrega de cuentas de acceso se ha seguido los procesos que se tenían establecidos dentro de esta unidad médica, para el buen uso de la información dentro del sistema AS400, como es la entrega personal de USUARIO Y CLAVE a los funcionarios... solicitud que era planteada mediante oficio y previo la firma de un documento que reposa dentro de los archivos de la Coordinación de TICs... ".*

Lo mencionado por el Coordinador General de TIC's del HJCA, no modifica el comentario de auditoría, pues no propuso lineamientos que permitan la identificación de los servidores responsables por el uso de usuarios asignados en el Sistema de Información Médica MIS AS400.

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, con memorando IESS-SDNSI-2017-0017-M de 2 de junio de 2017, no acotó sobre este punto.

El Coordinador General de TIC's del HCAM, encargado, actuante con período comprendido entre el 18 de diciembre de 2015 y el 31 de diciembre de 2016, en respuesta a lo expresado en la conferencia final de resultados, con memorando IESS-HCAM-CGTIC-2017-1125-M de 5 de junio de 2017, señaló:

> *"... Al respecto me permito* (sic) *que durante mi período de gestión de 18 de Diciembre a 31 de Diciembre de 2016 se* (sic) *detectado el mal uso de los usuarios genéricos y que algunos usuarios personales no tenían la información correcta y/o completa del responsable del uso del usuarios* (sic), *motivo por el cual con el fin de disponer usuarios atados a la persona responsable del usuarios* (sic) *se implementó a partir del 21 de noviembre de 2016 el uso de la información del registro civil para atar el usuario con la persona, y los usuarios que no tienen atada la misma información del registro civil se bloquean para que actualicen la misma cumpliendo las funciones establecidas en la Resolución C.D. 468 de 30 de mayo de 2014(...) .- como acciones adicionales me permito indicar que se ejecutó con fecha de 03 mayo de 2017 un proceso mediante el cual se envía a inactivación de los usuarios que no tienen información de registro civil atada al usuario, con el fin de regularizar los accesos disponibles así como permitir la trazabilidad y responsabilidad de los* CINCUENTA Y SEIS

registros efectuados al sistema médico MIS AS400. (Reporte de usuarios no atada a cédula activos), complementando con un proceso de realizar la creación de usuarios de forma documentada...".

Lo comentado por el Coordinador General de TIC's del HCAM, no modifica el comentario de auditoría, por cuanto, expuso acciones correctivas en relación a la observación realizada en este comentario, evidenciando que el control implementado para validar la identificación del usuario en el sistema se aplicó en el mes de noviembre de 2016, sin que este cambio se aplique por una sola vez al sistema, sino que se realizó de manera paulatina, por lo que se mantuvieron activos usuarios genéricos y sin identificar.

Conclusiones

- La Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado, la Coordinadora Informática del HTMC, encargada, los Coordinadores Generales de TIC's del HTMC y los Coordinadores Generales de TIC's del HJCA, titular y encargado; no establecieron los procedimientos para el otorgamiento de una identificación única a todos los usuarios internos, externos, temporales; y, la elaboración, aprobación y difusión para la creación de usuarios genéricos que interactúan con el Sistema de Información Médica MIS AS400, en casos de excepción, lo que ocasionó la imposibilidad de identificar a las personas responsables del uso de usuarios y contraseñas en el sistema e incrementando el riesgo de acceso no autorizado al sistema y sus bases de datos.

- Los Directores Nacionales de Tecnología de la Información encargados, no emitieron directrices a los Coordinadores de TIC's de los hospitales HCAM, HTMC y HJCA para la creación de usuarios de manera que todos se encuentren identificados con el nombre del servidor que es responsable del utilización de la clave de acceso al sistema de Información Médica MIS AS400 y procedimientos de excepción para el manejo de usuarios genéricos, la imposibilidad de establecer responsabilidades y acuerdos sobre el uso y confidencialidad de la información con los usuarios internos, externos y temporales no identificados a través de cédula y nombre; y, en el caso de usuarios genéricos para conexión de procesos automáticos u otro propósito, que estos sean catalogados de uso exclusivo y el

CINCUENTA Y SIETE

acceso de responsabilidad del área informática; lo que ocasionó la imposibilidad de identificar a las personas responsables del uso de usuarios y contraseñas en el sistema, incrementando el riesgo de acceso no autorizado al sistema y sus bases de datos.

Recomendaciones

Al Director Nacional de Tecnologías de la Información

12. Coordinará con la Dirección Nacional de Riesgos Institucionales, emitirán los lineamientos para la creación de usuarios de los sistemas informáticos, la que difundirán a nivel institucional, a fin de asegurar que los registros de usuarios creados en los sistemas, como en el caso del Sistema de Información Médica MIS AS400 identifiquen al responsable de su uso, así también establecerán los procedimientos de excepción para la creación de usuarios genéricos, para regular su acceso, caducidad, y responsabilidad sobre las actividades desarrolladas a través de su uso.

Al Coordinador General de TIC's del HCAM

13. Coordinará con las Direcciones: del Seguro General de Salud Individual y Familiar y Nacional de Tecnologías de la Información, dictara los lineamientos para la elaboración y ejecución de un plan de la depuración del sistema de los usuario que no se encontraron identificados, por parte de los administradores de las Unidades Médicas y jefaturas de áreas usuarias del Sistema de Información Médica MIS AS400, a fin de establecer su identificación y/o inactivación en caso de aplicar, con el objetivo de establecer las responsabilidades de los usuarios del sistema sobre las transacciones realizadas.

Cuentas de usuario del personal desvinculado de la Institución, se mantuvieron activas en el Sistema de Información Médica MIS AS400

En la base de datos del Sistema de Información Médica MIS AS400, constaron como usuarios activos, servidores desvinculados de la Institución, según constó en los registros presentados por las áreas de talento humano de los hospitales Carlos

CINCUENTA Y OCHO

Andrade Marín y José Carrasco Arteaga; no obstante, no fueron inactivados del aplicativo, según se detalla:

- Existen en el Sistema de Información Médica MIS AS400, 137 y 104 servidores que finalizaron su relación laboral en los hospitales HCAM y HJCA; sin embargo, sus cuentas de usuario siguieron constando como activas, de estos, en el sistema operativo, 47 y 96, respectivamente con estado de perfil "**ENABLED*"; así como 90 y 8 con estado "**DISABLED*".

- En los registros realizados en el HCAM, no se han inactivado a 12 cuentas de usuarios creados en forma temporal, pese a que sus perfiles se encontraron en el sistema operativo en estado "**DISABLED*", tal fue el caso de los servidores con la referencia de la Contraloría.

Estado	Perfil Usuario	Cédula	Referencia	Fecha creación	Año último ingreso
A	BD1701177		Consultas Contraloría	150827	15
A	CT1701001		Contraloría visualizar hc	150819	16
A	CT1701002		Contraloría visualizar hc	150819	15
A	EF1701936	0104123153	Contraloría	150731	15
A	EF1701937	1722161666	Contraloría	150731	15
A	EF1701938	1801622554	Contraloría	150731	15
A	EF1701939	1713977971	Contraloría	150731	
A	EF1701940	1720115144	Contraloría	150731	
A	EF1701945		Contraloría	150813	15
A	EF1701947	1716384282	Contraloría	150827	16
A	EF1701948	1714241195	Contraloría	150827	

El Director Nacional de Gestión de Talento Humano con memorando IESS-DNGTH-2016-4640-M de 17 de agosto de 2016, en relación a la desactivación de usuarios, emitió las siguientes disposiciones sobre Certificado de Paz y Salvo:

> *"... En el caso de las Unidades Médicas, el responsable de talento humano deberá solicitar al administrador de usuarios de los sistemas Esigef y Spryn, la desactivación de usuario del servidor que se desvincula; siempre y cuando haya trabajado en el área financiera y talento humano..."*

Al, respecto el Coordinador General de Talento Humano del HCAM con memorandos IESS-HCAM-CGTH-2017-0560-M e IESS-HCAM-CGTH-2017-0788-M de 15 de marzo de 2017 y 11 de abril de 2017, corroboró lo siguiente:

NOVENTA Y NUEVE

"... Con relación a desvinculación, cambio administrativo, vacaciones y otras novedades. PROCESO A CARGO DE LA COORDINACION GENERAL DE TIC'S.- en referencia a la... inactivación de los accesos de usuarios de los servidores desvinculados se lo hace y evidencia mediante el documento de Paz y Salvo previo al pago de la liquidación de haberes de los ex funcionarios...".

Por lo que las instrucciones conferidas por el Director Nacional de Gestión de Talento Humano, fueron replicadas en los hospitales Carlos Andrade Marín, Teodoro Maldonado Carbo y José Carrasco Arteaga, con relación a la inactivación de servidores mediante la aplicación del documento de Paz y Salvo.

El Coordinador General de TIC's del HCAM, en respuesta al requerimiento de información realizado por el equipo de auditoría con memorando IESS-AI-2017-0427-ME de 20 de marzo de 2017, con memorando IESS-HCAM-CGTIC-2017-0730-M de 12 de abril de 2017, con documento sin número, indicó, que:

"... Para dar de baja de un usuario se puede dar por medio de comunicaciones enviadas de salida de personal por parte de la Coordinación General de Talento Humano (ejemplo: Memorando Nro. IESS-HCAM-CGTH-2016-3599-M) y/o por dar cumplimiento al Memorando Nro. IESS-DNGTH-2016-4640-M de fecha 17 de agosto de 2017(sic) donde se indica las Disposiciones sobre certificado Paz y Salvo...".

Sin embargo, no evidenciaron los procedimientos y acciones para la inactivación periódica, y bajo demanda de usuarios desvinculados temporal y definitivamente, como en el caso de: vacaciones, comisiones de servicios, renuncia, despidos servidores internos; tampoco la inactivación de usuarios externos y esporádicos, una vez concluida sus actividades.

Por otra parte, el Coordinador General de TIC's del HTMC, con memorando IESS-HTMC-CGTIC-2017-2201-M de 20 de abril de 2017, presentó al equipo de auditoría la coordinación existente desde el 2015, para la inactivación de usuarios, donde la Coordinación de General de Talento Humano del hospital a través de su Coordinador de Planificación y Administración de Talento Humano, con memorandos con asunto *"Novedades de sueldo para el registro y control de nómina, TIC e inventario"* hizo conocer de cambios efectuados en el personal y que pueden afectar los accesos otorgados en los sistemas informáticos; al respecto el Coordinador de TIC's del HTMC, expresó:

SESENTA

"... En el Hospital de Especialidades Teodoro Maldonado Carbo no existe procedimiento legalmente establecido para la inactivación de los usuarios sea temporal o definitivo, sin embargo se tiene en funcionamiento como práctica interna para la inactivación de los usuarios las notificaciones que envía el área de Talento Humano sea vía correo electrónico o por Quipux. Esta práctica se realiza cada fin de año y a los tres meses de forma recurrente... ".

El Coordinador General de TIC's del HJCA con memorando IESS-HJCA-CGTIC-2017-0080-M de 31 de marzo de 2017, al respecto describió:

"... se inhabilita la clave por pedido escrito o en el paz y salvo según el caso.- se inactivación (sic)*... usuarios en base al distributivo...".*

Pese a la depuración efectuada conforme documentación adjunta del Coordinador General de TIC's del HJCA, se identificaron 104 usuarios activos, que correspondieron a servidores desvinculados según reporte proporcionado el área de talento humano del hospital.

La Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 10 de agosto de 2014; 11 de agosto de 2014 y el 16 de diciembre de 2015; y, 18 de diciembre de 2015 y el 31 de diciembre de 2016; y, los Coordinadores Generales de TIC's del HJCA, titular y encargado, actuantes en los períodos comprendidos entre el: 1 de septiembre de 2014 y el 30 de junio de 2015; y 1 de julio de 2015 y el 31 de diciembre de 2016, no solicitaron al Coordinador General de Talento Humano del hospital, el detalle de los servidores que se desvincularon de la Institución, tampoco elaboraron, ni pusieron a consideración del Gerente General del hospital al que pertenecen, las políticas y procedimientos para el acceso, manejo y procesamiento de la información del Sistema de Información Médica MIS AS400, que permitan la revisión regular del estado de actividad de las cuentas de usuarios y establecer los mecanismos de coordinación con la unidad responsable del talento humano, para la inactivación de los usuarios que correspondieron a servidores desligados temporalmente o definitivamente de la institución, en el caso de: vacaciones, comisiones de servicios, licencias, renuncia y despido; no dieron instrucciones a seguir para la activación e inactivación de cuentas de usuarios a personal externo y esporádicos, como el caso de usuarios creados por pedido de los entes de control, actividades de soporte, capacitación, prácticas profesionales, entre otros.

SESENTA Y UNO

Los Directores Nacionales de Tecnología de la Información, encargados, con períodos de actuación comprendidos entre el: 25 de junio de 2014 y el 7 de enero de 2015; y, 18 de mayo de 2015 y el 31 de diciembre de 2016, tampoco emitieron lineamientos para que las Coordinaciones Generales de Tecnología y Comunicaciones de los hospitales de tercer nivel del IESS implementen revisiones regulares de todas las cuentas de usuarios y los privilegios asociados, en conjunto con los dueños de los procesos, por lo que la información de los usuarios almacenada en la base de datos del Sistema de Información Médica MIS AS400, no fue consistente con el registro correspondiente al personal, administrado por la unidad de Talento Humano.

Lo expuesto ocasionó que las cuentas de usuario de servidores desvinculados se mantengan con estado activo en el Sistema de Información Médica MIS AS400, según constó en su base de datos; incrementando el riesgo de accesos no autorizados al sistema.

Los referidos servidores incumplieron lo dispuesto en las letras a) y b) del artículo 22, Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; los números 1 y 7 del artículo 41 De la Coordinación General de Tecnologías de la Información y Comunicación, del Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, referente a las funciones y perfiles de los órganos de gestión y dependencias que integran las Unidades Médicas de Nivel III; la letra f), del número 2.4.3, del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido por el Consejo Directivo del IESS, mediante Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referente a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información; y las Normas de Control Interno: 200-07 Coordinación de acciones organizaciones; 401-03 Supervisión, 410-04 Políticas, y procedimientos ; y, 410-12 Administración de soporte de tecnología de información.

El Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, establece:

SESENTA Y DOS

"... Art. 41.- De la Coordinación General de Tecnología de la Información y Comunicación.-... 1. Proponer las políticas para el acceso, manejo, y procesamiento de la información y de los servicios de red, a través de las herramientas de Tecnología de Información y Comunicación (TIC);... 7. Controlar la seguridad, integridad y proteger el carácter institucional de la información manejada por los usuarios...".

La Resolución C.D.457, referente a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información, estableció:

"... f) Implementar y administrar las seguridades para garantizar la integridad de la información almacenada en las bases de datos de las aplicaciones informáticas de la Institución...".

El Director Nacional de Gestión de Talento Humano del período comprendido entre el 26 de mayo de 2015 y el 31 de diciembre de 2016, no dio instrucciones adicionales a las emitidas con memorando IESS-DNGTH-2016-4640-M de 17 de agosto de 2016, que instruyó el formulario de Paz y Salvo como requisito para el pago previo a las liquidaciones e inactivación del usuario de los sistema informáticos del Instituto, para la coordinación entre los responsables de talento humano y TIC's de las Unidades Médicas, para la inactivación de los servidores, trabajadores del IESS, desvinculados temporal y definitivamente; lo que permitió mantener como usuarios activos a 137 y 104 servidores que salieron de los Hospitales HCAM e HJCA, respectivamente, lo que ocasionó que no se establezcan procedimientos estándares en los hospitales de tercer nivel a fin de asegurar la inactivación de cuentas de usuarios correspondientes a servidores desvinculados temporalmente y/o definitivamente de los sistemas informáticos del IESS, como es el caso del Sistema de Información Médica MIS AS400, incumplió lo dispuesto en el artículo Deberes de las o los servidores públicos, letras a) y b) de la Ley Orgánica de Servicio Público, e inobservando las Normas de Control Interno 100-01 Control interno 100-03 Responsables del Control Interno y 200-07 Coordinación de acciones organizacionales.

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0081, 0082, 0083, 0096, 0097, 0084, 0085 y 0110-0010-IESS-AI-2017 de 9 de mayo de 2017; a los Coordinadores Generales de TIC's del HCAM y del HJCA; a los Directores Nacionales de Tecnología de la Información, encargados; y, el Director Nacional de Gestión de Talento Humano, obteniendo las siguientes respuestas:

SESENTA Y TRES

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, en respuesta al oficio 0096-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 17 de mayo de 2017, señaló:

> *"... Una vez realizada una visión general de la infraestructura informática y procesos que se llevaba dentro del (sic) Coordinación General de TIC's del HJCA se emite un documento denominado* ***"INFORME EJECUTIVO DE LA SITUACION ACTUAL DE LA COORDINACION DE TICS"****, donde se hace constatar en otros la falta de procesos que estén acordes a la resolución 468 y la falta de una plataforma CORE de servidores o software sobre la cual se deben implementar los sistemas o servicios que ayudaran a generar una plataforma estándar y controlada de aplicativos que ayudarían a generar mejores tiempos de respuesta en los trabajos cotidianos que el personal desempeña y que garanticen el correcto uso y resguardo de la información que se genera en la parte administrativa... se han realizado las acciones necesarias para establecer políticas institucionales que deberían ser emitidas por la DNTI, las cuales como se puede observar no se tenían aprobadas y estandarizadas para las unidades médicas en el período de tiempo en el cual preste mis servicios a la institución, es importante indicar que el centralismos que maneja DNTI no permitió implementar una serie de proyectos bases en la plataforma CORE informática del HJCA y que se manejan en otras instituciones públicas del país...".*

Lo mencionado por el Coordinador General de TIC's del HJCA, no modifica el comentario de auditoría debido que no propuso ni estableció procedimientos para la validación periódica del acceso de usuarios en el caso de desvinculación, finalización de contratos, movimientos de personal, entre otros.

El Director Nacional de Gestión de Talento Humano, actuante con período comprendido entre el 26 de mayo de 2015 y el 31 de diciembre de 2016, en respuesta al oficio 0110-0010-IESS-AI-2017, con comunicación de 22 de mayo de 2017, señaló:

> *"... Las competencias específicas de cada Unidad Administrativa del IESS, se encontraban determinadas en la norma legal que rigió al IESS en la Resolución emitida por el Consejo Directivo del IESS No. C.D. 457, de 30 de agosto de 2013; a la fecha Resolución C.D 535, de 8 de septiembre de 2016, con vigencia a partir del 6 de mayo de 2017... Puntualización que se circunscribe en el Art.226 de la Constitución de la República que dispone: "Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la*

SESENTA Y CUATRO

Constitución.- Abundo en este sentido enfatizando que el Sistema AS400 es de exclusiva utilización en las Unidades Médicas del IESS, las mismas que cuentan con un Director Administrativo y un Director Médico, que se desempeñan y ejecutan funciones respecto de este tema, siendo entre otras, la supervisión específica del Sistema".- (...)No obstante lo puntualizado, acogiendo el contexto literal de la presente comunicación de resultados, la deducción del incumplimiento por parte de las gerencias y coordinaciones técnicas de tecnologías de información y comunicación de los mencionados nosocomios, respecto de los lineamientos orientados a una correcta administración pública, lo cual ha generado la inactivación señalada en el documento, permiten el presente comentario, mismo que es conducente a la corrección de las posibles falencias y a optimizar objetiva y oportunamente la mencionada inactivación de usuarios desvinculados de la institución del Sistema de Información Médica AS400...".

Lo mencionado por el Director Nacional de Gestión de Talento Humano, no modifica el comentario de auditoría por cuanto, no presentó descargados en relación a instrucciones impartidas que permitan la coordinación entre los responsables de talento humano y TIC's de las Unidades Médicas, para la revisión e inactivación periódica de los usuarios en los sistemas informáticos de servidores, trabajadores del IESS, desvinculados temporal y definitivamente.

El Coordinador General de TIC's del HCAM, que actuó en el período comprendido entre el 11 de agosto de 2014 y el 16 de diciembre de 2015, en respuesta al oficio 0082-0010-IESS-AI-2017, con comunicación de 22 de mayo de 2017, señaló:

"... Durante mi período de gestión como Coordinador General de TIC´s del HCAM si existieron las acciones y gestión correspondientes con el objetivo de depurar a todos los usuarios registrados en el MIS400 (sic) *que se encontraban desvinculados, para lo cual se requirió la información correspondiente y se procedió a la inactivación. Los requerimientos de información y las contestaciones correspondientes que estan relacionadas con la inactivación de usuarios pueden evidenciarse en los siguientes documentos.- IESS-HCAM-GG-CGTIC-2015-2209-M de 2015-10-21 Acerca de la Base de datos de Usuarios AS400 a nivel nacional.- Por tanto, es el jefe inmediato del funcionario el responsable de notificar la desvinculación, así como la Dirección Nacional de Talento Humano la responsable de notificar periódicamente los traspasos, renuncias y otros movimientos. Asimismo, en caso de que un funcionario tome un período de vacaciones le corresponde a Talento Humano y al jefe inmediato del funcionario notificar esta desvinculación temporal, para que con esa solicitud se proceda a la inactivación del Sistema...".*

Lo manifestado, por el servidor, no modifica el comentario de auditoría, en razón que no adjunto los documentos de soporte de sus afirmaciones, tampoco evidenció que se propusieron procedimientos para la revisión periódica y consiguiente inactivación de

SESENTA Y CINCO

usuarios del Sistema de Información Médica MIS AS400, de los servidores desvinculados temporal y/o definitivamente.

El Coordinador General de TIC's del HJCA, actuante en el período comprendido entre el 1 de julio de 2015 al 31 de diciembre de 2016; en respuesta al oficio 0097-0010-IESS-AI-2017, con memorando IESS-HJCA-CGTIC-2017-0148-M de 24 de mayo de 2017, señaló:

> *"... En relación a los... 104 usuarios activos y desvinculados de la institución, a la fecha se encuentra 21(sic) pendientes de revisión. En el período de enero a marzo del presente año ingresaron los ganadores de concursos, y los funcionarios que terminaron su gestión no presentaron el documento de "paz y salvo" necesario para su inactivación.- La coordinación de TIC HJCA recibe en algunos casos de los Jefes la inactivación de los usuarios de sus servicios.- (...) la Gerencia General convocó una reunión de Staff y entre los temas tratados está el proceso de depuración de claves sistema AS400 y se tratan los siguientes puntos: Disponer de un distributivo por parte de Talento Humano para depuración de usuarios AS400 asignado...".*

Lo mencionado, por el Coordinador General de TIC's del HJCA, no modifica el comentario de auditoría, en razón de que no propuso la formalización de procedimientos que permitan gestionar la depuración de los usuarios desvinculados definitiva o temporalmente la base de datos, en el caso de los pedidos de inactivación bajo demanda o de manera periódica haciendo uso de la base de datos de talento humano.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, con memorando IESS-SDNSI-2017-0017-M de 2 de junio de 2017, no acotó sobre este punto.

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, con comunicación de 29 de mayo de 2017, manifestó:

SESENTA Y SEIS

"... se solicitó a DNTI normas y políticas para el correcto manejo de los recursos informáticos, sin embargo, se puede apreciar... que las mismas estaban en proceso de aprobación y estandarizadas para las unidades médicas.- Existía la debía (sic) *coordinación con los permisos por vacaciones de los usuarios del Sistema AS400 como se puede verificar en correos electrónicos que se adjuntan los que expresan los permisos que concede la Coordinación de Talento Humano para que TICs haga cierre de agenda y re agendamiento respectivo de las citas médicas... ".*

Lo expresado por el citado funcionario, no modifica el comentario de auditoría, respecto de activación e inactivación de usuarios desvinculados.

El Coordinador General de TIC's del HCAM, actuante con período comprendido entre el 18 de diciembre de 2015 y el 31 de diciembre de 2016, en respuesta a lo expresado en la conferencia final de resultados, con memorando IESS-HCAM-CGTIC-2017-1125-M de 5 de junio de 2017, señaló:

"... Al respecto me permito indicar que con el fin de realizar una depuración de los usuarios se solicitó a la Coordinación General de Talento Humano del HCAM mediante Memorando Nro. IESS-HCAM CGTIC-2016-1514-M con fecha 29 de septiembre de 2017 (sic) *un listado de personal que salió de la institución con el fin de realizar una depuración de usuarios del sistema medico MIS AS400, este pedido no fue contestado.- Se ha levantado un proceso de inactivación de usuarios dado que no se recibe información de desactivación de usuarios a nivel nacional se debe proceder a ejecutar el programa del sistema que permite inactivar los perfiles que no hayan ingresado al sistema en los últimos 30 días, mismo que venía ejecutándose cada inicio de mes de 2015 octubre pero con parámetro de 180 días como trabajo calendarizado, el mismo que evitará accesos no autorizados al sistema.- Adicionalmente se está implementando la fecha de salida para usuario temporales, es decir incorporar un parámetro para que desactive usuarios temporales automáticamente al finalizar el período al cual estaba contratado... Complementariamente el área de talento humano informará de manera mensual los usuarios que salieron de la Institución para que los mismos sean dados de baja en el sistema médico...".*

Lo comentado por el Coordinador General de TIC's del HCAM, no modifica el comentario de auditoría, en razón, de que evidenció que el área de talento humano del HCAM, no entregó la información requerida para la depuración de accesos de los médicos que laboraron en el hospital al 29 de septiembre de 2016, por lo que posterior a la fecha de corte de esta acción de control, presentó propuestas de acciones correctivas en cuanto sus competencias para el mejoramiento del control en relación al manejo de desvinculaciones de personal y de control de acceso a la información del Sistema Información Médica MIS AS400 a usuarios genéricos y aquellos usuarios que no registraron actividad por tiempos prolongados en el sistema.

SESENTA Y SIETE

Conclusiones

- La Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado; y, los Coordinadores Generales de TIC's del HJCA, titular y encargado; no solicitaron al Coordinador General de Talento Humano del hospital, el detalle de los servidores que se desvincularon de la Institución, tampoco elaboraron, ni pusieron a consideración del Gerente General del hospital al que pertenecen, las políticas y procedimientos para el acceso, manejo y procesamiento de la información del Sistema de Información Médica MIS AS400, que permitan la revisión regular del estado de actividad de las cuentas de usuarios y establecer los mecanismos de coordinación con la unidad responsable del talento humano, para la inactivación de los usuarios que correspondieron a servidores desligados temporalmente o definitivamente de la institución, en el caso de: vacaciones, comisiones de servicios, licencias, renuncia y despido; no dieron instrucciones a seguir para la activación e inactivación de cuentas de usuarios a personal externo y esporádicos, como el caso de usuarios creados por pedido de los entes de control, actividades de soporte, capacitación, prácticas profesionales, entre otros, lo que ocasionó que las cuentas de usuario de servidores desvinculados se mantengan con estado activo en el Sistema de Información Médica MIS AS400, según constó en su base de datos; incrementando el riesgo de accesos no autorizados al sistema.

- Los Directores Nacionales de Tecnología de la Información, encargados, con períodos de actuación comprendidos entre el: 25 de junio de 2014 y el 7 de enero de 2015; y, 18 de mayo de 2015 y el 31 de diciembre de 2016, tampoco emitieron lineamientos para que las Coordinaciones Generales de Tecnología y Comunicaciones de los hospitales de tercer nivel del IESS implementen revisiones regulares de todas las cuentas de usuarios y los privilegios asociados, en conjunto con los dueños de los procesos, por lo que la información de los usuarios almacenada en la base de datos del Sistema de Información Médica MIS AS400, no fue consistente con el registro correspondiente al personal, administrado por la unidad de Talento Humano, lo que ocasionó que las cuentas de usuario de servidores desvinculados se mantengan con estado activo en el Sistema de Información Médica MIS AS400, según constó en su base de datos; incrementando el riesgo de accesos no autorizados al sistema.

SESENTA Y OCHO

- El Director Nacional de Gestión de Talento Humano, no dio instrucciones adicionales a las emitidas con memorando IESS-DNGTH-2016-4640-M de 17 de agosto de 2016, que instruyó el formulario de Paz y Salvo como requisito para el pago previo a las liquidaciones e inactivación del usuario de los sistema informáticos del Instituto, para la coordinación entre los responsables de talento humano y TIC's de las Unidades Médicas, para la inactivación de los servidores, trabajadores del IESS, desvinculados temporal y definitivamente; lo que permitió mantener como usuarios activos a 137 y 104 servidores que salieron de los Hospitales HCAM e HJCA, respectivamente, lo que ocasionó que no se establezcan procedimientos estándares en los hospitales de tercer nivel a fin de asegurar la inactivación de cuentas de usuarios correspondientes a servidores desvinculados temporalmente y/o definitivamente de los sistemas informáticos del IESS, como es el caso del Sistema de Información Médica MIS AS400.

Recomendación

Al Director Nacional de Tecnologías de la Información

14. Coordinará con la Dirección Nacional de Riesgos Institucionales y la Subdirección Nacional de Gestión de Talento Humano, establecerán los procedimientos aprobados y difundidos para que en conjunto con las áreas responsables de la administración de usuarios de los sistemas, realicen la implementación de controles para la revisión periódica y bajo demanda de los accesos autorizados a los sistemas, a fin de asegurar la coherencia entre las bases de datos de talento humano y las bases de datos de usuarios de los sistemas informáticos, como en el caso del Sistema de Información Médica MIS AS400, a fin inactivar los accesos otorgados a servidores, trabajadores y personal, desvinculados temporal y/o definitivamente de la Institución. Además establecerá los procedimientos para regular los accesos de terceras personas como el caso de proveedores, capacitadores, entes de control, entre otros, que serán de responsabilidad de las áreas requirentes de estos servicios.

SESENTA Y NUEVE

Acceso irrestricto a la información del Sistema MIS AS400 sin acuerdos de confidencialidad suscritos

El Sistema de Información Médica MIS AS400, almacenó las historias clínicas de los pacientes, registros y procedimientos médicos, inventario valorado de fármacos, agendamiento de citas, entre otros; son usuarios de este aplicativo el personal del *área médica* y administrativa de las Unidades Médicas del IESS, a través de consulta externa, hospitalización y emergencia; así también, de los consultorios y prestadores externos y consultorios anexos, que mantienen relación con la Institución, los usuarios y perfiles son creados por personal informático administrador del sistema a cargo de los Coordinadores Generales de Tecnologías de Información y Comunicación de cada hospital de nivel III, a base de las solicitudes presentadas por las Jefaturas de cada unidad.

Respecto de la restricción y confidencialidad de la información del Sistema de Información Médica MIS AS400, el Director del Seguro General de Salud Individual y Familiar y los Gerentes Generales de los Hospitales José Carrasco Arteaga y Carlos Andrade Marín, no emitieron los lineamientos, directrices ni requerimientos para restringir el acceso a las historias clínicas de los pacientes del IESS, tampoco los Coordinadores Generales de TIC's del HJCA y HCAM, realizaron acciones sobre este tema, el Coordinador General de TIC's del HCAM en memorando IESS-HCAM-CGTIC-2017-0730-M de 12 de abril de 2017, dirigido al equipo de auditoría en el que señaló:

> *"... la única de(sic) solicitud recibida es de Confidencialidad en el Sistemas AS400 (Diagnostico HIV) emitida por Coordinación Nacional de Vigilancia Epidemiológica, la misma que no se ha implementado por falta de definiciones funcionales...".*

El Coordinador General de Control de Calidad del Hospital de Especialidades Teodoro Maldonado Carbo, con memorandos IESS-HTMC-CGCC-2016-1242-M de 13 de octubre de 2016 y IESS-HTMC-CGCC-2016-1267-M de 18 de octubre de 2016, solicitó al Director Técnico Encargado, Director y Coordinador General de TICs del HTMC, la restricción al acceso de Historia Clínica en el Sistema de Información Médica MIS AS400, donde expresó:

> *"... velando por los derechos y el bienestar de los pacientes... en pro de la confidencialidad que es el derecho a que todos aquellos que lleguen a conocer datos relacionados con los mismos, por su participación directa o indirecta en* SETENTA

las funciones propias de las instituciones sanitarias... Informa de que existen diferentes áreas administrativas, las cuales tienen acceso a la Historia Clínica siendo esta una información muy sensible que debe ser protegida.- Por lo cual se solicita se restringa el acceso a la opción Trabajar con Historias Clínicas y Consulta de Historias Clínicas del sistema AS400 a los usuarios de las unidades que utilizan dicho sistema que no son personal médico y tienen habilitadas opciones mencionadas ya que es una información que no debe ser de acceso general, solo debe ser para uso de profesionales médicos y áreas competentes... ".

El Coordinador General de TIC's del HTMC, con memorando IESS-HTMC-2016-3872-M de 17 de octubre de 2016, en atención al memorando IESS-HTMC-CGCC-2016-1242-M, informó:

"... La Administradora de Usuarios del Sistema AS/400... procedió a restringir a todos los usuarios de la Jefatura Técnica de Admisión, los siguientes programas, mediante los cuales se puede acceder a los Registros Médicos de los pacientes en el Módulo de Admisión de Consulta Externa y Admisión de Hospitalización y Emergencias.- ***HC060C*** (sic) *Prepara archivos para impresión de reg. médic.-* ***IIHC070*** (sic) *Impresión de Historia Clínica.-* ***IHC070CL*** *Impresión de Historia Clínica unificada/unid.- Cabe indicar que existen otros usuarios Administrativos en las dependencias de Coordinación de Control de Calidad, los cuales tienen acceso indicado a los usuarios de los siguientes grupos de trabajo: Unidad de Calificación Médica, Trabajo Social, Gestión Hospitalaria, Atención al Cliente, Archivo y Documentación Clínica...".*

El Coordinador General de Control de Calidad del HTMC, con memorando IESS-HTMC-CGCC-2016-1274-M de 19 de octubre de 2016, dirigido al Coordinador General de TIC's del HTMC, añadió:

"... se me informa que la Unidad Técnica de Archivo y Documentación Clínica maneja las historias clínicas por lo cual justifica el acceso a las opciones de Historia Clínica, de igual manera la Unidad Técnica de trabajo Social realiza la elaboración de la Ficha Psicosocial e interactúan con los pacientes necesitando esta opción para revisar las condiciones del paciente.- el resto de unidades cuenta con personal médico por lo cual ellos deberán solicitar mediante sus jefaturas los usuarios de consulta para los fines pertinentes, el personal administrativo no debe tener acceso a la historia clínica, de esta manera protegemos la confidencialidad del paciente... ".

Con memorando IESS-HCAM-CGTIC-2017-0730-M de 12 de abril de 2017, el Coordinador General de Tecnologías, remitió el archivo de auditoría AUDIP01, del que se obtuvo una muestra a partir de la semana del 18 al 22 de julio, del 17 al 21 de octubre y del 21 al 25 de noviembre de los años: 2014, 2015 y 2016, correspondientes a los hospitales: HCAM, HTMC y HJCA, en el que se observó que el personal administrativo de las áreas de: TIC's, atención al cliente, subsidios, estadísticas,

SETENTA Y UNO

responsabilidad patronal, facturación, realizaron consultas e impresiones de historias clínicas, como se muestra a continuación:

Hospital	Perfil de grupo	Programa	Referencia	Consulta HC	Impresión HC
Carlos Andrade Marín	ADMINUM	CONTRO	SECRETARIA INFORMATICA HCAM	2	
	CMEDIC	MEDIC11	HCAM SOPORTE INFORMÁTICA DAD INFORMATICA	141	
	CADMI	ADMI00	ATENCION AL CLIENTE	1.216	54
	CADMI	HOS002CL	SERVICIO AL CLIENTE" y "ATENCIÓN AL CLIENTE		
	CMEDICA	CONTROU	SOPORTE INFORMÁTICA, INFORMÁTICA	55	
	CADMI	CONS01	FACTURACION	107	92
			SUBSIDIOS	387	241
	CFACTU	FACPR1	AUDITORÍA MÉDICA	876	
			AUDITORÍA CONTRALORIA	1	
José Carrasco Arteaga	CADMI	ADMI00	Sin referencia Labora en TIC´s		1
			TECNOLOGO INFORMÁTICO HJCA		3
	CMEDICHO	CMEDIC11	MEDICO MAESTRO Usuario de TIC´s	100	
	CADMI	ADMI01	ADMISIONISTA: CONSULTA EXTERNA, HJCA, ADMISIONISTA		275
	CADMIE	ADMI01	REVISIÓN AFILIADOS		133
			USUARIO DE RESPONSABILIDAD PATRONAL		43
	CFACTU	FACUSR	INFORMATICO AZUAY, MEDICO SPPSS AZUAY, MEDICO AUDITOR SPSS AZUAY, SUBDIRECCION DE PRESTACIONES, SUBDIRECCION DE SALUD DEL AZUAY, MEDICO AUDITOR	558	
Teodoro Maldonado Carbo	ADMINUM	CONTRO	ADMINISTRADORA AS/400	1	
	CMEDICHO	CMEDIC11	ADMINISTRADORA AMBIENTE HOSPITALARIO	497	
			411 usuarios no identificados d estadística		
			86 Usuarios de TIC		
	CADMI	ADMI00	ADMISIONISTA DE CONSULTA EXTERNA		102
	CADMI	ADMI01	ADMISIONISTA CONSULTA EXTERNA, CONSULTA DATOS ADMISION, CONSULTA EXTERNA, ADMISIONISTA DE CE Y HO		38
	CADMI	HOS002CL	ANALISTA ADMINISTRATIVO ASISTENTE ADMINISTRATIVO OFINISTA DE ESTADISTICA		95
	CFACTU	FACPR1	GRUPO RESPONSABILIDAD PATRONAL	166	
			USUARIO FACTURACION	58	
	CFARMA	FARMA00	QUIMICA FARMACEUTICA DOSIS QUIMICO FARMACEUTICO-FARMACIA	84	

Adicionalmente, el Sistema de Información Médica MIS AS400, dispone en el menú *"Control General del Sistema"* de los administradores, de la opción 12 *"Trabajar con*

SETENTA Y DOS

Querys" que permite la realización de consultas a través de la elaboración de sentencias SQL para extraer información de la base de datos, quienes otorgaron permisos a otros usuarios con diferente perfil a esta opción a través de dos mecanismos como: *"Trabajar con Usuarios/programas"* del menú de autorizaciones y *"UMUS Usuarios opciones asignadas"* en el menú ESC, al respecto, se observó que:

- A través del menú de autorizaciones, *"Trabajar con Usuarios/programas"*, en el Hospital Carlos Andrade Marín, se añadieron 8 accesos al programa de querys (consulta) a usuarios de los siguientes perfiles de grupo: *"CADMI", "CDIRE", "CFACTU", "CMEDIC", "INVBODUM"*, que cumplieron actividades de re agendamiento, planificación y estadística, consultas, control de bodegas de fármacos y kardex de insumos; en el Hospital José Carrasco Arteaga, se otorgó 1 acceso al programa de querys (consulta) a un usuario con perfil de grupo: INVBODUM, con la referencia *"USUARIO CONSULTA BODEGA"* y en el Hospital Teodoro Maldonado Carbo, no se encontraron autorizaciones añadidas a otros perfiles para utilizarlo; además en la Unidad Médica denominada *"SUPERUSUARIO??"*, existieron 19 autorizaciones otorgadas a usuarios con perfiles de grupo *"INVODUM"*, cuyas referencias correspondieron a *"QUÍMICA FARMACÉUTICA"* y *"SUBCONTROL DE FARMACOS"* y 16 sin referencia, que se crearon de acuerdo a la solicitud presentada por parte del Gerente Institucional Proyecto Servicios Dignos, al Gerente General de HCAM, constante en memorando IESS-CDPRES-2016-0096-M de 2 de junio de 2016, en el que expresó la necesidad de verificar los inventarios de insumos médicos, medicamentos y la agenda de unidades de esta institución; no obstante, a más de los perfiles de consulta a nivel nacional como usuarios de bodega se les otorgó la opción de *"querys"*, con acceso exclusivo de consulta.

- Con la opción *"UMUS Usuarios opciones asignadas"* en el menú ESC, en el Hospital Carlos Andrade Marín, se asignaron 13 accesos al menú de Escape a usuarios con perfil de grupo: CADMI, CADMIE, CFACTU, con las siguientes referencias: *"SUBDIRECCION DE ASEGURAMIENTO", "GESTION HOSPITALARIA", "ADMINISIÓN", "CONTROL DE CALIDAD", "GESTION HOSPITALARIA", "OFICINISTA", "FACTURACION", "AREA DE EMERGENCIAS"*; en los Hospitales: Teodoro Maldonado Carbo y José Carrasco Arteaga no se encontraron asignaciones al programa de querys mediante la opción de ESC a

SESENTA Y TRES

usuarios; y en la Unidad Médica denominada *"SUPERUSUARIO??"*, existieron 3 autorizaciones otorgadas a usuarios con perfiles de grupo "ADMINUMCA" y "INVODUM", cuyas referencias correspondieron a *"ASEGURADORA"* y *"COORDINACION DE MEDICAMENTOS"*.

La Administradora del Sistema de Información Médica MIS AS400 del HCAM, en la información adjunta al memorando IESS-HCAM-CGTIC-2017-0730-M de 12 de abril de 2017, indicó que todos los usuarios con acceso al programa *"CONTRO"* tienen acceso a *"Trabajar con querys"*; es decir todos los administradores del sistema, además, agregó que en el perfil de grupo *"CFACTU"* están autorizados todos los usuarios.

Además, el Sistema de Información Médica MIS AS400, permitió la creación de usuarios, con la capacidad de consultar e ingresar información de unas o varias Unidades Médicas, a través de su asignación a la Unidad Médica denominada *"SUPERUSUARIO??"*, con código de unidad médica *"9999999999"*, por lo que en la base de datos constaron 1.632 de un total de 1.787 usuarios activos, con acceso a nivel nacional a la información de acuerdo a su perfil de grupo y 155 se encontraron restringidos su acceso a las unidades médicas específicas.

Entre los 1.632 usuarios, se encontraron administradores del sistema de: Seguro Campesino, Subdirecciones Provinciales de Salud que manejan los acceso de prestadores y consultorios externos; y, otros que cumplen actividades administrativas, tales como agendamiento de citas del Call Center- IESS, bodegas de fármacos y facturación, riesgos trabajo, etc., sin que existiera evidencia de que los Coordinadores Generales de Tecnología de la Información, revisaron en conjunto con el área requirente la validez y vigencia de los accesos y perfiles otorgados, tal es el caso del pedido realizado por el Director del Seguro General de Salud Individual y Familiar, con memorando IESS-DSGIF-2016-0703-M de 9 de marzo de 2016, en el que solicitó al Gerente General del HCAM, con copia al Coordinador General de TIC's, se realice el cambio de Administrador del Sistema de Información Médica MIS AS400 de la DSGSIF; sin embargo, al 31 de diciembre de 2016, se determinó que no se inactivaron los accesos otorgados a esta servidora con usuarios ADMINPT y BD9999003 de *"Control General del Sistema"* y *"Control General del Sistema de*

SETENTA Y CUATRO

Inventarios", creados en la unidad médica denominada *"SUPERUSUARIO??"*, con código de unidad médica *"9999999999"*.

Los perfiles de grupo de usuarios del Sistema de Información Médica MIS AS400, señalados en los comentarios anteriores tuvieron acceso sin restricción para visualizar las historias clínicas de los pacientes del IESS, ejecución de querys; y, en el caso de los usuarios creados en la unidad médica con código *"9999999999"* se encontraron permitidos de realizar acciones de ingreso y consulta de la información en la base de datos del Sistema de Información Médica MIS AS400 a nivel nacional, según los perfiles de grupo asignados; sin que haya evidenciado la suscripción de acuerdos de confidencialidad del uso, manejo de la información y responsabilidades de los usuarios que utilizan el aplicativo, ni la emisión de procedimientos para su elaboración, control y archivo.

Respecto de la confidencialidad de las historias clínicas, los artículos 7 letra f) de la Ley Orgánica de Salud; 2, 7, 9, 14 y 15 del Reglamento para el manejo de información confidencial en el Sistema Nacional de Salud, Capítulos IV Seguridad en la Custodia de las Historias Clínicas y V Derecho a la Información y Confidencialidad de 29 de enero de 2015, disponen:

> *"...**Ley Orgánica de Salud Art. 7... f)** Tener una historia clínica única redactada en términos precisos, comprensibles y completos; así como la confidencialidad respecto de la información en ella contenida y a que se le entregue su epicrisis;...".*
>
> *"... **Reglamento.... Art 2.-** Confidencialidad.- Es la cualidad o propiedad de la información que asegura un acceso restringido a la misma, solo por parte de las personas autorizadas para ello. Implican el conjunto de acciones que garantizan la seguridad en el manejo de esa información.- ... **Art 7.-** Por documentos que contienen información de salud se entienden: historias clínicas, resultados de exámenes de laboratorio, imagenología y otros procedimientos tarjetas de registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales.- El uso de los documentos que contienen información de salud no se podrá autorizar para fines diferentes a los concernientes a la atención de los/las usuarios, evaluación de la calidad de los servicios, análisis estadístico, investigación y docencia. Toda persona que intervenga en su elaboración o tenga acceso a su contenido, está obligada a guardar la confidencialidad respecto de la información constante en los documentos antes mencionados.- **Art 9.**- El personal operativo y administrativo de los establecimientos del Sistema Nacional de salud que tenga acceso a información de los/las usuarios/as durante el ejercicio de sus funciones, deberá guardar reserva de manera indefinida respecto de dicha información y no podrá divulgar la información contenida en la historia clínica, ni aquella constante en*

SETENTA Y CINCO

todo documento donde reposen datos confidenciales de los/las usuarios/as ... ***Art. 14.-*** *La historia clínica sólo podrá ser manejada por personal de la cadena sanitaria. Como tal se entenderá a los siguientes profesionales: médicos, psicólogos, odontólogos, trabajadoras sociales, obstetrices, enfermeras, además de auxiliares de enfermería y personal de estadística.* ***Art. 15.-*** *El acceso a documentos archivados electrónicamente será restringido a personas autorizadas por el responsable del servicio o del establecimiento, mediante claves de acceso personales...".*

El Director Nacional de Tecnología de la Información, encargado, con memorando IESS-DNTI-2016-0815-M de 3 de marzo de 2016, envio al Coordinador General de Gestión Estratégica, subrogante un proyecto de compromiso de Confidencialidad, solicitando además remitir a las unidades de negocio y al BIESS, a fin de que, el personal que designe los suscriba previo a acceder a la información que se encuentra en las bases de datos custodiadas por la DNTI. Con memorando IESS-CGGE-2016-0041-M de 9 marzo de 2016, el Coordinador General de Gestión Estratégica, puso en conocimiento a la Directora General del IESS, el documento denominado Compromiso de confidencialidad; la que a su vez traslado a la Dirección Nacional de Talento Humano, dependencia que traslado a la Dirección Nacional de Gestión Documental para su difusión a las unidades de negocio, entre otras la Dirección del Seguro General de Salud Individual y Familiar.

El Consejo Directivo del IESS emitió el 28 de abril de 2016, la Resolución C.D 521 que contiene las *"Políticas que regulan las actividades relacionadas con el uso de Tecnologías de la Información y Comunicaciones";* en sus artículos 2 y 20 estableció:

"... ***Art. 2. Ámbito.-*** *Las políticas de tecnología de la información y comunicación serán aplicadas de manera obligatoria por las y los funcionarios, servidores y trabajadores que integran el IESS a nivel nacional, que utilicen el hardware, software y comunicaciones para el cumplimiento de sus actividades diarias.- La Dirección Nacional de Tecnología de la Información será la encargada de administrar y ejecutar estas políticas a través de procedimientos, asimismo las políticas deben cumplirse a nivel nacional por las dependencias que tienen a su cargo el uso de recursos tecnológicos de forma desconcentrada ...* ***Art. 20.-*** *Compromiso de Confidencialidad.- Las y los servidores de la institución deberán firmar compromisos de confidencialidad y de no divulgación de información de conformidad con lo dispuesto en la Constitución, las leyes y las necesidades de protección de información de la Institución.- La Dirección Nacional de Gestión de Talento Humano será la encargada de controlar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, gestionar la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de*

SETENTA Y SEIS 24

incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción...".

En este sentido, el Director Nacional de Tecnología de la Información con memorando IESS-DNTI-2016-3824-M de 7 de noviembre de 2016, se dirigió a las Direcciones Provinciales del IESS, con conocimiento de la Directora General del IESS, sobre los acuerdos de confidencialidad, requirió:

"... Con la finalidad de cumplir con lo que establece la Resolución C.D. 457 que contiene el Reglamento Funcional del Instituto Ecuatoriano de Seguridad Social en el artículo 4, numeral 2.4.3., y que entre otras, se refiere a: "f) Implementar y administrar las seguridades para garantizar la integridad de la información almacenada en las bases de datos de las aplicaciones informáticas de la Institución.", siendo obligación de las y los servidores del Instituto asegurar la confidencialidad y reserva de la información que administra, es necesario implementar la suscripción individual de un compromiso de confidencialidad para todo servidor o servidora del IESS como de instituciones públicas externas que acceden a la información de las bases de datos.- Agradeceré que dentro del ámbito de su competencia y jurisdicción se sirva a disponer a los servidores y /o servidoras que cumplan funciones de informáticos suscriban el Acuerdo de Confidencialidad en tres ejemplares... uno de los cuales deberá ser enviado a la Dirección Nacional de Tecnología de la Información para el registro correspondiente, otro deberá reposar en la carpeta individual del servidor y/o servidora en la Unidad de Talento Humano... El acuerdo de confidencialidad suscrito por el personal informático de cada jurisdicción, deberá ser remitido a esta Dirección en el término de 10 días, caso contrario se solicitara a la autoridad competente la aplicación de sanciones determinadas en la Ley Orgánica del Servicio Público y su reglamento...".

Respecto, de la disposición emitida por el Director Nacional de Tecnología de la Información el Coordinador General de TIC's del HJCA con memorando IESS-HJCA-CGTIC-2016-0270-M de 14 de noviembre de 2016, remitió copia de los acuerdos de confidencialidad del personal TIC bajo su cargo; el Coordinador General de TIC's del HCAM, con memorando IESS-HCAM-CGTIC-2017-0730-M de 12 de abril de 2017, remitió al equipo de auditoría, copias de los acuerdos de confidencialidad suscritos por el personal informático a su cargo, sin embargo, no evidenció que estos hayan sido reportados a la DNTI dentro de los 10 días establecidos a partir de su requerimiento IESS-DNTI-2016-3824-M de 07 de noviembre de 2016.

El Coordinador General de TIC's del HTMC, con memorando IESS-HTMC-CGTIC-2017-2201-M de 20 de abril de 2017, al respecto indico:

seiscientos y siete

"... No hay acuerdos de confidencialidad firmados por el personal de TICs; sin embargo actualmente se va a realizar una reunión con el área de Talento Humano para regularizar este punto el 21 de abril del 2017...".

Con memorando IESS-HCAM-CGTH-2017-0788-M de 11 de abril de 2017, el Coordinador General de Talento Humano del HCAM, al respecto de la suscripción de compromisos de confidencialidad, indicó:

"... La unidad de Talento Humano no está a cargo de la (SIC) *llevar el control sobre el proceso de accesos al Sistema de Información Médica, así como tampoco de la suscripción de los acuerdos de confidencialidad de las claves del sistema en mención... Considerar que únicamente en el contrato de servicios ocasionales en una de sus cláusulas incluye lo siguiente: "DÉCIMA TERCERA.- RESERVA Y CONFIDENCIALIDAD.- El/la CONTRATADO/A, se obliga a mantener la reserva, seguridad y manejo de la información, equipos y documentos que estén a su cargo por la actividad que desempeñará en el HCAM, a fin de precautelar la buena imagen institucional. El uso indebido será causal de la terminación anticipada del contrato"...".*

El Coordinador General de Talento Humano del HTMC con memorando IESS-HTMC-CGTH-2017-0571-M de 16 de marzo de 2017, al respecto también indicó lo expresado en la cláusula *"DECIMA TERCERA DEL CONTRATO DE SERVICIOS OCASIONALES.- RESERVA Y CONFIDENCIALIDAD".*

La Coordinadora General de Talento Humano del HJCA, con memorando IESS-HJCA-CGTH-2017-0631-M de 25 de abril de 2017, no adjuntó información al respecto de la suscripción de acuerdos de confidencialidad en la referida Unidad Médica, en la que se constató se maneja el mismo formato de contratos ocasionales, la que es emitida desde la Dirección Nacional de Gestión de Talento Humano del IESS.

Cabe indicar que en ninguno de los tres hospitales de tercer nivel, estos acuerdos de confidencialidad reposaron en el área de talento humano.

Lo comentado, se originó debido a que los Directores del Seguro General de Salud Individual y Familiar titulares y encargados, a su turno, con períodos comprendidos entre el: 17 de abril de 2014 y el 12 de septiembre de 2014; 6 de octubre de 2014 y el 11 de marzo de 2015; 12 de marzo de 2015 y el 16 de agosto de 2015; 19 de agosto de 2015 y el 14 de diciembre de 2015; y, el Director del Seguro General de Salud Individual y Familiar encargado y Director del Seguro General de Salud Individual y Familiar, desde el 8 de enero de 2016 y el 18 de febrero de 2016; y, desde el 19 de

SETENTA Y OCHO

febrero de 2016 y el 26 julio de 2016, respectivamente; y; del 28 de septiembre de 2016 y el 31 de diciembre de 2016; no dispusieron ni organizaron la implementación de procedimientos para restringir el acceso a las historias clínicas de los pacientes de las Unidades Médicas del IESS a través del Sistema de Información Médica MIS AS400, tampoco emitieron lineamientos y directrices para la elaboración y suscripción de acuerdos de confidencialidad por parte de los usuarios internos y externos de la información generada por este sistema y sus bases de datos; lo que ocasionó que no se establezcan a los usuarios del sistema las responsabilidades y compromisos de reserva de la información de los pacientes de las Unidades Médicas del IESS y que no garantice el cumplimiento de los requerimientos de confidencialidad establecidos por la Autoridad Sanitaria Nacional.

Los referidos servidores incumplieron lo dispuesto en los artículos 22.- Deberes de las o los servidores públicos, letras a) y b), de la Ley Orgánica del Servicio Público; 7 letra f) de la Ley Orgánica de Salud; 2, 7, 9, 14 y 15 del Reglamento para el manejo de información confidencial en el Sistema Nacional de Salud, Capitulo III Confidencialidad en los documentos con información de Salud, publicado en acuerdo ministerial 5216 Registro Oficial Suplemento 427 de 29 de enero de 2015; 5 de la Resolución C.D. 483 Reglamento Orgánico Funcional del IESS, emitida por el Consejo Directivo el 13 de abril de 2015; referente a las responsabilidades de la Dirección del Seguro General de Salud Individual y Familiar; literal i) numeral 2.2.1 Gestión del Seguro General de Salud Individual y Familiar, numero 11 de las atribuciones y responsabilidades, de la Resolución C.D 509 Reglamento Orgánico Funcional del IESS, emitida por el Consejo Directivo el 18 de febrero de 2016; e inobservaron la Norma de Control Interno: 401-03 Supervisión.

La Resolución C.D. 483 Reglamento Orgánico Funcional del IESS, emitida por el Consejo Directivo el 13 de abril de 2015; establece entre las atribuciones y responsabilidades de la Dirección del Seguro General de Salud Individual y Familiar:

> *"... **Art 5.- i)** Disponer y organizar la implementación y sistematización de la historia clínica de todos los afiliados y beneficiarios en las Unidades Médicas del IESS...".*
> SETENTA Y NUEVE

La Resolución C.D. 509 Reglamento Orgánico Funcional del IESS, emitida por el Consejo Directivo el 18 de febrero de 2016; establece entre las atribuciones y responsabilidades de la Dirección del Seguro General de Salud Individual y Familiar:

> *"... **2.2.1 Gestión del Seguro General de Salud Individual y Familiar.- ATRIBUCIONES Y RESPONSABILIDADES.- 11.** Disponer la implementación y sistematización de la historia clínica de todos los afiliados y beneficiarios en las Unidades Médicas del IESS...".*

El Director Nacional de Tecnología de la Información encargado con período de actuación comprendidos entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, no emitió directrices a los Coordinadores Generales de TIC's de los hospitales HCAM, HTMC y HJCA para llevar a cabo las revisiones regulares de las opciones y autorizaciones asignadas a los usuarios en cada módulo del Sistema de Información Médica MIS AS400, lo que ocasionó que los usuarios del aplicativo tengan acceso irrestricto a la información de historias clínicas, resultados de exámenes de laboratorio, imagenología, etc., registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales; así como la utilización de la opción *"Trabajar con querys"* y la creación de usuarios en unidad médica denominada *"SUPERUSUARIO??"* con código de unidad médica *"9999999999"*, incrementando el riesgo de acceso no autorizado y mal uso de la información del Sistema de Información Médica AS400, incumpliendo lo dispuesto en los artículos 22 Deberes de las o los servidores públicos, letras a) y b) de la Ley Orgánica del Servicio Público; letra e), del número 2.4.3, del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido por el Consejo Directivo del IESS, mediante Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referentes a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información; y, las Normas de Control Interno: 200-07 Coordinación de acciones organizaciones; y, 401-03 Supervisión, 410-04 Políticas, y procedimientos.

La Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referente a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información, establece:

> *"...e) Generar lineamientos y directrices para la gestión de infraestructura de la tecnología de información, bases de datos, redes y sistemas, desarrollo y mantenimiento de aplicaciones y soporte técnico a usuarios...".*

OCHENTA y

El Director Nacional de Gestión de Talento Humano por el período de actuación comprendido entre el 26 de mayo de 2015 y el 31 de diciembre de 2016, no coordinó con el Director Nacional de Tecnología de la Información, para la implantación de procedimientos referente a la suscripción, documentación y custodia de los compromisos de confidencialidad de los servidores y trabajadores del IESS; lo que ocasionó que no se organizaran acciones, ni se instruyeran a los responsables de las áreas de talento humano de las Unidades Médicas del IESS, ni controlara que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, tampoco gestionó la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, ni controló que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción; incrementando el riesgo de acceso no autorizado y mal uso de la información del Sistema de Información Médica AS400; incumpliendo lo dispuesto en las letras a) y b) del artículo 22.- Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; la Resolución C.D. 521 de 28 de abril de 2016, que emitió las *"Políticas que regulan las actividades relacionadas con el uso de Tecnologías y Comunicaciones"*; y, las Normas de Control Interno 100-01 Control Interno, 200-07 Coordinación de acciones organizacionales, 200-08 Adhesión a las políticas institucionales; que estableció:

> *"... **Art. 20.- Compromiso de Confidencialidad.-** (...) La Dirección Nacional de Gestión de Talento Humano será la encargada de controlar que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, gestionar la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, y controlar que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción...".*

Los Gerentes Generales del HCAM, actuantes en el período comprendido entre el: 11 de junio de 2014 y el 5 de junio de 2015; y, 8 de junio de 2015 y el 31 de diciembre de 2016; los Gerentes Generales del HTMC, titulares y encargados, actuantes en los períodos comprendidos entre el: 8 de agosto de 2014 y el 19 de diciembre de 2014; 18 de marzo de 2015 y el 17 de julio de 2015; 17 de julio de 2015 y el 7 de marzo de

OCHENTA Y UNO

2016; y, 8 de marzo de 2016 y el 13 de octubre de 2016; los Gerentes Generales del HJCA, titulares y encargados, actuantes durante los períodos comprendidos entre el: 5 de septiembre de 2014 y el 19 de mayo de 2015; 20 de mayo de 2015 y el 29 de abril de 2016; 2 de mayo de 2016 y el 27 de octubre de 2016; no vigilaron el cumplimiento de las políticas de administración pública en las áreas a su cargo, de conformidad con la normativa vigente para la confidencialidad de la información del Sistema de Información Médica MIS AS400; tampoco establecieron la normativa interna para que los Coordinadores Generales de TIC's cuenten con lineamientos y disposiciones que permitan la revisión en conjunto con el área requirente de la validez y vigencia de los accesos y perfiles otorgados a los usuarios permitiendo la consulta irrestricta de la información de historias clínicas, resultados de exámenes de laboratorio, imagenología, etc., registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales; así como la utilización de la opción "Trabajar con querys y creación de usuarios en unidad médica denominada *"SUPERUSUARIO??"* con código de unidad médica *"9999999999"*, ni emitieron las directrices para la suscripción de acuerdos de confidencialidad del uso, manejo de la información y responsabilidades de los usuarios que utilizan el Sistema de Información Médica AS400; así como su control y archivo; lo que ocasionó que la información relacionada a la historia clínica de los pacientes de las Unidades Médicas a su cargo, se encuentre disponible, y sin restricción mediante el acceso a opciones de consulta y/o impresión por parte de los usuarios de áreas administrativas dentro y fuera del hospital, que no pertenecieron a la cadena sanitaria; así como que no se establezcan las responsabilidades y compromisos de reserva del personal de las Unidades Médicas de tercer nivel, ni las sanciones en caso de su inobservancia, sin que se restringa el acceso a la información.

Los referidos servidores incumplieron lo dispuesto en las letras a) y b) del artículo 22.- Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; los artículos 14) y 15) del Reglamento para el manejo de información confidencial en el Sistema Nacional de Salud, Capitulo IV Seguridad en la Custodia de las Historias Clínicas, publicado en acuerdo ministerial 5216 Registro Oficial Suplemento 427 de 29 de enero de 2015; los números 2 y 23 del artículo 10 del Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, referente a las funciones de la Gerencia General de las

OCHENTA Y DOS

Unidades Médicas de Nivel III; y las Normas de Control Interno: 401-03 Supervisión, 410-04 Políticas y procedimientos.

El Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, establece:

> *"... Art. 10.- De la Gerencia General de la Unidad Médica.-... 2.Asegurar el cumplimiento de las políticas de administración pública en las áreas a su cargo, de conformidad con la normativa vigente;... 23. Establecer la normativa interna necesaria para el uso eficiente y eficaz de los recursos humanos, financieros, tecnológicos y materiales de la Unidad Médica...".*

La Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 10 de agosto de 2014; 11 de agosto de 2014 y el 16 de diciembre de 2015; y, 18 de diciembre de 2015 y el 31 de diciembre de 2016; la Coordinadora Informática del HTMC, encargada, los Coordinadores Generales de TIC's del HTMC encargados y titulares, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014; 13 de agosto de 2014 y el 7 de enero de 2015; 2 de marzo de 2015 y el 10 de abril de 2015; desde el 18 de mayo de 2015 y el 31 de mayo de 2015; 1 de junio de 2015 y el 22 de junio de 2015; y, del 29 de julio de 2015 y el 20 de marzo de 2016; y, 21 de marzo de 2016 y 13 de diciembre de 2016; los Coordinadores Generales de TIC's del HJCA, titular y encargado, actuantes en los períodos comprendidos entre el: 1 de septiembre de 2014 y el 30 de junio de 2015; y 1 de julio de 2015 y el 31 de diciembre de 2016; no propusieron al Gerente General del hospital al que pertenecen, las políticas para el acceso, manejo y procesamiento de la información del Sistema de Información Médica MIS AS400, para la coordinación entre los Jefes de Servicios de las áreas usuarias y la unidad a su cargo, para llevar a cabo las revisiones regulares de las opciones asignadas en cada módulo del aplicativo; tampoco supervisaron, ni reportaron a la Dirección Nacional de Tecnología de la Información, la suscripción de acuerdos de confidencialidad del personal de la unidad de TICs del HCAM y HTMC, conforme la disposición emitida por el Director Nacional de Tecnología de la Información constante en memorando IESS-DNTI-2016-3824-M de 7 de noviembre de 2016; lo que ocasionó que los usuarios del aplicativo tengan acceso irrestricto a la información de historias clínicas, resultados de exámenes de

OCHENTA Y TRES 2

laboratorio, imagenología, etc., registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales; así como la utilización de la opción *"Trabajar con querys"* y creación de usuarios en unidad médica denominada *"SUPERUSUARIO??"* con código de unidad médica *"9999999999"* y que no se establezcan las responsabilidades y compromisos de reserva del persona informático, respecto de la información de los pacientes y beneficiarios de los servicios de las Unidades Médicas.

Los referidos servidores incumplieron lo dispuesto en las letras a) y b) del artículo 22.- Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; los números 1 y 7 del Art. 41.- De la Coordinación General de Tecnologías de la Información y Comunicación, del Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, referente a las funciones y perfiles de los órganos de gestión y dependencias que integran las Unidades Médicas de Nivel III; y las Normas de Control Interno 200-07 Coordinación de acciones organizacionales; 410-12 Administración de soporte de tecnología de información.

El Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, establece:

> *"... **Art. 41.-** De la Coordinación General de Tecnología de la Información y Comunicación.-... **1.** Proponer las políticas para el acceso, manejo, y procesamiento de la información y de los servicios de red, a través de las herramientas de Tecnología de Información y Comunicación (TIC);... **7.** Controlar la seguridad, integridad y proteger el carácter institucional de la información manejada por los usuarios...".*

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0071, 0072, 0073, 0074, 0075, 0076, 0085, 0110, 0106, 0107, 0091, 0092, 0093, 0094, 0095, 0108, 0081, 0082, 0083, 0086, 0087, 0088, 0090, 0096, 0097-0010-IESS-AI-2017 de 9 de mayo de 2017; a los Directores del Seguro General de Salud Individual y Familiar, titulares y encargados; al Director Nacional de Tecnología de la Información, encargado; al Director Nacional de Gestión de Talento Humano; a los

OCHENTA Y CUATRO

Gerentes Generales del HCAM; a los Gerentes Generales del HTMC; a los Gerentes Generales del HJCA, titulares y encargados; y, a los Coordinadores Generales de TIC's del HCAM; a los Coordinadores Generales de TIC's del HTMC; a los Coordinadores Generales de TIC's del HJCA, titulares y encargados; obteniendo las siguientes respuestas:

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, en respuesta al oficio 0096-0010-IESS-AI-2017, con comunicación de 17 de mayo de 2017, señaló:

> *"... Una vez realizada una visión general de la infraestructura informática y procesos que se llevaba dentro del* (sic) Coordinación General de TIC's del HJCA se emite un documento denominado **"INFORME EJECUTIVO DE LA SITUACION ACTUAL DE LA COORDINACION DE TICS"**, donde se hace constatar en otros la falta de procesos que estén acordes a la resolución 468 y la falta de una plataforma CORE de servidores o software sobre la cual se deben implementar los sistemas o servicios que ayudaran a generar una plataforma estándar y controlada de aplicativos que ayudarían a generar mejores tiempos de respuesta en los trabajos cotidianos que el personal desempeña y que garanticen el correcto uso y resguardo de la información que se genera en la parte administrativa... *se han realizado las acciones necesarias para establecer políticas institucionales que deberían ser emitidas por la DNTI, las cuales como se puede observar no se tenían aprobadas y estandarizadas para las unidades médicas en el período de tiempo en el cual preste mis servicios a la institución, es importante indicar que el centralismos que maneja DNTI no permitió implementar una serie de proyectos bases en la plataforma CORE informática del HJCA y que se manejan en otras instituciones públicas del país...".*

Lo mencionado por el Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015; no modifica el comentario de auditoría debido a que no propuso ni coordinó que lleven a cabo revisiones regulares de las opciones asignadas en cada módulo del Sistema de Información Médico MIS AS400, a fin de precautelar la confidencialidad de la información institucional.

El Director del Seguro General de Salud Individual y Familiar encargado y Director del Seguro General de Salud Individual y Familiar, en funciones desde el 8 de enero de 2016 y el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 y el 26 julio de 2016, respectivamente, en respuesta al oficio 0074-0010-IESS-AI-2017, con comunicación de 19 de mayo de 2016, señaló:

OCHENTA Y CINCO

"... Mediante memorando No. IESS-DSGSIF-2016-1352-M de 10 de mayo de 2016, mediante el cual se pone en conocimiento de la Directora General del Instituto Ecuatoriano de Seguridad Social, el Manual de Procesos de Derivaciones...".

Lo mencionado por el Director del Seguro General de Salud Individual y Familiar, no modifica el criterio de auditoría, por cuanto no evidenció la entrega de lineamientos para la restricción de acceso a las historias clínicas generadas en el Sistema de Información Médicas MIS AS400.

El Gerente General del HJCA actuante durante período comprendido entre el 2 de mayo de 2016 y el 27 de octubre de 2016, en respuesta al oficio 0108-0010-IESS-AI-2017, con comunicación de 19 de mayo de 2017, al respecto señaló:

"... Durante mi gestión se trabajó en equipo con las diferentes autoridades del hospital y se generaron los documentos normativos que garantizan la restricción y confidencialidad de la información de las historias clínicas de los pacientes del IESS, es por ello que se elaboraron dos normativas fundamentales.- Normativa de funciones del Interno Rotativo del Hospital "José Carrasco Arteaga" de fecha 5 de julio de 2016.- b)Normativas de las practicas del externado en carreras de salud en el Hospital "José Carrasco Arteaga". La misma que al igual que la anterior Normativa, menciona la restricción y confidencialidad de la información de las historias clínicas de los pacientes del IESS...".

Lo mencionado, por el Gerente General del HJCA, evidenció la elaboración, aprobación y difusión de: *"Normativa de Funciones del Interno Rotativo del Hospital José Carrasco Arteaga"* y *"Normativa de Funciones de las practicas del Externado en carreras de Salud en el Hospital "José Carrasco Arteaga""*; estableciendo responsabilidades, obligaciones y sanciones respecto de la confidencialidad de las historias clínicas; sin embargo, no informó al equipo de auditoría al respecto del establecimiento de normativa interna que permita que los Coordinadores Generales de Tecnología de la Información y Comunicaciones que administran los perfiles y acceso a las historias clínicas en el Hospital José Carrasco Arteaga, cuenten con lineamientos y disposiciones para la revisión periódica de los accesos y perfiles otorgados a los usuarios, en conjunto con los responsables de las áreas y dependencias del hospital, a fin de salvaguardar la confidencialidad de la historia clínica en el Sistema de Información Médica AS400, por lo que no modifica el comentario de auditoría.

El Director Nacional de Gestión de Talento Humano, actuante con período comprendido entre el 26 de mayo de 2015 y el 31 de diciembre de 2016, en respuesta

OCHENTA Y SEIS 24

al oficio 0110-0010-IESS-AI-2017 de 9 mayo de 2017, con comunicación de 22 de mayo de 2017, señaló:

> *"... Las competencias específicas de cada Unidad Administrativa del IESS, se encontraban determinadas en la norma legal que rigió al IESS en la Resolución emitida por el Consejo Directivo del IESS No. C.D. 457, de 30 de agosto de 2013; a la fecha Resolución C.D 535, de 8 de septiembre de 2016, con vigencia a partir del 6 de mayo de 2017... Puntualización que se circunscribe en el Art.226 de la Constitución de la República que dispone: "Las instituciones del Estado, sus organismos, dependencias, las servidoras o servidores públicos y las personas que actúen en virtud de una potestad estatal ejercerán solamente las competencias y facultades que les sean atribuidas en la Constitución y la ley. Tendrán el deber de coordinar acciones para el cumplimiento de sus fines y hacer efectivo el goce y ejercicio de los derechos reconocidos en la Constitución.- Abundo en este sentido enfatizando que el Sistema AS400 es de exclusiva utilización en las Unidades Médicas del IESS, las mismas que cuentan con un Director Administrativo y un Director Médico, que se desempeñan y ejecutan funciones respecto de este tema, siendo entre otras, la supervisión específica del Sistema".- Cabe puntualizar que en los Contratos de Servicios Ocasionales suscritos por las partes, cuando se vincula a una servidora o servidor, se establece entre otras, la Cláusula Décima Tercera con el siguiente texto: "RESERVA Y CONFIDENCIALIDAD...".- Adicionalmente en la Cláusula Décima Cuarta se determina: "ADMINISTRACIÓN Y REGISTRO DEL CONTRATO".- El jefe inmediato del lugar donde presta sus servicios el contratado será el responsable de la correcta ejecución de todas y cada una de las cláusulas... informando oportunamente de las novedades y de su cumplimiento a la Dirección Nacional de Talento Humano(...) contenido específico para aquellos contratos celebrados a nivel central.- (...) a nivel provincial... informando oportunamente de las novedades y de su cumplimiento a los Directores Provinciales, Directores de las Unidades de Médicas, y a las Unidades Administradoras de Talento Humano del IESS de cada jurisdicción según el caso... ".*

Lo mencionado por el Director Nacional de Gestión de Talento Humano, no modifica el comentario de auditoría, por cuanto, no presentó descargos en relación a las acciones realizadas para el cumplimiento de lo establecido en la *"Política que regulan las actividades relacionadas con el uso de Tecnologías y Comunicaciones"* emitida en resolución C.D 521, de 28 de abril de 2016, respecto del control de compromisos de confidencialidad, suscripción, documentación e inclusión de estos acuerdos como parte de los procesos institucionales de incorporación de funcionarios y/o servidores sin excepción.

El Coordinador General de TIC's del HCAM, que actuó en el período comprendido entre el 11 de agosto de 2014 y el 16 de diciembre de 2015, en respuesta al oficio

DCHENTA Y SIETE

0082-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 22 de mayo de 2017, señaló

> *"... Al respecto, durante el período de mi gestión fueron implementados triggers que permiten identificar la información del Sistema a la que un usuario ingresó, lo cual está relacionado con el control de acceso y manejo de la información del Sistema...".*

Lo manifestado, por el servidor, no modifica el comentario de auditoría, pese a la implementación de pistas de auditoría con relación al acceso de la información; no asesoró en relación a la revisión de accesos a la información sensible como historias clínicas, uso de querys y acceso a unidades médicas por superusuarios (usuarios creados en unidad médica denominada *"SUPERUSUARIO??"*).

El Coordinador General de TIC's del HTMC, que actuó en el período comprendido entre el 21 de marzo de 2016 y el 13 de diciembre de 2016, en respuesta al 0090-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 22 de mayo de 2017:

> *"... Consta en su informe que fueron realizadas 86 consultas de Historias Clínicas por Usuarios TIC y una consulta realizada por una Administradora de AS400. En estos dos casos puedo indicar que estas consultas se realizaron cuando llegaban Quipux o Memorandos reasignados por la Gerencia General, Dirección Administrativa o Dirección Médica del HTMC con sumillas insertas: "Autorizado TIC Atender" provenientes ya sea de Fiscalía General del Estado, Agencia Municipal de Tránsito, CTE, Juzgados u otra institución en la cual existían procesos judiciales en las que estaban inmersos afiliados del IESS y requerían la Historia laboral de los mismos para continuar con los procesos. Lo que se hacía en estos casos era verificar los datos del afiliado, realizar el Query o Consulta de HC, adjuntarla en el Quipux y despachar ya sea a Gerencia General, Dirección Administrativa o Dirección Médica y luego ser enviada a la institución que requería la información, por tal motivo no existía la firma del acuerdo de confidencialidad pero sí un memorando con sumilla autorizado. En cuanto a los demás usuarios que Ud. Cita en su informe que realizaron consultas e impresiones de HC como Admisionistas, personal de Estadísticas, Dosis Unitaria, Facturación, Responsabilidad Patronal y Ambiente Hospitalario, tenían estos permisos en el sistema justificado por las actividades que realizan en el Hospital como Trabajo Social encargada de elaborar la ficha Psicosocial del afiliado y la Unidad Técnica de Archivo y Documentación Clínica (Estadística) encargada del manejo de las historias clínicas de todos los pacientes del HTMC. Pero de igual forma se realizaron las debidas restricciones a esta información solicitadas por el Coordinador de Control de Calidad del HTMC mediante memorando Nro. IESS-HTMC-CGCC-2016-1242-M y IESS-HTMC-CGCC-2016-1267-M de 13 y 18 de octubre de 2016 respectivamente como se informó mediante memorando Nro. IESS-HTMC-CGTIC-2016-3872-M hacer (sic) realizado las debidas restricciones...".*

OCHENTA YOCHO

Lo manifestado por el Coordinador General de TIC's del HTMC, no modifica el comentario de auditoría, por cuanto durante el período comprendido entre el 21 de marzo y el 12 de octubre de 2016, no propuso al Gerente General del hospital, procedimientos para restringir la consulta e impresión de Historias Clínicas en el Sistema de Información Médica MIS AS400, a fin de canalizar los requerimientos de entes de control y externos; tampoco se realizaron revisiones regulares de los accesos asignados y autorizados a fin de preservar la confidencialidad de la información.

La Coordinadora Informática del HTMC, encargada y Coordinadora General de TIC's del HTMC encargada; por cuanto en el período comprendido entre el 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014, en respuesta al oficio 0086-0010-IESS-AI-2017, con oficio JRI-2017-001 de 23 de mayo de 2017, señaló:

> *"...puedo informar que los usuarios médicos administradores acceden a revisar el historial clínico de un determinado paciente cuando acude el paciente al área informática para que se le facilite el código de examen de laboratorio que lo extravió y sin ese código no se puede realizar el examen; también envían pedidos de fiscalía para que se les facilite el expediente clínico de algún paciente ya que recién en el año 2015 la ley orgánica de salud dispone la confidencialidad de las mismas y mi gestión es de enero a agosto a 2014... Además debo recalcar que en el período de mi gestión la Dirección Nacional de tecnología de la Información no estableció las funciones y procedimientos que se debían cumplir.... ".*

Lo comentado por la Coordinadora Informática del HTMC, encargada y Coordinadora General de TIC's del HTMC, encargada, no modifica el comentario de auditoría, debido a que evidenció la falta de procedimientos de restricción implementados en el Sistema de Información Médica AS400, así tampoco se establecieron los niveles de autorización para el acceso a historias clínicas.

El Gerente General del HJCA, encargado con período de actuación comprendido entre el 20 de mayo de 2015 y el 29 de abril de 2016, en respuesta al oficio 0095-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 25 de mayo de 2017, señaló:

> *"... Al respecto debo indicar que la creación de Usuarios y Claves del Sistema Informático AS400 son gestionados por el Departamento de Tecnologías de la Información TICS, para dichos trámites durante mi período de gestión se utilizaron todos los formatos asignados para dicho fin. De la misma forma en reunión mantenida con el Coordinador General de TICS se emitió acta en la*

OCHENTA Y NUEVE

actual se dispone y coordina los lineamientos, directrices y requerimientos para restringir el acceso a las historias clínicas de los pacientes del IESS, adjunto encontrará copia de dicha Acta, misma que pertenece a mi archivo personal de gestión...".

El Gerente General del HCAM, actuante en el período comprendido entre el 8 de junio de 2015 y el 31 de diciembre de 2016, en respuesta al oficio 0107-0010-IESS-AI-2017 de 9 de mayo de 2017, con memorando IESS-HCAM-GG-2017-0409-M de 31 de mayo de 2017, señaló:

"... Memorando IESS-HCAM-CGJ-2016-3226-M de 17 de octubre de 2016, suscrito por la Coordinadora General Jurídica- HCAM, cuyo texto dice "La propuesta es que este texto se despliegue al acceder al sistema AS-400 y deberá ser aceptado para poder ingresar a dicho sistema (...)".- Con memorando Nro. IESS-HCAM-GG- 2016-1316-M, de 12 de diciembre de 2016, esta Gerencia General se dirige al Subdirector Provincial de Prestaciones del Seguro de Salud de Pichincha, para manifestarle que: (...) se ha visto la necesidad de que los funcionarios tengan presente, la importancia de la confidencialidad de la información de las historias clínicas, así como el correcto uso de las claves que permiten el acceso al Sistema Hospitalario MIS-AS400; por tal motivo, se ha trabajado en conjunto con la Coordinación General Jurídica, la Coordinación General de Talento Humano, la Coordinación General de TIC´S y la Coordinación General de Control de Calidad, y se ha propuesto un texto de confidencialidad de la información de historias clínicas ... mismo que deberá desplegarse al momento de acceder al sistema hospitalario MIS-AS400 y deberá ser aceptado por el usuario para poder ingresar a dicho sistema (...).- Memorando IESS-HCAM-CGJ-2016-2036-M de julio 20 de 2016, el Coordinador General Jurídico HCAM Subrogante , en atención al requerimiento realizado por el Coordinador General de Tecnologías de Información y Comunicación referente a que mediante el comité de historias Clínicas realizado el 22 de julio de 2016, solicitó se le redacte una cláusula para que sea incorporada al formulario de Datos de Usuarios al momento de realizar la entrega de la clave para el ingreso en el sistema AS400(...).- Acta de reunión de 02/01/2017, el comité de Historias Clínicas dice "intervención del... Coordinador de TIC´S, manifiesta el día miércoles me enviaron la aprobación para la implementación de la nota sobre confidencialidad de la Historia Clínica en el sistema AS-400...".

Lo mencionado por el Gerente General del HCAM, actuante en el período comprendido entre el 8 de junio de 2015 y el 31 de diciembre de 2016 y el Gerente General del HJCA, encargado con período de actuación comprendido entre el 20 de mayo de 2015 y el 29 de abril de 2016, no modifica el criterio de auditoría, en razón de que no se dictaron lineamientos para la revisión de accesos a las opciones que permitieron consulta e impresión de Historias Clínicas generadas en el Sistema de Información Médica AS400. Cabe indicar que hasta la fecha de corte del examen especial, no se evidenció la implementación de acuerdos de confidencialidad

aceptados por los usuarios del referido sistema, además de la socialización de los procedimientos para la solicitud, autorización y entrega de claves de usuario ni de la responsabilidad sobre el buen uso de las claves entregadas.

El Coordinador General de TIC's del HJCA, actuante en el período comprendido entre el 01 de julio de 2015 al 31 de diciembre de 2016; en respuesta al oficio 0097-0010-IESS-AI-2017, con memorando IESS-HJCA-CGTIC-2017-0148-M de 24 de mayo de 2017, señaló:

> *"... La Coordinación General de TIC HJCA remitió los acuerdo* (sic) *de confidencialidad a la DNT* (sic) *en memorando número IESS-HJCA-CGTIC-2016-0270-M.- a la fecha se lleva Acuerdo de confidencialidad escritos en HJCA, en la entrega y asignación de claves MIS-AS400, se espera recibir disposiciones a Nivel Central... Los usuarios de Subsidios y Responsabilidad Patronal en el sistema MIS-AS400 consultan e imprimen historias clínicas con el fin de revisar las Atenciones médicas, determinar y generar las sanciones respectivas a los patronos y/o empleadores.- Estadística y Atención al Cliente consultan e imprimen historias clínicas con el fin de consolidar datos, gestión de turnos y actividades propias al servicio.- Facturación consultan e imprimen historias clínicas con el fin de realizar las planillas respectivas para Dirección de Salud, Sppat (SOAT), RPIS entre otros y poder justificar las objeciones de Auditoría médica.- Medico Auditor consulta e imprimen historias clínicas con el fin de realizar el seguimiento a los diferentes casos médicos, así como a casos relacionados con Fiscalía, entre otros.- TIC HJCA accede a Historias Clínicas para brindar el soporte a usuarios internos y externos en base a requerimientos de información(...).- En relación a los Querys se gestionó la capacitación de un funcionario de TIC que labora en Planificación y cumplir lo establecido en la resolución CD 468 Articulo 40 numero 2 para reportes solicitados...".*

Lo mencionado por el Coordinador General de TIC's del HJCA, no modifica el criterio de auditoría por cuanto no evidenció que propuso las políticas para el acceso, manejo y procesamiento de la información del Sistema de Información Médica MIS AS400, para la coordinación entre los Jefes de Servicios de las áreas usuarias y la unidad a su cargo, para llevar a cabo las revisiones regulares de las opciones asignadas en cada módulo del aplicativo, como es el caso de las opciones de consulta e impresión de Historias Clínicas.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

NOVENTA Y UNO

El Director del Seguro General de Salud Individual y Familiar encargado y Director del Seguro General de Salud Individual y Familiar, en funciones desde el 8 de enero de 2016 y el 18 de febrero de 2016; y, desde el 19 de febrero de 2016 y el 26 julio de 2016, respectivamente, con comunicación IPBR-2017-004 de 28 de mayo de 2016, acotó:

> *"... Mediante memorando No.IESS-DSGSIF-2016-0154-M del 14 de enero de 2016, se remite las matrices de las provincias de Azuay, Chimborazo, Guayas, Imbabura, Manabí, Pichincha y Tungurahua, con datos de los funcionarios para la creación de roles y usuarios para el Sistema de Derivaciones Médicas; con Memorando No. IESS-DSGSIF-2016-0380-M del 28 de enero de 2016, se nombra al administrador de usuarios del Sistema de Derivaciones, quien "deberá coordinar con los responsables de cada Unidad Médica, con los Subdirectores Provinciales de Prestaciones de Salud y con la Subdirección de Regulación los usuarios que deberán ser creados, eliminados suspendidos temporalmente y cualquier otra condición que sea necesaria".- Con memorando No. IESS-SDNASS-2016-0807-M del 14 de marzo de 2016, el Subdirector Nacional de Aseguramiento del Seguro de Salud solicita a los Subdirectores Provinciales la Depuración de Usuarios en el sistema MIS/AS400...".*

Lo mencionado por el Director del Seguro General de Salud Individual y Familiar, no modifica el comentario de auditoría, en razón de que el requerimiento IESS-DSGSIF-2016-0380-M del 28 de enero de 2016, fue dirigido a la Directora de Afiliación y Cobertura, Encargada, por lo tanto, no aplicó al Sistema de Información Médica AS400, sino al Sistema de Derivaciones Médicas; en relación al requerimiento IESS-SDNASS-2016-0807-M del 14 de marzo de 2016, como se evidenció en un comentario anterior, no se presentaron las actividades realizadas para la depuración de usuarios en el Sistema de Información Médica MIS AS400.

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, con comunicación de 29 de mayo de 2017, no acotó información sobre este comentario.

El Gerente General del HJCA, actuante en período comprendido entre el 2 de mayo de 2016 y el 27 de octubre de 2016, con comunicación de 30 de mayo de 2017, acotó:

> *"a) Además de realizar la elaboración, aprobación y difusión de: "Normativa de Funciones del Interno Rotativo del Hospital José Carrasco Arteaga" y "Normativa de Funciones de las practicas del Externado en carreras de Salud en el Hospital José Carrasco Arteaga"; estableciendo responsabilidades, obligaciones y sanciones respecto de la confidencialidad de las historias clínicas; durante mi gestión se creó el Comité de Auditoría para el*

Noventa y dos

Mejoramiento de la Calidad de Atención de Salud e Historia Clínica, del cual participa como Vocal el Coordinador General de Tecnologías de la Información y Comunicación (TICs) del Hospital José Carrasco Arteaga.- Con todas estas medidas tomadas en equipo en el HJCA, se garantiza la confidencialidad y privacidad de la información de los pacientes, lo que fue reconocido por la ONG Accreditation Canada Internacional, quien otorgó la Acreditación Nivel Oro al Hospital José Carrasco Arteaga, dentro de su informe en la página 101 menciona textualmente: "Se encuentran implementadas todas las políticas secundarias relacionadas con la confidencialidad y privacidad de los pacientes, y el acceso oportuno a la investigación y practicas destacadas estan disponibles para el personal y los médicos apropiados...".

Lo manifestado por el Gerente General del HJCA, no demostró la emisión de lineamientos orientados a la ejecución de acciones para la restricción de los accesos otorgados al personal médico y administrativo a la historia clínica generada en el Sistema de Información Médica AS400, no obstante generó políticas complementarias en relación a la confidencialidad y privacidad de los pacientes del HJCA.

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, con memorando IESS-SDNSI-2017-0017-M de 2 de junio de 2017, no acotó sobre este punto.

El Coordinador General de TIC's del HCAM, actuante con período comprendido entre el 18 de diciembre de 2015 y el 31 de diciembre de 2016, en respuesta a lo expresado en la conferencia final de resultados, con memorando IESS-HCAM-CGTIC-2017-1125-M de 5 de junio de 2017, señaló:

"... Al respecto me permito indicar que ésta Coordinación solicitó a través del Comité de Historias Clínicas realizado el 22 de junio de 2016, trabajó la implementación de una cláusula de confidencialidad a ser incorporada en el formulario de creación de usuarios para el sistema médico MIS AS400, la misma que fue entregada por la Coordinación por la Coordinación General Jurídica- HCAM mediante Memorando Nro. IESS-HCAM-CGJ-2016-2036-M con fecha 20 de julio de 2016 el mismo que fue incorporado de inmediato como se puede evidenciar en solicitudes adjuntas.- Adicionalmente ésta Coordinación da a conocer a nivel de todo el hospital la necesidad de presentar el formulario indicado de manera obligatoria para la creación de usuarios.- Posteriormente en conjunto con la Coordinación General de Calidad-HCAM y la Dirección Nacional de Salud-IESS se trabajó en la implementación de un acuerdo de confidencialidad electrónico, para que el mismo sea aceptado por todos los usuarios del sistema y que el mismo se de aceptación obligatoria y de recordación periódica (cada 3 meses) el cual se incorporó e (sic) *producción a partir del 01 de Mayo de 2017 y aprobado mediante Memorando Nro. IESS-*

NOVENTA Y TRES

DSGSIF-2017-1135-M.- Subsecuentemente en trabajo en conjunto con la Dirección Nacional de Salud- IESS se trabajó en la depuración de usuarios y documentación de solicitudes y firmas de acuerdos de confidencialidad a nivel nacional.- A esta Coordinación no le llego el requerimiento mencionado en el Memorando Nro. IESS-DNTI-2016-3824-M de 7 de noviembre de 2016.- Adicionalmente se restricción (sic), *a partir del 22 de noviembre de 2016 para que las unidades médicas a nivel nacional puedan crear usuarios 999999999, y que ésta actividad sea de exclusividad de ésta Coordinación con el fin de controlar los acceso que se estaban generando en cada Subdirección Provincial.- En conjunto con la Dirección Nacional de Salud-IESS se ha pedido a todos los usuarios de salud nacional se envía actualizada la información de formularios de creación de usuarios y firma de acuerdos de confidencialidad mediante Memorando Nro. IESS-DSGSIF-2017-1364-M de fecha 4 de mayo de 2017 y la solicitud mediante Memorando Nro. IESS-DSGSIF-2017-1576-M de fecha de 30 de mayo de 2017 y dada contestación mediante Memorando Nro. IESS-HCAM-CGTIC-2017-1093-M de fecha 01 de junio de 2017...".*

Lo comentado por el Coordinador General de TIC's del HCAM, no modifica el comentario de auditoría, en razón de que no evidenció la revisión de opciones asignadas a los usuarios para la restricción de acceso a opciones para la consulta e impresión de historia clínica, *"trabajar con querys"*, y a los usuarios creados en unidad médica *"999999999"* en las Unidades Médicas del IESS; ni las acciones presentadas y acordadas en relación a la elaboración de un acuerdo de confidencialidad de la información tanto para los servidores médicos y administrativos, así como de la validación e inactivación de acceso al Sistema de Información Médica MIS AS400, se encontraron implementadas a la fecha de corte de esta acción de control, es decir 31 de diciembre de 2016.

Conclusiones

- Los Directores del Seguro General de Salud Individual y Familiar titulares y encargados, a su turno; no dispusieron ni organizaron la implementación de procedimientos para restringir el acceso a las historias clínicas de los pacientes de las Unidades Médicas del IESS a través del Sistema de Información Médica MIS AS400, tampoco emitieron lineamientos y directrices para la elaboración y suscripción de acuerdos de confidencialidad por parte de los usuarios internos y externos de la información generada por este sistema y sus bases de datos, lo que ocasionó que no se establezcan a los usuarios del sistema las responsabilidades y compromisos de reserva de la información de los pacientes de las Unidades Médicas del IESS y que no garantice el cumplimiento de los requerimientos de confidencialidad establecidos por la Autoridad Sanitaria Nacional.

NOVENTTA Y CUATRO

- El Director Nacional de Tecnología de la Información encargado, no emitió directrices a los Coordinadores Generales de TIC's de los hospitales HCAM, HTMC y HJCA para llevar a cabo las revisiones regulares de las opciones y autorizaciones asignadas a los usuarios en cada módulo del Sistema de Información Médica MIS AS400, lo que ocasionó que los usuarios del aplicativo tengan acceso irrestricto a la información de historias clínicas, resultados de exámenes de laboratorio, imagenología, etc., registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales; así como la utilización de la opción *"Trabajar con querys"* y la creación de usuarios en unidad médica denominada *"SUPERUSUARIO??"* con código de unidad médica *"9999999999"*, incrementando el riesgo de acceso no autorizado y mal uso de la información del Sistema de Información Médica AS400.

- El Director Nacional de Gestión de Talento Humano; no coordinó con el Director Nacional de Tecnología de la Información, para la implantación de procedimientos referente a la suscripción, documentación y custodia de los compromisos de confidencialidad de los servidores y trabajadores del IESS; lo que ocasionó que no se organizaran acciones, ni se instruyeran a los responsables de las áreas de talento humano de las Unidades Médicas del IESS, ni controlara que los compromisos de confidencialidad de la información, documento físico o electrónico, sean firmados de forma manuscrita o electrónica por todo el personal de la institución sin excepción, tampoco gestionó la custodia de los compromisos firmados, en los expedientes, físicos o electrónicos, de cada funcionario y/o servidor, ni controló que la firma de los compromisos de confidencialidad sean parte de los procedimientos de incorporación de nuevos funcionarios y/o servidores a la institución, sin excepción; incrementando el riesgo de acceso no autorizado y mal uso de la información del Sistema de Información Médica AS400.

- Los Gerentes Generales del HCAM; los Gerentes Generales del HTMC, titulares y encargados; y, los Gerentes Generales del HJCA, titulares y encargados; no vigilaron el cumplimiento de las políticas de administración pública en las áreas a su cargo, de conformidad con la normativa vigente para la confidencialidad de la información del Sistema de Información Médica MIS AS400; tampoco establecieron la normativa interna para que los Coordinadores Generales de TIC's cuenten con

NOVENTA Y CINCO

lineamientos y disposiciones que permitan la revisión en conjunto con el área requirente de la validez y vigencia de los accesos y perfiles otorgados a los usuarios permitiendo la consulta irrestricta de la información de historias clínicas, resultados de exámenes de laboratorio, imagenología, etc., registro de atenciones médicas con indicación de diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales; así como la utilización de la opción "Trabajar con querys y creación de usuarios en unidad médica denominada *"SUPERUSUARIO??"* con código de unidad médica *"9999999999"*, tampoco emitió las directrices para la suscripción de acuerdos de confidencialidad del uso, manejo de la información y responsabilidades de los usuarios que utilizan el Sistema de Información Médica AS400; así como su control y archivo; lo que ocasionó que la información relacionada a la historia clínica de los pacientes de las Unidades Médicas a su cargo, se encuentre disponible, y sin restricción mediante el acceso a opciones de consulta y/o impresión por parte de los usuarios de áreas administrativas dentro y fuera del hospital, que no pertenecieron a la cadena sanitaria; así como que no se establezcan las responsabilidades y compromisos de reserva del personal de las Unidades Médicas de tercer nivel, ni las sanciones en caso de su inobservancia, sin que se restringa el acceso a la información.

- La Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado; la Coordinadora Informática del HTMC, encargada, los Coordinadores Generales de TIC's del HTMC; los Coordinadores Generales de TIC's del HJCA, titular y encargado; no propusieron al Gerente General del hospital al que pertenecen, las políticas para el acceso, manejo y procesamiento de la información del Sistema de Información Médica MIS AS400, para la coordinación entre los Jefes de Servicios de las áreas usuarias y la unidad a su cargo, para llevar a cabo las revisiones regulares de las opciones asignadas en cada módulo del aplicativo; tampoco supervisaron, ni reportaron a la Dirección Nacional de Tecnología de la Información, la suscripción de acuerdos de confidencialidad del personal de la unidad de TIC's del HCAM y HTMC, conforme la disposición emitida por el Director Nacional de Tecnología de la Información constante en memorando IESS-DNTI-2016-3824-M de 7 de noviembre de 2016; lo que ocasionó que los usuarios del aplicativo tengan acceso irrestricto a la información de historias clínicas, resultados de exámenes de laboratorio, imagenología, etc., registro de atenciones médicas con indicación de

NOVENTA Y SEIS

diagnóstico y tratamientos, siendo los datos consignados en ellos confidenciales; así como la utilización de la opción *"Trabajar con querys"* y creación de usuarios en unidad médica denominada *"SUPERUSUARIO??"* con código de unidad médica *"9999999999"* y que no se establezcan las responsabilidades y compromisos de reserva del persona informático, respecto de la información de los pacientes y beneficiarios de los servicios de las Unidades Médicas.

Recomendaciones

Al Director General de Salud General Individual y Familiar

15. Coordinará con las Direcciones Nacionales de Riesgos Institucionales, Tecnologías de la Información, Coordinador General de TIC's del HCAM en calidad de Administrador del Sistema de Información Médica MIS AS400 y máximas autoridades de las Unidades Médicas, la identificación de las áreas y personal que deberán tener acceso autorizado a la consulta, impresión y entrega de historias clínicas mediante el referido sistema informático en las Unidades Médicas a nivel Nacional, la revisión de las opciones del sistema que permiten este acceso y su asignación a los usuarios, que deberá ser validado periódicamente por parte de los administradores de los accesos a los sistemas en conjunto con los responsables de las áreas requirentes del mismo, observando los requerimientos de la Autoridad Sanitaria Nacional, en relación a la confidencialidad e historia clínica electrónica, para preservar la reserva de la información de los pacientes.

16. Coordinará con la Direccion Nacional de Riesgos Institucionales, Tecnologías de la Información y Subdirección de Talento Humano, la implementación del acuerdo de confidencialidad suscrito por cada uno de los servidores, trabajadores y personal vinculado al Instituto Ecuatoriano de Seguridad Social y las Unidades Médicas, en relación al uso de sistemas de información que generan, almacena y transmiten información confidencial.

17. Coordinará con la Direccion Nacional de Riesgos Institucionales, Tecnologías de la Información, implementen la suscripción de acuerdos de confidencialidad con terceros, como el caso de proveedores, capacitadores, pasantías, entes de

NOVENTA Y SIETE

control, entre otros, los que serán de responsabilidad de las áreas requirentes de los servicios y requisito para la ejecución de sus actividades.

18. Dispondrá al Coordinador General de TIC's del HCAM, coordiné con los administradores del Sistema de Información Médica MIS AS400, para la restricción del uso de consultas por querys en las Unidades Médicas, estableciendo los procedimientos de excepción para su autorización y uso, accesos que deberán ser revisados periódicamente.

19. Dispondrá al Coordinador General de TIC's del HCAM, coordiné con los administradores del Sistema de Información Médica MIS AS400, para establecer los procedimientos para la restricción de los accesos a usuarios creados en la Unidad Médica denominada *"SUPERUSUARIO??"*, para el establecimiento del acceso a Unidades Médicas específicas. Toda vez, que estos accesos deberán ser revisados y aprobados periódicamente, por parte de las áreas usuarias.

Falta de formalización de procedimientos para acceso de usuarios VPN IESS AS400

El Director Nacional de Tecnología de la Información del IESS, otorgó a las empresas externas y prestadores médicos, el acceso VPN, como medio acceso remoto al Sistema de Información Médica MIS AS400, ubicado en el Centro de Cómputo del HCAM.

En el acta de trabajo de 4 de julio de 2016, sin suscribir por el Coordinador de Tecnología HCAM, Analista Informática DNTI, el Administrador Subdirección Nacional de Provisión de Servicios, la Técnica informática Coordinación de Medicamentos, la Oficinista Subdirección Nacional de Provisión de Servicios, la Oficinista de la Subdirección Provincial de Prestaciones del Seguro de Salud Pichicha; con el tema: *"Presentación de los procedimientos de: Creación, eliminación y cambio de opciones de usuarios y contraseñas administrativas"*, dentro de los puntos incluidos se trataron:

> *"... La Subdirección Nacional de Provisión de Servicios indica que las Subdirecciones y Jefaturas Provinciales, tomaran la responsabilidad de validación de los usuarios VPN que requieran acceso para el área de salud.- La Subdirección Nacional de Provisión de Servicios, indica que deberán remitir a la DNTI desde las Subdirecciones y Jefaturas Provinciales la documentación completa, y debidamente llena y firmada para ser tramitada, mínimo en 48 horas antes de la*

NOVENTA Y OCHO

necesidad de acceso.- La DNTI indica que el tiempo máximo de acceso de un usuario VPN será de 1 año calendario.- Será responsabilidad de los solicitantes/validadores notificar formalmente los cambios necesarios en los usuarios así como la dada de baja con la debida oportunidad.- Es responsabilidad de los solicitantes/validadores realizar el trabajo de verificación de convenios y/o contratos de los usuarios previo a solicitar la creación, modificación o eliminación a la DNTI.- Se indica que la DNTI, una vez recibida el acta, procederá con la depuración de los usuarios, previo a la extracción de una nueva lista para que sea enviada a las dependencias.- La Subdirección Nacional de Provisión de Servicios indica que una vez que las dependencias tengan el nuevo listado, deberán realizar una depuración y remitirla en un máximo de 72 horas... La DNTI propuso un período de 15 días.- La DNTI indica que los usuarios que no sean remitidos en dichas listas pasadas las 72 horas serán eliminados...".

La Analista Informática DNTI, remitió mediante correo Institucional, a los participantes de la elaboración, la revisión y suscripción del acta de trabajo, misma que hasta la fecha de corte de esta acción de control no se encontró formalizada; sin embargo, con memorando IESS-SDNPS-2016-1456-M de 6 de julio de 2016, la Subdirectora Nacional de Provisión de Servicios emitió *"Directrices para solicitudes de Usuarios VPN"*, a los Subdirectores Provinciales de Prestaciones de Salud, y con copia al Director Nacional de Tecnología de la Información y Coordinador General de TIC's del HCAM, donde entre otros, en los mismos términos constantes en el acta de trabajo, citada en párrafos anteriores, expresó:

"...Con la finalidad de que los requerimientos de usuarios VPN relacionados al Sistema MIS-AS400 sean atendidos de manera oportuna, agradeceré a ustedes se sirvan coordinar estos pedidos directamente con la Dirección Nacional de Tecnología de la Información, para lo cual se deberá verificar toda la información de respaldo con base en la normativa legal vigente.- El acta de solicitud para creación de usuarios VPN(adjunta), se deberá enviar escaneada a través del sistema de gestión documental y en físico, con las firmas de responsabilidad, tanto del solicitante como del Subdirector o Jefe Provincial.- Los documentos como contratos, certificados de acreditación o convenios para los dispensarios anexos, deberán estar debidamente validados, pues la creación del usuario VPN está bajo su absoluta responsabilidad.- En el acta de solicitud, deberá constar los horarios en los cuales podrán acceder a la red del IESS a través de VPN, además de las fechas de vigencia de este acceso...".

Con correo electrónico Institucional de 11 de septiembre de 2016, la Analista Informática de la DNTI, reportó a sus contrapartes del área de Salud y con conocimiento de la Subdirectora Nacional de Provisión de Servicios actuante entre el período comprendido entre el 4 de abril de 2016 y 30 de septiembre de 2016, lo siguiente:

NOVENTA Y NUEVE 99

"... Estamos teniendo inconvenientes pues lo que se acordó bajo el acta de reunión no se ha llevado a cabo.- El listado de usuarios no ha sido depurado y aún están activos todos los usuarios.- No se ha revisado quien verificará a los prestadores que se unen directamente por enlaces.- No se ha remitido el acta de legalización de los usuarios anteriores.- Se están enviando a la DNTI solicitudes directas sin respetar lo establecido, es decir que los Subdirectores Provinciales de Salud, remitirían, previa la validación de la pertinencia o no de la solicitud, tal es el caso, que incluso los médicos están enviando solicitudes directamente a la DNTI.- Se estableció que los usuarios nuevos serian creados solamente una vez depurados los anteriores, es decir, eliminados todos los que ya NO son necesarios, pero lamentablemente, no se ha enviado los listados depurados, mismos que en teoría iban a ser remitidos en un máximo de 72 horas. Por las necesidades que han remitido como urgentes, se han creado nuevos usuarios, lo que complica la depuración...".

La Analista Informática de la DNTI, mediante correo Institucional de 27 de abril de 2017, informó al equipo de auditoría sobre la depuración de usuarios con acceso a la VPN del IESS, señaló:

"... Se eliminó todos los usuarios caducados en Diciembre, existía una lista de usuarios con fecha de caducidad posterior al 31 de diciembre que no fueron validados, para los cuales se procedió con la eliminación según consta en el email adjuntos(SIC), .esto después de que la Coordinación del área solicitó directamente a dichos prestadores comunicarse con su Dispensario pues no estaban en las listas de autorización remitidas hasta ese momento, al no haber respuesta se caducó y posteriormente se eliminó todos pues no fueron renovados...".

Conforme lo expuesto, se concluyó que los usuarios con acceso a la VPN, durante el período 2016, no fueron depurados, debido a que no se cumplieron con los compromisos establecidos en el acta de trabajo de 4 de julio de 2016, por parte de la Subdirectora Nacional de Provisión de Servicios, en consecuencia los accesos de los usuarios no depurados, se encontraron sin ser validados por un lapso aproximado de 5 meses, esto es desde el 7 de julio hasta el 31 de diciembre de 2016, fecha en la que se caducaron automáticamente estos accesos y de los cuales la DNTI informó no se renovaron.

En adición, a lo mencionado, se determinó que la Coordinación General de Tecnologías de la información del HCAM, administró otro acceso VPN al Sistema de Información Médica MIS AS400 y su base de datos, a su cargo, que no dependió de la DNTI, por tanto no existieron lineamientos que permitan la coordinación de acciones para el acceso al Sistema de Información Médica MIS AS400.

Lo comentado se presentó debido a que el Director Nacional de Tecnología de la Información encargado con período de actuación comprendido entre el: 18 de mayo de 2015 y el 31 de diciembre de 2016, en conocimiento que la Subdirectora Nacional de Provisión de Servicios emitió las *"Directrices para solicitudes de Usuarios VPN"*, constantes en memorando IESS-SDNPS-2016-1456-M de 6 de julio de 2016, no elaboró, documento, ni difundió el procedimiento debidamente aprobado para la creación, eliminación y cambio de opciones de usuarios y contraseñas administrativas; por lo que no se establecieron los mecanismos de comunicación y coordinación entre las funciones de tecnología de información y las funciones propias de las áreas funcionales de la entidad; tampoco emitió lineamientos para que los accesos VPN al Sistema de Información Médica MIS AS400 sean regulados únicamente por la Dirección Nacional de Tecnología de la Información, a través del cumplimiento de estos procedimientos; ni se emitieron directrices para la coordinación de acciones con la Coordinación General de Tecnologías de la información del HCAM, pues administró otros accesos VPN al referido sistema, lo que ocasionó que no exista un procedimiento unificado de autorización para el acceso remoto al Sistema de Información Médica MIS AS400.

Los referidos servidores incumplieron lo dispuesto en las letras a) y b) del artículo 22, Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; la letra e), del número 2.4.3, del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido por el Consejo Directivo del IESS, mediante Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referentes a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información; y, la Norma de Control Interno 200-07 Coordinación de acciones organizaciones; 410-04 Políticas y procedimientos.

La Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referente a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información, establece:

> *"... será responsable de la planificación, coordinación y dirección de las actividades referentes a los procesos de Gestión de Tecnológica de Información y Comunicaciones y tendrá las siguientes funciones y responsabilidades.- e) Generar lineamientos y directrices para la gestión de infraestructura de la tecnología de información, bases de datos, redes y*

CIENTO UNO

sistemas, desarrollo y mantenimiento de aplicaciones y soporte técnico a usuarios...".

La Subdirectora Nacional de Provisión de Servicios que actuó en el período comprendido entre el: 5 de abril de 2016 y el 30 de septiembre de 2016, no supervisó el cumplimiento de las disposiciones emitidas en memorando IESS-SDNPS-2016-1456-M de 6 de julio de 2016; tampoco, en conocimiento de los acuerdos contenidos en acta de 4 de julio de 2016, y socializada en correo Institucional de 19 de julio de 2016, y de los incumplimientos reportados por la Analista Informática de la DNTI con correo institucional de 11 de septiembre de 2016, no dio seguimiento, ni supervisó el acatamiento de los lineamientos contenidos en las *"Directrices para solicitudes de Usuarios VPN"*, tampoco coadyuvó a la realización de los compromisos acordados en el acta de 4 de julio de 2016, respecto del listado de usuarios con acceso a la VPN Institucional, no solicitó a los Subdirectores Provinciales de Salud, los listados validados, lo que ocasionó que no se realice la depuración de accesos VPN al Sistema de Información Médica AS400, incrementando el riesgo de accesos no autorizados por parte de los consultorios, prestadores externos y anexos; incumpliendo lo dispuesto en las letras a) y b) del artículo 22.- Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; e inobservaron la Norma de Control 100-01 Control Interno, 401-03 Supervisión.

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0085 y 0111-0010-IESS-AI-2017 de 9 de mayo de 2017; al Director Nacional de Tecnología de la Información encargado; y, a la Subdirectora Nacional de Provisión de Servicios; obteniendo las siguientes respuestas:

La Subdirectora Nacional de Provisión de Servicios que actuó en período comprendido entre el 5 de abril de 2016 y el 30 de septiembre de 2016, en respuesta al oficio 0111-0010-IESS-AI-2017, con comunicación de 22 de mayo de 2017, al respecto, señaló:

"... Si el control interno debe ser descentralizado y jerárquico, la supervisión de las y los servidores que debían obtener un (SIC) su acceso al Sistema de Información Médica AS400, les correspondía a los jefes inmediatos y/o mediatos de las y los servidores públicos que requieren crear sus correspondientes usuarios, es decir, a los subdirectores provinciales, por cuanto se trataba de personal a su cargo.- Lo anterior implica que cuando en el memorando Nro. IESS-SDNPS-2016-1456-M de 6 de julio de 2016, en su parte final se redactó que se copiaran a la dependencia que estuvo a mi cargo, no se

CIENTO DOS

lo hizo como una responsabilidad prevista en la ley o en el reglamento del IESS a cumplir por mi parte o de la Subdirección Nacional de Provisión de Servicios (SNPS), puesto que la obligación de supervisión de los lineamientos generales emitidos desde la SNPS, correspondía a los jefes jerárquicos (...).- Tratándose del caso de la suscripción del acta, la responsabilidad personal, directa e intransferible de suscribirla, correspondía a los funcionarios intervinientes en la reunión que ocasionó la suscripción de dicho instrumento como consecuencia de su participación...".

Lo comentado, no modifica el comentario de auditoría, puesto que el acta de acuerdos para el procedimiento de solicitud para creación de la VPN, no fue formalizada, sin embargo, fue socializada, y puesta en conocimiento de la Subdirectora Nacional de Provisión de Servicios; por lo que no se instruyó a los Subdirectores Provinciales de Salud, la entrega de los listados de usuarios validados del acceso VPN institucional, para la depuración de estos accesos.

El Director Nacional de Tecnología de la Información, encargado, actuante en período comprendido entre el 18 de mayo de 2015 y 31 de diciembre de 2016, en respuesta al oficio 0085-0010-IESS-AI-2017, con memorando IESS-SDNSI-2017-0004-M de 22 de mayo de 2017, señalo:

"... El 28 de julio de 2016, la DNTI a través de mesa de Servicio se difundió directrices para procesar las solicitudes de creación de cuenta y accesos vía VPN, tanto para el personal de la institución como para el personal externo.- Cabe indicar que debido a los compromisos constantes en el Acta de Reunión de 4 de junio de 2016 y la falta de su respuesta a la insistencia, la DNTI se vio obligada a dar de baja a los usuarios VPN no validados y que no contaban con documentación de respaldo conforme los lineamientos señalados en correo... ".

Lo comentado por el Director Nacional de Tecnología de la Información, no modifica el comentario de auditoría, por cuanto no demostró la formalización de los procedimientos y compromisos constantes en acta de reunión de 4 de julio de 2016.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, con memorando IESS-SDNSI-2017-0017-M de 2 de junio de 2017, al respecto, señaló:

CIENTO TRES

> *"... debo acotar que con memorando N° IESS-SDNSI-2017-0015-M de 01 de junio de 2017 la Dirección Nacional de Tecnología de la Información emitió comunicado y directriz indicando que: "Para que las unidades de negocio mantengan un debido control de las solicitudes de creación de cuentas de acceso vía VPN para el ingreso a los sistemas y/o aplicativos que administran las unidades de negocio, posterior a la autorización y validación de la información enviarán a la Dirección Nacional de Tecnología de la Información las solicitudes para la atención pertinente, por lo tanto: "Es responsabilidad de los solicitantes/validadores realizar el trabajo de verificación de convenios y/o contratos de los usuarios previo a solicitar la creación, modificación o eliminación de acceso VPN a la DNTI"... ".- Dejando constancia que a partir de la presente fecha ninguna dependencia de salud o de la Institución en general, podrá crear de forma directa accesos de VPN... ".*

Lo manifestado por el servidor, no modifica el comentario de auditoría debido a que no se emitió lineamientos para que los accesos VPN al Sistema de Información Médica MIS AS400.

La Subdirectora Nacional de Provisión de Servicios de la DSGIF que actuó en período comprendido entre el 5 de abril de 2016 y el 30 de septiembre de 2016, con comunicación de 2 de junio de 2017, añadió:

> *"... Mediante correo electrónico de 30 de septiembre de 2016, el Administrador de la Subdirección Nacional de Provisión de Servicios (SDNPS), dio respuesta al correo electrónico de fecha 11 de septiembre de 2016, mediante el cual el mencionado funcionario puso en conocimiento de la Analista Informática DNTI, que el listado de usuarios remitido no es legible, y que sí el mismo no se podía modificar no iba a ser suscrito por parte del personal de la SDNPS. Adicionalmente se indicó que debían establecer un reemplazo de la Técnica Informática Coordinación de Medicamentos considerando que había dejado su cargo temporalmente debido a su período de maternidad...".*

Lo comentado por la Subdirectora Nacional de Provisión de Servicios no modifica el comentario de auditoría, por cuanto, no dio cumplimiento con los compromisos del acta de 4 de julio de 2016, en relación al listado de usuarios para depurar, tampoco lo manifestado, concuerda con el texto del correo de 30 de septiembre de 2016, en el cual se indicó una situación de forma en cuanto la redacción del documento presentado por la Ingeniera responsable en el área de Salud, según se detalla:

> *"1. El listado de usuarios presentado por la Ing... estuvo acompañado de una carta con la respectiva firma de responsabilidad, pero contenido no era legible en cuanto a la redacción se refiere. Este particular fue aclarado por la mencionada funcionaria, aduciendo que es un formato avalado por la DNTI y que se podía modificar. De acuerdo a las políticas de despacho de esta*

CIENTO CUATRO

Subdirección, no se firman documentos que no guarden coherencia en su texto o estructura...".

Conclusiones

- El Director Nacional de Tecnología de la Información encargado, en conocimiento que la Subdirectora Nacional de Provisión de Servicios emitió las *"Directrices para solicitudes de Usuarios VPN"*, constantes en memorando IESS-SDNPS-2016-1456-M de 6 de julio de 2016, no elaboró, documento, ni difundió el procedimiento debidamente aprobado para la creación, eliminación y cambio de opciones de usuarios y contraseñas administrativas; por lo que no se establecieron los mecanismos de comunicación y coordinación entre las funciones de tecnología de información y las funciones propias de las áreas funcionales de la entidad; tampoco emitió lineamientos para que los accesos VPN al Sistema de Información Médica MIS AS400 sean regulados únicamente por la Dirección Nacional de Tecnología de la Información, a través del cumplimiento de estos procedimientos; ni se emitieron directrices para la coordinación de acciones con la Coordinación General de Tecnologías de la información del HCAM, pues administró otros accesos VPN al referido sistema, lo que ocasionó no exista un procedimiento unificado de autorización para el acceso remoto al Sistema de Información Médica MIS AS400.

- La Subdirectora Nacional de Provisión de Servicios, no supervisó el cumplimiento de las disposiciones emitidas en memorando IESS-SDNPS-2016-1456-M de 6 de julio de 2016; tampoco, en conocimiento de los acuerdos contenidos en acta de 4 de julio de 2016, y socializada en correo Institucional de 19 de julio de 2016, y de los incumplimientos reportados por la Analista Informática de la DNTI con correo institucional de 11 de septiembre de 2016, no dio seguimiento, ni supervisó el acatamiento de los lineamientos contenidos en las *"Directrices para solicitudes de Usuarios VPN"*, tampoco coadyuvó a la realización de los compromisos acordados en el acta de 4 de julio de 2016, respecto del listado de usuarios con acceso a la VPN Institucional, no solicitó a los Subdirectores Provinciales de Salud, los listados validados, lo que ocasionó que no se realice la depuración de accesos VPN al Sistema de Información Médica AS400, incrementando el riesgo de accesos no autorizados por parte de los consultorios, prestadores externos y anexos.

CIENTO CINCO 04

Recomendaciones

Al Director Nacional de Tecnologías de la Información

20. Elaborará, documentará y difundirá el procedimiento debidamente aprobado para la solicitud de creación, activación, inactivación y caducidad automática del acceso de los usuarios de la VPN Institucional, donde regulará sus actividades y responsabilidades de las áreas requirentes.

21. Establecerá el procedimiento de monitoreo de la VPN gestionada por el Coordinador General de TIC's del HCAM, a fin de que estas actividades de administración de la red privada virtual, se alineen al procedimiento establecido por DNTI y evitar accesos no autorizados al Sistema de Información Médica MIS AS400, además analizará el riesgo de mantener este acceso, para la aplicación de los controles de acceso y seguridad.

Al Coordinador General de TIC's del HCAM

22. Coordinará con el Director Nacional de Tecnología de la Información a fin de estandarizar el acceso por medio de la VPN a su cargo, a los usuarios del Sistema de Información Médica MIS AS400.

Pistas de auditoría generadas para el Sistema MIS AS400, no permiten identificar el equipo desde el cual se generó la transacción

El Sistema de Información Médica MIS AS400, mantuvo dos tipos de pistas de auditoría, una por medio del sistema y otra por medio de base de datos a través de desencadenantes (triggers); las primeras desde el 2013 y las segundas a partir del 2015; en la información almacenada en estos registros de auditoría constó la dirección IP desde la cual se generó el registro, como mecanismo para mantener la trazabilidad de las transacciones.

Los registros de auditoría almacenados en la base de datos del sistema de Información Médica MIS AS400, correspondieron a direcciones IPs dinámicas (DHCP), esto significa que la dirección IP no se mantuvo fija en el tiempo, lo que ocasionó que no se pueda identificar el equipo desde el que se realizó una transacción.

CIENTO SEIS

Lo comentado, se presentó debido a que la Coordinadora de la Unidad Informática del HCAM, encargada y los Coordinadores Generales de TIC's del HCAM, titular y encargado, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 10 de agosto de 2014; 11 de agosto de 2014 y el 16 de diciembre de 2015; y, 18 de diciembre de 2015 y el 31 de diciembre de 2016; la Coordinadora Informática del HTMC, encargada, los Coordinadores Generales de TIC's del HTMC encargados y titulares, con períodos de actuación comprendidos entre el: 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014; 13 de agosto de 2014 y el 7 de enero de 2015; 2 de marzo de 2015 y el 10 de abril de 2015; desde el 18 de mayo de 2015 y el 31 de mayo de 2015; 1 de junio de 2015 y el 22 de junio de 2015; y, del 29 de julio de 2015 y el 20 de marzo de 2016; y, 21 de marzo de 2016 y 13 de diciembre de 2016; los Coordinadores Generales de TIC's del HJCA, titular y encargado, actuantes en los períodos comprendidos entre el: 1 de septiembre de 2014 y el 30 de junio de 2015; y 1 de julio de 2015 y el 31 de diciembre de 2016, no supervisaron que la configuración de los equipos de red, se ajusten a las necesidades de registro establecidas en las pistas de auditoría con que contó el Sistemas de Información Médica MIS AS400; debido a que estas son dinámicas (DHCP), esto significa que la dirección IP no se mantuvo fija en el tiempo, lo que ocasionó que las pistas de auditoría generadas para el Sistema MIS AS400, no permitan identificar el equipo desde el cual se efectuaron las transacciones en el sistema, dificultando efectuar revisiones posteriores.

Los referidos servidores, incumplieron lo dispuesto en las letras a) y b) del artículo 22, Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; los números 1 y 7 del artículo 41.- De la Coordinación General de Tecnologías de la Información y Comunicación, del Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, referente a las funciones y perfiles de los órganos de gestión y dependencias que integran las Unidades Médicas de Nivel III; y la Norma de Control Interno 410-07 Desarrollo y adquisición de software aplicativo.

CIENTO SIETE

El Reglamento Interno para la creación de la nueva estructura orgánica de las Unidades Médicas de Nivel III del IESS expedido por el Consejo Directivo del IESS, mediante Resolución C.D. 468, de 30 de mayo de 2014, establece:

> *"... Art. 41.- De la Coordinación General de Tecnología de la Información y Comunicación.-... 1. Proponer las políticas para el acceso, manejo, y procesamiento de la información y de los servicios de red, a través de las herramientas de Tecnología de Información y Comunicación (TIC);... 7. Controlar la seguridad, integridad y proteger el carácter institucional de la información manejada por los usuarios...".*

Los Directores Nacionales de Tecnología de la Información encargados con períodos de actuación comprendidos entre el: 25 de junio de 2014 y el 7 de enero de 2015;y, 18 de mayo de 2015 y el 31 de diciembre de 2016, no coordinaron ni dieron directrices a los Coordinadores Generales de TIC's de los hospitales HCAM, HTMC, HJCA, para la configuración de dispositivos de red, que se ajusten a las necesidades de registro establecidas en las pistas de auditoría con que contó el Sistemas de Información Médica MIS AS400; debido a que estas son dinámicas (DHCP), esto significa que la dirección IP no se mantuvo fija en el tiempo, lo que ocasionó la imposibilidad de conocer desde que equipo se realizaron las transacciones en el sistema, dificultando efectuar revisiones posteriores; incumpliendo lo dispuesto en las letras a) y b) del artículo 22, Deberes de las o los servidores públicos de la Ley Orgánica del Servicio Público; la letra j), del número 2.4.3, del Reglamento Orgánico Funcional del Instituto Ecuatoriano de Seguridad Social, expedido por el Consejo Directivo del IESS, mediante Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referentes a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información; y, la Norma de Control Interno 200-07 Coordinación de acciones organizaciones; 401-03 Supervisión.

La Resolución C.D.457, publicada en la Edición Especial del Registro Oficial 45 de 30 de agosto de 2013, referente a las atribuciones, deberes, responsabilidades y funciones de la Dirección Nacional de Tecnología de la Información, establece:

> *"... será responsable de la planificación, coordinación y dirección de las actividades referentes a los procesos de Gestión de Tecnológica de Información y Comunicaciones y tendrá las siguientes funciones y responsabilidades.- j) Acoger, ajustar e implementar estándares y mejores prácticas internacionales en los procesos de gestión de la tecnología de información y la comunicación...".*

CIENTO OCHO 24

De conformidad con lo dispuesto en el artículo 90 de la Ley Orgánica de la Contraloría General del Estado y 22 de su Reglamento, se comunicó los resultados provisionales, con oficios: 0081, 0082, 0083, 0086, 0087, 0088, 0090, 0096, 0097; 0084 y 0085-0010-IESS-AI-2017 de 9 de mayo de 2017; a los Coordinadores Generales de TIC's del HCAM; a los Coordinadores Generales de TIC's del HTMC; a los Coordinadores Generales de TIC's del HJCA; y, los Directores Nacionales de Tecnología de la Información encargados, obteniendo las siguientes respuestas:

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, en respuesta al oficio 0096-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 17 de mayo de 2017, señaló:

> *"... Una vez realizada una visión general de la infraestructura informática y procesos que se llevaba dentro del* (sic) Coordinación General de TIC's del HJCA se emite un documento denominado **"INFORME EJECUTIVO DE LA SITUACION ACTUAL DE LA COORDINACION DE TICS"**, donde se hace constatar en otros la falta de procesos que estén acordes a la resolución 468 y la falta de una plataforma CORE de servidores o software sobre la cual se deben implementar los sistemas o servicios que ayudaran a generar una plataforma estándar y controlada de aplicativos que ayudarían a generar mejores tiempos de respuesta en los trabajos cotidianos que el personal desempeña y que garanticen el correcto uso y resguardo de la información que se genera en la parte administrativa... *se han realizado las acciones necesarias para establecer políticas institucionales que deberían ser emitidas por la DNTI, las cuales como se puede observar no se tenían aprobadas y estandarizadas para las unidades médicas en el período de tiempo en el cual preste mis servicios a la institución, es importante indicar que el centralismos que maneja DNTI no permitió implementar una serie de proyectos bases en la plataforma CORE informática del HJCA y que se manejan en otras instituciones públicas del país...".*

El Coordinador General de TIC's del HCAM, que actuó en el período comprendido entre el 11 de agosto de 2014 y el 16 de diciembre de 2015, en respuesta al oficio 0082-0010-IESS-AI-2017 de 9 de mayo de 2017, con comunicación de 22 de mayo de 2017, señaló:

> *"... Al respecto, el período en el cual ejercí el cargo de Coordinador General de TICs del HCAM con el objetivo de implementar herramientas y procesos que permitan brindar las seguridades necesarias al Sistema de Información Médica MIS400* (SIC) se implementó como primera medida triggers o desencadenantes como se indica en el informe de resultados.- ... *Finalmente la implementación de un Directorio Activo hubiera permitido mantener la trazabilidad necesaria en el Sistema, trazabilidad que es requerida en el hallazgo producto del examen.-*
> CIENTO NUEVE

La contratación de la implementación de un Directorio Activo está contenida en el PAPP 2015 (Plan Anual de Política Pública), que fue puesto en consideración de la Gerencia General de la institución a través de memorando IESS-HCAM-GG-CGPEST-2015-1057-M de 1 de junio de 2015, suscrito por el Coordinador General de Planificación y Estadísticas del HCAM... ".

Lo mencionado por los Coordinadores Generales de TIC's del HCAM y HJCA, que actuaron durante el período comprendido entre el 11 de agosto de 2014 y el 16 de diciembre de 2015 y desde el 1 de septiembre de 2014 y 30 de junio de 2015, respectivamente; no modifica el comentario de auditoría debido a que pese a la implementación de pistas de auditoría con relación al acceso de la información; no demostraron acciones relacionadas al análisis de IPs y su aplicación en la administración de la red en los mencionados hospitales.

Posterior a las conferencias finales de comunicación de resultados, realizada los días 23, 24, 25 de mayo y 9 de junio de 2017, se presentaron los siguientes puntos de vista:

El Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015, con comunicación de 29 de mayo de 2017, señaló:

"... 3.- Luego de tener una serie de conversaciones... con personeros de DNTI en donde se explican las inquietudes encontradas dentro del área de TICS del HJCA se nos solicita que se envié correo electrónico con las propuestas para solventar las mismas, con fecha 30 de septiembre de 2014 se envía correo electrónico a... funcionaria de DNTI, donde se explican entre otros proyectos uno considerado importante que es la implementación de un Directorio Activo sobre la plataforma Windows, el mismo que garantizaría entre otros el control de autenticación dentro de los equipos finales de usuario, políticas de bloqueo de sesión...".

El Director Nacional de Tecnología de la Información, encargado, con período comprendido entre el 18 de mayo de 2015 y el 31 de diciembre de 2016, con memorando IESS-SDNSI-2017-0017-M de 2 de junio de 2017, no acoto su punto de vista a este comentario.

El Coordinador General de TIC's del HCAM, actuante con período comprendido entre el 18 de diciembre de 2015 y el 31 de diciembre de 2016, en respuesta a lo expresado en la conferencia final de resultados, con memorando IESS-HCAM-CGTIC-2017-1125-M de 5 de junio de 2017, señaló:

CIENTO DIEZ

"... Al respecto me permito indicar que en el Hospital Carlos Andrade Marín-IESS se tiene alrededor de 1500 equipos informáticos para todas las áreas y por ese motivo que se dispone de un Servidor DHCP configurado para que otorgue arrendamiento de IPs automáticamente de acuerdo a la VLAN que se le asigne y de acuerdo a la Sub red a la que pertenece, el tiempo de arrendamiento es de 45 días, es decir si una máquina no se enciende dentro de ese tiempo automáticamente es liberada esa IP y coge una disponible del pool de direcciones, esto se lo realiza por cuanto el parque informático es muy extenso y manejar IPs fijas es imposible, se maneja VLANS y subredes lo que permite una mejor administración, en el Servidor DHCP se guarda durante el tiempo de arrendamiento la Mac, el tiempo de arrendamiento y el nombre del equipo al que fue asignada esa IP.- Adicional en la parte Wifi-Personales y Wifi-HCAM se registra con nombres y la dependencia a la que pertenece en un directorio en el Firewall lo que permite identificar por ip a quien pertenece, pero de igual manera el arrendamiento es por tiempo establecido de 30 días.- Para los dispositivos móviles se tiene una red Wifi con arrendamiento de 2 días máximo por cuanto son equipos que no permanecen conectados todo el tiempo en el Hospital...".

La Coordinadora Informática del HTMC, encargada y Coordinadora General de TIC's del HTMC, encargada; por cuanto en el período comprendido entre el 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014, respectivamente; con oficio JRI-2017-002 de 5 de junio de 2017, acotó:

"... De acuerdo a la estructura o a la infraestructura establecida por el IESS la DNTI dejó configurando el Servidor de manera que se asignen las direcciones IPs de los equipos por DHCP por el volumen de equipos que maneja el Hospital Teodoro Maldonado Carbo.- La configuración de los Servidores fue realizada por personal de la DNTI en el caso del HTMC desde el año 2009 cuando en este Nosocomio se puso en producción el Sistema Multiempresa (AS400).- El HTMC optó en el año 2013 implementar el servicio del Active Directory para reforzar el tema de seguridad en los equipos...".

El Coordinador General de TIC's del HJCA, actuante en el período 1 de julio de 2015 al 31 de diciembre de 2016, con memorando IESS-HJCA-CGTIC-2017-0157-M de 6 de junio de 2017, acotó:

"... La red informática el (sic) *IESS, así como la asignación IP para nuestra unidad HEJCA esta supervisada por la DNTI, a su vez se dispone de un servidor local DHCP, para la gestión de RED.- Se dispone de un registro de IP's y funcionario para la asignación de recursos de red, por lo que se puede realizar un seguimiento.- Se dispone de una red con acceso WIFI con IP's asignadas de manera dinámica, esta debe renovar la tabla de asignación del IP's constantemente, puesto que supera el número de usuarios que laboral (sic) las 24 horas del día, este rango de IP's fue asignado por la DNTI...".*

Lo expuesto por el Coordinador General de TIC's del HCAM, La Coordinadora Informática del HTMC, encargada y Coordinadora General de TIC's del HTMC,

CIENTO ONCE

encargada; por cuanto en el período comprendido entre el 1 de enero de 2014 y el 30 de junio de 2014 y desde el 1 de julio de 2014 y el 12 de agosto de 2014, el Coordinador General de TIC's del HJCA, que actuó durante el período comprendido entre el 1 de septiembre de 2014 y 30 de junio de 2015 y el Coordinador General de TIC's del HJCA, actuante en el período 1 de julio de 2015 al 31 de diciembre de 2016, no modifica el comentario de auditoría, por cuanto no presentaron alternativas de identificación para los equipos desde donde se realizan las transacciones en el Sistema de Información Médica MIS AS400 de manera de que formen parte de la información registrada en las pistas de auditoría implementados.

Conclusión

Los Directores Nacionales de Tecnología de la Información encargados, no coordinaron ni dieron directrices a los Coordinadores de la Unidad Informática del HCAM y a los Coordinadores Generales de TIC's del HCAM, HTMC y HJCA y Coordinadora Informática del HTMC, quienes no supervisaron que la configuración de los equipos de red se ajusten a las necesidades de registro establecidas en las pistas de auditoría con que contó el Sistemas de Información Médica MIS AS400; debido a que estas son dinámicas (DHCP), esto significa que la dirección IP no se mantuvo fija en el tiempo, lo que dificultó identificar el equipo desde el que se realizaron las transacciones en el sistema, efectuar revisiones posteriores.

Recomendación

Al Director Nacional de Tecnologías de la Información

23. Analizará las alternativas que permitan registrar en las pistas de auditoría generadas en el Sistema de Información Médica MIS AS400, la identificación del equipo desde donde se ejecutaron las transacciones auditadas en el sistema, una vez definido el mecanismo, lo remitirá al Coordinador General de TIC's del HCAM a fin de replicar el procedimiento en las Unidades Médicas del IESS.

Eco. María Cristina Orbe Cajiao
AUDITORA INTERNA DEL IESS
CIENTO DOCE