

 UNIVERSIDAD NACIONAL DE COLOMBIA	MACROPROCESO: EVALUACIÓN, MEDICIÓN, CONTROL Y SEGUIMIENTO	CÓDIGO: U-FT-14.001.010
		VERSIÓN: 0.0
	FORMATO: INFORME EJECUTIVO	Página 1 de 4

EVALUACION A UNISALUD NIVEL CENTRAL Y SEDE BOGOTA (FASE I) ⁽¹⁾

1. INTRODUCCIÓN

UNISALUD es una “Unidad Especializada de la Universidad Nacional de Colombia, adscrita a la Rectoría, con organización propia y administración de recursos independientes”, cuya misión es “administrar y gestionar el aseguramiento en salud de sus afiliados, a través de la gestión del riesgo”, por lo tanto, la Oficina Nacional de Control Interno determinó incluir en su Plan de Auditoría para el año 2014 la evaluación a esta Unidad a Nivel Nacional y de la Sede Bogotá.

En consecuencia, para la evaluación al Nivel Nacional es importante tener en cuenta que en Junio de 2012 el Centro de Investigaciones para el Desarrollo de la Facultad de Ciencias Económicas –CID-, elaboró un estudio de sostenibilidad del servicio de salud ofrecido por UNISALUD, en el que uno de los objetivos fue: “(...) con base en la evaluación realizada, analizar en conjunto con las directivas de UNISALUD y la Universidad los posibles escenarios y las alternativas para garantizar la prestación eficiente del servicio, desde el punto de vista jurídico, técnico y financiero que constituyen en conjunto un análisis de sostenibilidad”.

Igualmente en enero de 2013, la ONCI hizo entrega de una evaluación a los protocolos de seguridad aplicados por UNISALUD para la reserva de las historias clínicas (HC) de afiliados que han registrado enfermedades de alto costo. En ese momento se evaluó exclusivamente el protocolo a HC de afiliados de alto costo, sin embargo, dentro de los procedimientos establecidos por UNISALUD, se encuentra el denominado *archivo de gestión y custodia de historia clínica*, cuyo objeto es “garantizar el adecuado manejo, custodia y archivo de las historias clínicas físicas de los usuarios de UNISALUD mediante la definición de actividades y responsables que permitan cumplir con la normatividad en cuanto a diligenciamiento, administración, conservación custodia y confidencialidad de la información”, el cual se constituye en el insumo para evaluar en esos términos la operatividad de la Sede Bogotá.

2. RESULTADOS DE LA EVALUACIÓN

Como resultado de la evaluación realizada por la ONCI, a continuación se presentan las observaciones del equipo evaluador, con base en las situaciones evidenciadas a través de los documentos consultados, las visitas de campo y las entrevistas realizadas, conforme a lo indicado inicialmente en la Guía de Evaluación.

2.1. Procedimiento Archivo de Gestión y Custodia de Historia Clínica

- Las HC² de los recién nacidos no se están identificando conforme lo establecido en el procedimiento U-PR-16.003.002 elaborado y aprobado en junio de 2011.

Se recomienda acoger lo indicado en la descripción de la actividad apertura e identificación de HC, para las historias de recién nacidos.

- La Unidad de Servicios no cuenta con el aplicativo para la impresión de los rótulos con la información requerida, según la actividad No. 1 del procedimiento³.

Con el fin de dar cumplimiento al procedimiento, la ONCI recomienda adelantar las gestiones que permitan utilizar nuevamente el aplicativo para la impresión de los rótulos con la información requerida.

- El área de archivo no cuenta con una maquina pica papel que garantice la destrucción total de los documentos que hacen parte de la depuración de las HC.

Frente a lo anterior se recomienda contratar o adquirir una máquina pica papel que garantice la destrucción total de los documentos que hacen parte de la depuración de las HC y ajustar la actividad en el procedimiento.

- Se evidenciaron HC que no se encuentran relacionadas en la BD de Control de HC, lo cual no permite garantizar su seguridad en términos de archivo y del contenido de su información.

Se recomienda a la Jefatura de Servicios de Salud de UNISALUD definir un mecanismo de operación y control que permita al personal responsable del área de archivo incorporar en la BD todas las historias clínicas que se generen en la Unidad.

- Se observan debilidades en la integridad de la información, dado que los datos de las dos fuentes (cuaderno y la base de datos de movimiento) no son consistentes.

Debido a que la actividad denominada evaluar y efectuar seguimiento al procedimiento, actualmente está bajo la responsabilidad del personal de HC, se recomienda a la Jefatura de Servicios de Salud establecer un mecanismo de control y seguimiento a los movimientos de las HC que garantice la

¹ Elaborado por los asesores y profesionales de la ONCI: Nubia Martínez Rippe, Mario Robayo Higuera, Hebert Fula Hernández y Luisa Fernanda Ríos Giraldo. Revisado por: Carlos Manuel Llano Alzate – Jefe ONCI. (Original firmado).

² Historia Clínica

³ Apertura e identificación de la Historia Clínica

confiabilidad e integridad de la información, tanto para la operatividad de rutina, así como también respecto a un plan de posibles contingencias.

- El personal de archivo no ejecuta ningún tipo de control relacionado con el número de folios de las HC que garantice la seguridad de la documentación.

Se sugiere a la Jefatura de Servicios de Salud aportar los mecanismos necesarios que permitan al personal del área de archivo mantener un control adecuado sobre el número de folios obrantes en cada una de las HC.

- No se evidencia un seguimiento formal por parte de área de archivo, al préstamo de las historias clínicas.

Se recomienda a la Jefatura de Servicios de Salud, requerir al área de archivo para que la solicitud de devolución de historias clínicas a los diferentes servicios se haga de manera formal cuando así se requiera, como parte del seguimiento y control al proceso ejecutado por esa instancia.

Adicionalmente, se sugiere a la Jefatura de Servicios de Salud en conjunto con la Oficina de Sistemas de UNISALUD, establecer en el sistema utilizado para el control de HC, algún tipo de alarma automática que permita tener un control sobre las historias que llegan al límite del tiempo permitido para el préstamo.

- La ONCI observa debilidades en el procedimiento, pues el responsable de ejecutarlo es el mismo responsable de hacer seguimiento a su gestión, lo cual no garantiza la objetividad en el seguimiento.

Se recomienda a la Jefatura de Servicios de Salud revisar la modificación del responsable de la actividad No. 5, con el fin de garantizar su cumplimiento y fortalecer el liderazgo en el seguimiento y control ante las actividades operativas ejecutadas en el área de archivo de HC.

2.1.1 De la base de datos administrada en el área de archivo.

- La BD que administra el área de archivo de HC carece de controles que permitan garantizar la seguridad y confiabilidad de la información, esto aunado a que las copias de seguridad del archivo no se hacen con una periodicidad que obedezca a la aplicación de las mejores prácticas orientadas al resguardo de la información. Por lo anterior, se potencializa el riesgo en la confidencialidad de la información y pérdida de la misma.

Se sugiere a la Jefatura de Servicios de Salud en conjunto con el área de sistemas de UNISALUD, identificar otro tipo de herramienta tecnológica que permita almacenar y administrar los movimientos de las HC de manera que garantice la disponibilidad de: reportes, indicadores u otro tipo de consulta necesarias, y

adicionalmente ofrecer seguridad al ingreso de la información mediante un control de acceso lógico.

2.2 Implementación y cumplimiento del protocolo de seguridad de la información

El área de sistemas de UNISALUD Sede Bogotá no cuenta con un procedimiento que describa las actividades secuenciales para la creación de las copias de seguridad y la restauración de las mismas a nivel de aplicación y de bases de datos. De igual forma se evidenció la aplicación de inadecuadas prácticas en la periodicidad de la generación de los backups dado que actualmente se generan solo dos veces por semana, lo cual podría representar un riesgo de pérdida de información.

Se recomienda al área de sistemas de UNISALUD Sede Bogotá, con la coordinación de la OTIC Bogotá, elaborar un procedimiento para la administración de las copias de seguridad y la restauración como actividad de control en la calidad de las mismas, el cual contenga actividades que controlen la periodicidad de la generación de los backups, para que en lo posible se realicen diariamente teniendo en cuenta los controles de custodia de los medios que no serían entregados a la firma⁴ en los días con ellos definidos. Igualmente, definir actividades de restauración en periodos específicos. Adicionalmente, acoger las mejores prácticas de TI⁵ en cuanto al recurso humano responsable. Este procedimiento permitiría transferir el conocimiento a nuevos funcionarios que puedan hacer parte del área lo cual colaboraría en la mitigación del riesgo de pérdida de información.

Se recomienda al área de sistemas de UNISALUD continuar con la gestión relacionada con el análisis y adquisición de hardware especial para las copias de seguridad, lo cual permitiría en gran medida garantizar la integridad y seguridad de la información contenida en los backups.

De acuerdo a la verificación documental, en la ODS No. 126 referida en este numeral la ONCI no observa la descripción de las responsabilidades, actividades y controles en términos de seguridad que se deben tener en cuenta por las partes en el momento de finalización del contrato para la entrega de la información custodiada.

Se recomienda al Jefe Administrativo y Financiero de UNISALUD, responsable de la interventoría de la ODS en conjunto con el área de sistemas de UNISALUD, definir los controles en términos de seguridad que se deben tener en cuenta por parte de la Unidad y la firma THOMAS MTI S.A. para la entrega de la información almacenada en los backups entregada en custodia hasta ese momento.

De acuerdo a la verificación de cumplimiento de algunas de las normas definidas para minimizar los riesgos potenciales de un Centro de Datos, se observaron elementos no pertenecientes a este lugar como por ejemplo insumos para impresoras y partes de

⁴ THOMAS MIT S.A.

⁵ Tecnología de la Información

equipos de cómputo, los cuales saturan el espacio disponible y podrían representar un riesgo que atente a la seguridad y confiabilidad de este espacio.

Se recomienda al área de sistemas de UNISALUD Bogotá efectuar un análisis de riesgos del Centro de Datos con el propósito de que sirva como insumo para dar cumplimiento a las normas definidas relacionadas con los Centros de Datos, en este sentido establecer controles relacionados con el control de acceso físico y almacenamiento de elementos no pertenecientes al Centro de Datos, entre otros aspectos.

La ONCI evidenció que desde el 2013, UNISALUD no cuenta con un Directorio Activo que le permita administrar los elementos de su red al igual que sus equipos de cómputo. En ese orden de ideas, no cuenta con políticas de seguridad y/o políticas de instalación de software entre otras tareas aplicadas a su red que contribuyan a minimizar el riesgo de falta de integridad, seguridad y pérdida de información.

Se recomienda a la DNTIC efectuar la gestión necesaria para emitir con prontitud el concepto técnico solicitado por UNISALUD de manera que se contribuya en la adquisición del hardware y software necesario para la instalación del Directorio Activo en la Unidad.

Se recomienda al área de sistemas de UNISALUD, en conjunto con la División Administrativa y Financiera de la Sede Bogotá continuar con las acciones necesarias para la adquisición de los elementos tecnológicos requeridos para la instalación del Directorio Activo en la Unidad en aras de contribuir con la seguridad de la información.

Aunque desde la práctica se manejan algunas acciones en caso de posibles fallas en el sistema de información, el área de sistemas de UNISALUD no cuenta actualmente con un Plan de Contingencia que contenga medidas de tipo técnico, organizacional y de gestión humana para garantizar la continuidad de la Unidad en caso de presentarse algún tipo de amenaza que pueda atentar contra la información contenida en las HC digitales.

Se recomienda al área de sistemas de UNISALUD, en coordinación con otras áreas como la jefatura médica efectuar un análisis de riesgos que permita identificar los tipos de riesgo que se podrían presentar en esta instancia, teniendo en cuenta que en el Centro de Datos reposa la base de datos de las HC digitales, información considerada crítica para la Unidad. Por lo anterior, se recomienda efectuar, con el insumo mencionado, un Plan de Contingencia que cumpla con las fases de Evaluación, Planificación, Pruebas de Viabilidad, Ejecución y Recuperación.

De acuerdo a la verificación documental, la ONCI identificó el diligenciamiento de dos tipos de formularios de compromiso con el buen uso de la tecnología informática, la confidencialidad y seguridad de la información, por personal de la Unidad. De acuerdo a lo manifestado por UNISALUD obedece a cambios efectuados por el área de Contratación en el registro, que aún no

han sido formalmente adoptados por el Sistema Integrado de Calidad.

Se recomienda al área de contratación efectuar la gestión necesaria para legalizar la modificación realizada en el “Formulario de compromiso con el buen uso de la tecnología informática, la confidencialidad y seguridad de la información”, en atención a lo dispuesto en el Anexo 1 “Parámetros generales para la elaboración de documentos, codificación, emisión, revisión, aprobación, modificación, control de cambios, distribución, eliminación, manejo e identificación de documentos obsoletos” del Sistema Integrado de Calidad de la Universidad.

En evaluación realizada por la ONCI⁶ en lo asociado al acceso lógico del controlador de dominio y de algunos sistemas de información, se identificó que “(...) la Universidad no cuenta con una política definida para el control de accesos lógicos, en este sentido se recomendó a la DNTIC elaborar políticas y/o directrices que permitan establecer controles de acceso lógico, al igual que la clasificación de la información⁷ en la Universidad, de manera que se asegure el acceso a los sistemas de información, a los programas, red y datos por usuarios autorizados”

Se recomienda a UNISALUD que una vez la DNTIC defina las políticas para el acceso lógico al controlador de dominio y a los sistemas de información, apliquen lo establecido en la normatividad en el marco de las buenas prácticas de TI de la Universidad.

Se recomienda al área de Sistemas de UNISALUD, instancia encargada de la administración de la base de datos, realizar una depuración de la misma, con el visto bueno de la(s) instancia(s) de UNISALUD que corresponda.

Se recomienda al área de sistemas de UNISALUD junto con la DNPPA generar un procedimiento que asegure las acciones relacionadas con la activación o suspensión de las cuentas de usuario en el sistema de información SISS IPS. Lo anterior, por medio de la comunicación oportuna de las novedades de los usuarios desde la DNPPA o las dependencias de UNISALUD, responsables de las actividades de activación o suspensión según el caso, lo cual aportaría en gran medida a la seguridad de la red, sistemas y datos de UNISALUD.

Se evidenció ausencia de administración o gestión de cambio del sistema de información SISS IPS, tal como lo define la Directriz Técnica.

Se recomienda al área de sistemas de UNISALUD definir en términos de responsabilidad y ejecución las actividades necesarias para efectuar la gestión de cambios del sistema de información. Este procedimiento debe contar con los controles necesarios para autorizar, priorizar, rastrear y/o administrar los cambios en el sistema de información SISS IPS teniendo en cuenta cualquier tipo

⁶ EVALUACIÓN AL MACROPROCESO GESTIÓN DE LA INFORMACIÓN – PROCESO GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES (TIC), Julio de 2014

⁷ Por ejemplo información clasificada como reservada, o no pública.



de mantenimiento efectuado a lo largo del ciclo de vida del sistema.

A pesar que el Protocolo para la Seguridad de la Información en UNISALUD, contempló en el numeral 2.2 la *“Identificación de riesgos del acceso a terceros personas”*, este ejercicio puntual no se desarrolló al nivel de detalle sugerido en el protocolo, como lo es *“Controles que se compromete a emplear la tercera persona para su manejo e impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento”*. Se establecieron acciones que minimizan los riesgos, sin tener el grado de detalle sugerido en la matriz.

Se recomienda la aplicación del Protocolo para la Seguridad de la Información en UNISALUD en todas sus partes, incluyendo la elaboración de la *“Matriz de identificación de riesgos del acceso de terceras personas”*. En el evento que del análisis que está realizando el administrador de documentos de calidad de la Vicerrectoría General a los documentos de UNISALUD respecto a los mapas de riesgo, no considere necesario esta matriz y la identificación de riesgos se encuentre inmerso en otra herramienta, se recomienda ajustar el protocolo para la Seguridad de la Información.

CONCLUSIÓN

Las Historias Clínicas en medio físico y digital se encuentran respaldadas de manera operativa por el sistema de información SISS NET, la base de datos de movimientos y su correspondiente archivo de gestión. Por lo anterior, la adecuada administración de los recursos de TI, de los activos de información y herramientas de tipo tecnológico, se considera primordial para respaldar y soportar mediante actividades de control la información a través de medidas preventivas y reactivas definidas por la Unidad garantizando la custodia, respaldo y disponibilidad de las historias clínicas.

En consecuencia, dada la ausencia de controles específicos para las historias clínicas físicas y el entorno de las historias clínicas digitales se considera necesario priorizar la ejecución de actividades y actualización de procedimientos que garanticen la confidencialidad, integridad de los datos y continuidad de los servicios, permitiendo minimizar los riesgos relacionados con pérdida y seguridad de la información.