Propuesta de Modelo de Prevención de Pérdida de la Información en historias clínicas de pacientes de TodoMed Ltda IPS Apoyado en las leyes “HIPAA”, “1581 del 2012” y “2015 del 2020”

Paul Andrés Pedroza Martínez

Claudia Lorena Perea Sanclemente

Director

Roberto Mauricio Cárdenas Cárdenas

Máster Universitario en E-Learning y Tecnología Educativa

Universidad Nacional Abierta y a Distancia - UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería

Maestría en Gestión de las Tecnologías de la Información

2022

Nota de Aceptación

Aprobado por el Comité de Grado en cumplimiento de los requisitos exigidos por la Universidad Nacional Abierta y a Distancia UNAD, para optar al título de Magister en Gestión de Tecnología.

_____

Jurado.

Dedicatoria

Dedico este proyecto especialmente a mi madre, mi esposa y mis hijos. A mi madre, Luz Enit Martínez Rey, por darme la vida y haberme enseñado muchos valores y cualidades, algunos de ellos como, el respeto, la honestidad, la perseverancia y la resiliencia; todos aplicados en este programa de post grado. A mi esposa, Paula Andrea Hincapié Méndez, por estar a mi lado siempre, en los mejores momentos de la vida, pero también en los más difíciles que he tenido, señalándome la luz al final del túnel, por ser mi faro y mi polo a tierra. Y finalmente a mis hijos, Gabriela y Matías Pedroza Hincapié, últimos en mi dedicatoria, pero no menos importantes, ya que son el motor de mi vida y simplemente sin ellos nada tiene valor o sentido para mí, por ellos he logrado culminar este programa y seguirán siendo mi motivación para afrontar siempre nuevos retos de crecimiento personal, familiar y profesional.

Paúl Andrés Pedroza Martínez

Dedico esta tesis a mi madre, Maria cristina Sanclemente, mi padre Armando Perea Echeverry y mi Hermano Sebastian Perea Sanclemente por su apoyo incondicional, por motivarme a ser mejor persona cada día, por creer en mí y por todo el amor que me dan. a mi abuelo Marco Tulio Sanclemente que viven en mi mente y mi corazón gracias por enseñarme con buenos ejemplos y por sentirte orgulloso de cada logro obtenido.

Claudia Lorena Perea Sanclemente

Agradecimientos

Agradezco infinitamente a todas las personas y organizaciones que de una u otra manera aportaron recursos, tiempo, desde el inicio hasta el final de este programa de post grado y con ello facilitaron que se pudiese alcanzar el objetivo que es el haber logrado nuestro título de Magister en Gestión de TI.

Un agradecimiento especial a la Universidad Nacional Abierta y a Distancia UNAD, a la empresa TodoMed Ltda, a mi compañera de proyecto Claudia Lorena Perea Sanclemente y a nuestro director, el docente Roberto Mauricio Cárdenas Cárdenas; sin ellos, esta investigación no hubiese sido posible.

Paúl Andrés Pedroza Martínez

Agradezco a Dios por haberme dado el privilegio de tener una familia maravillosa, mi razón de ser.

A la universidad nacional abierta y a distancia por brindarme el apoyo y conocimientos necesarios que me permitieron alcanzar el título de magister en gestión de TI.

A Todomed Ltda, por la confianza brindada y por permitir realizar todo el proceso investigativo dentro de la organización.

Finalmente agradezco a la universidad nacional abierta y a distancia, a mi compañero de tesis Ing. Paul Andrés Pedroza y director de tesis Mg Roberto mauricio Cárdenas por el tiempo, la dedicación y conocimientos transmitidos permitiendo alcanzar el título de magister en gestión de TI

Claudia Lorena Perea Sanclemente

Resumen

El presente documento investigativo, es una propuesta de modelo de prevención de perdida de información contenida en las historias clínicas electrónicas de la empresa TodoMed Ltda IPS la cual permitirá cumplir con las regulaciones colombianas aplicadas al sector salud.

Por medio de la investigación realizada en campo, se determinó que TodoMed Ltda IPS tiene un nivel bajo de madurez en cuanto a la prevención de pérdida de datos alojados en las historias clínicas electrónicas. TodoMed Ltda IPS de acuerdo con la ley "2015 del 2020" deberá implementar mecanismos de protección con el objetivo de minimizar riesgos relacionados con la fuga, perdida o exposición de información de historias clínicas. Nuestra Propuesta de Modelo de Prevención de Perdida de la Información en Historias Clínicas sugerirá como solución la configuración de un sistema DLP diseñado para identificar fallas en la transmisión de datos, por medio de un seguimiento para activar un plan de prevención y bloqueo de datos mientras el DLP está en uso, en movimiento y en reposo.

Adaptarse a la normativa de protección de datos resulta fundamental para cumplir con la ley y evitar las sanciones contempladas en la misma, que pueden llegar a ser muy duras y poner en riesgo la estabilidad económica de la empresa.

Por otro lado, aplicar las máximas garantías en la protección de los datos de los pacientes supone un indudable aumento de la reputación de la empresa. Actuar con transparencia fomenta la confianza en sus actuaciones, lo que se traduce en un crecimiento del negocio. Mejora el buen nombre y la imagen, por lo que los pacientes se sentirán más seguros y los clientes directos más satisfechos por los servicios prestados.

Palabras Claves: DLP, pérdida de datos, historia clínica electrónica, base de datos, procesos, TIC, leyes, ventajas, prevención, implementar, mitigar.

Abstract

This research document is a proposal for a model for the prevention of loss of information contained in the electronic medical records of the company TodoMed Ltda IPS which will allow compliance with Colombian regulations applied to the health sector.

Through field research, TodoMed Ltda IPS was found to have a low level of maturity in preventing data loss from electronic health records. TodoMed Ltda IPS according to the law "2015 of 2020" must implement protection mechanisms with the aim of minimizing risks related to the leakage, loss or exposure of medical record information. Our Proposal for a Model for the Prevention of Information Loss in Medical Records will suggest as a solution the configuration of a DLP system designed to identify failures in data transmission, through a follow-up to activate a data prevention and blocking plan while the DLP is in use, in motion and at rest.

Adapting to data protection regulations is essential to comply with the law and avoid the sanctions contemplated in it, which can be very harsh and put at risk the economic stability of the company.

On the other hand, applying the maximum guarantees in the protection of patient data means an undoubted increase in the reputation of the company. Acting with transparency fosters confidence in their actions, which translates into business growth. It improves good name and image, so patients will feel more confident and direct customers more satisfied with the services provided.

Keywords: DLP, data loss, electronic medical record, database, processes, ICT, laws, advantages, prevention, implement, mitigate.

Tabla de Contenido

Lista de Tablas

Pág.

Lista de Figuras

Pág.

Introducción

La seguridad de la información es un factor de alta importancia en la actualidad para las empresas, especialmente para aquellas que manejan información sensible o confidencial de las personas. Las instituciones prestadoras de salud (IPS) son compañías que manejan alto flujo de datos personales por medio de las historias clínicas de los pacientes, por lo tanto, la posibilidad de pérdida de información, especialmente aquella con datos sensibles, es un grave problema que puede poner en riesgo la integridad y seguridad del paciente y por consiguiente la confiabilidad en la IPS, desencadenando en posibles sanciones económicas o reputacionales. Debido a lo anterior, es necesario contar con tecnologías que robustezcan las políticas de seguridad y acceso a la información para garantizar la privacidad de dichas historias clínicas electrónicas.

El presente documento investigativo es una Propuesta de Modelo de Prevención de Perdida de la Información (DLP) en Historias Clínicas de Pacientes de TodoMed Ltda. IPS apoyado en la Ley de Portabilidad y Responsabilidad de Seguros de Salud de Estados Unidos (HIPAA) y la Ley 1581 del 2012, junto con Ley 2015 del 2020 de Colombia.

Una tecnología DLP es una de las más grandes estrategias para aumentar la seguridad en las historias clínicas electrónicas, ya que se enfoca en identificar datos confidenciales y analizar el contenido considerado como crítico. El DLP brinda protección a la confidencialidad de la información tanto para amenazas internas como externas, de igual manera, 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. Con base en la caracterización del proceso que realizaron los usuarios en el sistema de información de TodoMed Ltda. IPS, se logró identificar los riesgos de seguridad de la información, los cuales servirán de insumo esencial para el diseño de controles a partir de la propuesta del modelo DLP.

Planteamiento del Problema

La creciente demanda de tecnología en la última década ha generado que las medianas y grandes empresas hayan 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, se ha identificado la necesidad de establecer lineamientos y normatividad, tanto nacional como internacional, que proteja la privacidad, el acceso y uso de los datos (CEPAL, 2021).

Las Instituciones Prestadoras de Servicios de Salud (IPS) son organizaciones que deben acatar e implementar diferentes políticas para la protección y el uso de información, ya que manejan un alto flujo de datos confidenciales y sensibles resultado de las historias clínicas de los pacientes. 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 (Alzate & López, 2021).

Por otro lado, es importante recalcar que todas las empresas enfrentan a diario constantes riesgos con sus sistemas de información, y, por lo tanto, deben estar analizando como mitigarlos o minimizarlos. Adicionalmente, los riesgos aumentan significativamente cuando las compañías utilizan servicios en la nube para el manejo de la información. Es por esto, que el desarrollo de este trabajo de grado realizará un aporte significativo a las instituciones colombianas, especialmente a las del Valle del Cauca, ya que ayudará a la identificación de los riesgos relacionados con el tratamiento de la información, cuando ésta deba ser manejada en entornos en la nube y fuera de las instalaciones físicas de la entidad prestadora de salud (Grupo Evaluando, 2020).

Este trabajo de investigación pretende dar solución a una problemática identificada para la empresa TodoMed Ltda. IPS, relacionada con su transición a la Historia Clínica Electrónica aplicada en su sistema de información y con el manejo interno de los datos de sus pacientes.

El comienzo del sistema de información de TodoMed Ltda. IPS data de inicios del año 2018, el cual se trataba de un aplicativo desarrollado en lenguaje de programación JSON ejecutable en PHP. Este software se instalaba en cada Tablet para ayudar con el registro médico de evoluciones y diligenciar la historia clínica del paciente. El registro culminaba una vez el médico terminaba de ingresar la información, la cual se sincronizaba manualmente y era enviaba la evolución a una máquina virtual alojada en un servidor físico. Luego, las historias clínicas se convertían a formato PDF y eran alojadas en una carpeta ubicada en una NAS (Network Attached Storage) y desde ahí eran compartidas por medio de una plataforma web perteneciente a la IPS, para la posterior solicitud de autorización de medicamentos, servicios, insumos o suministros. Al finalizar el mes, el soporte de historia clínica era enviado por medio de USB y por la herramienta WeTransfer en su versión gratuita al área de facturación, para posteriormente organizarlas en las carpetas de red ubicadas en el servidor.

Este sistema de información al no operar en un modelo Cliente-Servidor, almacenaba de manera local en la Tablet el registro histórico por fecha de cada visita del paciente, lo cual no permitía llevar un control seguro, eficiente, homogéneo y verás de la información, ya que cualquiera persona con acceso a los dispositivos podía modificar y manipular los datos, desencadenando en información poco fiable e inútil para para realización de comparativos a evoluciones pasadas.

Adicionalmente, el sistema presentaba inconsistencias al sincronizar cuando hacían cambio en asignación de pacientes y cuando pasaba más de 3 días sin sincronizar, lo cual ocasionaba perdida de información en la historia clínica del paciente. La solución para la sincronización era revisar el código JSON e identificar el error, para posteriormente manipular el código y realizar correcciones.

En el año 2020 se inició la transición al sistema de información alojada en el web, desarrollado en lenguaje de programación PHP y Motor de Bases de Datos MySQL, debidamente integrada a la Infraestructura Tecnológica y Estructura de Datos o Información de la empresa.

El sistema de información captura los datos básicos del paciente, incluyendo el diagnóstico primario y secundario. Esta información se refleja cuando los médicos realizan la valoración inicial, la epicrisis, la apertura, la evolución y el control de la evolución del paciente. La información registrada como los ordenamientos son reportados ante MiPres y el equipo de admisiones registra los ordenamientos en el sistema CONEXIA de la IPS, con el fin de obtener la autorización de medicamentos, insumos, suministros y servicios.

El equipo de admisiones y autorizaciones programa los paquetes y servicios autorizados y direccionados. Por su parte, los líderes de terapias asignan los servicios que deben realizar el terapeuta y los líderes de enfermería asignan los servicios que deben realizar los enfermeros y cuidadores. El resultado de la asignación se ve reflejado en el sistema de información de cada empleado, desde ahí se registran las evoluciones médicas y terapéuticas realizadas cada día a los pacientes.

Adicionalmente, cada líder de terapias y enfermería realiza auditoria desde el sistema para determinar la pertinencia de las evoluciones antes del proceso de facturación, el cual es

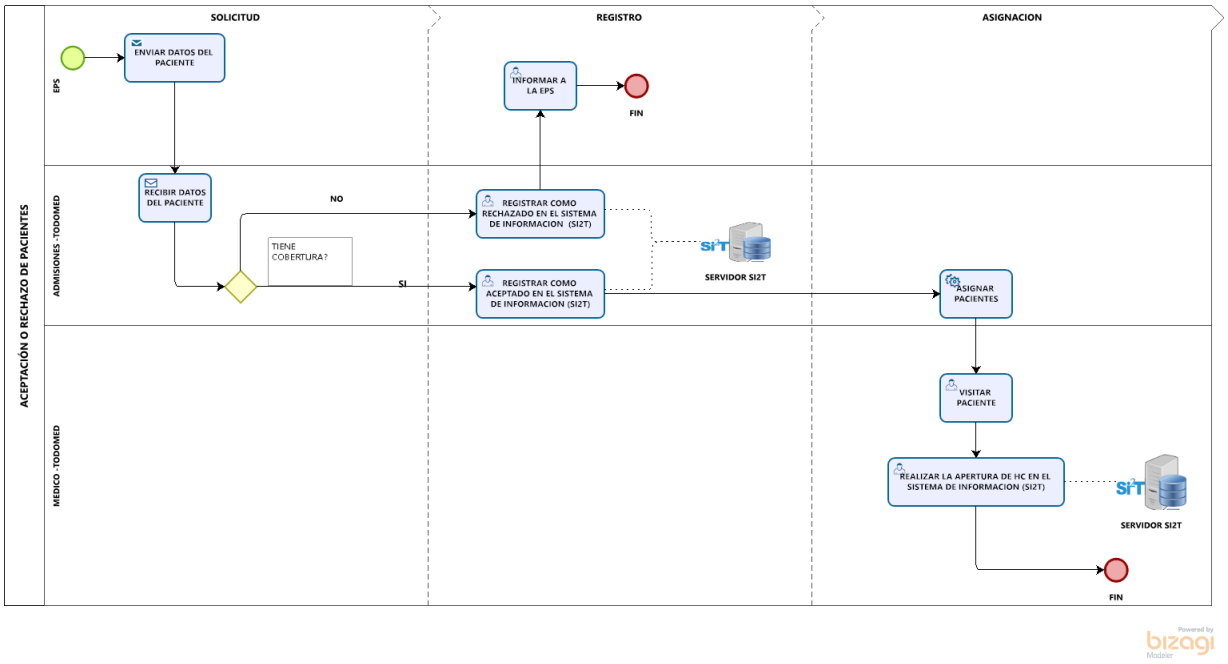
realizado en la última semana de cada mes. Para lo anterior, los líderes reciben de los profesionales el formato de firmas de los pacientes, el cual evidencia las visitas realizadas y es insumo para iniciar el proceso de facturación al cliente, y posteriormente, generar cada cuenta de cobro al profesional, la cual se transmite al área de compras. Otras acciones del proceso:

- El sistema de información tiene la opción de edición de las historias clínicas médicas y terapéuticas para realizar correcciones.
- Se generan de forma masiva las historias médicas y terapéuticas en formato PDF, las cuales se encuentran identificadas por cédula del paciente y por tipo de procedimiento. Esta información se envía al área de facturación por diferentes medios como: dispositivos USB, WeTransfer o carpeta de red.
- Se crean paquetes y servicios con valores predeterminados para facturar.
- Si se presenta fallas en el proceso, el área de sistemas las corrige sobre la BD.
- Si se presenta fallas en el sistema, la corrección la hace el proveedor y desarrollador del software.

A continuación, se presenta la sintetización de la problemática por medio del proceso:

Figura 1

Proceso de aceptación o rechazo



Nota. Elaboración propia.

Se realiza la descripción del Proceso Aceptación o Rechazo de Pacientes:

Enviar datos del paciente. La Entidad Promotora de Salud (EPS) emite por medio de un correo electrónico los datos básicos del paciente con el diagnóstico principal a TodoMed Ltda. IPS, solicitando la atención médica domiciliaria oportuna.

Recibir datos del paciente. La persona encargada de admisiones recibe el correo con la información del paciente y determina según el lugar de residencia y diagnóstico si TodoMed Ltda. IPS tiene cobertura para realizar la atención médica inicial.

Registrar como rechazado en el sistema de información (SI2T). Si el paciente vive en un lugar fuera de la cobertura de TodoMed Ltda. IPS se registra el paciente en el sistema de

información SI2T “Sistemas de Información Integrado TodoMed Ltda. IPS” y se pone como observación las causas de rechazo.

Informar a la EPS. Se emite un correo electrónico informando a la EPS las causas del rechazo en la atención al paciente.

Registrar como aceptado en el sistema de información (SI2T). Si el paciente vive en la zona de cobertura de TodoMed Ltda. IPS se registra en el sistema de información SI2T “Sistemas de Información Integrado TodoMed Ltda. IPS”.

Informar a la EPS. Se emite un correo electrónico informando a la EPS que el paciente ha sido aceptado y que será atentado en el transcurso de 24 horas.

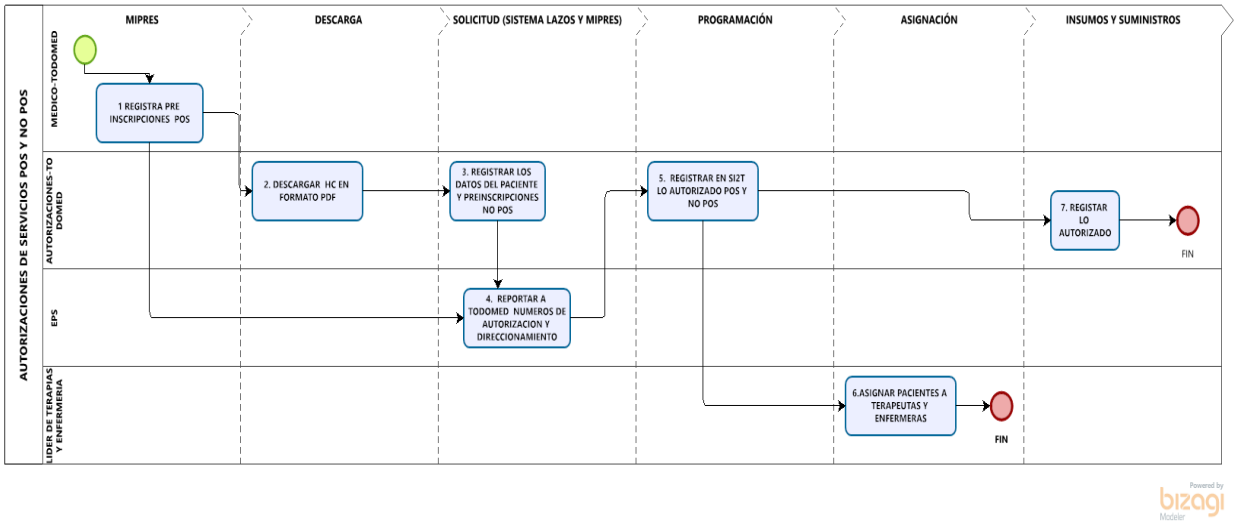
Asignar pacientes. El personal de Admisiones asigna el paciente al médico según el barrio y comuna.

Visitar paciente. El médico realiza la visita en el domicilio del paciente y procede a examinarlo.

Realizar la apertura de historia clínica en el sistema de información (SI2T). Realiza la apertura de historia clínica en el sistema de información SI2T “Sistemas de Información Integrado TodoMed Ltda. IPS”.

Figura 2

Proceso de Autorizaciones de servicios POS y NO POS



Nota. *Elaboración propia*.

Se realiza la descripción del Proceso Autorizaciones de Servicios POS y NO POS

Registrar preinscripciones POS. Durante la visita en casa del paciente, el médico ingresa al sistema MIPRES las preinscripciones tecnológicas en salud. Se entrega al paciente la formula según el medicamento.

Descargar HC en formato PDF. La persona de autorizaciones accede a la historia en el sistema de información SI2T y descarga el soporte en formato PDF.

Registrar los datos del paciente y preinscripciones NO POS. La persona de autorizaciones ingresa al sistema de lazos y MIPRES para poder reportar las solicitudes a la EPS y al Ministerio de Salud.

Reportar a TodoMed Ltda. IPS los números de autorización y direccionamiento. La EPS envía los servicios que han sido autorizados al personal de autorizaciones.

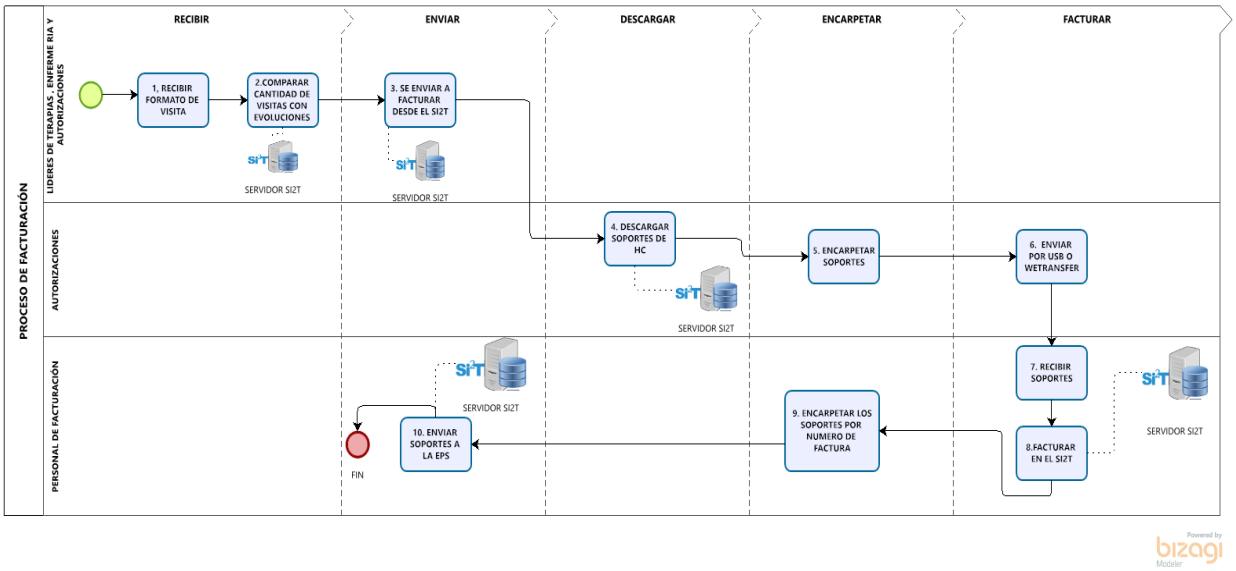
Registrar en SI2T lo autorizado POS y NO POS. La persona de autorizaciones programa los servicios, insumos o medicamentos en el sistema de información SI2T.

Asignar pacientes a terapeutas y enfermeras. Cada líder de terapia y enfermería asignan los servicios autorizados por el la EPS.

Registrar lo autorizado. El personal de autorizaciones programa los medicamentos, insumos y suministros autorizados por la EPS para ser entregados al paciente en el transcurso del mes.

Figura 3

Proceso de facturación



Nota. Elaboración propia.

Se realiza la descripción del Proceso de facturación:

Recibir formato de visita. Los líderes de terapias, autorizaciones y enfermería reciben el formato de visitas con las firmas de los pacientes, fecha, hora de visita y número de registro generado por el sistema después de realizar la nota evolutiva.

Comparar cantidad de visitas con evoluciones realizadas. Verifican que coincidan las fechas, hora de visita y el número del registro en las notas evolutivas de cada paciente.

Enviar a facturar desde el SI2T. Después de verificar que coincidan las notas y tiempos de visita preparan la información a facturación desde el SI2T.

Descargar soportes de HC. Autorizaciones descarga de manera masiva los soportes de las notas evolutivas de cada paciente para formar la HCE.

Encarpetar soportes. Se organiza cada soporte encarpetado por nombre del paciente y subcarpetas como lo pide la EPS.

Enviar por USB o WeTransfer. Se envía al área de facturación por USB o WeTransfer debido al peso de los archivos.

Recibir soportes. El área de facturación recibe los soportes y lo organiza en la carpeta del mes en curso.

Facturar en el SI2T. Inicia el proceso de facturar desde el sistema de información SI2T los servicios POS y NO POS de cada paciente.

Encarpetar los soportes por número de factura. Las facturas generadas se guardan en la carpeta del paciente y se crea otra carpeta con el número de factura.

Enviar soportes a la EPS. Los soportes son enviados a la EPS por medio magnético tal cual como lo solicitan y transmitidos por medio de los RIPS y factura electrónica al correo indicado por la EPS.

Pregunta de Investigación

Con la problemática anteriormente expuesta se diseña la pregunta de investigación, la cual es la siguiente: ¿Cómo mitigar los riesgos de perdida y/o fuga de información en historias clínicas de pacientes de TodoMed Ltda. IPS mediante tecnologías DLP alineadas a las leyes internacionales y nacionales de tratamiento de datos personales y datos de pacientes?

Objetivos

Objetivo general.

Diseñar una propuesta de modelo de Prevención de Pérdida de la Información en historias clínicas de pacientes de TodoMed Ltda IPS, apoyado en las leyes “HIPAA”, “1581 del 2012” y “2015 de 2020”.

Objetivos específicos.

Identificar y documentar los riesgos de seguridad a los que están expuestas las historias clínicas y documentos de pacientes de la IPS.

Establecer una propuesta de protección de los datos de pacientes o historias clínicas con tecnologías que permitan controlar los accesos y auditar las acciones de los usuarios de la IPS, alineado con el plan estratégico de la organización.

Diseñar una propuesta de modelo de prevención de perdida de información de historias clínicas de TodoMed Ltda. IPS.

Justificación

La principal motivación para la elaboración de este proyecto es la realización de un análisis profundo de los riesgos relacionados con la vulnerabilidad de la información privada, ubicada en internet o en servicios en la nube, de una Institución Prestadora de Servicios de Salud (IPS), enfocado especialmente en el manejo de historias clínicas de pacientes.

Debido a lo anterior, se hace necesario la correcta identificación de los riesgos y la aplicación de mecanismos de mitigación para así garantizar la correcta transferencia de información sin exponerla públicamente. Por lo tanto, podría ser necesaria la aplicación de marcos de referencia y/o estándares como ISO 27001, entre otros, para lograr un correcto desarrollo del proyecto de investigación.

Mediante la ISO 27001, se realizará la implementación de los estándares de seguridad para que las historias clínicas se pueda vincular inter-operablemente en las instituciones de salud. Este mecanismo permite el flujo de información entre la IPS y el Ministerio de Salud y Protección Social para que los pacientes tengan una atención rápida y segura (Ministerio de las TIC, 2020).

Al tener datos sensibles en las historias clínicas de los pacientes, cada EPS, IPS y demás entidades de la salud deben implementar un sistema seguro para proteger los datos. Por lo tanto, se requiere tener un recurso humano comprendido por ingenieros de sistemas con conocimiento en protección y prevención de datos clínicos. En infraestructura se requiere tener un ancho de banda de alta velocidad, algunos servicios virtualizados y el licenciamiento por parte de un fabricante para realizar la investigación y pruebas en la seguridad de la historia clínica (Cristea, 2017).

La implementación de normas y protocolos en seguridad apoyado de software de detención y respuesta del servidor permitirá brindar solución a fallas de seguridad generadas por sobrecargas y amenazas por falta de capacidad en almacenamiento, que puedan exponer datos sensibles de los pacientes en las historias clínicas alojadas en la nube (Araujo, 2022).

Por último, se cuenta con viabilidad para la realización del proyecto de investigación ya que se cuenta con el recurso humano capacitado y con experiencia, además de los recursos técnicos necesarios para el desarrollo del proyecto. Los productos resultados del proyecto que se entregará a las entidades de la salud son los protocolos diseñados basándose en la implementación de las normas de Icontec en gestión de la seguridad de la información, los lineamientos de la Ley de Portabilidad y Responsabilidad de Seguros de Salud de Estados Unidos (HIPAA), el ciclo PHVA de la seguridad informática y las buenas prácticas de implementación y administración de herramientas de DLP para las historias clínicas de todas las entidades de salud en el momento de aplicar la Ley 2015 de 2020 (Congreso de Colombia, 2020).

Marco Contextual

El presente marco describe las condiciones actuales de la problemática en las historias clínicas electrónicas en Colombia.

Vulnerabilidad Historia Clínica Electrónica

Dentro de la vulnerabilidad de la historia clínica, se pueden establecer cinco importantes amenazas que puedan afectar esta información, las cuales, se encuentran a continuación:

***Divulgación Accidental*:** el trabajador revela la información de los pacientes a otras personas; uno de los medios más comunes puede ser el mensaje a través de correo electrónico enviado a la dirección incorrecta.

Curiosidad de los empleados: se puede observar cuando un trabajador que posee autorizaciones accede a información de pacientes por curiosidad o para satisfacer sus propios intereses.

***Violación de la privacidad por un trabajador*:** un trabajador con acceso a la información de pacientes transmite los datos al exterior con el fin de lucrarse o por algún tipo de animadversión hacia un individuo.

Violación de datos por un externo con intrusión física: una persona externa ingresa a las instalaciones físicas y de forma forzada accede al sistema y toma la información sin autorización.

***Intrusión no autorizada en la red del sistema*:** un individuo externo, ingresa a la red del sistema de la empresa y accede a la información del paciente o hace que el sistema deje de funcionar (Achury, 2018).

Seguridad de la Información

La Seguridad de la información sigue en constante desarrollo, tiene como objetivo la prevención de los riesgos relacionados a las tecnologías de la información en una empresa, manteniendo la integridad, disponibilidad y confidencialidad.

Areitio, (2008). Seguridad en la Información la seguridad es un proceso continuo multidimensional, que debe tenerse en cuenta en la definición, en la gestión y en la reingeniería de empresas y procesos de negocio. La Seguridad puede observarse en diferentes planos de la sociedad, como una comunidad, una organización, es un sistema embebido, en un producto, o en un servicio (Incibe, 2018).

Eugene Spafford, experto en seguridad de datos y profesor de ciencias informáticas en la Universidad Purdue (indiana, EEUU) dijo que "el único sistema seguro es aquel que esta apagado o desconectado, enterrado en un refugio de cemento, rodeado por gas venenoso y custodiado por guardianes bien pagados y bien armados, Aun así, yo no apostaría mi vida por el" la anterior frase se ha hecho famosa en el mundo de la seguridad (Intelligenia, 2017).

Voutssas (2010), indica en su artículo preservación documental digital y seguridad informática Defino "Seguridad Informática" como: el proceso de establecer y observar un conjunto de estrategias, políticas, técnicas, reglas, guías, prácticas y procedimientos tendientes a prevenir, proteger y resguardar de daño, alteración o sustracción a los recursos informáticos de una organización y que administren el riesgo al garantizar en la mayor medida posible el correcto funcionamiento ininterrumpido de esos recursos (Gutiérrez, 2020).

De acuerdo a lo anterior se considera La seguridad de la informática como la unión de medidas preventivas tendientes al blindaje de las diferentes salidas de datos físicos e intangibles que puedan generar un riesgo inminente a personas o empresas. en la actualidad se basa la

seguridad de la información con medidas correctivas generando pérdidas económicas incalculables que no están previstas en los estados financieros de ninguna empresa (Portafolio, 2017).

Muchas empresas se han obligado concentrar esfuerzos para la obtención de mecanismos que permitan atomizar actos no deseables dentro de un sistema informático, como el fundamento principal en el logro de altos estándares de seguridad incluyéndolos como objetivos específicos alineados con el direccionamiento de su planeación estratégica (Grupo RGI, 2021).

Políticas de seguridad

Actividades, controles y políticas de seguridad que se deben implementar con base a recursos humanos, hardware y software. La seguridad de la información depende de la gestión y los procedimientos adecuados, de los empleados de la organización, proveedores, clientes, accionistas y del nivel de seguridad de los medios técnicos. Las políticas de seguridad se desarrollan con el objetivo de resguardar la información y los sistemas de una Empresa, y certificando la integridad, confidencialidad y disponibilidad de la información. Los documentos relativos a las políticas de seguridad deben contemplar los procedimientos para hacer cumplir las reglas, las responsabilidades en todos los niveles. Todos ellos deben tener el apoyo gerencial de la organización (Vega, 2018).

Pensar en seguridad de datos y construir defensas desde el primer momento es de vital importancia para la empresa. Los ingenieros de seguridad deben tener como objetivo principal, proteger la red de las amenazas desde su inicio hasta que son confiables y seguras. El objetivo para los cuales se recopilan datos personales debe especificarse claramente al paciente en el momento en el cual se recopilen. Además, se debe informar a los pacientes sobre las prácticas y políticas de la empresa al momento que se recopilen los datos personales, con el fin que puedan

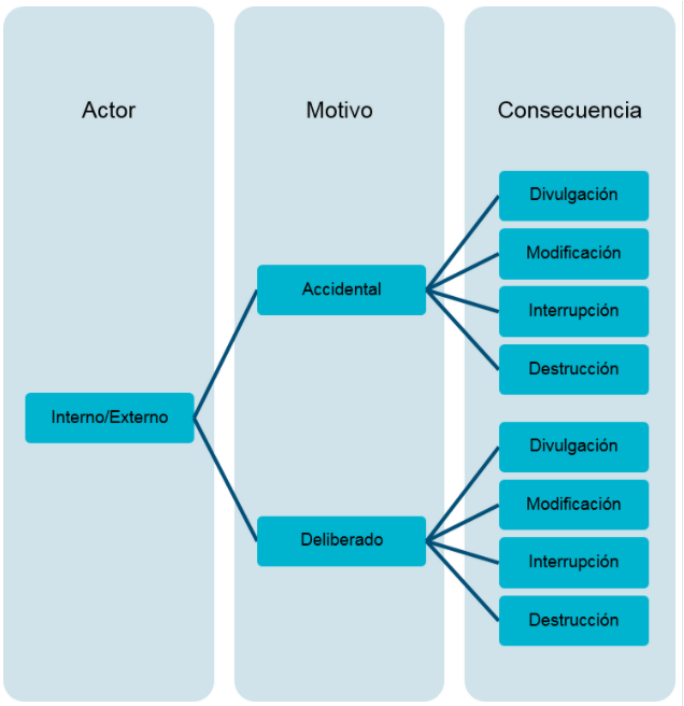
tomar una decisión con respecto al suministro de tales datos. Es preciso aclarar que sin el consentimiento del paciente con respecto a la recopilación de los datos no puede ser válido (Powerdata, 2022).

Data Loss Prevention (Prevención De Perdida De Datos)

Un DLP está diseñado para identificar fallas en la transmisión de datos, por medio de un seguimiento identificar y activar un plan de prevención y bloqueo de datos mientras está en uso, en movimiento y en reposo. Es importante identificar la diferenciar de una pérdida a una fuga de información. La pérdida es accidental y una fuga es intencional, sin embargo, hay casos donde existen fugas accidentales (como perdida de información confidencial ya sea por medio de laptop, pendrive. envió de correos con información confidencial a la persona incorrecta). La fuga involucra a personas o entidades que acceden a cierta información sin privilegios para después divulgarla. mientras que la perdida es aquella información que pudo dañarse, modificarse, destruirse o interrumpirse sin que sea interceptada por alguna persona o entidad (Incibe, 2019).

Figura 4

Árbol de decisiones para la identificación de riesgos informáticos



***Nota*:** Tomado de ESET (2016). Reporte de sustentabilidad. Disponible en https://www.eset.com/fileadmin/ESET/LATAM/Gestion_sustentable/eset-reporte-2016-es.pdf

Para cumplir con los estándares de la empresa y las normativas del sector, las organizaciones deben proteger información confidencial e impedir su divulgación involuntaria. La información confidencial puede incluir datos financieros o información de identificación personal (PII), tales como números de tarjeta de crédito, números de seguridad social o registros médicos (Incibe, 2018).

El sector de salud se ve desafiado a implementar medidas de seguridad para enfrentar las amenazas actuales. Tener acceso rápido a los expedientes médicos de los pacientes es esencial en la práctica médica de hoy y al mismo tiempo significa mantener los datos en un formato

electrónico. Hay que asegurar que la información es segura y sólo se puede acceder para una "necesidad de saber" es obligatorio. Por lo tanto, una solución de Prevención de Pérdida de Datos es una necesidad. No proteger información confidencial puede resultar en multas que llegan a valores de millones de dólares. Algunos de los casos más conocidos incluyen instituciones como Departamentos de Salud y Servicios Sociales, Universidades Médicas, Compañías de Seguros y Hospitales Generales. Así que independiente si usted es un profesional de seguridad de TI o Administrador de TI de un hospital, universidad médica, clínica de salud, compañía de seguros o cualquier otra organización de terceros involucrados en la industria, una solución de Prevención de Pérdida de Datos debe estar en su lista (Endpoint Protector, 2022).

Hay diferentes tipos de soluciones DLP, orientado a la necesidad de la organización, pero sin perder el enfoque en la prevención de la pérdida de datos. La protección de los datos sigue siendo una de las principales prioridades de las empresas. A medida que van creciendo estructuralmente y desarrollando nuevas actividades económicas, así mismo es importante garantizar que la estructura de seguridad de la empresa esté actualizada y sea capaz de mitigar el riesgo de pérdida, exposición de datos. Hay diferentes tipos de soluciones DLP, orientado a la necesidad de la organización, pero sin perder el enfoque en la prevención de la pérdida de datos (Incibe, 2019).

Se encuentra en dos opciones hardware y software una vez instalada la solución monitorea rastrea y genera informes de todos los datos de tráfico de la Red. Network de DLP escanea el contenido qué pasa por protocolos y puertos de una empresa ayudando a garantizar la seguridad de esta. Esta solución permite recopilar la información en la base de datos para ser administrada fácilmente (Ostec, 2015).

DLP Storage

Permite identificar los archivos confidenciales almacenados y compartidos, reconoce puntos sensibles para prevenir la filtración de información incluso controlar datos en la nube (Ostec, 2015).

DLP Endpoint

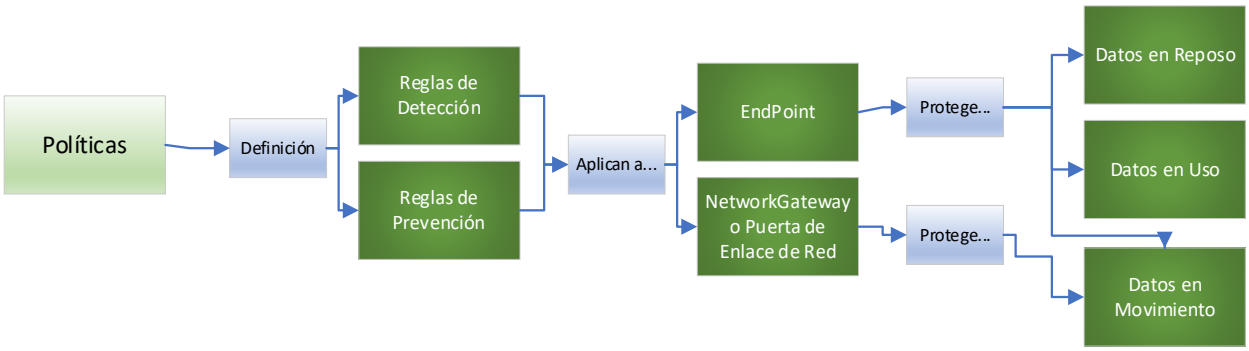
Los puertos USB pueden generar riesgos de fuga de información o filtrado de datos, esta acción puede darse de forma accidental o intencional. La solución Endpoint ayuda a prevenir las estaciones de trabajo y dispositivos usados por los empleados para impedir la salida de los datos por medio de dispositivos extraíbles o aplicaciones usadas para transferir archivos. La clasificación de la información, la delimitación de roles y responsabilidades son indispensables en la implementación de la solución (Ostec, 2015).

DLP Server

Es el responsable de la administración de las partes previas, así como también de la administración de políticas ("Despliegue de Políticas" y "Registro de Violación de las Políticas"). Las políticas son lo más importante de un sistema DLP por que permiten la distinción o identificación de los datos en niveles públicos y sensitivos. Las organizaciones definen sus propias políticas de acuerdo con las necesidades del negocio (Endpoint Protector, 2022).

Figura 5

Funcionamiento de las políticas DLP



Nota. Adaptado de DLP protege tus datos contra fugas de información, de Incibe, 2019, https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion.

Luego de que la organización define y crea sus propias políticas de DLP, estas se convierten en reglas y posteriormente el DLP es forzado a ser usado en todo el ciclo de vida de la información o los datos. En la figura #2 se presentan todos los pasos desde como las políticas se transforman en reglas y posteriormente protegen la información. DLP se basa especialmente en 2 métodos diferentes, los cuales son “Prevención” y “Detección”:

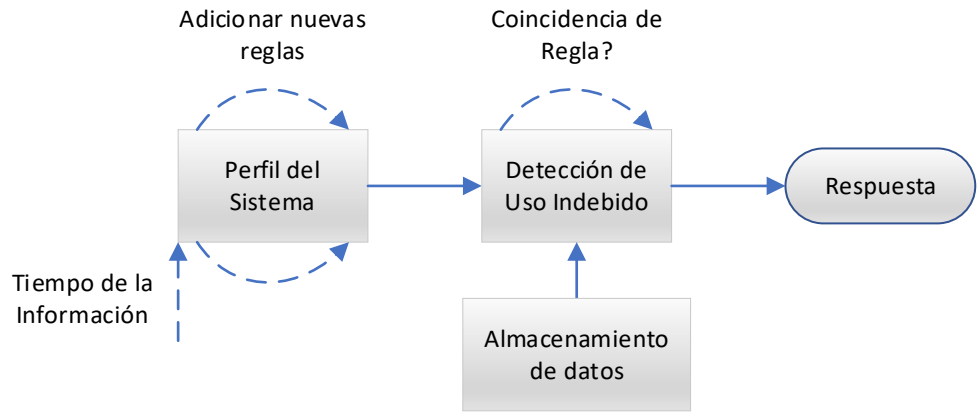
Método de Prevención: Este método asegura que la información clasificada como confidencial no puede ser movida fuera de los sistemas de la organización. Este es el tipo de tecnología que garantiza el acceso a los datos sólo a personas autorizadas e identificadas. Los sistemas de prevención crean políticas automáticamente para asegurar que los datos o la información confidencial no es manipulada ni almacenada por personas no autorizadas. Estas políticas permiten controlar si la información es almacenada o no, al tiempo que habilita a los usuarios con el uso de herramientas y/o servicios que les permiten realizar sus tareas con

normalidad. Los métodos de prevención se anticipan a potenciales eventos de riesgo de pérdida de información antes de que estos puedan ocurrir (Fernández, 2015).

***Método de Detección*:** Este método hace refiere al uso de una variedad de técnicas y métodos para encontrar patrones que tengan un comportamiento anormal en el conjunto de datos. Estos comportamientos se denominan también anomalías. Una anomalía significa un comportamiento inusual o inesperado diferente a lo normal. Dentro de las principales ventajas del método de detección, podemos encontrar su capacidad para detectar nuevos ataques. Sin embargo, es normal encontrar una gran cantidad de falsas alarmas. En la figura (3) se muestra un modelo de detección típico. Este normalmente está compuesto por 4 fases: 1. Recopilación o almacenamiento de datos, recopila las actividades normales de los usuarios y las guarda. 2. Perfil del sistema, crea perfiles de sistema normales. 3. Método de detección, determina el comportamiento anormal a partir de los perfiles normales del sistema, y, por último, 4. Respuesta, proporciona informes sobre el comportamiento anormal y el momento o tiempo en el que ocurrió (Fernández, 2015).

Figura 6

Funcionamiento de un Sistema de Detección Convencional



Nota. Adpatado de Detección de anomalías de red mediante técnicas de machine learning de Villar, F, 2019, https://ruc.udc.es/dspace/bitstream/handle/2183/25166/F.J.Villar_Detecci%C3%B3n_de_anomal%C3%ADas_de_red_mediante_t%C3%A9cnicas_de_machine_learning_2019.pdf

En los últimos años, los métodos de detección fueron clasificados de acuerdo a las técnicas de aprendizaje usadas:

Detección Supervisada: Este método basado en el aprendizaje a partir de la supervisión puede ser clasificado en 2 casos:

***Clasificación del Problema en 1 Clase*:** Aprendizaje sólo a partir de datos normales o a partir de datos anormales.

***Clasificación del Problema en 2 Clases*:** Se basa en 2 tipos de eventos para el aprendizaje, normales y anormales al mismo tiempo.

Detección de Valores Atípicos: Se basa en aprendizaje no supervisado, implica datos de entrenamiento (normales y anormales) sin etiquetas.

Detección de novedades: Está basado en aprendizaje semi supervisado, el aprendizaje asume que los datos de entrenamiento se etiquetan solamente como normales, sin necesidad de etiquetas para la clase anormal (Zaragoza, 2020).

Clasificación de información: Se debe categorizar las necesidades de la entidad para implementar las políticas de prevención de datos, cada regla debe estar correctamente definida para que la solución DLP pueda filtrar y descubrir los activos críticos en la base de datos. Una incorrecta configuración representará inconsistencias como: bloqueo de acciones legítimas afectando la operación de la entidad o dar paso a posibles fugas de información (Ostec, 2015).

Con un plan de prevención de pérdida de datos, frente a algún suceso inesperado en poco tiempo se activará una de las copias automáticas para reanudar la actividad con todos los datos intactos, que es el activo más importante de las empresas. Para que esto sea posible, debemos controlar cada detalle con un sistema de alertas para que nada se escape y hacer revisiones y actualizaciones periódicas para tener todo operando de manera correcta. Una vez la empresa cuente con una clasificación de los datos a proteger, el siguiente paso es crear o actualizar tus políticas para manejar esas categorías de datos. Las soluciones DLP suelen aplicar reglas o políticas preconfiguradas, basadas en diversas regulaciones, por ejemplo: HIPAA (Álvarez, 2018).

Cloud Computing

Es la entrega de servicios informáticos, incluidos servidores, almacenamiento, base de datos, redes, software, análisis e inteligencia, a través de la nube en internet, para ofrecer una innovación más rápida, recursos flexibles y economías de escala. Usualmente este servicio se cobra por los servicios en la nube que se utilizan, ayuda significativamente a reducir costos operativos, administrar infraestructura de una forma más eficiente y escalada a medida que se cambian las necesidades del negocio. Existen tres tipos de servicios en la nube, la primera es la nube publica operada por una tercera parte o por proveedores de servicio en la nube, quienes entregan sus recursos como servidores, internet etc. La nube privada se refiere a los recursos usados exclusivamente un solo negocio organización. Por último, las nubes hibridas son aquellas combinadas por la nube pública y privada, unidas por tecnología que permite compartir datos y aplicaciones entre ellas. Este tipo de servicio ofrece a los negocios mayor flexibilidad, mayor implementación y optimización de su infraestructura, seguridad cumplimiento (Microsoft, 2018).

Leyes

Ley 1581: Protección De Datos Personales En Colombia.

Reconoce y protege el derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada. Cuando hablamos de datos personales nos referimos a toda aquella información asociada a una persona y que permite su identificación. Por ejemplo, su documento de identidad, el lugar de nacimiento, estado civil, edad, lugar de residencia, trayectoria académica, laboral, o profesional. Existe también información más sensible como su estado de salud, sus características físicas, ideología política, vida sexual, entre otros aspectos. Los datos personales conforman la información

necesaria para que una persona pueda interactuar con otras o con una o más empresas y/o entidades para que sea plenamente individualizada del resto de la sociedad, haciendo posible la generación de flujos de información que contribuyen con el crecimiento económico y el mejoramiento de bienes y servicios. Así, por ejemplo, cuando hacemos una solicitud de crédito ante una entidad financiera, se requiere diligenciar formularios con nuestra información personal, o cuando realizamos una compra y para realizar la factura de venta solicitan datos como el número de documento de identidad, correo electrónico, dirección y teléfono de contacto, entre otros (Congreso de la República, 2012).

Definiciones

Para los efectos de la presente ley, se entiende por:

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales;

Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento;

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables;

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento;

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos;

Titular: Persona natural cuyos datos personales sean objeto de Tratamiento;

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión (Congreso de la República, 2012).

Ley 2015: Normatividad de la Historia Clínica Electrónica en Colombia.

Objeto. La presente ley tiene por objeto regular la Interoperabilidad de la Historia Clínica Electrónica - IHCE, a través de la cual se intercambiarán los elementos de datos clínicos relevantes, así como los documentos y expedientes clínicos del curso de vida de cada persona.

A través de la Historia Clínica Electrónica se facilitará, agilizará y garantizará el acceso y ejercicio de los derechos a la salud y a la información de las personas, respetando el Hábeas Data y la reserva de esta. Parágrafo. El Ministerio de Salud y Protección Social reglamentará los datos clínicos relevantes. El Ministerio de Salud y Protección Social adoptará un plan de implementación de la Interoperabilidad de la Historia Clínica Electrónica – IHCE para el intercambio de los datos clínicos relevantes, el cual deberá tener en cuenta las condiciones específicas de los sujetos obligados. En todo caso, el plazo máximo de implementación será de cinco (5) años contados a partir de la entrada en vigor de la presente ley.

Esta estrategia obedecerá a criterios de interoperabilidad, privilegiando los datos, avances y sistemas existentes en los distintos prestadores dentro del sistema de salud, generando así un ahorro en la implementación de la Interoperabilidad de la Historia Clínica Electrónica -IHCE.

En todo caso, facúltese al Ministerio de Salud y Protección Social para definir los términos de implementación de la interoperabilidad de los documentos y expedientes de la historia clínica electrónica como una fase superior al intercambio de datos clínicos relevantes (Congreso de Colombia, 2020).

Delimitación

Espacial

TodoMed Ltda IPS es una empresa palmirana, constituida en el año 2004 como sociedad Ltda. enfocada en la Prestación de Servicios de Salud y en la venta de medicamentos de Alto Costo para pacientes con la patología VIH/SIDA, inicialmente. En el año 2008, se consolida como Institución Prestadora de Servicios (IPS) ofreciendo el programa para pacientes VIH/SIDA en un modelo de atención integral. En el año 2012, amplía su portafolio ofreciendo servicios en Atención Domiciliaria como una excelente opción para atender en el seno de su hogar a los pacientes. A finales de ese mismo año da apertura a su programa de Salud Mental brindando rehabilitación e internación de pacientes con problemas de drogadicción. En el año 2019, pensando en necesidades sentidas del mercado inicia un nuevo servicio de Cuidado Integral en Casa para particulares en la ciudad de Palmira, el cual está dirigido a toda la población que lo necesite. En estos primeros 17 años TodoMed Ltda IPS se ha consolidado como una de las más importantes IPS del Suroccidente del país. Desde su constitución se ha caracterizado por prestar un servicio humanizado, fundamentado en principios y valores institucionales que le han permitido crecer como organización con una estructura integral e innovadora, tal como se denota en sus modelos de atención. Cuenta actualmente con una amplia cobertura en el Suroccidente Colombiano, en los departamentos de Valle, Cauca y Nariño, a través de las 8 modernas sedes de atención ubicadas en las ciudades de Palmira, Cali, Tuluá, Popayán y Pasto. TodoMed Ltda IPS genera 521 empleos directos, de los cuales 424 corresponden al Departamento del Valle del Cauca y 97 a los Departamentos de Cauca y Nariño. Cabe destacar que de los empleos generados 158 corresponden a la ciudad de Palmira. Así mismo, la organización en su aporte al desarrollo social de la región, crea el Club Atlético Deportivo TodoMed Ltda IPS con el propósito de promocionar y fomentar

la práctica del atletismo en jóvenes de zonas vulnerables de la región, a la fecha se brinda apoyo integral a 71 jóvenes con talento deportivo. La calidad y competencia del talento humano de TodoMed Ltda IPS y la excelente infraestructura y tecnología en sus sedes acondicionadas para brindar una adecuada atención y la eficiencia en los procesos, le han permitido lograr alta satisfacción de los usuarios.

Para el año 2024, TodoMed Ltda IPS espera constituirse como la mejor opción de servicios de salud especializados con sus modelos de Atención Integral en VIH/SIDA; Atención Domiciliaria y Salud Mental, logrando un crecimiento sostenible, con impacto social y ambiental. Como resultado de su compromiso con la calidad, TodoMed Ltda IPS en el año 2017 obtuvo por parte del ICONTEC la Certificación de su Sistema de Gestión de la Calidad conforme a la norma ISO 9001:2015. El resultado de este logro garantiza la confiabilidad de la organización para entregar los servicios con enfoque de la "Atención Centrada en el Paciente" la gestión del riesgo, y la humanización de los servicios.

Servicios

Atención a Pacientes VIH/SIDA. Esta unidad de servicio se especializa en el manejo integral de pacientes con VIH/SIDA. El propósito del modelo de atención es garantizar a los usuarios el acceso a los servicios de salud con calidad, confiabilidad, seguridad, responsabilidad y ética. La alta adherencia a los tratamientos y la aplicación estricta de los protocolos de VIH/SIDA del Ministerio de Salud y Protección Social en forma oportuna, continua y eficiente, ha logrado reconocimiento local y nacional, ya que le permiten al paciente alcanzar su calidad de vida, motivando su autocuidado y auto realización. Actualmente 1.626 pacientes se benefician de este programa.

Atención Domiciliaria. Este programa se enfoca en el manejo de un equipo interdisciplinario para apoyar permanentemente el cuidado médico, terapéutico y de enfermería, que centraliza todos los servicios en el domicilio del usuario, disminuyendo las estancias hospitalarias y las complicaciones derivadas de ello. A través del mismo se fortalecen las habilidades de autocuidado en el paciente y la familia. Dicha atención se fundamenta en el desplazamiento de equipos de salud y la participación activa del núcleo familiar, con lo cual se garantiza el cumplimiento de la meta terapéutica basada en la experiencia del equipo humano, los recursos técnicos y tecnológicos, para entregar de manera continua una atención oportuna, humanizada, personalizada y segura. TodoMed Ltda IPS a través de este programa atiende un total de 1.100 pacientes.

Atención Salud Mental. Esta unidad se especializa en el manejo integral de pacientes consumidores de sustancias psicoactivas y trastorno mental, a través de la internación y rehabilitación en adicciones; orientado a mejorar su calidad de vida y la integración familiar, social y laboral. El programa es innovador, dada la calidad del equipo de profesionales altamente calificados, basados en el respeto, los valores sociales y los deberes y derechos del usuario, generando resultados positivos toda vez que se obtiene el restablecimiento de la salud de los pacientes para llevar una vida constructiva y pueda reinsertarse en la sociedad como persona productiva para sí misma y en su entorno inmediato. Actualmente se cuenta con 60 pacientes internados en la ciudad de Palmira.

Temporal

Este proyecto investigativo está planteado para realizarse en un término de 4 meses, específicamente comprendidos en los meses de septiembre hasta diciembre del año 2021.

Alcance de la Investigación

El alcance de esta investigación tiene como propósito de ayudar a la empresa TodoMed Ltda IPS en la identificación de los riesgos de pérdida o fuga de información de la historia clínica electrónica de sus pacientes, apoyándose en el uso de nuevas tecnologías como los son las Herramientas de Prevención de Perdida de Información o “Data Loss Prevention” apoyados en las leyes “HIPAA”, “1581 del 2012” y “2015 del 2020”.Se presenta el detalle del alcance de los resultados esperados por medio de la siguiente tabla:

Tabla 1

Alcance del proyecto

Descripción Del Proyecto	Entregables	Características de la Entrega	Criterios de Aceptación	Restricciones	Supuestos
Diseñar una propuesta de modelo de Prevención de Perdida de la Información en historias clínicas de pacientes de la TodoMed Ltda IPS apoyado en las leyes “HIPAA”, “1581 del 2012” y “2015 de 2020”	Identificar y documentar los riesgos de seguridad a los que están expuestas las historias clínicas y documentos de pacientes de la IPS y que puedan ser mitigables con tecnologías de seguridad en la nube Diseñar una propuesta de protección de los datos de pacientes o historias clínicas con tecnologías que permitan controlar los accesos y auditar las acciones de los usuarios de la IPS. Dicho plan debe estar	Documento Documento	Riesgos identificados y documentados por medio del proceso y matriz de riesgo propuesta de mitigación de riesgos identificados en una HCE	1. aumento en el tiempo en la programación	1. El proyecto investigativo se realizará en las instalaciones de TodoMed Ltda IPS ubicado en la ciudad de Palmira y Cali 2. la prueba piloto se realizará en las instalaciones de TodoMed en la sede de cuidado en ubicada

	alineado con el plan estratégico de la organización				físicamente en la ciudad de palmira
	Proponer soluciones DLP y planes de acción aceptados por la IPS con las tecnologías propuestas en las fases de identificación de riesgos y diseño	Documento de propuesta de implementación	la propuesta del modelo de protección de pérdidas de datos debe de tener un alcance alineado con los objetivos organizacionales de TodoMed Ltda IPS	1- Restricción de costo y alcance 2- Equipos en obsolescencia 3- incumplimiento en políticas de seguridad 4- incumplimiento en las normativas 5- aumento en el tiempo de ejecución	

Nota. Elaboración propia.

Estado del Arte.

Según ISOTools la seguridad de la información es la implementación de procedimientos para resguardar la operación de una empresa de ataques informáticos, fugaz y perdidas de información "La seguridad informática protege el sistema informático, tratando de asegurar la integridad y la privacidad de la información que contiene. Por lo tanto, podríamos decir, que se trata de implementar medidas técnicas que preservarán las infraestructuras y de comunicación que soportan la operación de una empresa, es decir, el hardware y el software empleados por la empresa" (Isotools, 2017).

De acuerdo a Rojas (Rojas Valduciel, 2017) la seguridad de la información y de la informática esta unido con la seguridad computacional donde actualmente se genera el mayor porcentaje de datos de una empresa "Dentro de esta categoría, La seguridad informática y la seguridad de la información se puede mencionar la seguridad computacional, la cual se ciñe a la protección de los sistemas y equipos para el procesamiento de datos” (Torres, 2020).

Según (ISOTools, 2017) tener buenas prácticas basados en esquemas normativos ayudaran a la continuidad de la compañía mediante la recuperación y disposición de la información "que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo (…) es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información" (Isotools, 2017).

Las fugas de datos son un riesgo que ha ido aumentando durante los últimos años y la industria debe tener en cuenta que esto representa la pérdida de uno de los activos más importantes para una empresa. La información es un activo que los empleados pueden haber generado, tener acceso o podría estar a cargo de su almacenamiento, por lo que la pregunta es si las empresas deben confiar en que los empleados seguirán la política de seguridad de datos o si las empresas utilizan una herramienta de aplicación para ayudar a asegurarse de que los usuarios cumplen con las políticas de seguridad. La verdad en el mundo real es que los empleados cometen errores y es difícil asegurar que una empresa tendrá empleados 100% honestos (OEA, 2019).

Algunos ejemplos de pérdida de datos son WikiLeaks fundado por Julián Assange, que expuso información secreta de gobiernos y organizaciones militares que causaron un gran impacto para los regímenes políticos y las empresas privadas. También, el caso de Edward Snowden, en su libro (Snowden, 2013) quien ha sido responsable de la filtración más importante en la historia de la NSA. En consecuencia, los autores consideraron que las fugas de datos son un problema visible y las tecnologías de prevención de pérdida de datos (DLP) ayudará a la industria a aumentar el cumplimiento de las políticas de seguridad de la información. Además, los autores buscaron estudios previos sobre soluciones tecnológicas DLP comerciales y de código abierto, y se encontró que hay un poco de trabajo académico en la evaluación DLP, por lo que será una investigación realmente útil ya que va a presentar el estado de la técnica de la evaluación tecnológica DLP a la academia (Doğantekin, 2019).

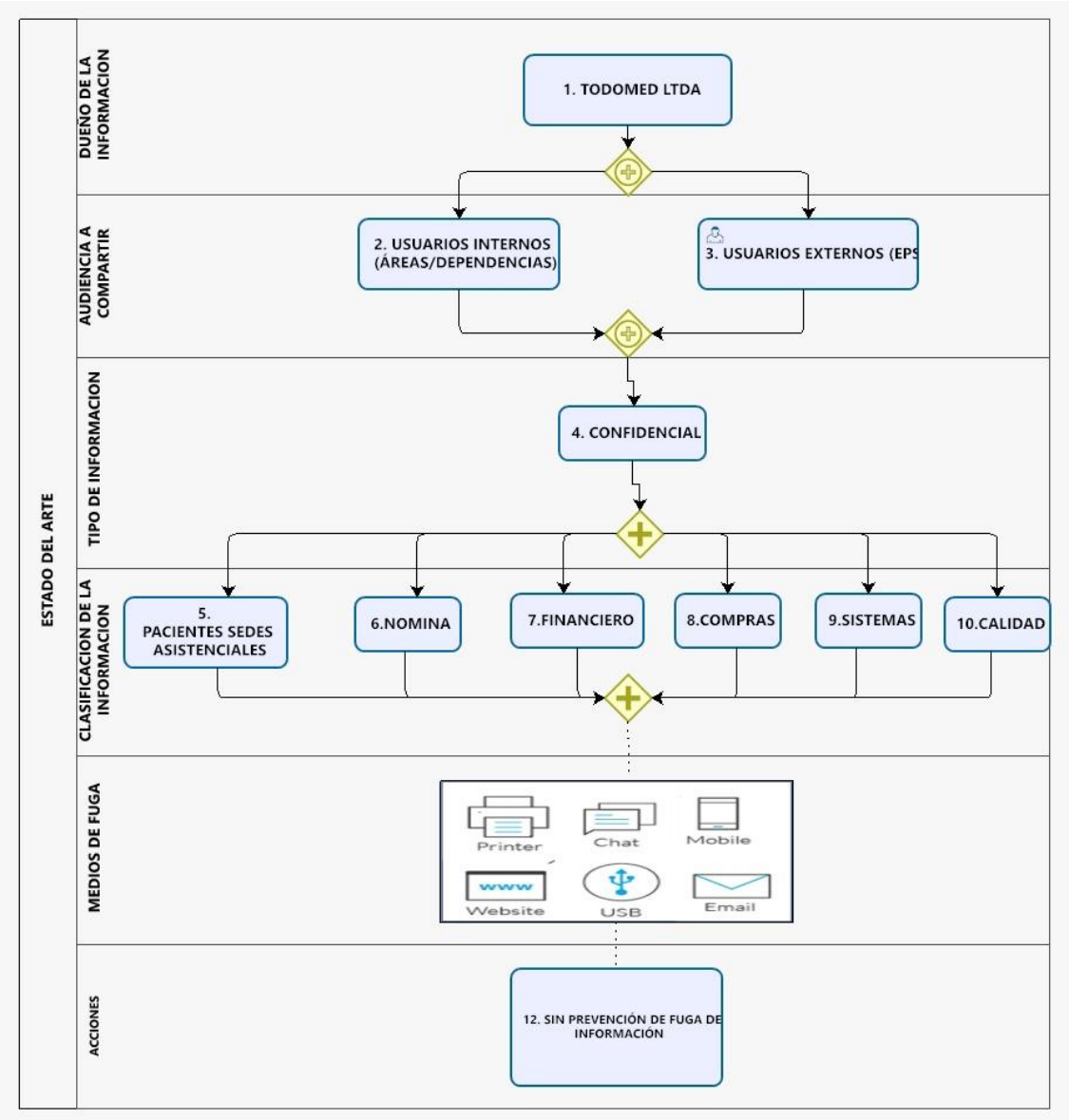
Es importante mencionar que los estudios académicos actuales sobre DLP enfocan en las últimas técnicas para realizar la prevención de pérdida de datos y no está relacionado con la evaluación de la tecnología DLP, por lo que la principal contribución de este documento es

presentar una pieza académica de trabajo para proponer un modelo con tecnología DLP apoyado en las leyes “HIPAA”, “1581 del 2012” y “2015 de 2020” (Helpsystems, 2021).

Basada en los criterios de información sensible relacionados con la nueva matriz de seguridad de TodoMed Ltda IPS, extensiones de archivos de datos comunes y de evasión, características DLP como el rendimiento, las capacidades y la experiencia del usuario, violación de políticas relacionadas con datos sensibles de acuerdo con las leyes colombianas. Se encontró trabajo relacionado con la tecnología de evaluación DLP, pero no siguió una metodología científica ni presentó detalles de la evaluación, por lo que tenía una alta probabilidad de una investigación de sesgo. Los autores reconocieron este defecto en el estado del arte de la evaluación de la tecnología DLP y se dio cuenta de la necesidad de una obra académica en esta área.

Figura 7

Estado del arte



Nota. Elaboración propia.

Identificación y Documentación de Riesgos

Toda empresa independientemente de su actividad económica tiene una serie de riesgos intrínsecos que acompañan su operatividad, estos riesgos pueden ser de origen interno o externo. Los riesgos internos son aquellos que por su naturaleza dependen de nuestra gestión dentro de la Empresa y de los distintos departamentos que la componen, como pueden ser los riesgos operacionales, concentración en ventas y proveedores, Poca diversificación de productos y/o servicios, iliquidez entre otros. Mientras que los riesgos externos son los que afectan al exterior y no están bajo el control de la organización, como los riesgos políticos, legales, ambientales, tecnológico.

La clasificación de riesgos empresariales no puede ser una lista cerrada, y no todas las empresas tendrán y se verán afectadas por los mismos riesgos. Lo importante es tener de una estrategia de gestión de riesgos con la que evaluemos y minimicemos al máximo el impacto que puedan tener en la empresa. Por eso es necesario hacer un seguimiento constante a los riesgos para conocer cuáles son los problemas que amenazan a TodoMed Ltda IPS y la posibilidad latente que acaben siendo perjudiciales para la empresa.

Teniendo en cuenta el foco de nuestra investigación vamos a centrar nuestro trabajo en los riesgos que afectan o pudieran afectar a TodoMed Ltda IPS y le vamos a dar una calificación donde 1 sería el riesgo más bajo y 5 el riesgo más alto. Lo anterior basado en la actividad económica de la empresa y sus datos históricos.

Riesgo legal

Son aquellos riesgos que enfrenta la empresa y que están relacionados con el incumplimiento de las leyes, normas y regulaciones del gobierno y otros organismos de vigilancia que controlan las empresas, por lo que presta mayor importancia la prevención en el manejo de información de nuestros pacientes. Este riesgo está calificado con 5.

Riesgo Tecnológico

Son todos aquellos originados por la contingencia de que la interrupción, alteración, o falla de la infraestructura de TI, sistemas de información, bases de datos y procesos de TI, que no cuenten con una gestión adecuada de seguridad y provoque pérdidas financieras a la institución. Teniendo en cuenta el contexto en el que desarrollamos nuestro trabajo investigativo y la amenaza de un fallo en el sistema que podría comprometer la seguridad cibernética y la inteligencia empresarial. Este riesgo está calificado con 5.

Riesgo Operativo

Son todos los factores de riesgo que tiene la empresa producto de su actividad económica, sobre todo debido a fallas en los procesos de la empresa, sistemas internos, errores tecnológicos, errores humanos o a raíz de eventos externos como un desastre natural. Debido a su naturaleza de ser un riesgo interno y gobernable por la empresa, este riesgo está calificado con 4.

Riesgo Reputacional

Son todas las posibilidades de pérdida en la reputación de una organización de forma que afecte de forma negativa a la percepción que el entorno social tiene sobre la misma. Este daño reputacional puede producir una pérdida directa o indirecta del valor de una compañía. Independientemente que este riesgo no se pueda cuantificar inmediatamente, si puede tener impactos económicos en la empresa a corto y largo plazo.

Siendo TodoMed Ltda IPS, una empresa del sector salud, su éxito comercial y financiero va directamente ligado a su reputación. Este riesgo está calificado con 5.

Documentación de Riesgos de seguridad de las historias clínica y documentos de la IPS

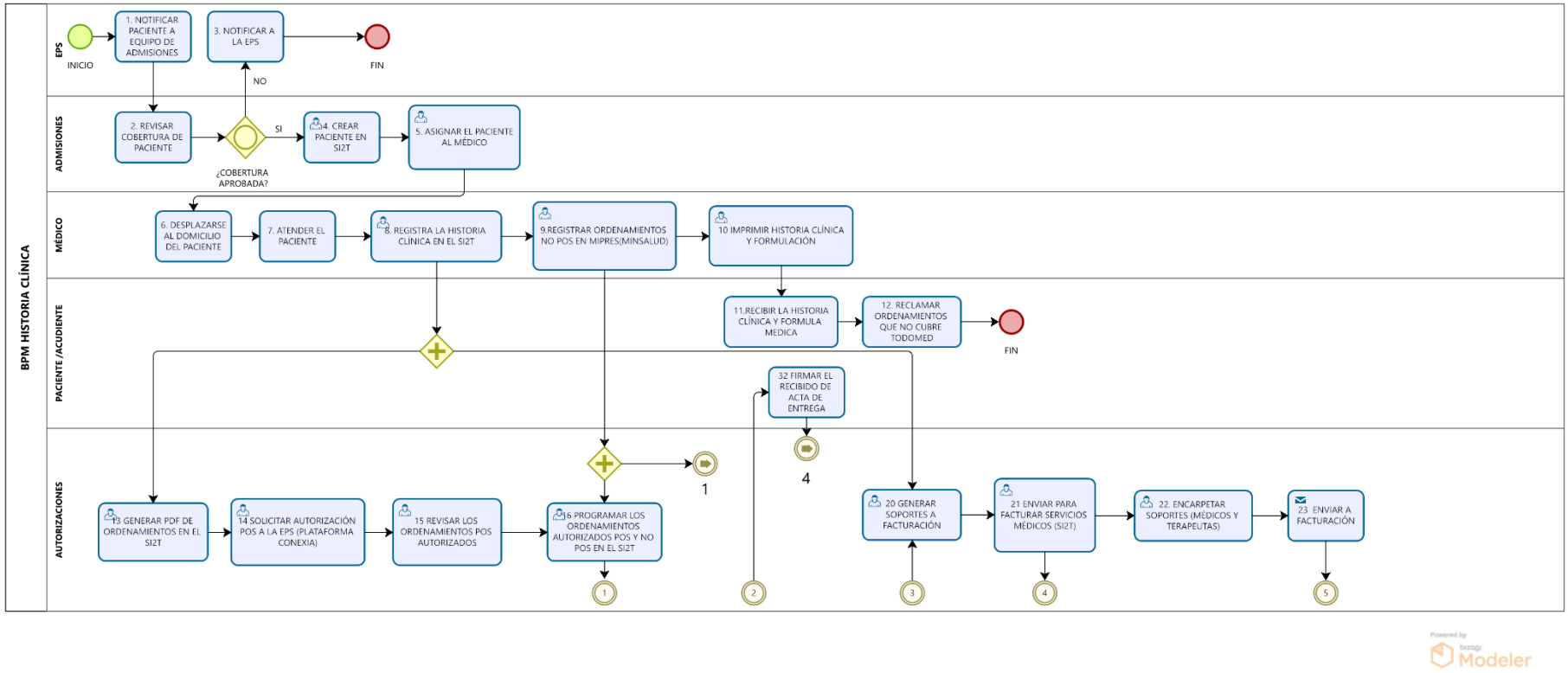
Inicialmente se realizó un levantamiento de la información del paso a paso manejado por la empresa TodoMed Ltda. IPS, estableciendo cada una de las actividades y procesos relacionados con la gestión de historias clínicas, teniendo en cuenta software, documentos y cargos que intervienen en este proceso.

Es importante destacar que la empresa cuenta con un software denominado SI2T, en el que se hace registro y manejo de las historias clínicas de los pacientes; en esta plataforma interviene la EPS, el personal de admisiones, el paciente y/o acudiente en caso de ser menor de edad, el médico, el personal de autorizaciones, el líder de terapias y enfermería, el personal de central logística, la herramienta tecnológica MIPRES y el personal de facturación.

Se hace claridad que las historias clínicas se manejan de forma digital y sólo se imprimen para ser entregados a los pacientes; la información que contiene es muy delicada, por lo que se debe proponer un modelo de protección de la información. A continuación, se resumen cada una de las actividades y pasos para el manejo de historias clínicas a través de un diagrama de flujo elaborado en el programa Bizagi

Figura 8

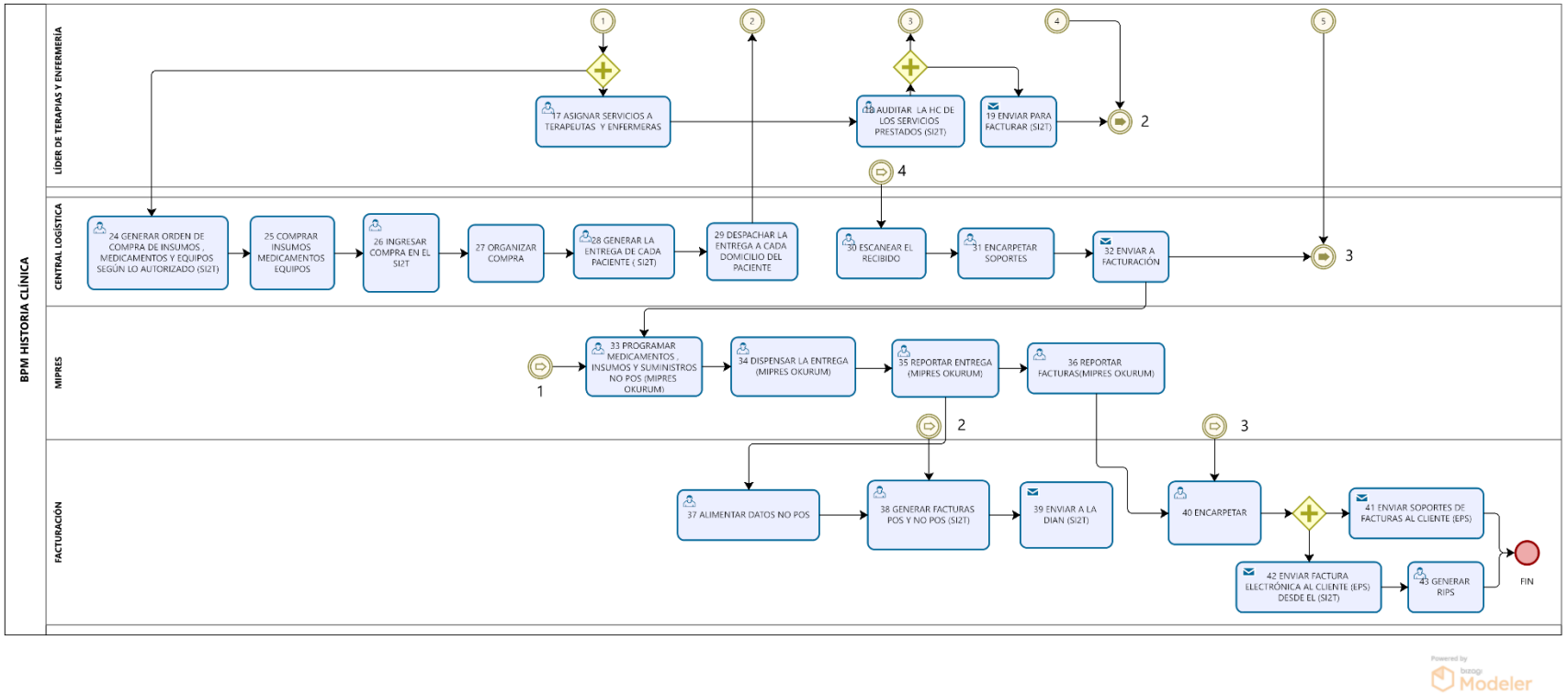
Diagrama de procesos de la gestión de historias clínicas



Nota. Elaboración propia.

Figura 9

Continuación Diagrama de procesos de la gestión de historias clínicas



Nota. Elaboración propia.

Identificación y Valoración de Riesgos

Inventario de Activos.

La identificación y valoración de los riesgos es una herramienta poderosa en las organizaciones para la toma de decisiones y la priorización y la planificación de las actividades. Existen diversas metodologías y procedimientos para la valoración de los riesgos en seguridad de la información, entre las que se encuentra la definida por la Norma ISO 27001, la cual fue utilizada para la identificación y valoración de los riesgos de TodoMed Ltda.

Como primer paso se definió la elaboración de una matriz en la cual se realice la identificación, el análisis y la valoración de los riesgos asociados a activos digitales o de información de la compañía.

Para la construcción de la matriz, se realizó un análisis del diagrama de flujo de atención al paciente para la determinación de los activos digitales o de información y de los procesos de la compañía a los cuales estaban asociados. Posteriormente, se describió el activo para evitar confusiones o ambigüedades en el análisis, al tiempo que se determinó el tipo de activo y si contenía datos personales sensibles o no sensibles, junto con el periodo de retención de los datos. Luego, se procedió a la determinación de las dimensiones de la seguridad de la información, las cuales son Confidencialidad, Disponibilidad e Integridad, y se definió la calificación actual de cada una de las dimensiones con respecto al activo. Por último, se hizo una valoración del impacto del activo con respecto a cada una de las dimensiones, con las siguientes calificaciones:

Impacto extremo (5 puntos). Perdida financiera vital, cobertura de medios negativa internacional, sanciones legales y monetarias, lesiones o muertes.

Impacto importante (4 puntos). Perdida financiera importante para el negocio, impacto negativo de medios a nivel nacional a largo plazo, pérdida de cuota de mercado, investigaciones por entes reguladores, lesiones.

Impacto moderado (3 puntos). Perdida financiera considerable, impacto negativo en medios nacionales a corto plazo, acciones correctivas enviadas por entes reguladores, tratamiento médico ambulatorio para lesionados.

Impacto menor (2 puntos). Perdida financiera menor, daño en la reputación local, incidente con entes reguladores, sin lesiones.

Impacto incidental (1 punto). Perdida financiera insignificante, sin repercusiones en medios de comunicación locales, incidente no reportable a entidades de control, sin lesiones.
No aplicable (0 puntos)

Catálogo de amenazas. Las amenazas que pueden afectar los activos digitales o de información pueden provenir de diversas fuentes, tanto de causas naturales e imprevistas como desde personas y de manera premeditadas. Se realizó un listado de las posibles amenazas para la construcción del catálogo de amenazas, basándose de lo expuesto en la Norma ISO 27001.

Tabla 2

Catálogo de amenazas

	AMENAZA
A1	Fuego
A2	Condiciones climáticas desfavorables
A3	Inundaciones
A4	Contaminación, polvo, corrosión
A5	Desastres Naturales
A6	Desastres ambientales
A7	Eventos importantes en el medio ambiente
A8	Interrupción de la fuente de alimentación
A9	Interrupción de las redes de comunicación
A10	Interrupción del suministro de red
A11	Fracaso o interrupción de los proveedores de servicios
A12	Interferencias
A13	Emisiones comprometidas
A14	Espionaje
A15	Robo de dispositivos, soportes de almacenamiento y documentos
A16	Pérdida de dispositivos, soportes de almacenamiento y documentos
A17	Mala planificación o falta de adaptación
A18	Divulgación de información sensible
A19	Información o productos de una fuente no confiable
A20	Manipulación de hardware o software
A21	Manipulación de información
A22	Acceso no autorizado a los sistemas de TI
A23	Destrucción de dispositivos o soportes de almacenamiento
A24	Fallo de dispositivos o sistemas

A25	Mal funcionamiento de dispositivos o sistemas
A26	Falta de recursos
A27	Vulnerabilidades o errores del software
A28	Violación de leyes o regulaciones
A29	Uso no autorizado o administración de dispositivos y sistemas
A30	Uso incorrecto o administración de dispositivos y sistemas
A31	Abuso de Autorizaciones
A32	Ausencia de personal
A33	Terrorismo
A34	Coerción, extorsión o corrupción
A35	Robo de identidad
A36	Comportamientos anti-éticos
A37	Abuso de datos personales
A38	Software malicioso
A39	Ataques DoS o denegación de servicio
A40	Ingeniería Social
A41	Reproducción de mensajes
A42	Entrada no autorizada a las instalaciones
A43	Pérdida de datos

Nota. Adaptado de Fase 4 planificación del SGSI, ISO 27001, 2020, https://normaiso27001.es/fase-4-planificacion-del-sgsi/

Determinación del riesgo. Se analizó cada uno de los activos identificados con respecto al catálogo de amenazas, para determinar cuáles de las amenazas tenía injerencia directa y fuerte sobre el activo. Para la determinación del riesgo de la amenaza al activo se tiene en cuenta tanto la probabilidad de ocurrencia como el impacto de cada una de las dimensiones. En una primera instancia, se definió la probabilidad de ocurrencia de la amenaza del activo mediante la siguiente clasificación:

Probabilidad mínima o muy baja (0 puntos). No existen antecedentes ni agresores o incidentes.

Probabilidad potencial o baja (1 punto). Existe historial de incidentes dentro del sector, sin embargo, no hay registros dentro de la empresa. Se esperan de manera esporádica.

Probabilidad creíble o media (2 puntos). Existe historial de incidentes dentro de la compañía. Se esperan de manera periódica sin frecuencia determinada.

Probabilidad definida o alta (3 puntos). Existe un amplio historial de incidentes en la empresa, con un origen identificado. Se esperan incidentes de manera frecuente.

Para la determinación del impacto de cada una de las dimensiones, se tomó la información diligenciada en la valoración del impacto del activo y se contrastó con los datos de probabilidad de ocurrencia del activo y mediante la siguiente tabla definió el impacto de la Confidencialidad, de la Disponibilidad y de la Amenaza.

Tabla 3

Valoración del impacto

Probabilidad de ocurrencia	**Valoración del impacto de un activo**					
	No Aplica (0)	**Incidental (1)**	**Menor (2)**	**Moderado (3)**	**Importante (4)**	**Extremo (5)**
Muy baja (0)	0	0	0	0	0	0
Baja (1)	0	1	2	3	4	5
Media (2)	0	2	3	4	5	6
Alta (3)	0	3	4	5	6	7

Nota. Adaptado de Fase 4 planificación del SGSI, de ISO 27001, 2020 https://normaiso27001.es/fase-4-planificacion-del-sgsi/

Con la información definida del impacto de cada dimensión, se determinó el impacto de la amenaza por medio del cálculo del promedio de las puntuaciones de cada dimensión. Por último, para la clasificación del riesgo, se realizó la sumatoria de los puntajes obtenidos de la probabilidad de ocurrencia con el impacto de la amenaza y se contrastó con los rangos de puntajes de las clasificaciones del riesgo definidas en la siguiente tabla:

Tabla 4

Clasificación del riesgo

Calificación del Riesgo	**Descripción**
Muy alto (7-10)	El riesgo es totalmente inaceptable. Se deben tomar medidas inmediatas para reducir y mitigar estos riesgos.
Alto (5-6)	El riesgo es inaceptable. Las medidas para reducir y mitigar el riesgo deberían implementarse lo antes posible
Medio (3-4)	El riesgo puede ser aceptable en el corto plazo. Los planes para reducir y mitigar los riesgos deberían incluirse en los planes y presupuestos futuros
Bajo (0-2)	Los riesgos son aceptables. Se deben implementar medidas para reducir y mitigar aún más el riesgo junto con otras mejoras de seguridad y mitigación.

Nota. Adaptado de Fase 4 planificación del SGSI, de ISO 27001, 2020 https://normaiso27001.es/fase-4-planificacion-del-sgsi/

Resultados de la valoración del riesgo

Como resultado del inventario de los activos, se pudo determinar en el proceso de gestión de historia clínicas, los siguientes hallazgos:

Tabla 5

Inventario de activos

Nombre del proceso	**Nombre del activo**	**Descripción del activo**
Gestión de historia clínica	SI2T	Software para la gestión de historias clínicas.
Atención al paciente	Historia clínica	Documento en el que se describe el historial médico de un paciente
Atención al paciente	Fórmula médica	Documento que se describe el medicamento y tratamiento a seguir por parte del paciente
Autorización	PDF de ordenamiento POS y NO POS	Documento que describe los requerimientos de medicamentos o tratamientos POS.
Autorización	Autorización POS	Documento que muestra las autorizaciones registradas en el POS.
Autorización	Soportes médicos	Es un documento que muestra los soportes médicos y terapéuticos.
Compras	Orden de compra de insumos, medicamentos y equipos	Documento que hace un listado de insumos, medicamentos y equipos solicitados por las dependencias con sus respectivos valores.
Facturación	Facturas POS y NO POS	Factura con los respectivos valores autorizados por el POS y NO POS.

Facturación	Factura electrónica al cliente	Documento que registra los valores y descripciones de medicamentos y tratamientos cancelados.

Nota. Elaboración propia.

A cada uno de los activos se les indicó el proceso al que pertenecen, el nombre, la descripción, además de datos como el tipo de archivo y el periodo de retención el cual es de todos los documentos a 20 años, Luego de esta información, se realizó la valoración del impacto de cada uno de los activos, teniendo en cuenta las dimensiones de seguridad informativa de confidencialidad, disponibilidad e integridad; los resultados se encuentran en la siguiente tabla:

Tabla 6

Valoración del impacto de los activos

Nombre del activo	**Confidencialidad**	**Disponibilidad**	**Integridad**
SI2T	Importante (4)	Importante (4)	Importante (4)
Historia clínica	Importante (4)	Importante (4)	Importante (4)
Fórmula médica	Importante (4)	Moderado (3)	Importante (4)
PDF de ordenamiento POS y NO POS	Importante (4)	Moderado (3)	Importante (4)
Autorización POS	Importante (4)	Moderado (3)	Importante (4)
Soportes médicos	Importante (4)	Importante (4)	Importante (4)

Orden de compra de insumos, medicamentos y equipos	Moderado (3)	Moderado (3)	Importante (4)
Facturas POS y NO POS	Importante (4)	Moderado (3)	Importante (4)
Factura electrónica al cliente	Extremo (5)	Moderado (3)	Importante (4)

Nota. Elaboración propia.

Con el establecimiento de la valoración del impacto, se pudo lograr el cálculo del riesgo en cada una de las amenazas, de tal manera que se realizara una valoración por cada uno de las dimensiones de la seguridad informática; a continuación, se muestran los resultados:

Tabla 7

Valoración del riesgo en la seguridad informática

Activo	Amenaza	Probabilidad / Ocurrencia	Deterioro Confidencialidad	Deterioro Disponibilidad	Deterioro Integridad	Impacto confidencialidad	Impacto disponibilidad	Impacto en la integridad	Impacto de la ameneza	Clasificación del riesgo
SI2T	Interrupción de la fuente de alimentación	Muy baja (0)	Importante (4)	Importante (4)	Importante (4)	0	0	0	0,0	Bajo
	Interrupción del suministro de red	Muy baja (0)	Importante (4)	Importante (4)	Importante (4)	0	0	0	0,0	Bajo
	Interferencias	Muy baja (0)	Importante (4)	Importante (4)	Importante (4)	0	0	0	0,0	Bajo
	Divulgación de información sensible	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto
	Manipulación de información	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto

	Vulnerabilidades o errores del software	Media (2)	Importante (4)	Importante (4)	Importante (4)	5	5	5	5,0	Muy alto
	Software malicioso	Media (2)	Importante (4)	Importante (4)	Importante (4)	5	5	5	5,0	Muy alto
	Pérdida de datos	Media (2)	Importante (4)	Importante (4)	Importante (4)	5	5	5	5,0	Muy alto
Historia clínica	Divulgación de información sensible	Media (2)	Importante (4)	Importante (4)	Importante (4)	5	5	5	5,0	Muy alto
	Manipulación de información	Media (2)	Importante (4)	Importante (4)	Importante (4)	5	5	5	5,0	Muy alto
	Destrucción de dispositivos o soportes de almacenamiento	Muy baja (0)	Importante (4)	Importante (4)	Importante (4)	0	0	0	0,0	Bajo
	Pérdida de datos	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto

	Vulnerabilidades o errores del software	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto
Fórmula médica	Interrupción del suministro de red	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Divulgación de información sensible	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Manipulación de información	Media (2)	Importante (4)	Moderado (3)	Importante (4)	5	4	5	4,7	Muy alto
	Vulnerabilidades o errores del software	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Pérdida de datos	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
PDF de ordenamiento	Interrupción del suministro de red	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo

POS y NO POS	Divulgación de información sensible	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Manipulación de información	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Vulnerabilidades o errores del software	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Pérdida de datos	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
Autorización POS	Interrupción del suministro de red	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Divulgación de información sensible	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Manipulación de información	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Vulnerabilidades o errores del software	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo

	Abuso de Autorizaciones	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Pérdida de datos	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
Soportes médicos	Fuego	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto
	Interrupción del suministro de red	Muy baja (0)	Importante (4)	Importante (4)	Importante (4)	0	0	0	0,0	Bajo
	Divulgación de información sensible	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto
	Manipulación de información	Baja (1)	Importante (4)	Importante (4)	Importante (4)	4	4	4	4,0	Alto
	Pérdida de datos	Muy baja (0)	Importante (4)	Importante (4)	Importante (4)	0	0	0	0,0	Bajo
Orden de compr	Interrupción del suministro de red	Muy baja (0)	Moderado (3)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo

a de insumos, medicamentos y equipos	Divulgación de información sensible	Muy baja (0)	Moderado (3)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Violación de leyes o regulaciones	Baja (1)	Moderado (3)	Moderado (3)	Importante (4)	3	3	4	3,3	Alto
	Mala planificación o falta de adaptación	Baja (1)	Moderado (3)	Moderado (3)	Importante (4)	3	3	4	3,3	Alto
	Manipulación de información	Baja (1)	Moderado (3)	Moderado (3)	Importante (4)	3	3	4	3,3	Alto
	Vulnerabilidades o errores del software	Muy baja (0)	Moderado (3)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Pérdida de datos	Muy baja (0)	Moderado (3)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
Facturas POS	Interrupción del suministro de red	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo

y NO POS	Violación de leyes o regulaciones	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Manipulación de información	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Vulnerabilidades o errores del software	Baja (1)	Importante (4)	Moderado (3)	Importante (4)	4	3	4	3,7	Alto
	Abuso de Autorizaciones	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Pérdida de datos	Muy baja (0)	Importante (4)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
Factura electrónica al cliente	Interrupción del suministro de red	Baja (1)	Extremo (5)	Moderado (3)	Importante (4)	5	3	4	4,0	Alto
	Violación de leyes o regulaciones	Muy baja (0)	Extremo (5)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo
	Manipulación de información	Baja (1)	Extremo (5)	Moderado (3)	Importante (4)	5	3	4	4,0	Alto

Vulnerabilidades o errores del software	Baja (1)	Extremo (5)	Moderado (3)	Importante (4)	5	3	4	4,0	Alto
Abuso de Autorizaciones	Baja (1)	Extremo (5)	Moderado (3)	Importante (4)	5	3	4	4,0	Alto
Pérdida de datos	Muy baja (0)	Extremo (5)	Moderado (3)	Importante (4)	0	0	0	0,0	Bajo

Nota. Elaboración propia.

Como conclusión de la identificación de riesgos en la seguridad informática, se realizó una priorización de los activos según la valoración de las amenazas halladas en la matriz, por lo cual, se estableció de la siguiente manera:

Tabla 8

Identificación de los riesgos en TodoMed

Priorización	Nombre del activo	Amenazas destacadas	Valoración del riesgo
1	SI2T	Vulnerabilidades o errores del software	Muy alto
		Software malicioso	Muy alto
		Pérdida de datos	Muy alto
2	Historia Clínica	Divulgación de información sensible	Muy alto
		Manipulación de información	Muy alto
3	Fórmula médica	Manipulación de información	Muy alto
4	Factura electrónica al cliente	Manipulación de información	Alto
		Vulnerabilidades o errores del software	Alto
		Abuso de Autorizaciones	Alto
		Interrupción del suministro de red	Alto
5	Orden de compra de insumos, medicamentos y equipos	Violación de leyes o regulaciones	Alto
		Mala planificación o falta de adaptación	Alto
		Manipulación de información	Alto
6	Soportes médicos	Divulgación de información sensible	Alto

		Manipulación de información	Alto
		Fuego	Alto
7	Facturas POS y NO POS	Violación de leyes o regulaciones	Alto
		Manipulación de información	Alto
		Vulnerabilidades o errores del software	Alto
8	PDF de ordenamiento POS y NO POS	Vulnerabilidades o errores del software	Alto
		Pérdida de datos	Alto
9	Autorización POS	Abuso de Autorizaciones	Alto

Nota. Elaboración propia.

Propuesta de Protección de Datos de Historias Clínicas

Una vez realizado el análisis del estado actual de la entidad en términos de seguridad y resguardo de la información, se procede a una etapa de planeación en la cual se definen las siguientes características:

Figura 10

Planificación de la propuesta de protección de datos

Nota. Adaptado de Fase de planificación [Figura], de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

En cada una de las etapas se deben tener en cuenta los siguientes parámetros:

Figura 11

Etapas en la planificación

Nota. Adaptado de Fase de planificación [Figura], de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Como resultado e identificación de las características anteriores, se determinan los siguientes productos que servirán como insumo para el posterior diseño del modelo de prevención de pérdida de la información.

Política de Seguridad y Privacidad de la Información

Como modelo inicial se requiere plantear una política de Seguridad y Privacidad de la información que en ultimas refleja el apoyo y buena voluntad de los directivos en la implementación del modelo de protección para las historias clínicas y datos sensibles.

El documento que se genera a partir de la política incluye los objetivos, el alcance, el nivel de cumplimiento y los involucrados. Para su implementación esta política debe ser aprobada y divulgada dentro de la entidad. La entidad debe evaluar los requerimientos necesarios para ser ajustados o desarrollados en la elaboración de las políticas de seguridad y privacidad, así como en la implementación.

Procedimientos de Seguridad de la Información

Una de las etapas fundamentales consiste en la creación y desarrollo de procedimientos que permitan realizar una gestión y flujos para la información de la entidad principalmente en el uso y manejo de historias clínicas. Se sugiere la creación de los siguientes procedimientos:

- Procedimiento de identificación y clasificación de Activos.
- Procedimiento de gestión de usuarios y contraseñas.
- Procedimiento de control de acceso físico.
- Procedimiento de protección de activos e información.
- Procedimiento de mantenimiento y depuración de información.
- Procedimiento de gestión de cambios.
- Procedimiento de protección contra códigos maliciosos.
- Procedimiento de transferencia de información.
- Procedimiento de gestión de incidentes de seguridad de la información.

Roles y Responsabilidades de Seguridad y Privacidad de la Información

Se requieren definirlos roles y responsabilidades de los diferentes aspectos relacionados a la privacidad y seguridad de la información, legalmente se deben aprobar, socializar y realizar seguimiento para que todos los involucrados hagan cumplir con las políticas y procedimientos establecidos de acuerdo al rol que ejerzan desde la organización; comprende los niveles directivos, de procesos y operativos, de forma que permitan la correcta toma de decisiones. El siguiente cuadro sirve como base para aquellas actividades que deben ser realizadas a los diferentes roles/responsables:

Tabla 9

Responsabilidades en la protección de datos

Dominio	**Responsabilidades**
Servicios tecnológicos	- Liderar la gestión de riesgos de seguridad sobre la gestión de TI y de información de la entidad. - Gestionar el desarrollo e implementación de políticas, normas, directrices y procedimientos de seguridad de gestión de TI e información. - Definir mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de implantación de las medidas de seguridad. - Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias. - Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio.

	- Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información.
Estrategia de TI	- Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la entidad. Se debe guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información.
Gobierno de TI	- Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Además, debe monitorear y gestionar la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
Sistemas de información	- Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la entidad. - Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información del estado colombiano. - Desarrollar pruebas periódicas de vulnerabilidad sobre los diferentes sistemas de información para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. - Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.

	- Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de la información.
Gestión de la información	- Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. - Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información.
Uso y apropiación de la información	- Desarrollar el plan de formación y sensibilización de la entidad incorporando el componente de seguridad de la información en diferentes niveles. - Supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora. - Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.

Nota**.** Adaptado de Responsabilidades [Tabla], de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

Inventario de activos de información

Para la correcta implementación de Políticas, Procedimientos, Roles y responsabilidades, se requiere realizar un levantamiento de la información que está bajo custodia de la empresa, con el fin de lograr crear una criticidad y correcta clasificación. La entidad debe desarrollar una metodología de gestión de activos que le permita implementar correctamente la metodología del

modelo de protección. La siguiente tabla permite clasificar la información de modo que permita establecer prioridades al momento de la implementación del modelo.

Tabla 10

Clasificación de activos

Criterios específicos	**Niveles**			
Confidencialidad	Información pública reservada	Información pública clasificada	Información pública	Información no clasificada
Integridad	Integridad Alta (A)	Integridad Media (M)	Integridad Baja (B)	Integridad no clasificada
Disponibilidad	Disponibilidad Alta (A)	Disponibilidad Media (M)	Disponibilidad Baja (B)	Disponibilidad no clasificada

Nota. Adaptado de Criterios de clasificación [Tabla], de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

La criticidad de la información puede ser medida de la siguiente forma:

Tabla 11

Nivel de criticidad de la información

Nivel	**Descripción**
Alta	Activos de información en los cuales la clasificación de la información en dos o todas las propiedades, ya sea desde la confidencialidad, integridad, y disponibilidad, es alta.
Media	Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades o al menos una de ellas es de nivel medio.
Baja	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Nota**.** Adaptado de Criterios de clasificación [Tabla], de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

Identificación, Valoración y Tratamiento de Riesgos

La identificación de los riesgos como punto tratado anteriormente permite ajustar la información a un esquema que determina su exposición a eventos que puedan conllevar a su perdida, duplicidad, no integridad o exposición entre otros. Una vez identificados los riesgos la gestión de los mismos se convierte en el paso a seguir y se plasma en las siguientes etapas; se toma el ciclo PHVA como integración de esta importante metodología dentro de las etapas que se establece según el MinTic:

Tabla 12

Pasos para la gestión del riesgo

Etapa	Pasos para la gestión del riesgo
Planear	- Establecimiento del contexto. - Valoración del riesgo - Planificación del tratamiento del riesgo. - Aceptación del riesgo.
Hacer (Implementar)	- Implementación del Plan de Tratamiento del Riesgo.
Verificar (Gestionar)	- Monitoreo y revisión continua de los riesgos.
Actuar (Mejora Continua)	- Aseguramiento de la mejora del Proceso de Gestión del Riesgo en la Seguridad de la Información.

Nota**.** Adaptado de Etapas de la gestión del riesgo. [Tabla], de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Plan de Comunicaciones

La empresa debe definir un Plan de comunicación, sensibilización y capacitación que incluya la estrategia para que la seguridad de la información se convierta en cultura organizacional, al generar competencias y hábitos en todos los niveles (directivos, funcionarios, terceros) de la entidad. Este plan será ejecutado, con el aval de la Alta Dirección, a todas las áreas de la Entidad. Dentro del plan de comunicaciones se debe tener en cuenta los siguientes aspectos:

Tabla 13

Aspectos de plan de comunicaciones

Niveles	Etapas	Acciones
Básico	Sensibilización	- Identificación de necesidades según los cargos (Ejecutivos, personal de seguridad, dueños de sistemas, administradores de sistemas y personal de soporte, usuarios finales). - Creación del programa de sensibilización y capacitación. - Definición del material a desarrollar. - Financiamiento del programa. - Implementación del programa. - Evaluación.
Intermedio	Entrenamiento	- Definición de habilidades a desarrollar en el personal, por lo general se recomienda que sea a personal de TI. - Creación de convenios de estudio. - Selección de personal para entrenamiento. - Evaluación.

Avanzado	Educación	- Identificación de necesidades de habilidades de educación formal. - Creación de convenio con instituciones formales. - Selección de personal. - Evaluación.

Nota. Adaptado de Plan de comunicaciones, de MINTIC, 2016, https://www.mintic.gov.co/gestionti/615/articles-5482_G14_Plan_comunicacion_sensibilizacion.pdf

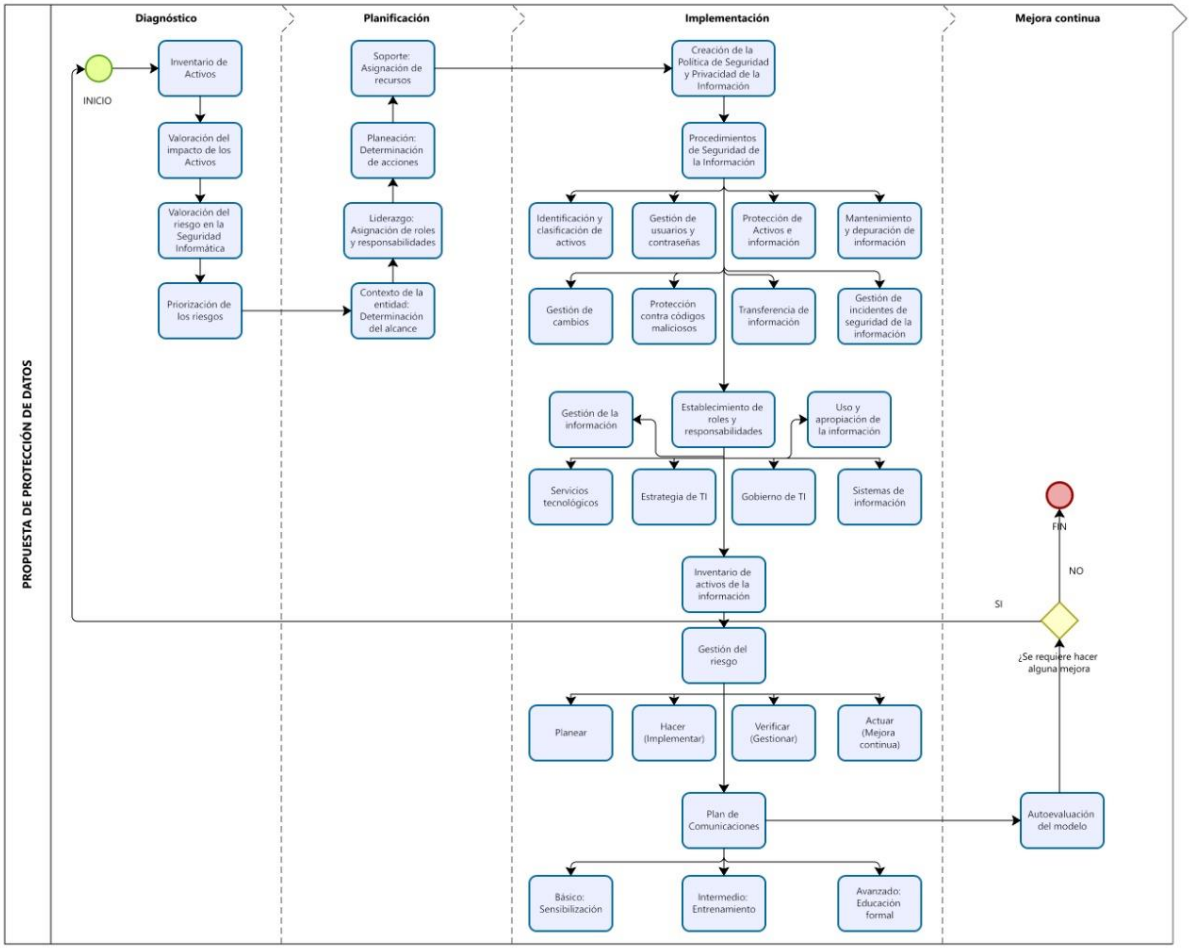
Tecnologías de apoyo

Dentro de la propuesta de protección de datos se establece la importancia de la implementación de un DLP, el cual sirve como medio para la prevención de pérdida de datos, el cual complementa el Modelo de Protección de la información de la historia clínica.

A continuación, se resume la estructura de la propuesta de protección de datos para la empresa TodoMed:

Figura 12

Propuesta de protección de datos TodoMed



Nota. Elaboración propia.

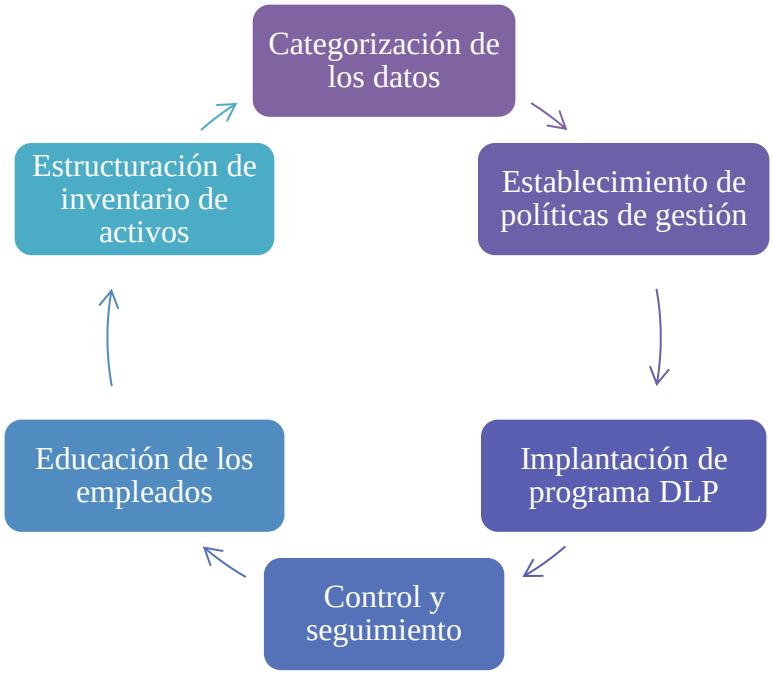
Propuesta de Modelo de prevención de pérdida de información de historias clínicas

TodoMed

Teniendo en cuenta la propuesta de protección de datos, se establece la generación de una estrategia de prevención de la pérdida de datos (DLP), de tal manera que se evite la fuga de información o el acceso a personal no autorizado a los datos que se tienen en la empresa TodoMed. Por ello, se establece la siguiente estructura, teniendo en cuenta que es un proceso cíclico que debe garantizar la protección constante de los datos de los pacientes y de la compañía en general.

Figura 13

Propuesta de Modelo de prevención de pérdida de información



Nota. Elaboración propia.

En la estructuración del inventario de activos, se tiene en cuenta que en la empresa TodoMed, se contemplan los siguientes:

SI2T.

Historia Clínica.

Fórmula médica.

Factura electrónica al cliente.

Orden de compra de insumos, medicamentos y equipos.

Soportes médicos.

Facturas POS y NO POS.

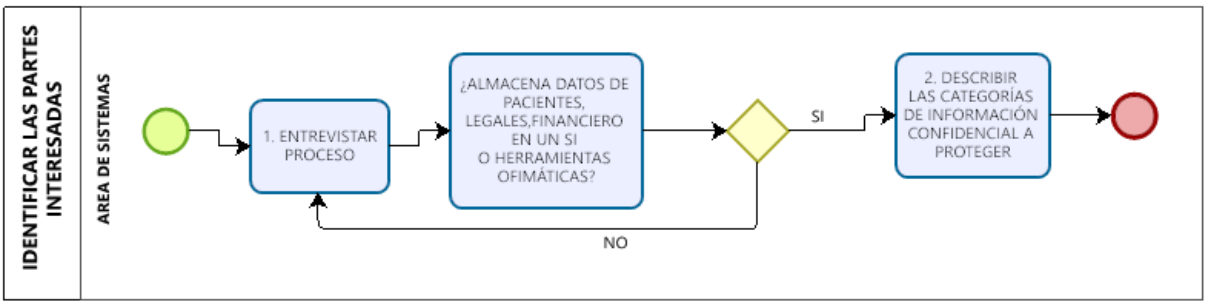
PDF de ordenamiento POS y NO POS.

Autorización POS.

En la categorización de los datos se tiene en cuenta inicialmente el reconocimiento de las diferentes partes interesadas, donde se determina que se encuentran los datos de los pacientes, los datos legales y los datos financieros de la empresa.

Figura 14

Partes interesadas

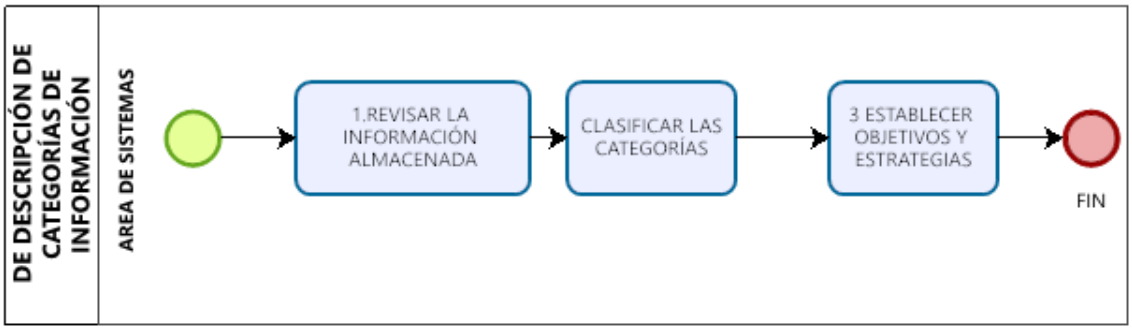


Nota. Elaboración propia.

Luego, se hace necesario el establecimiento de las categorías a tener en cuenta dentro de la empresa, de tal manera que con ello se creen las estrategias y objetivos para mitigar la pérdida de información.

Figura 15

Categorización de los datos



Nota. Elaboración propia.

Las categorías designadas por la empresa TodoMed, son las que se describen a continuación:

Datos en movimiento: son aquellos datos que se moverán de forma constante al interior de la empresa, por lo que se requiere tener una protección alta y se debe garantizar que no se desvíen a otros lugares no autorizados.

Datos en reposo: estos son aquellos que se encuentran en bases de datos, en la nube, computadoras, que no requieren de constante movimiento. Se debe generar barreras que impidan su réplica, ya sea por medio de negación de permiso, bloqueo de computadores o bloqueo en uso de USB.

Datos en el punto final: son datos que pueden llegar a ser copiados desde dispositivos móviles o tabletas, por lo que se requiere del cifrado de la información para que no sea replicada.

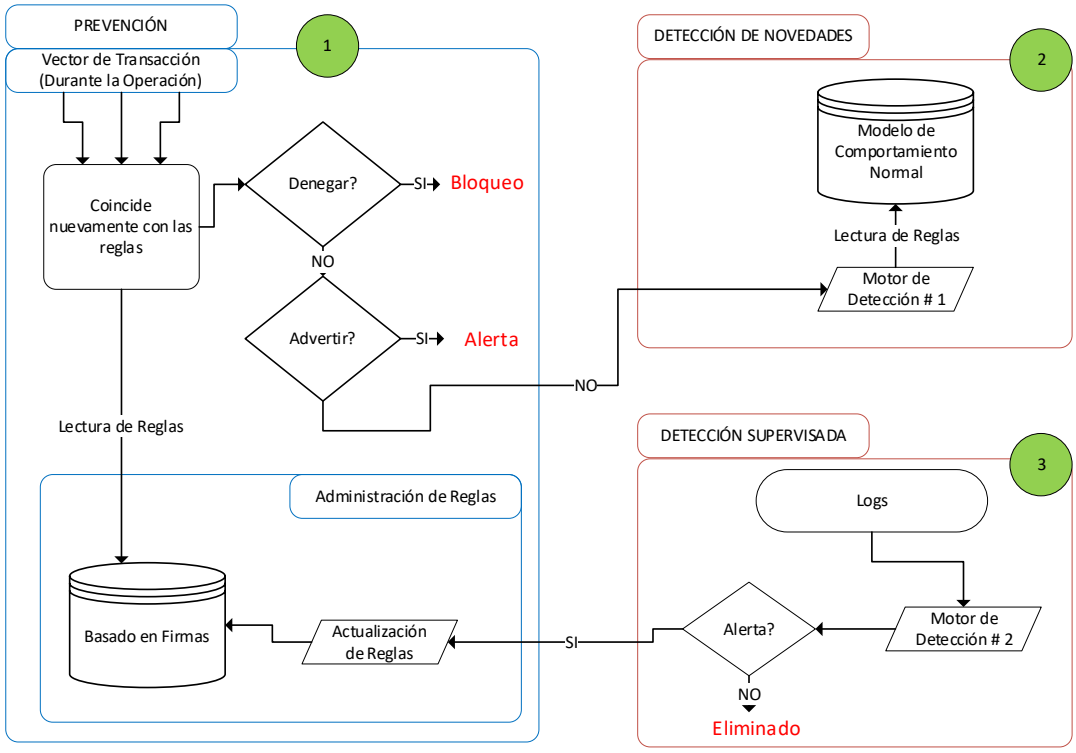
Propuesta de Implementación de DLP

Arquitectura

El sistema de DLP propuesto para TodoMed Ltda IPS consta de 2 fases principales, las cuales son PREVENCIÓN y DETECCIÓN. La Fase de Prevención está basada en firmas para prevenir ataques conocidos y reducir o minimizar la cantidad de alertas. La Fase de Detección se centra en detectar novedades a partir de un árbol de toma de decisiones para detectar ataques invisibles, detener propagación y prevenir la perdida de información. En el diagrama a continuación se pueden observar 3 etapas para la solución DLP, siendo estas, Etapa de Prevención, Etapa de Detección de Novedades y Etapa de Detección Supervisada:

Figura 16

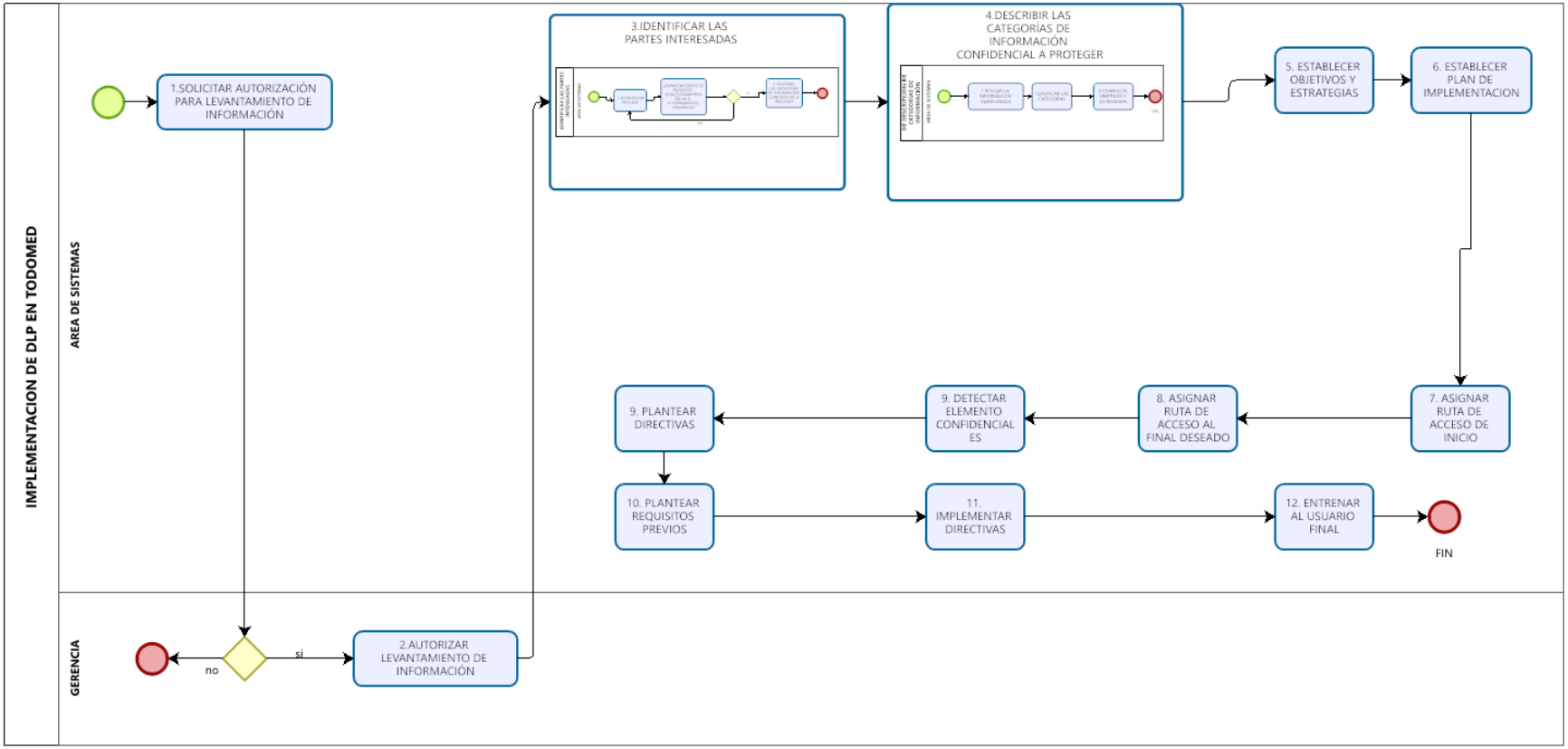
Sistema DLP Propuesto



Nota. Elaboración propia.

Figura 17

Propuesta de Implantación del DLP en TodoMed



Nota. Elaboración propia.

Etapa de Prevención

Para TodoMed Ltda IPS la propuesta abarca un primer nivel de protección o seguridad basado en firmas. Esta tecnología identifica comportamientos o patrones anormales de usuarios sospechosos incluidos en listas denominadas "Listas negras". Estas listas negras normalmente se construyen a partir de políticas o requerimientos propios de cada organización.

En la tabla a continuación, podemos ver un ejemplo de cómo un Administrador de TI puede establecer reglas de alertas o bloqueos a partir de la coincidencia de acciones ejecutadas por usuarios en los sistemas informáticos. El módulo de prevención de un Sistema DLP, puede describir o reconocer ataques potenciales a partir de esta información predefinida, por lo que está en la capacidad de bloquear eventuales ataques antes de que estos se llegaran a poner en marcha, sin embargo, no tiene el alcance para detectar o reconocer nuevos ataques que no estén identificados:

Tabla 14

Prevención en un sistema DLP

ID	Usuario	Contraseña	Comando	Lista	Nivel	Dirección IP
1	cperea	P@lmira$20	Ninguno	Ninguna	1	172.16.1.56
2	ppedroza	B$3cuR3#	Eliminar, Actualizar	Tabla1	2	172.16.1.33
3	llozano	Anita1234	Eliminar, Actualizar	Tabla1	2	172.16.1.27
4	ccamacho	YamahaR10	Cargar, Eliminar, Actualizar	Tabla2	2	172.16.1.76
5	emartinez	Sp1d3rm@n3	Cargar, Eliminar, Actualizar	Tabla2	2	172.16.1.221

Nota. Elaboración propia.

Etapa de Detección

Se implementará un sistema de detección de actividades y/o novedades mediante patrones de comportamiento normal de los usuarios. Estos son denominados o también conocidos como listas blancas. Estas listas blancas que almacenan patrones de comportamiento normal de los usuarios sirven para detectar desviaciones o comportamientos anormales de dichos usuarios cuando estos se produzcan.

El principal objetivo de los módulos de detección es cubrir lo que los módulos de prevención no pueden o tengan falencias.

Etapa de Detección Supervisada

En el segundo nivel de la fase de detección, los sistemas DLP permiten la implementación de un módulo de detección supervisa.

Normalmente, todas las acciones que un usuario ejecuta en un sistema informático se almacenan en un registro conocido también como log. De igual manera, este tipo de información siempre resulta compleja de leer para el ojo humano, por lo que la detección supervisada incluye herramientas que se encargan de tomar esta información, procesarla y detectar a partir de ella comportamientos normales o anormales de los usuarios en los sistemas de información. Ejemplos de estos comportamientos son, bloqueo de cuentas por intentos de acceso con contraseñas incorrectas, eliminación de archivos, creación de archivos, acceso a carpetas o documentos para los que el usuario está o no autorizado por políticas de la organización, etc.

En la implantación del DLP, es necesario el establecimiento de los objetivos y estrategias, ajustadas a la valoración del software de DLP que más se ajuste a los requerimientos de la empresa TodoMed, permitiendo ejecutar el plan de implementación, el acceso de inicio y final,

la detección de elementos confidenciales, la implementación de directivas y el entrenamiento al usuario final.

Algunas recomendaciones de software DLP se consignan a continuación:

Tabla 15

Recomendaciones de DLP

Nombre del DLP	Descripción
Check Point Data Loss	Protege preventivamente a la empresa de la pérdida involuntaria de información valiosa y confidencial, además de monitorear el movimiento de los datos, cumpliendo con estándares y normativas. (Check Point, 2022)
ManageEngine Device Control Plus	Permite controlar, bloquear y monitorear dispositivos USB y periféricos para evitar el acceso no autorizado a sus datos confidenciales, además de proteger los datos de personal no autorizado. (Manageengine, 2022)
McAfee Total Protection for DLP	Protege rápida y eficazmente los datos de la compañía sin importar donde se encuentren. Realiza análisis en minutos y tiene una ampliación para abordar políticas a la nube. (McAfee , 2019)
SecureTrust DLP Discover	Evalúa y mejora de forma proactiva la postura de seguridad de las empresas, además de eliminar el problema de cumplimiento de la industria de tarjetas de pago (PCI), la privacidad de datos y la gestión de riesgos para grandes y pequeñas empresas. (Securtrust, 2022)
Symantec Data Loss Prevention	Ayuda a comprender cómo se utiliza la información confidencial en la compañía, estableciendo que datos hay y quién los maneja. Este DLP escanea computadoras portátiles y dispositivos móviles, recursos compartidos

	de archivos de red, bases de datos y aplicaciones en la nube autorizadas y no autorizadas, como Office 365, G-Suite, Box y Salesforce. (Broadcom, 2022)

Nota. Elaboración propia.

Se hace aclaración que la selección del DLP se debe hacer con aprobación de la alta dirección, por lo que el alcance de este proyecto determinó la sugerencia de algunos ejemplos.

Por último, la educación debe estar abordada desde la sensibilización, el entrenamiento y la educación formal, para que cada empleado comprenda la importancia de protegerla información de la organización y se pueda capacitar adecuadamente al personal involucrado en el seguimiento y control, de tal manera que se mitigue la pérdida de la información.

Conclusiones

Los riesgos de seguridad identificados en la empresa TodoMed fueron que, el activo SI2T, puede estar amenazado por vulnerabilidades o errores del software, software malicioso y pérdida de datos; la historia clínica puede verse afectada por amenazas tales como la divulgación de información sensible y manipulación de información; la fórmula médica puede estar afectada por la manipulación de información; la factura electrónica puede estar amenazada por la manipulación de información, vulnerabilidades o errores del software, abuso de autorizaciones e interrupción del suministro de red; la orden de compra de insumos, medicamentos y equipos se puede afectar por la violación de leyes o regulaciones, la mala planificación o falta de adaptación y la manipulación de información; los soportes médicos puede estar expuestos a amenazas tales como la divulgación de información sensible, la manipulación de información y el fuego; las factores POS y NO POS, se pueden ver afectadas por violaciones de leyes o regulaciones, manipulación de información y vulnerabilidades o errores del software; el PDF e ordenamiento POS y NO POS se puede ver impactados por las vulnerabilidades o errores del software y la pérdida de datos y por último, las autorizaciones POS, pueden estar expuestas a abuso de autorización.

La propuesta de protección de datos está compuesta por cuatro etapas que son el diagnóstico, la planificación, la implementación y la mejora continua; en la primera etapa se contempla la consolidación del inventario de activos, la valoración y evaluación de riesgos y la priorización de estos; seguido de la segunda etapa compuesta por la determinación del alcance, la asignación de roles, la determinación de acciones y la asignación de recursos; dando continuidad al proceso por medio de la tercera etapa, compuesta por la creación de la política de seguridad y privacidad de la información, los procedimientos de seguridad de la información, el

establecimiento de los roles, la gestión del riesgos desde la perspectiva del ciclo PHVA y el plan de comunicaciones; por último, se tiene la cuarta etapa compuesta por la autoevaluación del modelo y la gestión de mejoras.

La propuesta de modelo de prevención de pérdida de información de historias clínicas de TodoMed está basado en un DLP, en el que se tiene en cuenta la estructuración de los activos, la categorización de los datos, el establecimiento de políticas de gestión, la implantación futura de un programa DLP, el control y seguimiento y la educación de los empleados. Las etapas a tener en cuenta son el levantamiento de los datos, la identificación de las partes interesadas, la descripción de las categorías de información, el establecimiento de objetivos y estrategias, el establecimiento del plan de implementación, la asignación de la ruta de acceso, la asignación de la ruta final de acceso, la detección de elementos confidenciales, el planteamiento de directivas, el planteamiento de requisitos previos, la implementación de directivas y el entrenamiento del personal.

Recomendaciones

Es importante que la empresa TodoMed realice acciones orientadas a la protección de la información, especialmente aquellas que mitiguen el impacto de riesgos como la manipulación de la información, la divulgación de información sensible y las vulnerabilidades o errores de software.

Para el establecimiento de la propuesta de protección de datos, es importante que la empresa TodoMed esté en un constante seguimiento al manejo de la información, de tal manera que las acciones que se implementen puedan ser evaluadas para estar involucrando la mejora continua.

El uso de las Tecnologías de la Información y Comunicación a través de un programa DLP, le permitiría a la empresa TodoMed poder automatizar los procesos que mitiguen el impacto de los riesgos de la seguridad, por lo que se debe elegir el que más sea compatible con el software que maneja las historias clínicas y que tenga en cuenta todos los diferentes tipos de información que se manejan en la organización.

Es importante que la empresa TodoMed inicie la estructuración para la implementación del modelo de prevención de perdida de datos DLP.

Referencias Bibliográficas

Achury, N. (2018). *Vulnerabilidades de las historias clínicas digitales ocasionadas por los Trabajadores de salud.* https://repository.unad.edu.co/bitstream/handle/10596/25666/%20naachuryp.pdf;jsessionid=901D1353A23072861E9C7440E64F775E.jvm1?sequence=1

Álvarez, C. (2018). *¿Qué es GDPR?: La nueva ley europea de protección de datos.* https://www.bbva.com/es/gdpr-nueva-ley-europea-proteccion-datos/

Alzate, G., & López, Y. (2021). *El tratamiento de datos personales de los pacientes colombianos con enfermedades crónicas en telemedicina.* http://repository.unaula.edu.co:8080/bitstream/123456789/2057/1/unaula_rep_pre_der_2021_tratamiento_datos_personales.pdf

Araujo, E. (2022). *Cómo mantener los datos de sus pacientes en completo sigilo.* https://espanol.apolo.app/como-mantener-datos-de-pacientes-sigilo/

Broadcom. (2022). *Prevención de pérdida de datos.* https://www.broadcom.com/products/cyber-security/information-protection/data-loss-prevention#:~:text=Symantec%20Data%20Loss%20Prevention%20(DLP,your%20information%20everywhere%20it%20goes.

CEPAL. (2021). *Tecnologías digitales para un nuevo futuro.* https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf

Check Point. (2022). *Prevención de pérdida de datos (DLP).* https://www.checkpoint.com/es/quantum/data-loss-prevention/

Congreso de Colombia. (2020). *Ley 2015* . https://dapre.presidencia.gov.co/normativa/normativa/LEY%202015%20DEL%2031%20DE%20ENERO%20DE%202020.pdf

Congreso de la República. (2012). *Ley 1581.* https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

Cristea, L. (2017). *La protección de datos de carácter sensible en el ámbito Europeo.* https://www.tdx.cat/bitstream/handle/10803/442972/Tlcu.pdf?sequence=1&isAllowed=y

Doğantekin, V. (2019). *Los informantes que han transformado el escenario político.* https://www.aa.com.tr/es/mundo/los-informantes-que-han-transformado-el-escenario-pol%C3%ADtico/1448386

Endpoint Protector. (2022). *Data Loss Prevention para Salud.* https://www.endpointprotector.es/solutions/healthcare

Endpoint Protector. (2022). *Software de Prevención de Pérdida de Datos (DLP) líder en la industria.* Obtenido de https://www.endpointprotector.es/lp/endpoint-protector-3?utm_term=data%20loss%20prevention&utm_campaign=837915060&utm_content=&utm_source=google&utm_medium=cpc&CID=837915060&CK=data%20loss%20prevention&CAP=&utm_term=data%20loss%20prevention&utm_campaign=L

Fernández, G. (2015). *Elementos de sistemas operativos,de representación de la información y de procesadores hardware y software.* https://oa.upm.es/36552/1/SORYP.pdf

Grupo Evaluando. (2020). *Amenazas y riesgos de la nube.* https://evaluandocloud.com/amenazas-riesgos-la-nube/

Grupo RGI. (2021). *Planeación estratégica.* https://www.rgi.com.co/planeacion-estrategica-que-es-y-para-que-sirve/

Gutiérrez, D. (2020). *Fuentes y medios de prueba electrónicos, dotación de seguridad jurídica a los documentos electrónicos.* https://repository.ucatolica.edu.co/bitstream/10983/24711/1/Art%C3%ADculo%20de%20grado%207%C2%B0%20Final%20definitivo%20Julio-20%20Diego%20Guti%C3%A9rrez.pdf

Helpsystems. (2021). *Tecnologías para una estrategia de Seguridad de Datos por capas.* Obtenido de https://www.helpsystems.com/es/blog/tecnologias-para-una-estrategia-de-seguridad-de-datos-por-capas

Incibe. (2018). *Introducción a los sistemas embebidos.* https://www.incibe-cert.es/blog/introduccion-los-sistemas-embebidos

Incibe. (2018). *Si manejas información de tarjetas bancarias, este artículo te interesa.* https://www.incibe.es/protege-tu-empresa/blog/si-manejas-informacion-tarjetas-bancarias-este-articulo-te-interesa

Incibe. (2019). *DLP protege tus datos contra fugas de información.* https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

Incibe. (2019). *DLP protege tus datos contra fugas de información.* https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

Intelligenia. (2017). *Guía sobre Seguridad Informática o Ciberseguridad.* http://blog.intelligenia.com/2017/11/guia-seguridad-informatica-ciberseguridad.html

Isotools. (2017). *Sistemas de Gestión de Riesgos y Seguridad.* https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

Manageengine. (2022). *l motor que impulsa la protección de datos.* https://www.manageengine.com/latam/device-control/

McAfee . (2019). *McAfee Total Protection for Data Loss Prevention.* https://www.mcafee.com/enterprise/en-us/assets/solution-briefs/sb-total-protection-for-dlp.pdf

Microsoft. (2018). *¿Qué es la informática en la nube?* https://azure.microsoft.com/es-es/overview/what-is-cloud-computing/#uses

Ministerio de las TIC. (2020). *MinTIC divulga la Ley que regula el intercambio de información para la historia clínica.* Obtenido de https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/126025:MinTIC-divulga-la-Ley-que-regula-el-intercambio-de-informacion-para-la-historia-clinica

OEA. (2019). *Desafíos de riesgo cibernético en el sector financiero para Colombia y América Latina.* Obtenido de https://www.oas.org/es/sms/cicte/docs/Desafios-del-riesgo-cibernetico-en-el-sector-financiero-para-Colombia-y-America-Latina.pdf

Ostec. (2015). *DLP: ¿Qué es y cómo funciona?* Obtenido de https://ostec.blog/es/seguridad-perimetral/dlp-que-es-y-como-funciona/

Portafolio. (2017). *Siete consejos para proteger los sistemas informáticos de su compañía.* Obtenido de https://www.portafolio.co/innovacion/siete-recomendaciones-para-proteger-los-sistemas-informaticos-de-su-compania-506755

Powerdata. (2022). *Seguridad de datos: En qué consiste y qué es importante en tu empresa.* Obtenido de https://www.powerdata.es/seguridad-de-datos#:~:text=En%20l%C3%ADneas%20generales%2C%20seguridad%20de,datos%20de%20una%20posible%20corrupci%C3%B3n.

Securtrust. (2022). *Soluciones de riesgo y cumplimiento de clase mundial.* https://www.securetrust.com/

Torres, J. (2020). *valuación de vulnerabilidades de seguridad en Software Android en el año 2021*. https://revistas.ulatina.ac.cr/index.php/tecnologiavital/article/download/465/586?inline=1

Vega, W. (2018). *Políticas y seguridad de la información.* http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

Zaragoza, J. (2020). *Análisis y comparación de algoritmos de detección de anomalías.* https://riunet.upv.es/bitstream/handle/10251/150529/Zaragoza%20-%20An%C3%A1lisis%20y%20comparaci%C3%B3n%20de%20algoritmos%20de%20detecci%C3%B3n%20de%20anomal%C3%ADas.pdf?sequence=1