MODELO DE PREVENCIÓN DE PÉRDIDA DE LA INFORMACIÓN EN HISTORIAS CLÍNICAS DE PACIENTES DE LA IPS TODOMED LTDA. ALINEADO CON LAS LEYES "HIPAA", "1581 DEL 2012" Y "2015 DE 2020"

MODEL OF DATA LOSS PREVENTION IN THE PATIENT MEDICAL REGISTERS FROM IPS TODOMED LTDA ALIGNED WITH THE LAWS "HIPAA", "1581 OF 2012" AND "2015 OF 2020".

Paul Andrés Pedroza Martínez[1]

Claudia Lorena Perea Sanclemente[2]

Mauricio Cárdenas[3]

Universidad Nacional Abierta y a Distancia —UNAD—

Resumen

Con la creciente demanda y el uso de nuevas tecnologías, las cuales habilitan a los usuarios para que puedan usar la información a través de diversos medios, como lo son el almacenamiento en medios extraíbles y correos electrónicos, así como alojar, compartir y colaborar sobre documentos en línea desde repositorios en la nube, las organizaciones se ven obligadas a implementar mecanismos de protección con el fin de mitigar riesgos relacionados con la fuga, pérdida o exposición de información. Siendo los datos el activo de mayor valor e importancia para una organización, la puesta en marcha de tales mecanismos de protección son una obligada realidad y necesidad.

A ello no son ajenas las instituciones prestadoras de servicios de salud. Es en este sentido que como proyecto de investigación se decidió desarrollar un modelo, que partir de los resultados obtenidos en campo, permita a la IPS TodoMed Ltda. implementar mecanismos de seguridad y protección especialmente orientadas a la prevención de pérdida de información o Data Loss Prevention (por sus siglas en inglés DLP).

Esta investigación se enmarcará totalmente en las regulaciones colombianas para el sector salud y de igual manera para el uso de las tecnologías, tratando de implementar lo que marcos como Hipaa, Icontec, ISO u otros aplicables, propongan para la protección de la información, pero sin sobrepasar los

[1] papedrozam@unadvirtual.edu.co

[2] clpereas@unadvirtual.edu.co

[3] roberto.cardenas@unad.edu.co

alcances delimitados en las leyes locales relacionadas con la "historia clínica electrónica" y "protección de datos personales".

Palabras clave: cloud, salud, riesgo, historia clínica electrónica, legal, DLP.

Abstract

En este documento, se aborda la tecnología DLP (Data Loss Prevención o prevención de pérdida de información) para aumentar la seguridad en la confidencialidad de los registros o datos de pacientes en su Historia Clínica Electrónica. El método de prevención es la primera fase en las tecnologías DLP, este usa firmas para bloquear ataques conocidos, de esta manera, también mejorar la precisión del sistema y disminuir la cantidad de alertas. Por otro lado, la fase de detección tiene dos niveles, que son: detección en línea y detección fuera de línea. La detección en línea es usada para detectar nuevas amenazas que llegan a los sistemas, mientras que la detección fuera de línea se encarga de detectar el comportamiento anormal de usuarios en un período de tiempo mediante la detección supervisada.

Keywords: patients, information, DLP, IPS, prevention, security.

1. Introducción

En estos tiempos, la seguridad de la información es un factor de alta importancia, por ello, para garantizar la privacidad del paciente y la seguridad de su Historia Clínica Electrónica, es necesario contar con tecnologías para robustecer las políticas de seguridad y acceso a dicha información. La pérdida de datos o información es un problema de gran importancia en relación con la privacidad de la historia clínica electrónica, especialmente cuando se incluye información sensible y cualquier pérdida o fuga de información ocasiona problemas que afecten la confidencialidad y privacidad del paciente.

La prevención de perdida de información (DLP) es una de las más grandes estrategias y/o soluciones para aumentar la seguridad en la historia clínica electrónica, mientras se enfoca en identificar datos confidenciales y analiza el contenido considerado como crítico. DLP brinda protección a la confidencialidad de la información ante amenazas internas y/o externas. De igual manera, por su naturaleza, incluye controles automáticos para evitar que información marcada como confidencial se almacene, elimine, envíe o termine en lugares no autorizados de forma intencional o no intencional.

Las soluciones DLP presentan 2 modelos: Método de prevención y Método de detección.

Estos modelos pueden identificar comportamientos basados en el conocimiento de expertos o basados en comportamientos de actividades u operaciones anteriores.

El método de prevención se enfoca en amenazas externas y proporciona bloqueo a comportamientos no autorizados (ataques conocidos).

Por otro lado, el método de detección opera sobre amenazas internas y proporciona detección de mal uso por parte de autorizados y detección de nuevos ataques.

2. Metodología (o desarrollo del tema, según sea el caso)

El Método de observación directa será el medio para recolectar datos de los procesos actuales que lleva la IPS en el tratamiento de la historia clínica del paciente, sin intervenir en el ambiente en el que se desenvuelve. Se procederá de forma manifiesta siendo la institución prestadora de salud consiente de que se estará observando.

3. Población

Se tomará como población objeto el proceso que realiza el personal asistencial y administrativo en las historias clínicas del paciente de TodoMed IPS, ubicada en la ciudad de Cali.

4. Muestra

Toda información recolectada por cuestiones de ética investigativa será acordada con la IPS para tener permiso de exponerlo en el presente documento. Se pactará con la IPS las reuniones para observar cada proceso. Se escribirán las interacciones, se corregirá el texto original, exponiendo una versión para la autorización, y, finalmente, se procederá a los ejercicios de comprensión e interpretación.

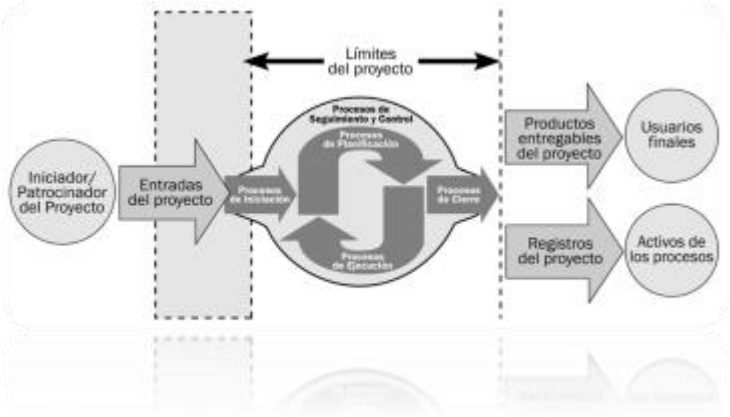
Para lograr el éxito del proyecto, el estudiante e investigador hará las veces de gerente de proyecto que será responsable de planificación, implementación de las actividades, el monitoreo, control del proyecto, identificación de riesgos y planes de respuesta para estos riesgos, verificación de que el producto final entregado a las instituciones prestadoras de servicios de salud cumple con los criterios de aceptación acordados y la calidad esperada para entender a cabalidad los riesgos y la manera de mitigar estos en una transición de sistemas de Información a la nube.

Definiciones de los conceptos básicos de PMI para el método de gestión de proyectos:

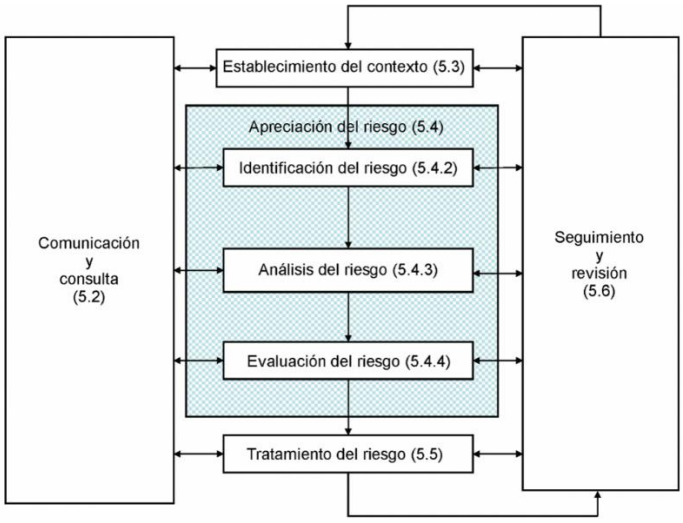
- Gestión o gerencia de proyectos: uso de conocimientos, habilidades, herramientas y técnicas para proyectar actividades que cumplan con los requisitos de esto.

- Proyecto: un esfuerzo temporal realizado para crear un producto, servicio o resultado único.
- Ciclo de vida: las fases como un proyecto pasan de principio a fin.

El ciclo de vida del proyecto de se enmarcará dentro de los límites establecidos por PMI para la implementación del proyecto, como se ilustra en los siguientes diagramas:



De igual manera, estará regido por el Estándar Internacional de Gestión de Riesgos ISO 31000 bajo el siguiente modelo y flujo de gestión o administración del riesgo:



5. Discusión

Con el creciente uso o demanda de la tecnología en la última década, las medianas y grandes empresas han optado por registrar todo tipo de información relacionada a su operación en sistemas de información basados en hardware y software. En la medida que estos sistemas han ido evolucionando, a la par van

apareciendo nuevas tecnologías y normatividades o regulaciones nacionales y mundiales para la correcta protección de los datos.

En ese orden de ideas, las instituciones prestadoras de servicios de salud no están al margen de la aplicación de estas normas y regulaciones para garantizar la protección de la información de pacientes, los cuales son su razón de ser.

De igual manera, en el segmento empresarial de la salud existen organizaciones internacionales que exigen la inclusión de sistemas de geo disponibilidad y geo replicación que garanticen la continuidad y protección en el tiempo de la historia clínica de los pacientes.

En principio, todas las empresas enfrentan a diario constantes riesgos con sus sistemas de información y constantemente deben estar analizando como mitigarlos o minimizarlos. Al llevar la información fuera de sus premisas, en otras palabras, a la nube, los riesgos se hacen mucho mayores, y es por ello que esta investigación aportará en la medida de lo posible a las instituciones colombianas, especialmente a las del Valle del Cauca a la identificación de todos los riesgos relacionados con la exposición de la información, especialmente aquella que contiene datos personales y clínicos, fuera de las instalaciones físicas de la entidad prestadora de salud, en esta caso, haciendo especial énfasis en herramientas en la nube.

6. Conclusiones

Proteger los datos de historia clínica de pacientes por medio de un modelo prevención de perdida de la información, es indispensable para cualquier entidad de salud. Los datos son los activos intangibles más importantes y es necesario asegurarlos y protegerlos; desde el robo por ataques informáticos, robo de información por parte de empleados malintencionados, pérdida de dispositivos de almacenamiento.

Frente a estos casos, DLP (Data Loss Prevention) tiene la capacidad de prevenir ataques de uso de errores por privilegios en usuarios, pero no puede detectar ataques de día cero.

La tasa de detección de DLP está cerca del 100%, dependiendo del tipo de ataque, fuga o perdida de información, así mismo, dependiendo también del sistema y/o modelo que se implemente.

Referencias

Alfaro, M. A., & Alfaro, M. A. (s.f.). Ventajas del SaaS. *Revista Gerencial*. https://visaempresarial.com/pe/noticias/ventajas-del-software-como-un-servicio_392

Allen, M. (2018). Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates. *National Public Radio*, 1–19.

https://www.propublica.org/article/health-insurers-are-vacuuming-up-details-about-you-and-it-could-raise-your-rates

AMPLab (n.d.). *AMPLab - UC Berkeley*. https://amplab.cs.berkeley.edu

Enisa (s.f.). *Acerca de Enisa*. *Agencia de la Unión Europea para la Ciberseguridad.* https://www.enisa.europa.eu/about-enisa/about/es

Garofalo, J. (2014). Why SaaS is Broken (and how we're going to fix it). *Blitzen Blog*. https://blitzen.com/blog/why-saas-is-broken/

Ortiz Guerrero, N. A. (n.d.). Elaboración de los proyectos de investigación. Monografias.com. https://www.monografias.com/trabajos/elabproyec/elabproyec.shtml

Prognostic and Health Management Technology for MOCVD Equipment. (n.d.). *Industrial Technology Research Institute*. https://www.itri.org.tw/eng/Content/MSGPic01/contents.aspx?&SiteID=1&MmmID=6206517061363572 02&CatID=62065325610362016 3&MSID=654532365564567545

Real Academia de Ingeniería. (2014) (1.0). Computación en la nube. http://diccionario.raing.es/es/lema/computación-en-la-nube

Siwicki, B. (2018). Next-gen cloud computing: How healthcare can prepare for the future. *Healthcare IT News*. https://www.healthcareitnews.com/news/next-gen-cloud-computing-how-healthcare-can-prepare-future

Velandia, L. N. M., Gómez, L. A. P., Piragauta, J. D., Herrera, F. S., aros, c. g., bello, g. p., & bello, g. p. (2018). computación en la nube. En *El papel de las TIC en la transformación de la sociedad* (pp.111–124). Editorial Los Libertadores. https://doi.org/10.2307/j.ctv11wjdp.10

Why Digital Advertising Agencies Suck at Acquisition and are in Dire Need of an AI Assisted Upgrade. (2018). *Insincerely Yours*. https://ishti.org/2018/04/15/why-digital-advertising-agencies-suck-at-acquisition-and-are-in-dire-need-of-an-ai-assisted-upgrade/

Wikipedia (n.d.). Fraguado. https://es.wikipedia.org/wiki/Fraguado