Adaptación de una Metodología Para el Análisis y Gestión de Riesgos Informáticos Para Organizaciones del Sector Salud en Colombia

Jorge Asdrúbal Tamayo Reinel

Proyecto de Grado Para Optar al Título de

Magister en Gestión de Tecnología de Información

Director

Roberto Mauricio Cárdenas C

Máster Universitario en Elearning y Tecnología Educativa

Línea de Profundización: Proyecto Aplicado (Gestión de Seguridad en TI)

Universidad Nacional Abierta y a Distancia

Escuela de Ciencias Básicas, Tecnologías e Ingeniería

Maestría en Gestión de Tecnología de Información

Bogotá D.C.

2020

Agradecimientos

A la Universidad Nacional Abierta y a Distancia UNAD por brindar espacios de aprendizaje de calidad para todos los colombianos. A su cuerpo docente, en especial a mi Director de Proyecto Máster Roberto Mauricio Cárdenas C, por su constante guía y acertadas recomendaciones.

Dedicatoria

A mis padres por su guía y constante apoyo, en especial en los momentos más difíciles.

A mi hija por ser mi más profunda inspiración.

A mi esposa por su cariño y comprensión.

Resumen

Título: Adaptación de una Metodología Para el Análisis y Gestión de Riesgos Informáticos Para Organizaciones del Sector Salud en Colombia.

Palabras Clave: Seguridad TI, Health IT, Historia Clínica, Metodología, Riesgo Informático.

Descripción: Dentro de un posible marco de amenazas, vulnerabilidades y sus correspondientes eventos probables no deseados, es necesaria la aplicación de metodologías de evaluación y gestión de riesgos informáticos, es así, como es común recurrir a distintos métodos de evaluación y gestión, pero al ser estos muchas veces generales, no tienen en cuenta características propias de los procesos informáticos dedicados al sector salud. En algunos casos encontramos metodologías que no categorizan la información, siendo los registros médicos personales información sensible de acuerdo con la legislación colombiana, también es posible encontrar algunas metodologías que proponen la evaluación y categorización del impacto, pero debido a las consecuencias nefastas que tiene para la vida de una persona la perdida de la confidencialidad de su historia clínica, su impacto es siempre catastrófico.

El presente trabajo de grado desarrolla una propuesta que se encamina a la selección y adaptación de una metodología de análisis y gestión de la información que incorpore parámetros que permitan tener en cuenta las particularidades del medio colombiano como también la extrema importancia que guarda la información personal de pacientes.

Abstract

Title: Adaptation of a methodology for analysis and management of information technologies risks for organizations in the Colombia health sector

Keywords: IT Security, Health IT, Clinic History, Methodology, IT Risk

Description: Within a possible framework of threats, vulnerabilities and their corresponding and derived probable unwanted events, the application of computer risk assessment and management methodologies is necessary, which is how it is common to use different evaluation and management methods, but at Being these many times general, they do not take into account characteristics of the computer processes dedicated to the health sector. In some cases we find methodologies that do not categorize the information, with personal medical records being sensitive information in accordance with Colombian legislation, it is also possible to find some methodologies that propose the evaluation and categorization of the impact, but due to the dire consequences it has for A person's life the loss of the confidentiality of their medical history, its impact is always catastrophic.

This degree project develops a proposal that is aimed at the selection and adaptation of an analysis and information management methodology that incorporates parameters that allow taking into account the particularities of the Colombian environment as well as the extreme importance of patient personal information.

Tabla de Contenido

Lista de Figuras

Lista de Tablas

Introducción

Los sistemas de información dentro de las instituciones enmarcadas en el sector de la salud han cobrado especial relevancia a nivel mundial en las últimas décadas, debido a las grandes ventajas que supone tener acceso al historial clínico de pacientes de forma rápida, económica y eficiente por parte de los distintos actores que participan en los procesos de atención, pero así mismo dichos sistemas de información son susceptibles de riesgos de seguridad. Los Sistemas Electrónicos en Salud (EHS) tienen varias ventajas, como la disminución de costos de atención médica y un procesamiento más rápido y eficiente. Sin embargo, el uso de EHS aumenta las preocupaciones en seguridad, privacidad e integridad de los datos producto de la atención médica (Yüksel et al., 2017).

Dentro de la importancia que tiene la debida gestión de la seguridad de la información en cualquier tipo de organización, sea o no parte del sector salud, esta el hecho de mantener su integridad, privacidad y disponibilidad, pero si hablamos de pequeñas o grandes instituciones que prestan servicios en salud, nos encontramos con el agravante que este tipo de instituciones realizan el tratamiento de información personal de carácter médico de pacientes, que incluye datos acerca de enfermedades, tratamientos, salud mental, medicación o condiciones específicas de los pacientes, así como, puede contener datos biométricos, genéticos , raza y en otros casos puede llegar a permitir inferir otros datos como etnia e incluso la orientación sexual, por tal razón la legislación colombiana a través de la ley 1581 de 2012 cataloga esta información como

sensible, por lo que se hace necesario, aun más, la aplicación de metodologías de evaluación y gestión de riesgos informáticos.

A nivel organizacional es común recurrir a distintos métodos de análisis, evaluación y gestión de riesgos aplicados a organizaciones, pertenecientes o no al sector salud, pero al ser estas metodologías de carácter general, no tienen en cuenta características propias de los sistemas informáticos dedicados a soportar procesos de carácter médico.

Es así como a nivel internacional se hace una diferenciación entre privacidad y tratamiento de información relativa a pacientes de instituciones médicas e información producida y tratada por otro tipo de organizaciones, por tal motivo se aplican marcos normativos diferenciados y metodologías específicas en el gobierno y gestión de la información personal concerniente a pacientes y funcionarios de instituciones médicas.

En el presente documento se analizarán distintas perspectivas que buscan solucionar la anterior problemática, así como, encontrar las particularidades más importantes que diferencian al medio colombiano de otros países y así encontrar una metodología de análisis y gestión de riesgos informáticos, que sea capaz de hacer parte de un Sistema de Gestión de Seguridad de la Información (SGSI) para organizaciones pertenecientes al sector salud colombiano.

Planteamiento del Problema

La salvaguarda de la información en los sistemas informáticos ha sido una preocupación permanente tanto para usuarios, profesionales de la información como para los entes reguladores, de tal forma se han desarrollado diferentes metodologías y procedimientos encaminados al análisis y evaluación de riesgos en la seguridad de la información, ahora cuando se aborda la seguridad de información de carácter médico, sanitario o historial clínico de pacientes en instituciones del sector salud e instituciones conexas vinculadas contractualmente con las primeras, que a su vez hacen tratamiento de la mencionada información, se hace necesario un especial cuidado debido a la alta sensibilidad de la misma en razón al alto impacto que puede tener la perdida de la confidencialidad en la información del paciente, el daño irreversible que supone la fuga de información médica privada, como una enfermedad o cierta condición de salud, puede afectar de forma devastadora a un individuo (Joint NEMA/COCIR/JIRA, 2007).

Es de tener presente que los sistemas que soportan la actividad en el sector salud son complejos en varios aspectos, que se encuentran a la par de otros contextos como los centros nucleares, la aviación y la defensa militar, en razón a la complejidad de cada organización, el error y la posibilidad de accidentes que no es posible eliminar, así que se deben utilizar todas las acciones posibles para que estas sean, al menos, controlables (Verbano & Turra, 2010, p. 625).

El análisis y gestión de los riesgos informáticos en organizaciones en el sector de la salud no es una responsabilidad exclusiva de centros de salud, clínicas u hospitales, sino que se comparte con todos aquellos que se relacionan con el sector y por su puesto con los entes

gubernamentales. Garantizar la seguridad de los Registros Electrónicos de Salud (EHR) requiere una responsabilidad compartida entre entidades, que incluyen a los desarrolladores de sistemas de información EHR y aquellos en la organización de atención sanitaria que son responsables de configurarlos, implementarlos y usarlos junto con los reguladores gubernamentales que crean las políticas que rigen su diseño, desarrollo y uso (Sittig et al., 2018, p. 7).

Los riesgos informáticos que se presentan en las instituciones con actividades en el sector salud derivan de la misma complejidad de los sistemas de información que a su vez involucran distintos componentes y arquitecturas, donde intervienen componentes de Software, hardware, dispositivos de red y telecomunicaciones entre otros, un ejemplo muy general de la configuración de un sistema de información en el sector de la salud se puede observar en la Figura 1.

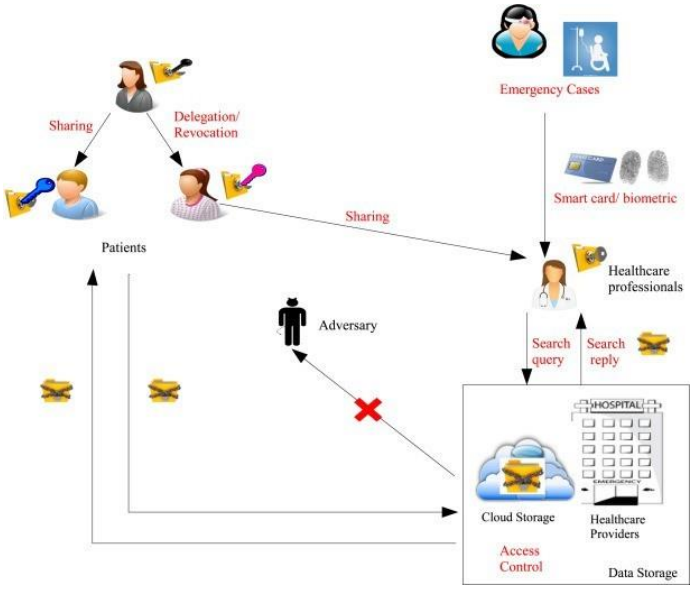

Figura 1. Visión general de configuración de los servicios informáticos en el área de la salud. Fuente: "Research issues for privacy and security of electronic health services" por Yüksel et al., 2016, Future Generation Computer Systems, 68, p. 2. Copyright 2016 por Elsevier B.V.

No se pueden ocultar las claras diferencias que existen entre empresas netamente comerciales, industriales o bancarias comparadas con organizaciones enmarcadas dentro del sector salud, estas últimas tienen en la gran mayoría de casos la misión de velar por la vida humana, por lo cual sus procesos misionales son críticos desde todo punto de vista.

"Por ejemplo, si bien la mayoría de los bancos o empresas pueden cerrar en el caso de un desastre natural o un grave problema de TI, un establecimiento de atención médica, en general, debe permanecer abierto. La operación bajo condiciones adversas es esencial para tratar a pacientes actuales y para mantener y restablecer la salud de la comunidad en caso de un desastre" (Joint NEMA/COCIR/JIRA, 2007, p. 3).

Lo anterior deriva en una preocupación que se percibe en la comunidad internacional, por ejemplo investigaciones han demostrado que los adultos estadounidenses de todas los rangos de edades consideran que sus datos de salud se encuentran entre los más sensibles de la información personal y por tal razón los clasifican en segundo lugar dentro una lista de diferentes tipos de información (Pereira et al., 2017, p. 2).

En general cada paciente que visita a un profesional de la salud espera que su información personal, que es necesaria para procesos de diagnósticos o documentación como imágenes o fotografías, sea mantenida con la mayor reserva por parte del profesional, "la expectativa que tiene y desean los pacientes en cuanto a la confidencialidad con respecto a su información personal de atención médica comienza con la misma relación tradicional médico-paciente" (Sutton, 2013, p. 1177).

Bajo el panorama anterior era de esperar procesos de análisis y gestión de riesgos de la información, siendo estos componentes indispensables en un Sistema de Gestión de Seguridad de

la Información (SGSI), de forma extendida y presentes en la mayoría de las instituciones Prestadoras de servicios de Salud (IPS) a nivel mundial y por su puesto en Colombia, pero de acuerdo a las estadísticas de la "International Organization for Standardization" (ISO), las organizaciones cuyos SGSI se apegan de forma comprobable a unos de los estándares de seguridad más reconocidos y aceptados a nivel mundial como lo es la norma ISO/IEC 27001:2013, contadas a partir de la cantidad de certificaciones expedidas por la ISO a instituciones del sector salud llega a la cifra de sólo 278 para el año 2018 a nivel mundial, de un total de 28931 certificaciones entregadas, con lo cual el sector salud se ve con una participación aproximada del 0,96% , ahora para Colombia el panorama no es más alentador, ya que tan solo una (1) organización del sector salud registra dicha certificación que representa aproximadamente el 0,74% del total (International Organization for Standardization, 2018).

Es de notar que la conformidad al estándar ISO/IEC 27001:2013 es independiente a la metodología para análisis y gestión de riesgos seleccionada, pero si es punto importante e ineludible y solicitado por dicha norma la realización de este proceso bajo cualquiera de la variedad de metodologías o marcos de trabajo "Frameworks" existentes, de una forma constante y consistente como parte de un ciclo de mejoramiento continuo. Mas sin embargo hasta el momento no se encontraba ningún estudio que analice la conveniencia de la adopción de una metodología u otra en particular para el medio colombiano, que tenga en cuenta las particularidades de este y en especial que facilite su implementación con miras a mejorar el indicador de SGSI conformes a la norma ISO/IEC 27001 en Colombia.

Justificación

Las instituciones pertenecientes al sector salud en Colombia manejan gran variedad de información relativa a sus procesos propios misionales y otros de apoyo de los primeros, una parte muy importante de toda esta información corresponde a la información de carácter médico de sus usuarios, denominados pacientes, dentro de esta información encontramos las historias clínicas, que desde hace unas décadas atrás han tenido un proceso de migración del papel a sistemas de información digitales dadas las ventajas que supone las nuevas tecnologías de la información, "las organizaciones sanitarias necesitan de la informatización de sus procesos de soporte, lo que ha conllevado en los últimos años una transformación digital de dichas organizaciones" (Altés Jordi, 2013) y como lo menciona el (MinTic, 2010) al hacer referencia a la adopción de medio digitales para el tratamiento de la información, "los medios electrónicos se han constituido en un canal que permite su acceso de manera ágil y sencilla, a la vez que facilitan la mejora en la calidad de los servicios así como ahorros en costos y tiempos de acceso".

Pero así mismo como se masifican tales sistemas de información dadas sus bondades, se deberá garantizar la confidencialidad de dicha información en vista a que ciertamente la perdida de la confidencialidad podrá traer graves consecuencias para los pacientes. Dentro de las ventajas de los Sistemas Electrónicos en Salud (EHS) tenemos la disminución de costos de atención médica y un procesamiento más rápido y eficiente. Sin embargo, el uso de EHS aumenta las preocupaciones en seguridad, privacidad e integridad de los datos producto de la atención médica (Yüksel et al., 2017, p. 2).

Dentro de la importancia que tiene la debida gestión de la seguridad de la información de carácter médico de pacientes se encuentra el hecho que esta incluye datos acerca de enfermedades, salud mental o condiciones específicas de los pacientes, datos biométricos y genética que en dado caso permite inferir datos como raza, etnia e incluso la orientación sexual, tal información sobre una persona es desde todo punto de vista sensible, por tal razón es necesaria la aplicación de metodologías de evaluación y gestión de riesgos informáticos muy estrictas.

Debido a la alta importancia que tiene mantener la privacidad de la información de los pacientes, se han discutido y desarrollado gran variedad de estudios a nivel internacional en busca de metodologías, modelos de análisis y marcos de trabajo que permitan minimizar los riesgos de seguridad de la información y de los sistemas de información que sirven de herramientas, inclusive desde la fase de diseño de los últimos, "la realización de Sistemas de información de salud (HIS) requiere una evaluación rigurosa que aborde los problemas de tecnología, humanos y de organización" (Yusof et al., 2008, p. 386), lo anterior sumado al hecho de la alta complejidad que involucran los distintos procesos misionales de las instituciones médicas ha resultado en variados puntos de vista y teorías.

> *"En los últimos años, los sistemas de las organizaciones del sector salud han estado involucrados en una serie de distintos cambios, que van desde los tecnológicos a los normativos, y todos piden una mayor eficiencia. Además, el progreso biomédico en las últimas décadas ha contribuido a elevar el nivel de complejidad organizativa en los hospitales ..."* (Cagliano et al., 2011, p. 695).

Dada la extrema importancia que tiene la información personal de pacientes, contratistas y trabajadores del sector salud, extraña la casi nula conformidad de las IPS en Colombia a la norma ISO/IEC 27001:2013, que de alguna forma en mayor o menor grado entrega un indicador importante de la exitosa adopción de un SGSI, que ratifique un proceso de análisis y gestión de riesgos constante y permanente, dado que estos no pueden ser esfuerzos de un único momento y que se deben adaptar y mejorar debido a un repertorio de riesgos en constante cambio y evolución. Es así como la adopción de una metodología o marco de trabajo en el análisis y gestión de riesgos de la información, que tenga en cuenta las particularidades del sector salud en Colombia sería un muy buen vehículo facilitador para promover su implementación de forma exitosa dentro de un SGSI.

Objetivos

3.1 Objetivo General

Desarrollar una estrategia de evaluación e implementación de una metodología para gestión y análisis de riesgos informáticos derivados del tratamiento de la información confidencial y de carácter sensible de pacientes de instituciones del sector salud colombiano, aplicando un análisis cualitativo de los marcos de trabajo existentes en la gestión de la seguridad de la información.

3.2 Objetivos Específicos

- Analizar distintas metodologías de análisis y gestión de riesgos en tecnologías informáticas con una posible aplicación a un marco organizacional relacionado con el sector de la salud.
- Seleccionar la metodología que, de acuerdo con análisis previo, mejor se adapte a las particularidades del medio colombiano y su sector de la salud.
- Adaptar la metodología seleccionada para evaluar y gestionar riesgos informáticos derivados del tratamiento de la información confidencial y de carácter médico de pacientes de instituciones del sector salud en Colombia.

Marco Referencial

4.1 Estado del Arte

Existen distintas metodologías para el análisis y gestión de riesgos de la información aplicados a distintos tipos de organizaciones, los cuales pueden hacer parte de un sistema de gestión de seguridad de la información para el cumplimiento o no de un marco normativo, como por ejemplo la norma ISO/IEC 27001, pero siempre con el objetivo claro de mitigar los riesgos asociados a la seguridad de la información.

Para cumplir con el objetivo anterior se han construido distintas metodologías "entre las principales propuestas para el análisis y gestión del riesgo se puede destacar MAGERIT, OCTAVE o CRAMM" (Santos Olmo Parra et al., 2016, p. 2898), y también se han desarrollado distintos trabajos en el sentido de aplicar con éxito las primeras, en organizaciones del sector salud en Colombia, tal es el caso de los trabajos realizados por los siguientes autores:

José Leonardo Cordero Moreno y Yadimyr Oswaldo García Reyes que desarrollaron el proyecto "Análisis de riesgos y recomedaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo, Santander" cuyo objetivo general era realizar el análisis de riesgos y recomendaciones en los niveles de seguridad informática mediante el uso de aplicaciones que permitan evidenciar vulnerabilidades en los sistemas de información y telecomunicaciones del Hospital E.S.E. San Bartolomé de Capitanejo, Santander.

Hector Ricardo Triana Acevedo que desarrolló el proyecto de "Diagnóstico y planeación del modelo de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, E.S.E.", el cual tuvo como objetivo realizar el diagnóstico y planeación del modelo de

gestión de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, E.S.E.

Henry Eduardo Bastidas Paruma, Ivan Arturo López Ortiz y Hernando José Peña Hidalgo, los cuales desarrollarón el proyecto de "Análisis de riesgos y recomedaciones de seguridad de la información al area de información y tecnología del hospital Susana López de Valencia de la ciudad de Popayán", que tenía como objetivo general el diseñar mejoras a los niveles de seguridad informática mediante la aplicación del proceso de análisis y evaluación de riesgos de seguridad de la información en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital Susana López de Valencia E.S.E de la ciudad de Popayán.

A nivel internacional se han formulado distintas metodologías para abordar las particularidades de sectores productivos especificos, como el desarrollado por Antonio Santos-Olmo, Luis Enrique Sánchez, Esther Álvarez, Monica Karel Huerta y Eduardo Fernández-Medina, dirigida a empresas clasificadas como PYME (Pequeña y Mediana Empresa) con posible aplicación a organizaciones del sector salud, titulado como "Metodología para el análisis dinámico y gestión de riesgos en ISO27001", con el objetivo de presentar una nueva metodología, llamada MARISMA, destinada a llevar a cabo un análisis de riesgos simplificado y dinámico, que sea válido para todas las empresas, incluidas las PYME, y para proporcionar soluciones a los problemas identificados durante la aplicación del método denominado "Action Research".

Para el caso de las organizaciones pertenecientes al sector salud, el trabajo realizado por el consorcio Joint NEMA/COCIR/JIRA Security and Privacy Committee (SPC) que desarrolló un trabajo de forulación de "Gestión de riesgos de seguridad de la información para sistemas de

salud” con el objetivo de describir un proceso que pueda utilizarse para diseñar sistemas relacionados con el sector salud. También para aplicar la misma metdología a los centros de salud para evaluar y mitigar riesgos de seguridad de TI asociados a los datos y los sistemas.

4.2 Marco Conceptual y Teórico

Descripción de Metodologías en el Análisis y Gestión de Riesgos Informáticos Aplicadas en el Sector Salud.

Desde el punto de vista tradicional “Existen dos pilares fundamentales para realizar el análisis de riesgos: los estándares y normas, de un lado, y las metodologías, de otro” (Gómez et al., 2010, p. 109), desde cualquiera de los dos pilares es necesario una correcta aplicación dependiendo de los procesos y tipo de información propios de cada organización, así como de las características de los sistemas informáticos que generan de alguna forma riesgos en la seguridad y privacidad de la información en el sector de la salud, mostradas en la Figura 2.

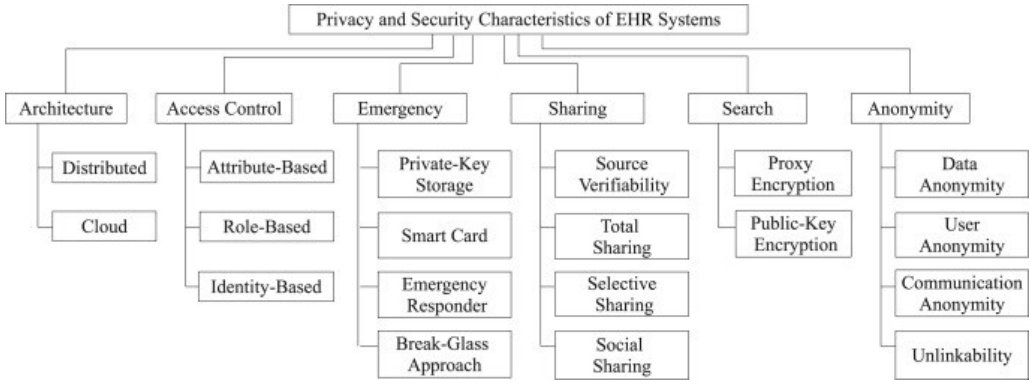

Figura 2. Clasificación de las características de privacidad y seguridad en sistemas informáticos en el sector de la salud.
Fuente: “Research issues for privacy and security of electronic health services” por Yüksel et al., 2016, Future Generation Computer Systems, 68, p. 3. Copyright 2016 por Elsevier B.V.

Con el objetivo de la salvaguarda de la información y la minimización de los riegos informáticos inherentes a los procesos propios de cada organización "surge la necesidad de crear estándares para el análisis y gestión de riesgos; éstos se conocen comúnmente como Frameworks o Marcos de Trabajo" (Gómez et al., 2010, p. 112).

Ahora en el análisis, evaluación y gestión de riesgos de la información sensible de pacientes en el sector salud, ha sido abordada de varias formas, una opción es la adopción de una norma internacional de aplicación general como ISO 31000, distintos autores platean alternativas como utilizar y adaptar una metodología de carácter estándar o marco de trabajo tradicional, que no particulariza el tipo de información, como "OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) que consiste en una metodología desarrollada por el CERT/CC2 que tiene por objeto facilitar la evaluación de riesgos en una organización" (Gómez et al., 2010, p. 112), un ejemplo más lo encontramos en el uso de la metodología MAGERIT "es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos" (Cordero José & García Yadimyr, 2015, p. 22), así la metodología MAGERIT es usada por Cordero & García en el análisis y gestión de riesgos informáticos para una institución colombiana de tipo hospitalaria como caso de estudio.

En el caso de MAGERIT se trata de una metodología de análisis y gestión de riesgos de los sistemas de información elaborado por la "dirección general de modernización administrativa, procedimientos e impulso de la administración electrónica" perteneciente a la secretaría general técnica del ministerio de hacienda y administraciones públicas del gobierno de España, que se

enmarcan dentro de un modelo de gestión de riesgos tradicional compuesto por dos procesos principales, que se muestran en la figura 3.

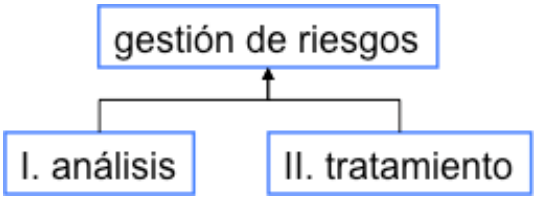

Figura 3. Actividades de la gestión de riesgos.
Fuente: "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" por Dirección General de Modernización Administrativa de España (Dirección General de Modernización Administrativa de España, 2012, p. 19).

Para cumplir las anteriores actividades la metodología MAGERIT establece tres fases principales:

Caracterización de los activos: identificación, clasificación, dependencias y valoración.

Caracterización de las amenazas.

Evaluación de las salvaguardas.

En las anteriores fases se resaltan los activos, las amenazas y las salvaguardas, siendo los primeros los elementos que componen o íntimamente relacionados con el sistema de información evaluado. Las amenazas son básicamente los posibles eventos relacionados con los activos que tienen efectos negativos para la organización y las salvaguardas son las medidas que tratan de evitar el daño producto de las amenazas.

A partir del desarrollo de las anteriores fases es posible concluir los impactos para la organización y el riesgo (probabilidad de materialización de una amenaza). A partir de las

salvaguardas y su eficacia se estima el riesgo residual como también el impacto residual, de esta forma se trata de limitar el posible daño como también la probabilidad de la materialización de la amenaza, en la figura 4 se muestra la estructuración de los diferentes elementos de análisis mencionados.

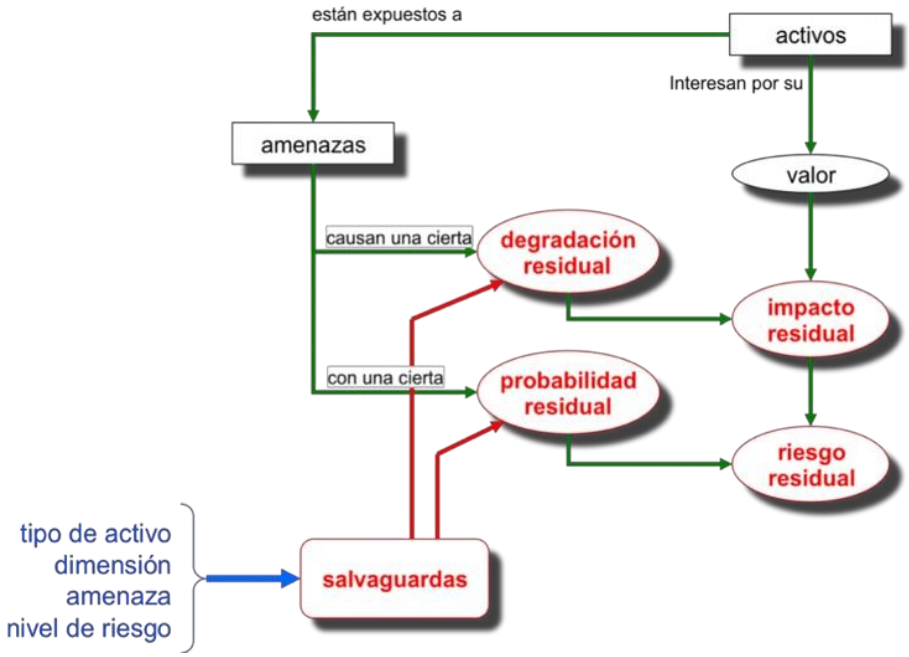

Figura 4. Elementos de análisis del riesgo residual.
Fuente: "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información" por Dirección General de Modernización Administrativa de España (Dirección General de Modernización Administrativa de España, 2012, p. 32).

Otro punto de vista es englobar el análisis de riesgos informáticos dentro del conjunto general de gestión de riesgos hospitalarios, tal es el caso de Cagliano, Grimaldi & Rafele que desarrollan una metodología sistémica para la gestión de riesgos en el sector sanitario en base al caso de estudio de una institución médica italiana que sugieren extrapolar con investigaciones futuras a otras organizaciones del sector salud, el marco de trabajo consiste en buscar dar forma

operativa a la teoría de “Reason” de fallas, mediante el desarrollo de una metodología para investigar los procesos de atención médica y los riesgos relacionados que afectan directa o indirectamente a los pacientes (Cagliano et al., 2011, p. 695).

En la anterior metodología se propone una serie de pasos que giran alrededor de la evaluación de confiabilidad humana en su interacción con los distintos procesos y elementos que componen el sistema hospitalario y que están dirigidas hacia la correcta atención y cuidado de los pacientes. Los mencionados pasos se resumen de la siguiente manera.

- Análisis del contexto.
- Mapeo de procesos.
- Identificación y evaluación de riesgos.
- Modos de falla y análisis de ineficiencias (FMEA–Waste analysis).

En el primer paso se analiza el contexto del sistema hospitalario, gracias a la obtención de información relevante a través de una cuidadosa consideración de documentos, como procedimientos de trabajo, organigramas, mapas de responsabilidad y planes de turnos, el equipo de trabajo obtiene un primer conocimiento de las actividades del proceso y flujos relacionados de información cuantitativa e información clínica y organizacional (Cagliano et al., 2011, p. 698).

En el mapeo de procesos se relacionan más en profundidad actividades y actores participantes responsables, a través del desglose de la estructura de actividades basado en tablas de flujo de procesos de acuerdo con las actividades identificadas.

En la fase de identificación y evaluación de riesgos se identifica la exposición total a riesgos de las actividades documentadas en el paso anterior, partiendo del entendimiento procedimental y deduciendo riesgos relacionados con cada actividad y lógicamente de la experiencia del grupo evaluador, referenciados de acuerdo con una estructura de riesgos desglosada, ver figura 5.

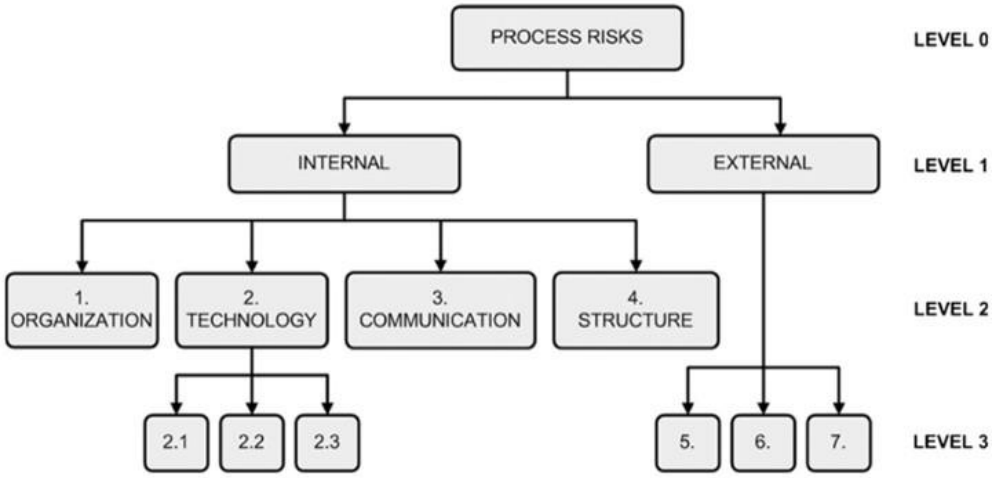

Figura 5. Desglose de estructura de riesgos.
Fuente: "A systemic methodology for risk management in healthcare sector" por Cagliano, Grimaldi & Rafele, 2011. Copyright 2011 por Elsevier Ltd.

En el último paso de "Modos de falla y análisis de ineficiencias", se definen una serie de tablas que relacionan un tipo especial de fallas con las actividades que impactan, que se podrían interpretar como amenazas al normal y deseado desempeño de las actividades consideradas. Dichas tablas están compuestas por un código de falla, la descripción del modo de falla, las fuentes de riesgos, la descripción de las causas, el método para detectar las fallas y las medidas sugeridas para mitigar las fallas, como también la valoración del éxito de la aplicación de las medidas sugeridas.

Pero al hablar de metodologías generalistas aplicadas en escenarios socio económicos difíciles, como los prevalecientes en Colombia en especial en el sector rural, el aspecto de recursos económicos disponibles para las instituciones del sector salud es limitado, por tanto la aplicación de estándares destacados que incorporan el análisis y gestión del riesgo informático, supone proyectos con elevados presupuestos de implementación y mantenimiento en las instituciones, "en relación con los estándares más destacados se ha podido constatar que la mayor parte de ellos han intentado incorporar procesos para el análisis y la gestión del riesgo, pero que son muy difíciles de implementar y requieren una inversión demasiado alta" (Santos Olmo Parra et al., 2016, p. 2898).

Sumado a lo anterior, el hecho de generalizar los estudios de seguridad en un plan de gestión integral de seguridad en instituciones médicas puede traer problemáticas derivadas del uso de metodologías no apropiadas en cada uno de los casos, aun cuando sus objetivos sean congruentes.

“Como mejor práctica, los procesos de administración de riesgos de seguridad de paciente, operador y de seguridad de TI deben estar separados pero vinculados. Difieren tanto en el vocabulario como en los conocimientos necesarios para una adecuada gestión del riesgo. Si se combina como un único proceso de evaluación, uno u otro no se trata adecuadamente” (Joint NEMA/COCIR/JIRA, 2007, p. 2).

Es necesario tener en cuenta que antes de la aplicación de una metodología cualquiera, es necesario entender las particularidades y complejidades que tienen las organizaciones ubicadas dentro del sector salud, en vista que el éxito de un proyecto de análisis y gestión de riesgos informáticos depende de los lineamientos estratégicos organizacionales y los procesos

misionales, que para el caso de instituciones médicas son particulares y muy diferenciados de otras organizaciones.

"… estándares o métodos sin una visión estratégica clara es el gran riesgo que se corre al aplicar de forma independiente o en forma desarticulada, los diferentes modelos o metodologías, los cuales se vuelven un fin en sí mismos y que no tengan un foco estratégico claro" (Gómez et al., 2010, p. 117).

Del otro lado tenemos metodologías de análisis y gestión de riesgos informáticos específicas, que permiten en primera medida la introducción de mecanismos que controlen los montos de inversión económica a mediano y largo plazo, "el análisis de riesgos es un proceso costoso que no se puede repetir cada vez que se realiza una modificación. Por eso es importante desarrollar metodologías específicas que permitan mantener los resultados del análisis de riesgos" (Santos Olmo Parra et al., 2016, p. 2898).

Dado lo anterior es muy importante para las instituciones en el sector salud tener procesos de análisis y gestión de riesgos informáticos optimizados, debido a la relación que existe entre gastos en seguridad de la información y la evaluación de riesgos, sumado al hecho que la eliminación de estos riesgos debe ser eficiente desde todo punto de vista (Santos Olmo Parra et al., 2016, p. 2898).

De esta forma otra alternativa es el desarrollo de nuevas metodologías dirigidas a la evaluación integral de sistemas de información relacionados con el tratamiento de información médica sensible de pacientes, tal es el caso del marco de trabajo (HOT-fit) "human, organization and technology-fit" utilizado por Yusof M, Papazafeiropoulou A, Paul R, Stergioulas L. que se enfocaron en la creación de un nuevo marco de referencia para la evaluación de tecnologías de

sistemas de información en el sector salud, desarrollado para un caso de estudio que consiste en el estudio de una institución médica de primer nivel y donde los autores argumentan que la aplicación del marco desarrollado es útil no solo para la evaluación integral de un sistema en particular como el caso de estudio, sino potencialmente también, para cualquier Sistema de Información de Salud en general (Yusof et al., 2008, p. 386).

En el anterior marco de trabajo la seguridad se enmarca en un componente mayor denominado Calidad del Sistema, que se evalúa desde una perspectiva tecnológica que se relaciona estrechamente con otra humana y organizacional, así el investigador debe definir y especificar parámetros de evaluación que permitan calificar tanto la seguridad como el resto de los indicadores de calidad del sistema.

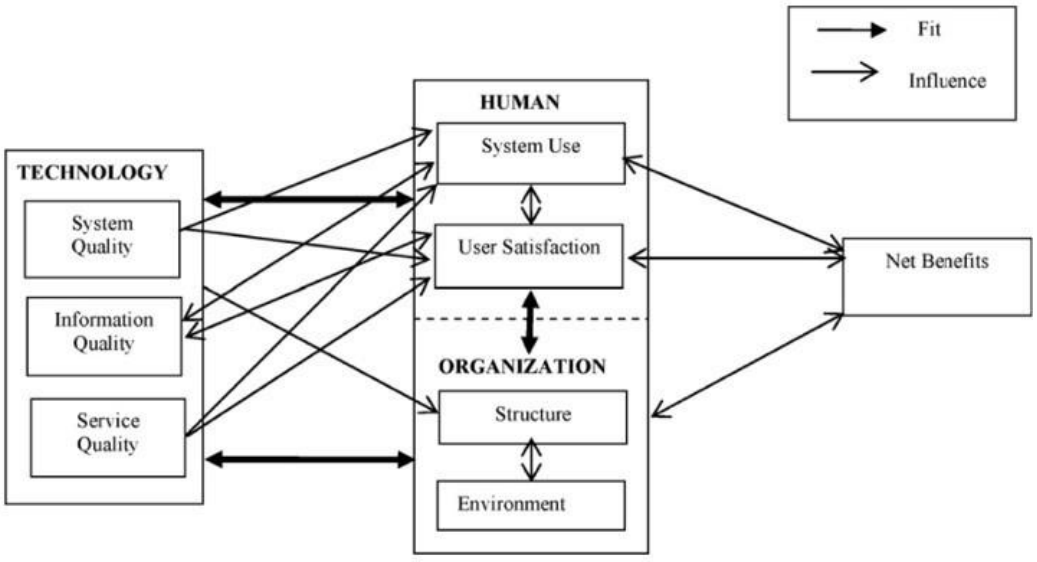

Figura 6. Propuesta de marco de trabajo (HOT-fit).
Fuente: "An evaluation framework for Health Information Systems" por Yusof M, Papazafeiropoulou A, Paul R, Stergioulas L, 2007. Copyright 2007 por Elsevier Ireland Ltd.

Casos como el anterior muestran un marco de trabajo de análisis que abarca las aplicaciones informáticas desde distintas dimensiones que incluyen el análisis de riesgos de la información y el mantenimiento de la privacidad, pero para casos con una perspectiva organizacional total e integral de riesgos informáticos en el sector salud, tenemos el publicado por el comité de seguridad y privacidad "unión NEMA/COCIR/JIRA".

Las estrategias seguidas por los distintos autores para la formulación de nuevas metodologías específicas para la evaluación y gestión de riesgos de instituciones del sector salud ha tenido en común, una revisión de la literatura en cuanto a gestión de riesgos en sistemas informáticos en general y otros específicos del área sanitaria, acompañado de casos de estudios particulares en instituciones médicas que dan un punto de apoyo práctico sumado a las experiencias en el proceso de desarrollo.

En el caso de la metodología propuesta por la "unión NEMA/COCIR/JIRA" muestra una metodología de análisis y gestión de riesgos de TI respaldada por un conjunto de experiencias, dicha metodología es posible de resumir en los siguientes pasos:

• Enumerar un listado de activos susceptibles, como por ejemplo de hardware, software, red de datos, infraestructura TI, datos de configuración de aplicaciones informáticas o hardware, información de pacientes o funcionarios de la organización, información de soporte de procedimientos médicos, etc. Los anteriores deben tener el suficiente detalle que permita la evaluación de amenazas de los mencionados activos.

• Compendio de las regulaciones existentes en cuanto a seguridad de la información, es decir, es necesario una recopilación detallada y minuciosa de todos los requerimientos técnicos y legales que se deben cumplir con miras a proteger la privacidad de la información. Dentro de las

fuentes comunes de posibles requerimientos encontramos la normatividad vigente, que se mencionara más adelante, los proveedores del software y hardware, requerimientos de los clientes para el caso de usuarios pertenecientes a organizaciones o instituciones que pretenden mayores estándares de seguridad, las políticas existentes al interior de la institución, manuales de buenas practicas tales como ITIL y requerimientos derivados de la experiencia propia de la institución. En el anterior aspecto se debe decir que en países como Alemania cada componente de los sistemas informáticos deben cumplir con una serie de requerimientos, "dada la inmensa sensibilidad de la información bajo auditoría en instituciones de salud, los requisitos del sistema solo se aceptan cuando cumplen completamente con las regulaciones" (Bresser Laura et al., 2014, p. 222).

• Elaboración de un listado de amenazas y posibles impactos producto de la materialización de las amenazas sobre los activos mencionados en el primer paso.

• Entregar una valoración de riesgos y vulnerabilidades identificadas, con base en el producto de la severidad del impacto causado sobre el activo que pueda ser objeto de un ataque o perdida de privacidad, lo que permita una categorización de estos.

• Enunciar un conjunto de medidas tendientes a la mitigación de riesgos.

Es de anotar que la anterior metodología hace referencia en su segundo paso a utilizar insumos tales como la normatividad vigente, para el país o región en la que se encuentra la institución objeto de estudio, esto con el fin de adaptarse al marco legal particular sobre el tratamiento y privacidad del historial clínico de pacientes o información derivada en cada país o región, como ejemplo encontramos los marcos normativos de la Unión Europea (UE)

denominado GDPR “General Data Protection Regulation” y el Estadounidense (US) denominado HIPAA “Health Insurance Portability and Accountability Act”.

Los dos anteriores marcos normativos presentan diferencias y lógicamente similitudes, principalmente en sus objetivos, “Las similitudes identificadas reflejan los valores centrales del HHS (the federal Department of Health and Human Services) y la UE con respecto al mantenimiento de la confidencialidad y la privacidad de los datos personales y la información de salud protegida, respectivamente” (Tovino, 2017, p. 974).

Metodología

En una primera fase del proyecto se utilizará una metodología de estudio descriptiva transversal, cuyo resultado pretende obtener una descripción tabulada inicial de las características y bondades que presentan distintos tipos de marcos de trabajo para la gestión de riesgos en TI, así como de metodologías específicas desarrolladas en un contexto internacional. La investigación se enmarca en los dos posibles enfoques, principalmente cualitativo y minoritariamente cuantitativo ya que "la investigación descriptiva encaja en las dos definiciones de las metodologías de investigación, cuantitativas y cualitativas, incluso dentro del mismo estudio" (Abreu, 2012, p. 192).

La metodología descriptiva permite organizar la información de otros estudios para realizar comparaciones relevantes para el desarrollo del proyecto y establecer parámetros que permitan contrastar las particularidades de cada uno de los métodos a evaluar, la metodología de investigación propuesta "utiliza a la descripción como una herramienta para organizar los datos en patrones que surgen durante el análisis. Esos patrones ayudan a la mente en la comprensión del estudio cualitativo y sus implicaciones"(Abreu, 2012, p. 193), para lo cual se suele apelar al uso de tablas o gráficos.

En consecuencia, de lo anterior y acorde a la metodología de investigación tradicional adoptada, se establecen los siguientes pasos para la ejecución de la primera fase:

1. Recopilación y comparación de la información.
2. Justificación de cada uno de los parámetros de selección.

3. Formulación de un cuadro comparativo.
4. Selección de metodología de acuerdo con el análisis e interpretación de resultados.

En una segunda fase se adoptará una metodología explicativa que permita aclarar las razones que inclinaron la selección de una alternativa en favor de otra, considerando puntos de vista que logren sustentar y ampliar el análisis teórico y den pie a la formulación de puntos de adaptación de la alternativa seleccionada, contestando interrogantes como ¿cuál es la causa del problema? y ¿porqué ocurre?, uno de los objetivos de la investigación de tipo explicativa es "construir y ampliar las razones detrás de la teoría. Si existen varias explicaciones para un fenómeno particular la investigación explicativa determina la mejor respuesta" (Abreu, 2012, p. 194). De esta forma se llevarán a cabo los siguientes pasos:

5. Descripción de la metodología seleccionada
6. Adaptación de metodología seleccionada
7. Definición de recomendaciones de implementación para la metodología seleccionada y adaptada.

6. Comparativa de Metodologías de Análisis y Gestión de Riesgos

A continuación, se examinarán de forma general un conjunto de metodologías de análisis y gestión de riesgos encaminadas a ser parte de la implementación de un sistema de gestión de seguridad de la información SGSI, para dar cumplimiento o no de un marco normativo específico, pero aplicables a entornos en el sector salud desde un punto de vista sistémico, que permita contrastar dichas metodologías de análisis.

6.1 Familia de normas ISO/IEC 27000

Aún cuando la familia de normas ISO/IEC 27000 nos es una metodología para análisis y gestión de riesgos, sino un conjunto de normas directrices para la implementación de todo un Sistemas de Gestión de Riesgos de la Información SGSI, en el cual el análisis de riesgos y su tratamiento es uno de sus componentes, se considera que su estudio inicial da un contexto muy importante para la profundización en cada metodología de análisis y mucho más en la medida que brinda una idea de la importancia que tiene el análisis y gestión de riesgos de la información y la forma como se articula el mismo en un proyecto más ambicioso de implementación de un SGSI, el cual al final debería ser el objetivo a mediano o por lo menos a largo plazo en cualquier organización perteneciente al sector de la salud en Colombia.

El marco normativo internacional de la familia de normas ISO/IEC 27000, tiene una especial relevancia debido al reconocimiento internacional que goza la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), prueba de ello es el creciente número de certificaciones que entrega la ISO a nivel internacional

que pasa de un total de 5797 para el año 2006, a unas 33290 certificaciones para el año 2016, donde destaca el país de Japón con un total de 8945 certificaciones para el mismo año (International Organization for Standardization, 2018). La familia de normas ISO/IEC 27000 propone un estado deseado (TO-BE) para aquellas empresas con la voluntad de lograr implementar de forma efectiva y práctica un SGSI, para lo cual deberán adoptar una metodología capaz de salvar la brecha desde un estado actual (AS-IS).

Antes de analizar una metodología valida para la implementación de un SGSI y su correspondiente metodología de análisis y gestión del riesgo, con base en la familia de normas ISO/IEC 27000, es importante enunciar aquellas normas referenciales y tener claro el alcance de cada una:

Norma ISO/IEC 27000: Es la encargada de definir formalmente el vocabulario utilizado en toda la familia de normas.

Norma ISO/IEC 27001: Es la única certificable de esta familia de normas y es la que entrega los requerimientos necesarios para la adopción de un SGSI, entendiendo este proceso como "establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos globales del negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad adaptados a las necesidades de las organizaciones individuales o a partes de ellas." (ICONTEC, 2006, p. 1).

Norma ISO/IEC 27002: Esta norma tiene como objetivo el de entregar un modelo referencial organizacional que sirva tanto como guía en la implementación de controles como también en la definición de controles aceptables en un proceso de adopción o mejora de un SGSI. Básicamente es un documento referente "para la selección de controles dentro del proceso

de implementación de un Sistema de Gestión de Seguridad de la información (SGSI) con base en la ISO/IEC 27001, o como un documento guía para organizaciones que implementan controles de seguridad de la información" (ICONTEC, 2013, p. 1).

En esta norma enuncia 14 numerales para el control de la seguridad de la información denominados dominios, que a su vez conforman de forma global 35 categorías de la seguridad conocidas como objetivos de control segregados en 114 controles, que sirven para la selección de controles de acuerdo con el contexto organizacional o como guía en la formulación de otros controles aplicables.

Norma ISO/IEC 27003: Es la encargada de indicar los aspectos importantes y necesarios para la realización de un proceso de implementación exitoso de un SGSI, desde su especificación y diseño hasta su plan de implementación. La norma tiene como nombre formal "Tecnología de información - Técnica de seguridad - Guía de implementación de un sistema de gestión de seguridad de la información cuyo objetivo es el establecimiento de las especificaciones y diseño de un SGSI" (Valencia-Duque & Orozco-Alzate, 2017, p. 77).

Norma ISO/IEC 27005: Proporciona un marco directriz organizacional de carácter general en la gestión de la seguridad de la información, tratando de garantizar el correcto desarrollo de un SGSI a través de un enfoque en la gestión del riesgo, con el objetivo de "gestionar los riesgos que podrían comprometer la seguridad de la información de la organización" (ICONTEC, 2008, p. 1).

Pueden existir distintos caminos para lograr salvar brechas entre un estado AS-IS hasta uno TO-BE, que en este caso consiste en la exitosa implementación de un SGSI en una organización del sector salud, tales caminos consisten en metodologías, debido a que el marco normativo

entregado por la familia de normas ISO/IEC 27000 es un fin, mas no un cómo. “las normas establecen el deber ser, y no la forma como se logra, de allí la importancia de establecer metodologías que permitan orientar a las organizaciones en la forma como se debe abordar este tipo de procesos” (Valencia-Duque & Orozco-Alzate, 2017, p. 74).

6.1.1 Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000

En este punto tomamos como referencia la metodología expuesta por Valencia-Duque & Orozco-Alzate (2017) la cual es el producto de la combinación de la aplicación y seguimiento de las recomendaciones del estándar internacional ISO/IEC 27003:2010 y la experiencia acumulada de los autores en SGSI. La anterior es abordada desde una perspectiva sistémica que guarda una estructura secuencial compuesta por 5 fases que se enuncian a continuación:

- Fase 1. Obtener la aprobación de la Dirección para iniciar el proyecto.
- Fase 2. Definir el alcance, los límites y la política del SGSI.
- Fase 3. Realizar el análisis de los requisitos de seguridad de la información.
- Fase 4. Realizar la valoración de riesgos y planificar el tratamiento de riesgos.
- Fase 5. Diseñar el SGSI.

La **fase 1** puede resultar algo obvia, pero no lo es en absoluto, dado que para empezar la implementación de un SGSI no es un proyecto independiente de las áreas de TI en las organizaciones, sino que el mismo debe ser un proyecto organizacional e incluso estratégico en la medida que el mismo se alinea con los objetivos de la organización, la implementación de un SGSI “es un proyecto organizacional y como tal requiere la aprobación y el apoyo de la

Dirección para avanzar en su adecuada implementación" (Valencia-Duque & Orozco-Alzate, 2017, p. 77).

De acuerdo con Valencia-Duque & Orozco-Alzate (2017), la correcta ejecución de la fase 1 se lleva a cabo con el seguimiento de los siguientes pasos:

- Establecimiento de las prioridades de la organización para desarrollar un SGSI.
- Definir el alcance preliminar del SGSI.
- Creación del plan del proyecto para ser aprobado por la Dirección.

Dentro del seguimiento de los anteriores pasos es necesario guardar especial atención en la documentación que respalda y da vía libre a la implementación del SGSI por parte de la alta dirección, lo que además de mostrar el compromiso que tiene la dirección, también es la garantía para la aprobación de recursos para la ejecución del proyecto y demuestra la conformidad con el levantamiento preliminar de requisitos expresados por la misma dirección.

La **fase 2** comprende los siguientes pasos:

- Definición del alcance.
- Definición de la política y objetivos de seguridad.
- Aprobación de la dirección.

En la formulación de cualquier proyecto la definición de los alcances es una tarea obligada, en la medida que permite establecer claramente los objetivos, en el caso particular de esta metodología debe expresar que es lo que se busca proteger.

Dentro de la definición de la política, esta debe girar alrededor de los objetivos mencionados anteriormente que quiere alcanzar la organización, es decir los compromisos de la organización respecto a la seguridad de la información.

De acuerdo con Valencia-Duque & Orozco-Alzate (2017), es importante diferenciar los dos tipos de objetivos que abarca un SGSI, como lo son los objetivos generales y los objetivos de control. Los primeros deben estar articulados con las políticas y los segundos que son derivados del proceso de análisis.

La **fase 3** de análisis de los requisitos de seguridad de la información, contemplan el establecimiento de los activos informáticos de la organización junto con el responsable por la seguridad de este y su propietario, dichos activos deberán ser valorados de acuerdo con su importancia.

Los elementos necesarios de identificar para un correcto establecimiento de requisitos, parte central de esta fase, se encuentran consignados en la norma ISO/IEC 27003:2010 y de acuerdo con Valencia-Duque & Orozco-Alzate (2017), corresponden a:

- Activos de información importantes que se encuentren dentro del alcance del SGSI.
- Visión de la organización y sus efectos sobre los requisitos futuros.
- Formas actuales de procesamiento de información.
- Requisitos legales, reglamentarios, obligaciones contractuales, normatividad, acuerdos con usuarios, clientes y proveedores, condiciones de pólizas y otros aplicables.

En la **fase 4** se trata de la valoración y tratamiento de los riesgos que involucran los activos vistos en la fase anterior, utilizando como referente la norma ISO/IEC 27005 y se considera el punto principal en la implementación del SGSI y hace parte de la temática central del presente documento. Es importante resaltar nuevamente, que existe variedad de referentes encaminados a la valoración de riesgos y planificar el tratamiento de los mismos, tales modelos que pueden ser

utilizados pueden ser por ejemplo: OCTAVE, CRAMM, NIST SP 800-30, MAGERIT, MEHARI, FAIR, RISK FOR COBIT 5.0, MARISMA-AGR y el estándar normativo ISO 31000, más adelante se tratarán en detalle algunos de estos y sus correspondientes metodologías con el fin de contrastar al conjunto de referentes y metodologías.

La fase 4 en general esta constituida por los siguientes pasos:

- Establecimiento de contexto.
- Parámetros de probabilidad.
- Parámetros de impacto.
- Determinación de la vulnerabilidad.
- Criterios de aceptabilidad del riesgo.
- Valoración del riesgo.
- Evaluación del riesgo.
- Tratamiento del riesgo.

Para la determinación de la vulnerabilidad es necesario primero entender a que se refiere y en ese sentido se debe considerar como al grado de exposición que tiene la información frente a la materialización de un riesgo, es medida de forma porcentual y calculada a partir del impacto y la probabilidad. De acuerdo con Valencia-Duque & Orozco-Alzate (2017), la formula para calcular la vulnerabilidad consiste es la siguiente:

$$Vx = (P * I)/max(P * I)$$

Donde Vx es la vulnerabilidad para el escenario de riesgo considerado.

P es la probabilidad que tiene el riesgo de materializarse.

I es el impacto que tendría para la organización la ocurrencia del riesgo.

En todo proceso de análisis y gestión del riesgo es necesario entender que existirán riesgos cuya probabilidad nunca llegará a ser cero, en otros casos la mitigación del riesgo puede resultar extremadamente costosa, para estos casos u otros será necesario establecer parámetros de aceptabilidad del riesgo que satisfagan una expectativa coherente de nivel de seguridad a nivel organizacional.

La familia de normas ISO/IEC 27000 abarca la norma ISO/IEC 27005:2009 para la valoración del riesgo, lo que no significa que sea la única opción y de hecho en este documento se abordan varias de ellas, pero en esta primera parte estudiaremos la norma ISO/IEC 27005:2009 donde la valoración se lleva a cabo a partir del seguimiento de los tres pasos siguientes, que consisten en:

- Identificación de los escenarios de riesgo
- Estimación del riesgo
- Evaluación del riesgo

Al final la evaluación del riesgo consiste en una actividad de comparación de vulnerabilidades teniendo en cuenta los niveles de aceptación mencionados anteriormente, “la evaluación de riesgos permiten diseñar mapas de riesgos, o mapas de calor, informes de vulnerabilidad por cada criterio de seguridad de la información y diversos indicadores que permiten monitorear el nivel de avance en la gestión del riesgo” (Valencia-Duque & Orozco-Alzate, 2017, p. 84).

El tratamiento del riesgo consiste en las actividades necesarias para llevar el riesgo a un nivel aceptable de acuerdo con los parámetros de aceptabilidad y apoyándose en controles,

siguiendo un orden dado por la priorización de vulnerabilidades, que se debe documentar en un plan de tratamiento de riesgos.

Como se menciono anteriormente es necesario conciliar los parámetros de aceptabilidad con los recursos disponibles, dado que es imposible mitigar el 100% de los riesgos, de ahí la necesidad de evaluar el costo de los controles vs el beneficio, en todo caso el costo de los controles no podrá superar el techo presupuestal y se deberá dar prioridad de tratamiento a aquellos riesgos que marcan una mayor vulnerabilidad.

La norma **ISO/IEC 27005** brinda 4 opciones parea manejar o tratar los riesgos que son:

- Reducción del riesgo.
- Retención del riesgo.
- Evitar el Riesgo.
- Transferencia de Riesgo.

Lo anterior será parte del plan de tratamiento del riesgo, que según Valencia-Duque & Orozco-Alzate (2017) será estructurado de la siguiente forma:

> … escenario de riesgo, riesgo residual, alternativa de tratamiento, controles a implementar, responsable de su implementación (rol), valor estimado, fechas estimadas de implementación, efecto esperado del control en función de la disminución de la probabilidad o impacto, riesgo residual esperado después del plan de mitigación.

La **fase 5** corresponde al diseño del SGSI, se trata de la última fase y se siguen los siguientes 3 pasos de forma sucesiva:

- Documentación del sistema.
- Implementar el plan de tratamiento de riesgos.

- Monitoreo de la seguridad de la información.

El segundo paso de acción de esta fase consistente en la implementación del plan de tratamiento de riesgos, que deberá garantizar los niveles de seguridad aprobados por la alta gerencia con la aplicación y mantenimiento de los controles dados en la fase 3 de acuerdo con los recursos asignados.

6.2 Conjunto de Normas ISO 31000:2018 Para la Evaluación y Gestión de Riesgos

El conjunto de normas ISO 31000 corresponden a un enfoque generalista en la gestión de riesgos y es posible su aplicación dentro de un SGSI, ya que no entra en contravía con la norma ISO/IEC 27001 y al contrario se encuentra plenamente alineada y así ISO 31000 “enfatiza los principios y las directrices para llevar a cabo la gestión del riesgo” (Melo Reyes, 2019, p. 1). Al poseer un enfoque generalista no tiene limitaciones al sector o tipo de organización donde se aplica, por ejemplo, empresas públicas o privadas y su aplicación genera confianza al ser un estándar aceptado y reconocido a nivel mundial, “proporciona principios, un marco y un proceso para gestionar el riesgo. Puede ser utilizado por cualquier organización, independientemente de su tamaño, actividad o sector” (International Organization for Standardization, 2020).

Para llevar a cabo el proceso de implementación es necesario llevar a cabo una serie de pasos desde la verificación de la correcta comunicación hasta el propio tratamiento del riesgo, estos son “fases de establecimiento del contexto, identificación del riesgo, análisis del riesgo, evaluación del riesgo, y tratamiento del riesgo” (Melo Reyes, 2019, p. 8).

6.2.1 Pasos en la Implementación de ISO 31000

Paso 1. Comunicación y consulta

Su aplicación parte de un paso inicial de planificación de la Comunicación y Consulta con las partes interesadas tanto internas como externas, que garanticen los medios y herramientas para una comunicación continua y efectiva, debido a que la comunicación con los distintos interesados es crucial durante la ejecución del proyecto de implementación y continuidad del ciclo PHVA, es de recordar que un sistema de gestión de riesgos general debe hacer parte de la totalidad de procesos organizacionales y en un SGSI harán parte aquellos procesos organizacionales que hagan captura, almacenamiento, tratamiento y difusión de la información.

Paso 2. Establecimiento del contexto

Seguido a tener garantizada la correcta comunicación con las partes interesadas es necesario el reconocer el contexto organizacional, que trata de determinar las particularidades de cada organización que dan lugar a la formulación de los alcances, áreas organizacionales y criterios en la gestión del riesgo. No se puede olvidar que este contexto es tanto interno como externo a la organización. “Para diseñar el marco de referencia se debe entender el contexto de la organización” (Melo Reyes, 2019, p. 8)

Paso 3. Identificación de riesgos

En este paso se documentan la totalidad de riesgos, internos o externos, que son capaces de afectar la consecución de los objetivos planteados en los alcances. Este paso es muy importante, en la medida que aquellos riesgos no detectados o que se pasen por alto o que simplemente se subestimen no serán tenidos en cuenta en los subsiguientes pasos y por consiguientes no sufrirán de un tratamiento. También es de tener en cuenta que la lista inicial no es un ente estático e

inmutable en razón a que hablamos de un ciclo PHVA, en el cual la lista muy posiblemente seguirá creciendo con cada nuevo ciclo.

Paso 4. Análisis de riesgos

Identificación de las fuentes y causas de los riesgos encontrados en el paso anterior, así como las consecuencias por la materialización de estos, lo anterior involucra un tipo de análisis cuantitativo o cualitativo e incluso una combinación de los dos para servir de insumo en su evaluación.

Paso 5. Evaluación de riesgos

En este punto se entrega como producto una clasificación de los riesgos, a partir de la comparación del nivel de riesgo resultado del análisis de riesgos contra los criterios de riesgos expuestos durante la evaluación del contexto de la organización, que permita identificar cuales son críticos o prioritarios para la organización y requieren de especial atención o en general cuales requieren de algún tipo de tratamiento, “el proceso de evaluación de riesgos determinará qué riesgos requieren tratamiento y cómo son las prioridades de tratamiento para esos riesgos” (Gede Wisnu A., 2019, p. 2672).

Paso 6. Tratamiento de riesgos

Engloba un análisis de alternativas para el tratamiento de riesgos, controles existentes e implementación de controles. Básicamente consiste en la transformación de los riesgos mediante la aplicación de algún tipo de opción de tratamiento, “las alternativas de control que se pueden aplicar como eliminación del riesgo, reducir la probabilidad, reducir las consecuencias, transferir el riesgo” (Gede Wisnu A., 2019, p. 2672)

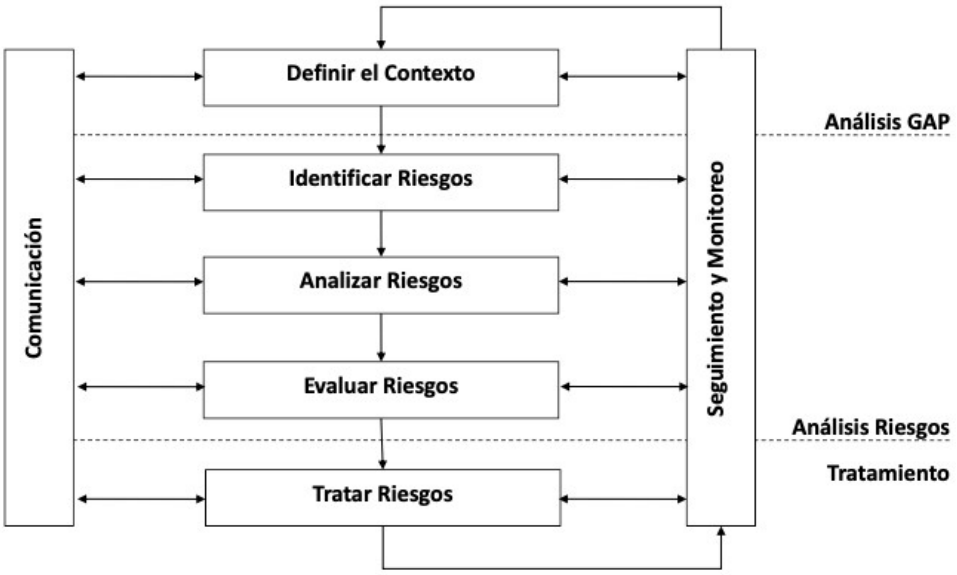

Figura 7. Ciclo de procesos de ISO 31000.
Fuente: International Organization for Standarization.

Es importante tener en cuenta que bajo la perspectiva de la norma ISO 31000 nos encontramos en un ciclo de mejoramiento continuo que involucra volver a repetir cada uno de los pasos anteriores, es decir, identificar nuevamente los riesgos (lo que puede conllevar a un aumento con respecto a los identificados anteriormente), un nuevo análisis de riesgos, evaluación de riesgos teniendo presente objetivos de control actualizados y posiblemente tipos de tratamiento distintos a los anteriormente tomados.

6.3 Metodología dinámica para el análisis y gestión de riesgos MARISMA-AGR

En el caso de la anterior metodología estudiada, se veía todo un proceso de implementación de un SGSI, pero también se hacia notable el hecho que el eje central correspondía a los pasos contenidos dentro del análisis y gestión de riesgos de la información,

“Sin duda esté es el eje principal del SGSI, cuyo principal referente es la norma ISO/IEC 27005” (Valencia-Duque & Orozco-Alzate, 2017, p. 82), es así como en este punto se abordará otra perspectiva en la valoración de riesgos y la planificación del tratamiento de riesgos distinta a la ISO/IEC 27005, pero con objetivos congruentes denominada MARISMA-AGR, expuesta por Santos Olmo Parra (2016), esta enfocada en su aplicación a pequeñas y medianas empresas (PYMES), aún cuando es posible y adecuada su aplicación a grandes empresas “bajo la premisa de que cualquier sistemas de Análisis de Riesgos valido para las PYMES también será extrapolable a grandes compañías” (Santos Olmo Parra et al., 2016, p. 2900).

Uno de los enfoques de MARISMA-AGR se encuentra en la reducción de costos de implementación y sobre todo en costos de mantenimiento, donde este último involucra el concepto de mejoramiento continuo. Se basa en una metodología (MARISMA) que contempla los aspectos necesarios en la gestión de la seguridad de la información y en cuyo alcance organizacional se consideran las instituciones en el sector salud, “aunque la investigación realizada se centra inicialmente en las PYMES los resultados podrían aplicarse en otros sectores como el de salud” (Santos Olmo Parra et al., 2016, p. 2897).

Al igual que en la familia de normas ISO/IEC 27000, la metodología MARISMA-AGR realiza una vinculación entre los controles de seguridad de la información y el propio análisis y gestión del riesgo. Los pasos de la metodología se pueden resumir en 3 procesos que se enuncian a continuación:

Generación de Esquemas para el Análisis de Riesgos (GEAR).

Generación del Análisis y Gestión del Riesgo (GAGR).

Mantenimiento Dinámico del Análisis de Riesgos (MDAR).

En la siguiente figura se puede observar el esquema de interrelación de los anteriores procesos y su secuencialidad a nivel de flujo de información.

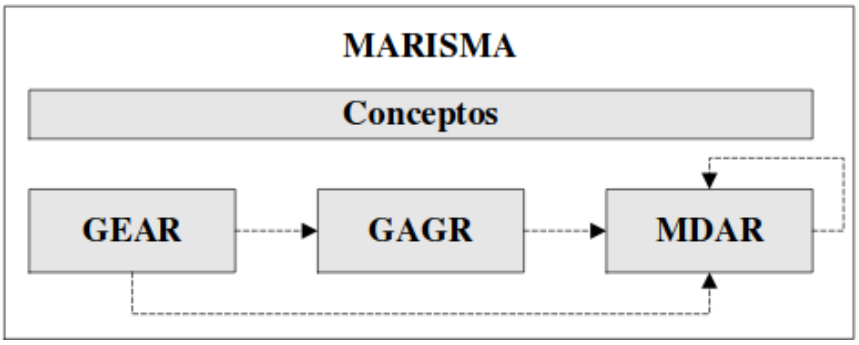

Figura 8. Esquema de procesos de MARISMA.
Fuente: Santos Olmo Parra et al., (2016).

De forma general se puede decir que el proceso GEAR constituye un elemento diferenciador frente a otras metodologías, en vista que se desarrolla la construcción de una estructura de relaciones entre distintos componentes del análisis de riesgos y los controles, a partir de experiencias previas que al final se traduce en reducción de costos, guardando un riguroso equilibrio entre calidad y costo.

El proceso GEAR este compuesto por 3 fases denominadas:

- Entradas.
- Tareas.
- Salidas.

De acuerdo con Santos Olmo Parra et al. (2016), la primera fase de Entradas esta conformada en primera instancia por la experiencia y conocimiento del Grupo de Expertos del Dominio (GED), quienes aportan información basada en la implementación de otros procesos de análisis de riesgos consignadas en una estructura de relaciones entre activos, riesgos y otros

elementos relevantes con los controles. La anterior estructura es llamada esquema, la cual puede ser llevada a otros proyectos con procesos similares de aplicación de la metodología, dicho esquema es el insumo principal para el proceso GAGR, lo que significa que la reutilización de este lleva a un ahorro de esfuerzos y costes.

Es posible que el GED mantenga distintos esquemas de acuerdo con el tipo, tamaño, procesos y demás características propias de múltiples organizaciones consignadas en un repositorio, este mismo se puede consultar y utilizar con el objetivo de aplicar a otras organizaciones similares y con requerimientos equivalentes.

Como parte de las entradas también tenemos otras metodologías que dan pautas de selección de elementos como tipo de activos, controles, amenazas u otros, como por ejemplo ISO/IEC 27005 o MAGERIT.

Otra entrada son las normativas que deben ser tenidas en cuenta para su cumplimiento, tal es el caso de Leyes, decretos o normas para la protección de datos personales.

La fase de tareas engloba a 6 tareas que se dividen en tareas tendientes a establecer los elementos de entrada y tareas para determinar relaciones en los elementos de entrada, en el primer grupo se encuentran 4 tareas y al segundo grupo pertenecen las dos restantes.

Las relaciones son parte del conocimiento que tiene el GED, pero están sujetos a cambios permanentes en la medida que se lleva a cabo el proceso de mejoramiento continuo que permite ajustarse a las necesidades de la institución y el afinamiento de las relaciones. El resultado final de esta fase es el diagrama o conjunto de diagramas de relaciones entre elementos, denominado esquema base.

Las tareas para el establecimiento de los elementos de entrada inician con la **selección de activos** de la información y especialmente en la agrupación por tipos de activos, esto facilitará el establecimiento de las relaciones con el resto de elementos como por ejemplo los controles que igualmente serán seleccionados en esta tarea de establecimiento de entradas, para lo cual Santos Olmo Parra et al. (2016) sugiere la utilización de los 114 controles facilitados por la norma ISO/IEC27002:2013 más los sub-controles derivados.

Otra tarea contemplada en esta fase de Entradas corresponde a la **selección de amenazas**, entendiendo a las amenazas como posibles eventos que provocan uno o varios incidentes de consecuencias adversas para la institución. Estas amenazas pueden ser buscadas en la normatividad vigente o en todo tipo de normas al respecto y por su puesto del conocimiento y experiencia del GED, las mismas serán agrupadas de acuerdo con su contexto.

Para la reducción del riesgo o nivel de exposición a la posible materialización de una amenaza, conocido como vulnerabilidad, se procede con la tarea de la **selección de controles**, estos serán incluidos dentro del esquema y se relacionarán directamente con los otros elementos del análisis de riesgos mencionados, ahora si tenemos definida una lista de controles podremos estimar cuantitativamente el grado de exposición o vulnerabilidad a partir del nivel de cumplimiento o no del control. De igual forma a la selección de amenazas, la selección de controles se realizará de acuerdo con la normatividad o metodología aplicable y al conocimiento y experiencia del GED. Como se menciono anteriormente esta metodología sugiere el uso de los 114 controles mencionados por la norma ISO/IEC 27001:2013 más los sub-controles que describe la norma ISO/IEC 27002:2013.

La siguiente tarea comprende la **selección de criterios de riesgo** que orienten la estimación y valoración de las amenazas con respecto al grado de posible concreción frente a un activo, los anteriores serán incluidos dentro del esquema de relaciones con el objetivo de automatizar el proceso de evaluación de riesgos. De acuerdo con Santos Olmo Parra et al. (2016), la base del esquema en cuanto a selección de criterios será dictada por la metodología MAGERIT y el estándar ISO/IEC 27005 estructurado a partir de los criterios de **C**onfidencialidad, **I**ntegridad, **D**isponibilidad, **A**utenticidad y **T**razabilidad (CIDAT).

La siguiente tarea tiene por objetivo la **definición de relaciones entre Tipos de Activos x Amenazas x Criterios de Riesgo** con el objetivo de simplificar, y por ende reducir costos de implementación, en este punto se hace evidente la necesidad de la experiencia y conocimiento del GED encargado de realizar las asociaciones entre activo - amenaza - criterio de riesgo.

La última tarea de esta fase corresponde al **establecimiento de relaciones entre amenazas x controles**, que tiene por objetivo definir en el diagrama la vinculación que tiene el conjunto de amenazas y el conjunto de controles definidos anteriormente y de esta forma facilitar la evaluación del riesgo, en este punto vuelve a tener un papel muy importante el GED puesto que a través de su conocimiento y experticia sugieren las relaciones que deben existir entre amenaza y control.

Hasta aquí tenemos el primer proceso en la generación de los esquemas para el análisis del riesgo y pasamos al siguiente, consistente en la **aplicación del análisis del riesgo**, que trata en si de la evaluación del riesgo a los que se encuentran expuestos los activos informáticos con el consiguiente plan de acción para su gestión, de acuerdo con Santos Olmo Parra et al. (2016)

“proponer un plan responsable de seguridad (Cl/RS) para gestionar los riesgos de la forma más eficiente posible y con el menor esfuerzo y coste”.

Las entradas de este proceso consisten en un esquema del repositorio y el interlocutor de la organización objeto del análisis. La primera entrada se selecciona de acuerdo con el objeto y características de la organización y el segundo define los activos informáticos para tener en cuenta.

Las salidas consisten en un informe con el resultado del cumplimiento de controles, acompañado del listado de activos informáticos, la matriz de riesgos y el plan de mejora sugerido para la organización que será analizado por el consultor de seguridad. Es de anotar que estas salidas se convertirán en parte del repositorio organizacional que lógicamente sustentan el plan de Mantenimiento Dinámico del Análisis del Riesgo (MDAR).

6.4 Metodología MAGERIT para el análisis y gestión de riesgos de los sistemas de información.

La metodología MAGERIT en su versión 3, corresponde a una metodología de carácter abierto para el análisis y gestión de riesgos que tiene gran aceptación a nivel mundial y que es utilizado por la administración pública del gobierno español, “desarrollada por el Ministerio de Administraciones Públicas de España, que se ofrece como marco y guía para la Administración Pública. Dada su naturaleza abierta, también se utiliza fuera de la Administración” (Agencia de la Unión Europea en Ciberseguridad, 2005).

La documentación completa de la metodología es posible consultarla y descargarla en su totalidad, dado su carácter abierto, en la siguiente dirección:

https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es#.XeCCEb97mRt

Se puede hacer la descarga tanto en idioma español como en ingles, también es posible consultar las anteriores versiones de la metodología.

La metodología surge como una respuesta al creciente aumento de la gestión y almacenamiento de la información digital en el gobierno Español y en primera instancia trata de concientizar de los riesgos derivados de la adopción de nuevas tecnologías de la información, "toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión" (Gobierno de España, 2012a).

Según la Administración Electrónica del (Gobierno de España, 2012a) los objetivos directos que tiene la aplicación de la metodología consisten en:

- Buscar concienciar a los responsables de la información las organizaciones de la existencia de riesgos y de la necesidad de gestionarlos.
- Entregar una metodología sistemática para analizar los riesgos derivados del uso de TIC.
- Servir como ayuda para el descubrimiento, planificación y el tratamiento oportuno que permita mantener los riesgos bajo control Indirectos
- Preparar a la organización para enfrentar procesos de evaluación, auditoría, certificación o acreditación, según corresponda.

6.4.1 Estructuración de la Metodología MAGERIT para su consulta

En una primera parte (Capítulo 2) se recogen los aspectos generales en cuanto a vocabulario conceptos y el significado del análisis y gestión de riesgos enmarcado en un SGSI. Posteriormente (Capítulo 3) se desarrolla un estudio más formal de los pasos a seguir en un análisis de los riesgos. En el capítulo 4 se procede a la formalización las actividades necesarias para realizar una correcta gestión de riesgos.

En lo referente a la implementación por primera vez de proyectos de gestión de riesgos, se es posible gracias al apoyo del capítulo 5, que también es válido en casos de cambios importantes a procesos de gestión de riesgos existentes. Para el capítulo 6 se formaliza el proceso de planeación de la seguridad. En el capítulo 7 se trata la seguridad en los procesos de desarrollo de sistemas de información y se finaliza en el capítulo 8 con una serie de consejos derivados de un estudio de problemáticas recurrentes en los proyectos de implementación de análisis de riesgos.

6.4.2 Pasos en la Implementación de la Metodología MAGERIT

La metodología MAGERIT se estudia a través de una serie de pasos que permite su aplicación en un ambiente productivo organizacional, que inicia con el **Paso 1** que se encarga de la identificación de los activos informáticos, los cuales pueden ser catalogados en distintos tipos de acuerdo con el rol que desempeñan en el tratamiento de la información. Por ejemplo, un equipo servidor físico que en su disco duro almacena una base de datos se considera del tipo Hardware y la base de datos se considera dentro del tipo de Activo de la Información.

Adicionalmente se contempla la valoración de los activos, labor muy importante dado que pueden cometerse errores al realizarlo de forma superficial o descuidada, por ejemplo, dado el caso en que una organización tiene un equipo computador de sobremesa obsoleto y totalmente depreciado, que almacena una base de datos de clientes de la cual no se tiene ningún tipo de copia, el activo de tipo hardware (computador) tiene un valor insignificante, pero reconstruir el activo de base datos de datos de clientes en caso de perdida total, puede ser una labor muy costosa de lograr, sin contar con el hecho de la afectación en la operación de la organización mientras se logra la reconstrucción de la base de datos que se constituye en un costo por la interrupción del servicio, lucro cesante, perdida de capacidad de operación, sanciones, etc. Es por eso por lo que la metodología propone evaluar los activos desde las perspectivas de análisis cuantitativas o cualitativas, teniendo en cuenta la función que tiene el activo en el normal desempeño de los procesos y las dimensiones del activo (confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad). El objetivo es establecer el costo de su reconstrucción, reemplazo o sustitución equivalente, lo cual en algunos casos puede ser difícil de evaluar sobre todo en los intangibles, “la valoración económica exacta puede ser escurridiza y motivo de agrias disputas entre expertos. El capítulo 4 del ‘Catálogo de Elementos’ presenta unas pautas para la valoración sistemática de activos” (Gobierno de España, 2012b, p. 25).

El **Paso 2** en la metodología consiste en identificar cada una de las amenazas que pueden llegar a afectar a los activos independientemente de si son probables o poco probables, estas pueden provenir de cualquier origen, como natural, del entorno, defectos técnicos, de personas por forma accidental o deliberada.

Este segundo paso considera igualmente realizar una valoración de las amenazas identificadas, tanto en el sentido de la degradación del activo como de la probabilidad de materializarse la amenaza, la primera medida es un porcentaje del valor del activo y la segunda es una medida cuantitativa o cualitativa de la posibilidad o frecuencia con que puede ocurrir algo. Ahora en el caso de la materialización de la amenaza se debe medir el impacto que sufre el activo, el impacto se estima a partir de conjugar el valor del activo en una o varias dimensiones y el grado de degradación, con lo anterior es directa la estimación del riesgo potencial o daño probable, "conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia" (Gobierno de España, 2012b, p. 29).

Un objetivo de las metodologías de análisis de riesgos es precisamente identificar los riesgos, que técnicamente son la cuantificación de los daños probables sobre un activo, ahora habiendo determinado el impacto y su probabilidad de ocurrencia, el riesgo será directamente deducible. Una forma de observarlo de forma gráfica es a través de un mapa de calor, que básicamente es un plano cartesiano en el cual el eje de las abscisas corresponde a la probabilidad y el eje de las ordenadas al impacto y en la que se puede diferenciar distintas zonas de riesgo.

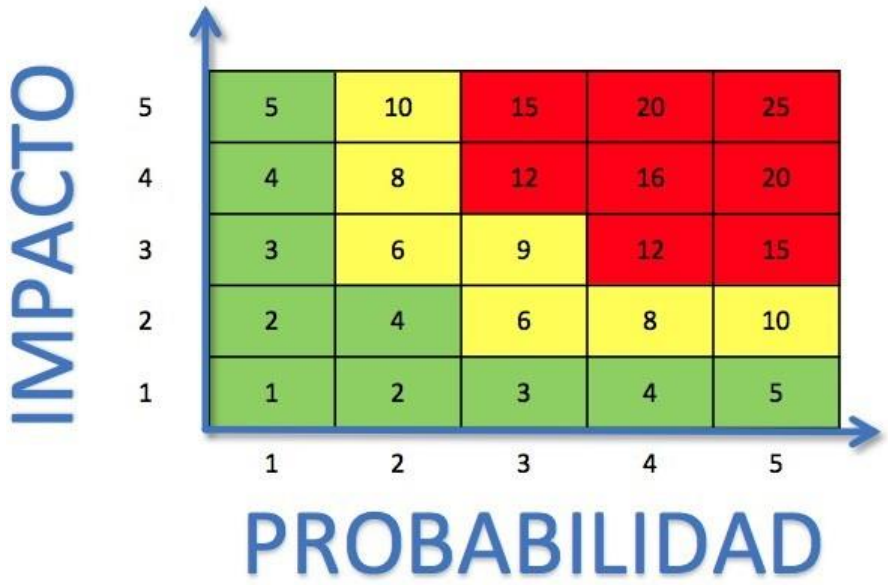

Figura 9. Mapa de calor de valoración del riesgo.
Fuente: El autor

El **Paso 3** estudia las Salvaguardas o contra medidas, tanto su selección, tipo, el efecto como la eficacia de estas. Entendiendo primero que las salvaguardas son mecanismos que tienen el objetivo de mitigar los riesgos "procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieres elementos técnicos, otras seguridad física y por último, está la política de personal" (Gobierno de España, 2012b, p. 31).

En este paso es necesario iniciar por el proceso de la selección de las salvaguardas, que aplican para cada uno de los activos identificados, en vista que una salvaguarda mitiga el riesgo de una forma muy particular, esta selección se realiza teniendo en cuenta las siguientes recomendaciones dadas por la metodología MAGERIT que resultan en salvaguardas que no aplican, no justifican y aquellas seleccionadas:

- El tipo de activos a proteger.
- Dimensión o dimensiones de seguridad que requieren protección.
- Amenazas de las que necesitamos protegernos.
- Si existen salvaguardas alternativas.

Se debe asumir y tener presente un criterio de proporcionalidad que se basa en:

- Mayor o menor valor del activo, centrándonos en lo más valioso.
- Mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes identificados.
- La cobertura del riesgo que proporcionan salvaguardas alternativas.

La mitigación del riesgo por efecto de las contra medidas o salvaguardas tiene dos efectos cuantificables que son reducir la probabilidad de la amenaza y limitando el daño causado, el primero es de carácter preventivo y el segundo es una respuesta ante la materialización de la amenaza y sus consecuencias. De acuerdo con los efectos anteriores y al tipo de contra medida la metodología MAGERIT clasifica las salvaguardas así:

Aquellas con efecto preventivo:

- Preventivas [PR]
- Disuasorias [DR]
- Eliminatorias [EL]

Cuyo efecto limita la degradación:

- Minimizadoras [IM]
- Correctivas [CR]
- Recuperativas [RC]

Efecto de consolidar a las demás

- De monitorización [MN]
- De detección [DC]
- De concienciación [AW]
- Administrativas [AD]

En el **Paso 4** evaluamos el impacto residual, teniendo primero en cuenta que cada una de las salvaguardas ofrece un cierto grado de eficacia en la protección y su madurez de implantación, de acuerdo con la metodología se pueden catalogar en inexistentes, inicial (ad-hoc), reproducible intuitivamente, proceso definido, gestionado (medible) y optimizado. Es posible notar que las salvaguardas de acuerdo con su madurez y eficacia tendrán un efecto mayor o menor en el impacto que puede llegar a tener la materialización de la amenaza, así entre un mayor grado de protección obtendremos un menor impacto y el impacto que permanece se conoce como residual.

Dado que el impacto es una métrica previamente evaluada, en este paso se recalcula teniendo en cuenta la eficacia y madurez de las salvaguardas aplicadas.

El **Paso 5**, al igual que en el paso anterior se tiene en cuenta las salvaguardas seleccionadas que ofrecerán una protección que disminuye la probabilidad de ocurrencia, con lo cual se ha

modificado el riesgo en una medida mayor o menor dependiendo de la eficacia y madurez de las salvaguardas aplicadas, de esta forma existirá una medida entre el riesgo inexistente hasta el nuevo valor del calculo del riesgo, esta diferencia cuantitativa se denomina riesgo residual.

Dado que la aplicación de la salvaguarda ha afectado la probabilidad, además del impacto evaluado en el paso anterior, el recalculo del riesgo será el mismo, pero teniendo en cuenta el nuevo impacto y riesgo.

6.4.3 Formalización de las Actividades

A partir de los pasos anteriores es posible definir un proceso o método de análisis de riesgos basado en tareas que se resume en la siguiente tabla:

Tareas Principales	**Tareas Secundarias**
MAR.1 - Caracterización de los activos	MAR.11 - Identificación de los activos
	MAR.12 - Dependencias entre activos
	MAR.13 - Valoración de los activos
MAR.2 - Caracterización de las amenazas	MAR.21 - Identificación de las amenazas
	MAR.22 - Valoración de las amenazas
MAR.3 - Caracterización de las salvaguardas	MAR.31 - Identificación de las salvaguardas pertinentes
	MAR.32 - Valoración de las salvaguardas
MAR.4 - Estimación del estado de	MAR.41 - Estimación del impacto
	MAR.42 - Estimación del riesgo

riesgo	

Tabla 1. Tareas que componen el método de análisis MAGERIT v.3

6.4.4 Proceso de Gestión del Riesgo en la Metodología MAGERIT

Como se menciono en el capítulo 4, la metodología MAGERIT considera la gestión del riesgo a partir de un análisis y su tratamiento, lo cual se puede observar en la figura 3. En este punto nos queda analizar el tratamiento, que básicamente es el conjunto de medidas que se toman a la luz de la evaluación del riesgo que se realizó, y al que esta expuesta la información de la organización, de acuerdo con (Gobierno de España, 2012b, p. 47) las decisiones que se toman en este sentido están condicionadas por los siguientes factores:

- La gravedad del impacto y/o del riesgo.
- Las obligaciones a las que por ley esté sometida la Organización.
- Las obligaciones a las que por reglamentos sectoriales esté sometida la Organización.
- Las obligaciones a las que por contrato esté sometida la Organización.

Los anteriores factores pueden verse afectados o no, de acuerdo con ciertas particularidades de la organización, como por ejemplo su tamaño, reputación, situación interna, etc.

Al final cada riesgo significativo será catalogado de forma gradual como asumible, apreciable, grave y crítico. Donde la catalogación como riesgo asumible deberá soportarse con una justificación muy clara y prudente.

En el tratamiento del riesgo se debe considerar una variedad de opciones que inicia con la más simple de todas, que es la eliminación de la fuente del riesgo frente a riesgos no asumibles,

lo que se traduce en prescindir de activos, por ejemplo si el origen del riesgo es una base de datos, el tratamiento puede consistir en eliminar dicha base de datos, pero aquí surge un interrogante bastante obvio y es ¿hasta que punto podemos llegar con la eliminación de activos sin afectar los procesos de negocios de la organización?, de acuerdo con (Gobierno de España, 2012b, p. 53) "En un sistema podemos eliminar varias cosas, siempre que no afecten a la esencia de la Organización", lo que nos lleva a la conclusión que una organización deberemos eliminar aquellos activos que no sean necesarios y aislar o segregar sistemas que no se deban interrelacionar a través de redes de datos, tratando de separar a los activos más importantes. Es posible considerar también eliminar un activo a cambio de otro, por ejemplo, si el riesgo deriva de un sistema operativo del que no se tiene soporte, el tratamiento puede consistir en eliminar el sistema operativo y reemplazarlo por otro que si tiene soporte. Todo lo anterior irremediablemente nos lleva a un nuevo proceso de revaluación y análisis, "Las decisiones de eliminación de las fuentes de riesgo suponen realizar un nuevo análisis de riesgos sobre el sistema modificado" (Gobierno de España, 2012b, p. 53).

La siguiente opción dentro del tratamiento de los riesgos la encontramos en la mitigación, que a su vez puede consistir en reducir la probabilidad que la amenaza se materialice o en reducir el impacto de la materialización de la amenaza. Lo anterior se logra incluyendo o mejorando salvaguardas, que puede ser logrado con la implementación de nuevos activos, como por ejemplo, un cortafuegos en la red de datos, pero con la consecuencia que el nuevo activo tendrá asociado nuevos riesgos, es así, como será necesario realizar un nuevo proceso de evaluación y análisis para el nuevo activo como también para el sistema tratado inicialmente, teniendo

presente que el nuevo activo, en términos generales, no generen un estado de riesgo o impacto mayor que el sistema original.

Otra opción de tratamiento es la Compartición, aún cuando en otros contextos de análisis puede denominarse “transferencia del riesgo”, a los ojos de MAGERIT no es correcto, ya que dicha transferencia puede ser parcial, lo que significa que se esta compartiendo el riesgo. Ahora dado que el riesgo tiene impactos que pueden ser encasillados como cualitativos y cuantitativos, así mismo, la compartición puede ser de índole cuantitativo, como por ejemplo asegurando un activo a través de una póliza de seguros o cualitativo cuando se comparte con un tercero, por ejemplo, prestigio o implicaciones legales, “se comparte por medio de la externalización de componentes del sistema, de forma que se reparten responsabilidades: unas técnicas para el que opera el componente técnico; y otras legales según el acuerdo que se establezca” (Gobierno de España, 2012b, p. 54).

Por último encontramos el tratamiento a través de la financiación, que consiste básicamente en una respuesta de la aceptación de un riesgo, debido a que en estos casos se deberá estudiar cuidadosamente la opción de destinar un fondo de recursos para hacer frente a la materialización del riesgo y enfrentar las consecuencias esperadas, “a veces se habla de ‘fondos de contingencia’ y también puede ser parte de los contratos de aseguramiento” (Gobierno de España, 2012b, p. 54).

7. Selección de una Metodología para Análisis y Gestión de Riesgos en el Sector Salud Colombiano

7.1 Particularidades del Sector Salud en Colombia

Como primer paso en la selección de una metodología para el análisis y gestión de riesgos en el sector salud en Colombia fue necesario establecer que hace distinto, en términos generales, a las instituciones médicas colombianas de otras ubicadas en otros países. En principio cualquier metodología de las estudiadas en este documento puede ser aplicada a instituciones médicas, de igual forma las prácticas médico científicas aplicadas por los profesionales de la salud en Colombia, corresponden a procedimientos estándares aceptados mundialmente, mas sin embargo, se encontró que el contexto socio económico colombiano es muy distinto del observado en aquellos países donde fueron desarrolladas las metodologías estudiadas.

Los estándares normativos y metodologías tratados hasta ahora tenían como denominador común, que no han sido desarrollados en Colombia, al contrario, los principales avances vistos en la aplicación al sector salud corresponden a medios socio económicos del primer mundo. En general una de las primeras diferencias encontradas entre contextos del primer mundo y el colombiano es la variable de cobertura que ofrece el sistema de aseguramiento, deducido a partir del gasto público en salud y que no corresponde a la totalidad del territorio nacional, pero que ha venido creciendo en los últimos años, “durante el último cuarto de siglo se ha logrado un aumento sustancial en la cobertura del sistema de aseguramiento” (Bernal et al., 2017, p. 222).

Pese al mencionado crecimiento, que ha beneficiado a segmentos poblacionales de bajos recursos, no se alcanza todavía el 100% del cubrimiento, lo anterior dadas las limitaciones en el

gasto público y las particularidades geográficas del territorio nacional, “los mayores aumentos en cobertura beneficien a los segmentos más pobres de la población, aunque la cobertura en algunas zonas aisladas de la geografía nacional sigue siendo deficiente” (Bernal et al., 2017, p. 222).

Otra problemática que fue identificada en el sector salud colombiano, es la deuda acumulada producto de los varios actores del sector, como también la necesidad de sanear los pasivos del sector público, sumado a la urgencia de capitalización de las EPS (Bernal et al., 2017, p. 223).

En Colombia la financiación del Sistema General de Seguridad Social en Salud (SGSSS) corresponde a la conjugación de varias fuentes, las cuales permiten a los ciudadanos tener acceso al plan de beneficios en salud, que “se financia con recursos fiscales y parafiscales que son administrados por una entidad del orden nacional denominada Administradora de Recursos del Sistema general de Seguridad Social en Salud (ADRES)” (Restrepo, 2018, p. 6).

Dentro del SGSSS se cuentan con un plan de beneficios compuesto por el cubrimiento de atención, servicios médicos y medicamentos que cubre un porcentaje importante de las necesidades de la población, aun cuando se contempla una segunda clase de prestaciones relacionada con la protección individual del derecho a la salud, que debe ser avalada por médicos o jueces en condiciones especiales que comprometan seriamente la salud de una persona (Restrepo, 2018, p. 6), adicionalmente se encuentran 2 prestaciones en salud más, la primera de ellas es a través de un seguro obligatorio para atención de victimas en accidentes de tránsito denominado SOAT y otro para accidentes o enfermedades de origen laboral llamado Aseguradora de Riesgos Laborales (ARL).

En cifras para el año 2016 de acuerdo a (Restrepo, 2018, p. 6) citando al Ministerio de Salud y Protección Social, los recursos tramitados a través del Plan de Beneficios del SGSSS fue de alrededor de 39 billones de pesos, esta cifra corresponde aproximadamente al 4,8% del PIB de Colombia y fue equivalente a un valor porcentual de alrededor del 75% del gasto total en salud. En lo referente a las prestaciones agrupadas como aquellas para la protección individual del derecho a la salud, en el mismo año 2016, se encontró que ascendió a un monto cercano a los 3,5 billones de pesos. En el año 2017 los recursos destinados por casos cubiertos por el SOAT fueron de cerca a los 3,4 billones de pesos y aquellos originados por las aseguradoras de riesgos laborales fueron de cerca de 3,1 billones de pesos y por último se encontró 1,54 billones, para el mismo año 2016, derivados de las acciones contenidas en el Plan Decenal de Salud Pública y el Plan de Acciones Colectivas, que fueron los beneficios con el objetivo de atacar ciertos determinantes sociales por medio de la promoción de la salud.

Se tomo una población para Colombia en el año 2016 de 47’213.862, producto de la interpolación entre las cifras oficiales del 2018 de 48’258.494 habitantes y del 2005 de 41’468.384 (DANE, 2018), considerando un gasto público per cápita de $826.000 al año, que fue alrededor de US$ 275 por persona al año, donde fue asumida una tasa cambiaria promedio de $3000 por US$1 para el año 2016.

A continuación, se muestra la comparación cuantitativa realizada a partir del total del gasto público en salud de Colombia contra estados representativos pertenecientes a la Organización para la Cooperación y el Desarrollo Económicos (OCDE), lo que pudo aclarar el grado de inversión pública en salud que hizo Colombia.

7.2 Comparación del Gasto Público en Salud Colombiano Frente a Economías miembros de la OCDE

De acuerdo con lo encontrado en las cifras de la OCDE (2019), el gasto público en salud en el año 2016, en Alemania fue del 9,4%, Francia 9,5%, España 6,4%, Estados Unidos 14,5% del PIB, que traducido en gasto público per cápita fue de US$3.992, US$3.534, US$1.703 y US$8.371 respectivamente.

País	Gasto Público %PIB	Gasto Público per cápita ($US)
Alemania	9,4	3992
Colombia	4,8	275
España	6,4	1703
Estados Unidos	14,5	8371
Francia	9,5	3534

Tabla 2. Comparación del gasto público en salud

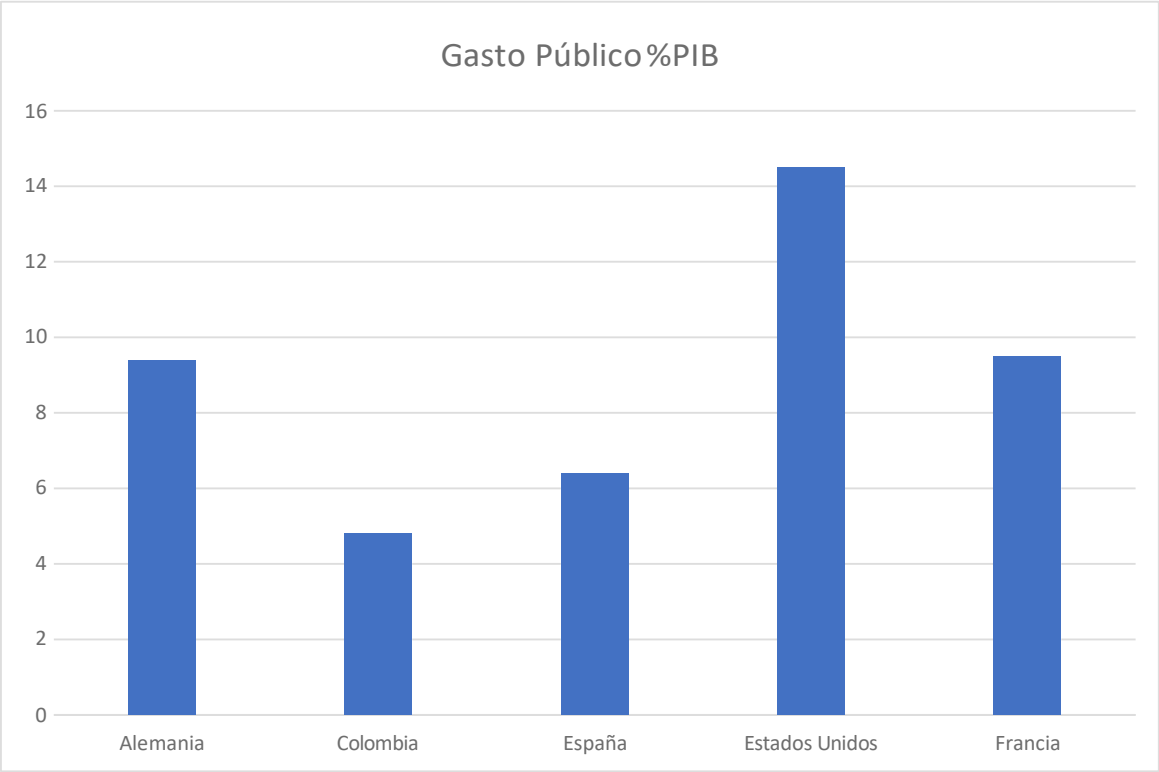

Figura 10. Porcentaje del PIB destinado al gasto en salud por países.
Fuente: El autor, basado en cifras de la OCDE

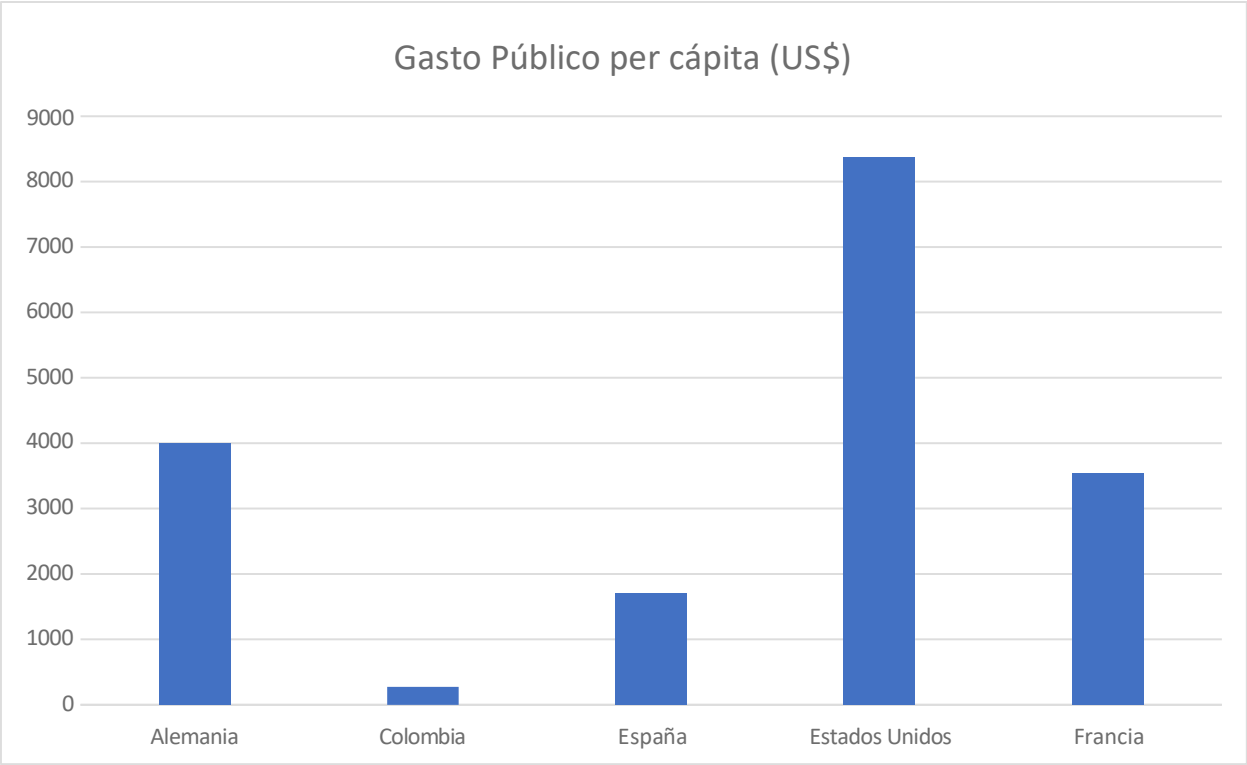

Figura 11. Gasto público en salud per cápita por países.
Fuente: El autor, basado en cifras de la OCDE

De lo anterior se concluyó que el gasto público en salud en Colombia es muy bajo en comparación con países del primer mundo, porcentualmente hablando el gasto público en salud en Colombia fue de tan solo el 3,3% del gasto público de Estados Unidos y en el mejor de los casos de solo el 16,1% del gasto público que realizó España.

7.3 Distribución de los Activos Financieros en el Sector Salud en Colombia

La clasificación de Instituciones Prestadoras de Salud (IPS) en Colombia corresponde a una segmentación de acuerdo al tipo de atención que prestan respecto al grado de complejidad del servicio, y dichas clasificaciones son distintas para instituciones públicas, privadas y mixtas, en el caso de las instituciones públicas se clasifican en tres segmentos que son complejidad baja, media y alta (Prada-Ríos et al., 2017, p. 52).

Para el caso de IPS de carácter mixto o privado se encontró que no existe una clasificación de las IPS, así que en el caso de querer hacer un análisis de los activos en el sector salud en Colombia, que tenga en cuenta las características del tipo de servicio prestado y quien lo presta, se dificultó incluir las IPS privadas, "no existe ninguna taxonomía en el país que clasifique todas las IPS, públicas o privadas, de acuerdo con los servicios prestados" (Prada-Ríos et al., 2017, p. 53).

Por lo anterior se hizo crucial encontrar un sistema clasificatorio y los elementos necesarios para desarrollarlo, que permitiera organizar los datos y presentarlos de forma tal que se logre extraer información comparativa que involucre a instituciones tanto del sector público como del privado, es así como (Prada-Ríos et al., 2017) propuso la adopción del Sistema de Cuentas de Salud (SCS), promovido por la Organización para la Cooperación y el Desarrollo Económico (OCDE) como referente a nivel de modelo conceptual estándar para la clasificación de las instituciones de prestación de servicios médicos de salud. Como fuentes de información se propuso primero el Registro Especial de Prestadores de Salud de Colombia (REPS) como fuente oficial de la oferta a nivel nacional, el Sistema de Información de Hospitales Públicos (SIHO) y la Superintendencia de Salud en Colombia.

De acuerdo con lo anterior resultó la siguiente clasificación o taxonomía propuesta por el estudio de (Prada-Ríos et al., 2017) en base al Sistema de Cuentas de Salud.

CODIFICACIÓN	CATEGORÍA	SUBCATEGORÍA
HP1	Hospitales	Hospitales Generales
		Hospitales de Salud Mental y Adicciones
		Hospitales de Especialidades
HP2	Establecimientos de cuidados residenciales a largo plazo	Centros residenciales de cuidado médico a largo plazo
		Centros de salud mental y abuso de sustancias
		Otros establecimientos residenciales de cuidado largo plazo
HP3	Prestadores de atención ambulatoria	Consultorios médicos
		Consultorios medicina general
		Consultorios de especialistas en salud mental
		Consultorios de médicos especialistas
		Consultorios odontológicos
		Consultorios de otros profesionales de salud
		Centros de atención ambulatoria
		Centros de planificación familiar
		Centros de salud mental y adicciones
		Centros independientes de cirugía ambulatoria
		Centros de diálisis
		Otros centros ambulatorios
		Prestadores de servicio de salud en casa
		Otros servicios ambulatorios
HP4	Prestadores de servicios auxiliares	Transporte de pacientes y rescate de emergencias
		Laboratorios médicos y de diagnóstico
		Otros prestadores de servivios auxiliares

HP5	Minoristas y otros prestadores de bienes médicos	Farmacias
		Vendedores al por menor y otros prestadores de bienes médicos duraderos y de aparatos médicos
HP6	Prestadores de promoción y prevención	Centros de promoción y prevención

Tabla 3. Taxonomía de acuerdo al Sistema de Cuentas de Salud propuesto por Prada-Ríos et al. (2017)

Según lo datos consultados del REPS (a corte de abril de 2015) existían 8461 IPS, la distribución de la participación en la oferta de prestadores de servicio se encuentra discriminada así (Prada-Ríos et al., 2017, p. 61) :

CODIFICACIÓN	CATEGORÍA	IPS	% Participación
HP1	Hospitales	1404	16,6%
HP2	Establecimientos de cuidados residenciales a largo plazo	7	0,1%
HP3	Prestadores de atención ambulatoria	5593	66,1%
HP4	Prestadores de servicios auxiliares	483	5,7%
HP5	Minoristas y otros prestadores de bienes médicos	70	0,8%
HP6	Prestadores de promoción y prevención	904	10,7%
	TOTAL	**8461**	100%

Tabla 4. Distribución de los prestadores de servicios de salud a abril 2015 REPS

De acuerdo con la tabla 4 se logró identificar que el mayor número de IPS se concentra en los prestadores de atención ambulatoria, con un 66,1% del total de IPS, en esta categoría HP3 se encontró por ejemplo puestos de salud, consultorios manejados por profesionales de la salud, centros de servicios ambulatorios, etc. (ver tabla 3).

Así fue como de la recuperación y tabulación de los datos de recursos económicos manejados por las IPS de acuerdo con los reportes financieros entregados por el SIHO, para el caso de IPS públicas y los reportes de la Superintendencia de Salud producto de la circular única, para el reporte de datos financieros de las IPS privadas a 2014, se construyó la siguiente tabla, teniendo en cuenta que del universo de IPS en Colombia, aquellas que reportaron estados financieros fueron el 65,4 % (Prada-Ríos et al., 2017, p. 62):

Codificación	Categoría	Patrimonio	Pasivos	Activos	% Activos respecto al total
HP1	Hospitales	7.907.984	2.952.752	10.860.735	90,47%
HP2	Establecimientos de cuidados residenciales a largo plazo	20.094	2.527	22.621	0,19%
HP3	Prestadores de atención ambulatoria	755.834	361.296	1.117.130	9,31%
HP4	Prestadores de servicios auxiliares	2.200	935	3.135	0,03%
HP5	Minoristas y otros prestadores de bienes médicos	48	41	89	0,00%

HP6	Prestadores de promoción y prevención	1.063	647	1.710	0,01%
	TOTAL	**8.687.223**	**3.318.198**	**12.005.420**	100%

Tabla 5. Resumen de datos financieros de IPS en Colombia a junio 2014 en Millones de pesos

A partir de la tabla 4 se logró observar como más del 90% de los activos en el sector salud en Colombia se encuentran concentrados en los hospitales, que solo representan el 16,6% del total de IPS en el país.

7.4 Análisis y Selección de una Metodología

Habiendo visto las particularidades del contexto colombiano, respecto a su sector salud, se estableció que la cobertura no es completa y en zonas aisladas de la geografía nacional sigue siendo deficiente. La mayor cantidad de prestadores de servicios de salud en Colombia (66.1%) son prestadores de servicios ambulatorios y estos solo representaban el 9.3% de los activos totales registrados. La destinación de recursos al gasto en sector salud en Colombia se encontró muy inferior al de economías desarrolladas.

De las anteriores particularidades se dedujo que la mayor parte de las IPS en Colombia cuentan con presupuestos muy inferiores a la media del país, que de por si, es muy inferior a la media en economías desarrolladas. De esta forma se evidenció la importancia que tiene el factor económico dentro de la selección de una metodología para el análisis y gestión de riesgos informáticos para prestadores de servicios de salud en Colombia, lo que muy posiblemente, puede en algún momento hacer dudar a los prestadores de servicios el dar la aprobación presupuestal para la implementación de un SGSI e incluso para un proyecto para el análisis y

gestión de riesgos informáticos, terminando por decidir englobar estos dentro de sistemas de gestión de riesgos generalista, “se debe tener en cuenta que el análisis de riesgos es un proceso costoso” (Santos Olmo Parra et al., 2016, p. 2898).

En alguna medida fue posible asociar los centros de prestación de servicios ambulatorios o consultorios de profesionales de la salud independientes como Pequeñas o Medianas Empresas (PYMES), sin que fuera necesario dejar de tener presente las particularidades misionales y el objeto social de cada organización, una forma como se advirtió que el comportamiento a nivel económico o de inversiones era similar a una PYME, fue observando los activos vinculados a prestadores de salud del tipo HP2, HP3, HP4, HP5 y HP6, que de acuerdo a las cifras entregadas por el REPS y SIHO citadas por (Prada-Ríos et al., 2017), mostraban los siguientes datos financieros promedios para este tipo de prestadores de servicios:

Codificación	Activos	Cant. IPS	Promedio Activos por IPS
HP2	22.621	7	3.231,57
HP3	1.117.130	5593	199,74
HP4	3.135	483	6,49
HP5	89	70	1,27
HP6	1.710	904	1,89

Tabla 6. Promedio de activos manejados por IPS en Colombia a junio 201 en Millones de pesos

Es así como en temáticas relacionadas con la seguridad de la información, como puede suceder en la PYMES, se presentan muchos casos en donde dichas temáticas son abordadas a la ligera o simplemente desconocer la verdadera magnitud de su importancia, en este caso por parte de prestadores de servicios de salud distintos a instituciones hospitalarias HP1, “debido principalmente a la asignación de responsabilidades a personal sin la debida formación. Así

mismo, la mayoría de las organizaciones carecen de políticas de seguridad y sistemas de evaluación del riesgo" (Santos Olmo Parra et al., 2016, p. 2897).

Dado el anterior panorama, de bajos presupuestos de inversión y personal poco idóneo en temas de seguridad de información, se concluyó la dificultad en la implementación de un proceso de análisis y gestión de riesgos de la información y mucho más difícil la planeación de un SGSI, "el análisis de riesgos es a menudo complejo y requiere conocimientos especializados, y que una evaluación de la situación actual requiere de herramientas de análisis de riesgos comerciales, las cuales no son fáciles de usar sin conocimientos técnicos adecuados" (Santos Olmo Parra et al., 2016, p. 2897).

	METODOLOGÍA / GUÍA NORMATIVA			
	Norma ISO 27005	**Norma ISO 31000**	**MARISMA - AGR**	**MAGERIT**
APLICABILIDAD AL SECTOR SALUD	SI	SI	SI	SI
CON UN ENFOQUE A ORGANIZACIONES CON BAJO PRESUPUESTO	NO	NO	SI	NO
CON UN ENFOQUE HACIA PEQUEÑAS ORGANIZACIONES	NO	NO	SI	NO
ENMARCADA DENTRO DE UN PROCESO DE MEJORAMIENTO CONTINUO	SI	SI	SI	SI
APLICABLE A UN MARCO NORMATIVO ISO/IEC 27001	SI	SI	SI	SI
REQUIERE ALTO NIVEL DE EXPERTICIA DE PROFESIONALES EN SU IMPLEMENTACIÓN	SI	SI	SI(1)	SI
NIVEL DE CONFIABILIDAD EN RESULTADOS INICIALES	MUY ALTO	MUY ALTO	ALTO(2)	MUY ALTO

(1) Requiere alto nivel de experticia en los profesionales que constituyen el Grupo de Expertos del Dominio (GED) y construyen el Esquema para Análisis y Gestión de Riesgos inicial, pero no necesario en un proceso de mantenimiento dinámico.

(2) Encontrar un nivel muy alto de confiabilidad se logra en un proceso de mejoramiento continuo llamado Mantenimiento Dinámico del Análisis del Riesgo que se consigue a mediano plazo.

Tabla 7. Resumen de comparativa de metodologías o guías normativas

Habiendo cursado un análisis de las anteriores particularidades del medio colombiano se hizo presente la necesidad de tomar una decisión de selección de una metodología, que guardando la rigurosidad técnica requerida, mantuviera costos de implementación controlados que pudieran ser asumidos por el mayor porcentaje de IPS en Colombia, y más aún, costos reducidos en su mantenimiento y proceso de mejora continua a largo plazo, es así que con estas condiciones fue posible identificar y optar por la metodología MARISMA AGR como la candidata más ajustada a tales condiciones, dado que dicha metodología es “un proceso orientado a las PYMES y enfocado a reducir los costes de generación y mantenimiento del proceso de análisis y gestión del riesgo” (Santos Olmo Parra et al., 2016, p. 2900), donde no se paso por alto el hecho que de acuerdo a lo analizado en el numeral 6.2, su aplicación a instituciones médicas es perfectamente plausible, y no se olvido que su carácter dinámico facilita su proceso de mejora continua y su recomendable implementación y aplicación dentro de un SGSI bajo la norma ISO 27001.

8. Propuesta de Adaptación Metodológica al Marco Nacional Colombiano

Habiendo propuesto la metodología MARISMA AGR como procedimiento más plausible para una mayoritaria adopción en el ámbito colombiano, dadas las particularidades de este, se hizo necesario evaluar dicha metodología para encontrar que aspectos eran susceptibles de adaptaciones como miras a la mejora de su facilidad de implementación en instituciones prestadoras de servicios de salud.

Se hizo una revisión de los pasos de la metodología que se pudieron resumir en 3 procesos que se enuncian a continuación:

1. Generación de Esquemas para el Análisis de Riesgos (GEAR).
2. Generación del Análisis y Gestión del Riesgo (GAGR).
3. Mantenimiento Dinámico del Análisis de Riesgos (MDAR).

Analizado el paso 1 (GEAR), se notó que su importancia radica en el hecho en que aquí se debe realizar la selección de los elementos que permiten dar cumplimiento a los requerimientos, para cada IPS, en donde estas últimas y para este caso correspondían a los 6 tipos de prestadores de servicios clasificados anteriormente, este primer paso al final dará como resultado un repositorio de esquemas, pero para lo cual, se requiere una serie de entradas entre las cuales se debe tener en cuanta la legislación aplicable y el conocimiento de expertos de seguridad.

8.1 Definición del Marco Normativo Aplicable

Como parte de la adaptación al contexto colombiano e IPS, se estableció que debe iniciar con la selección del margo normativo y legislativo que hace parte de las entradas, pero ya aquí no de forma general, sino dando nombre propio a cada unos de los actos legislativos aplicables. Para el caso de Instituciones Prestadoras de Servicios de Salud se encontró que son la resolución 1995 de 1999 del ministerio de salud, de acuerdo con lo estipulado en el artículo 8 de la Ley 10 de 1990, con respecto a las normas científico - administrativas, de obligatorio cumplimiento por las entidades que integran el sistema de salud, en donde se establece la normatividad para el manejo de historias clínicas.

Ley estatutaria 1581 de 2012, la cual dicta disposiciones generales para la protección de datos personales, que se encuentra parcialmente reglamentada en el decreto 1377 de 2013, que tiene por objeto "(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma".

8.2 Conocimiento por parte del grupo de expertos de Seguridad

Se estableció que el hecho de relacionar cada uno de los elementos seleccionados para el análisis del riesgo, como por ejemplo Tipos de Activos con Amenazas y Criterios de Riesgo, es una tarea que requiere conocimiento especializado, más aún cuando posteriormente se es necesario formular los controles pertinentes, pero dado que este conocimiento proviene de

profesionales altamente calificados y experimentados que requieren largas jornadas en la evaluación y formulación de una estructura de relaciones, los costos pueden ser elevados. Una manera que se estableció para reducir tales costos propios de la metodología es la reutilización de dicho conocimiento, que es "adquirido en las diferentes implantaciones, que es almacenado en una estructura denominada esquema para ser reutilizado con posterioridad, reduciendo los costes" (Santos Olmo Parra et al., 2016, p. 2900).

Una problemática detectada en la consecución del objetivo anterior, de reducir costes puede darse en casos tales, como aquel en el que el profesional a cargo de establecer los elementos necesarios para el análisis y formular la estructura de relaciones, desconozca parcial o totalmente las particularidades de las instituciones prestadoras de servicios de salud y cada uno de los tipos de las IPS consideradas.

Una forma de solucionar lo anterior fue a partir del hecho en que, se sugiere adoptar una clasificación de IPS valida tanto para el sector privado como el público, como el propuesto por (Prada-Ríos et al., 2017), que fue mostrada anteriormente, permitiendo así la creación de 6 esquemas reutilizables que sean validos para cada tipo de IPS. En este punto y como parte del proceso de adaptación de la metodología al país, se sugiere la participación del gobierno colombiano, en la creación de una base de datos de acceso general a las organizaciones del sector salud, a esquemas predefinidos para cada tipo de IPS u organización en el sector salud, de esta forma el profesional encargado del proceso de análisis y gestión de riesgos contaría con un gran avance inicial, que permitiría reducir los costes de implementación tanto para IPS de carácter público como también privado, teniendo en cuenta que el primer beneficiado serían todos los

pacientes y usuarios, que ven incrementado su nivel de protección de la información personal sensible.

8.3 Aplicación del Análisis de Riesgos

Con los elementos anteriores disponibles como lo son listado de controles, listado tipos de activos, listado de amenazas, relaciones entre los elementos anteriores es posible desarrollar un análisis de riesgos sobre la información de la organización, mas sin embargo, puede preocupar que con la adopción de un esquema aplicable al conjunto de IPS ubicadas en un mismo tipo, se puede dejar de lado cierta particularidad de la organización que se esta estudiando y que al final diera como resultado un estudio mediocre en calidad o alcance, pero es en este momento, donde se tiene que tener en cuenta que tratamos con la una metodología dinámica (cíclica) que va mejorando sus resultados a medida que se aplica una y otra vez, debido a la acumulación del conocimiento y experiencia por parte de la organización. También es de tener en cuenta que se debe sopesar la relación costo - beneficio, es decir que lo que se busca es un resultado suficientemente bueno y económico, como para cerrar las brechas más importantes de seguridad y no un estudio muy costoso que identifique y mitigue de un solo golpe todas los riesgos, “no se busca la opción óptima sino una opción razonablemente buena que permita grandes reducciones de tiempos” (Santos Olmo Parra et al., 2016, p. 2904).

Un ejemplo de lo anterior lo podemos tener al momento de identificar los activos de información, momento en cual pueden surgir dudas o problemas de reconocer y tratar como tal, pero dada la disponibilidad de un esquema aplicable al tipo de IPS analizada, es posible tener dicho listado de activos más importantes para ser considerados, como es el caso de las historias

clínicas de los pacientes, pero que indudablemente es uno de los más importantes. De la forma anterior se tendrá un listado lo suficientemente bueno como para abarcar la mayoría y más importante relación de activos de la organización, “se buscarán activos generales que se puedan valorar de forma sencilla tanto desde el punto de vista cuantitativo como cualitativo” (Santos Olmo Parra et al., 2016, p. 2905).

Como estrategia de implementación se sugiere el seguimiento del siguiente plan de tipo paso a paso, donde a continuación se resumen las tareas con que cuenta la metodología MARISMA AGR, incluyendo las anotaciones de adaptación propuestas a un escenario colombiano.

I. Generación de esquemas para el análisis de riesgos

Corresponde a la selección de elementos de entrada para el análisis y es aquí, en esta primera etapa, donde se deberá guardar el mayor cuidado referente al control de costos de desarrollo e implementación, lo cual se logra a partir de la consulta de repositorios y trabajos similares en instituciones taxonómicamente equivalentes. Las subtareas son:

a. Selección de tipos de activos
b. Selección de amenazas
c. Selección de controles
d. Selección de criterios de riesgo
e. Establecimiento de relaciones entre (Tipos de activos, Amenazas y Criterios de Riesgo)
f. Establecimiento de relaciones entre (Amenazas y Controles)

II. Generación del Análisis y Gestión del Riesgo

Este paso se trata de la evaluación de los riesgos a los que están expuestos los principales activos y formular el plan de gestión de dichos riesgos. Es de tener presente que la generación de un plan de tratamiento puede ser definido teniendo en cuenta las experiencias previas en instituciones similares.

a. Identificación de activos.
b. Realización del "check-list" lista de chequeo de los controles.
c. Valoración del listado de amenazas
d. Generación de la matriz de (Activos x Amenazas x Criterios de Riesgo)
e. Generación del análisis de riesgos
f. Generación del plan de tratamiento de riesgos

Las primeras 3 subtareas pueden ser realizadas de forma paralela e independiente. La subtarea (d) requiere completar las subtareas (a) y (c). La subtarea (e) requiere del resultado de las tareas (b) y (d) y la subtarea (f) requiere del resultado de la tarea (e).

III. Mantenimiento dinámico del análisis de riesgos

Esta última etapa de mantenimiento se debe enmarcar dentro del concepto de ciclo de vida, por lo cual se deberá reevaluar el proceso en general de forma periódica, constante y consistente, partiendo de una revaluación de los resultados de las matrices generadas previamente. Este proceso dinámico además de responder una práctica periódica también deberá ejecutarse cada vez que sea necesario tomar acciones oportunas, como por ejemplo después de la aparición de incidentes de seguridad o como parte de planes de

mejoramiento resultantes de procesos de auditoría u otros eventos que lo ameriten, lo que a la final se traduce en un recalculo del riesgo.

a. Gestión de los certificados de Cultura de la Seguridad
b. Gestión de los incidentes de seguridad
c. Gestión de métricas generales
d. Realización de auditorías periódicas
e. Recalculo Dinámico del Análisis de Riesgos
f. Gestionando el cuadro de mando (Dashboard) de Seguridad

Conclusiones

En el escenario de la aplicación de un sistema generalista de gestión de riesgos organizacional, es muy posible que se pasen por alto ciertas particularidades que tiene la información, como su clase, tratamiento, gestión en los sistemas informáticos y documentales, que bajo otra perspectiva podrían ser detectados, evaluados y mitigados gracias a la mirada experta de profesionales informáticos.

La aplicación de metodologías de análisis y gestión de riesgos generalistas que no tienen en cuenta las características de alta sensibilidad de la información personal de pacientes manejada por las organizaciones del sector salud, pueden en algunos casos dejar por fuera la contemplación de riesgos muy importantes para la seguridad de la información personal, y más aún, dejar sin un análisis de su impacto y lógicamente sin un tratamiento que permita, ante una eventual materialización del riesgo, un plan de acción que logre su mitigación.

En la actualidad existen diversas metodologías y/o marcos normativos para el análisis y gestión de riesgos de la información aplicables a un Sistema de Gestión de Riesgos de la Información (SGSI), pero a través de la identificación de ventajas o desventajas en una posible aplicación en una organización perteneciente al sector de la salud, facilita dar claridad a dudas o

inseguridades en una posible adopción, debido a las condiciones económicas limitadas a las que están sometidas muchas organizaciones del sector salud en Colombia.

La metodología MARISMA-AGR para el análisis y gestión de riesgos de la información presenta ventajas diferenciadoras frente a otras a nivel de costos de implementación, dados sus objetivos de economizar recursos en organizaciones con presupuestos muy limitados.

Se concluye que al definir una estrategia de aplicación paso a paso de una metodología adaptada a las particularidades socio económicas del medio colombiano, se facilita su comprensión y aplicación al interior de las organizaciones dentro de un SGSI en el sector salud, dados los indicadores económicos que muestran la mayoría de IPS en Colombia.

Finalmente se concluye que a través de un proceso de evaluación de metodologías fue posible identificar y adaptar una, que logra facilitar y disminuir los costos de implementación de procesos de análisis y tratamiento de riesgos informáticos en el sector salud colombiano, que se enmarquen dentro de un SGSI, y promueve el mejoramiento de las condiciones en la que es gestionada la información y de igual forma las condiciones en que es tratada la información personal de pacientes, proveedores y trabajadores del sector salud colombiano.

Trabajos a Futuro

Un posible y muy deseable paso que seguir sería la aplicación práctica de la metodología MARISMA-AGR a una mediana o pequeña organización perteneciente al sector salud en Colombia, que permita constatar la conveniencia de su adopción, además de las bondades que presenta el proceso de Mantenimiento Dinámico del Análisis del Riesgo, además podría dar las pautas necesarias para otro trabajo a futuro, consistente en la recopilación de distintos Esquemas para Análisis y Gestión de Riesgos que permita la construcción de un repositorio general de esquemas para el sector salud colombiano, que logre reducir drásticamente los costos de implementación y mantenimiento de un Sistema de Gestión de Riesgos y Seguridad de la Información (SGSI).

Dadas las similitudes que tiene el medio colombiano con otros países de la región, se podría realizar un estudio a nivel latinoamericano que evalué la conveniencia de adaptar la metodología seleccionada a un marco de aplicación más general, que permita el aseguramiento de efectuar procesos de análisis y gestión de riesgos informáticos en instituciones médicas latinoamericanas con condiciones de recursos económicos muy limitadas.

Referencias Bibliográficas

Abreu, J. L. (2012). Hipótesis, Método & Diseño de Investigación (Hypothesis, Method & Research Design). *Daena: International Journal of Good Conscience*, *7*(2), 187-197.

Agencia de la Unión Europea en Ciberseguridad. (2005). *Magerit* [Enisa]. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_magerit.html

Altés Jordi. (2013). Papel de las tecnologías de la información y la comunicación en la medicina actual. *Seminarios de La Fundación Española de Reumatología*, *14*(2), 31-35. https://doi.org/10.1016/j.semreu.2013.01.005

Bernal, R., González, J. I., Henao, J. C., Junguito, R., Meléndez, M., Montenegro, A., Ramírez, J. C., Uribe, J. D., & Villar, L. (2017). *Informe de la Comisión del gasto y la inversión pública: Presentación y Resumen Ejecutivo*.

Bresser Laura, Köhler Steffen, & Schwaab Christoph. (2014). *The Development of an Application for Data Privacy by Applying an Audit Repository based on IHE ATNA*. IOS Press; nlebk. http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=1640459&lang=es&site=eds-live

Cagliano, A. C., Grimaldi, S., & Rafele, C. (2011). A systemic methodology for risk management in healthcare sector. *Safety Science*, *49*(5), 695-708. https://doi.org/10.1016/j.ssci.2011.01.006

Cordero José, & García Yadimyr. (2015). *Análisis de riesgos y recomendaciones de seguridad*

de la información del Hospital E.S.E. San Bartolomé de Capitanejo, Santander. http://repository.unad.edu.co/handle/10596/6366

DANE. (2018). *Censo Nacional de Población y Vivienda 2018*. https://www.dane.gov.co/files/censo2018/informacion-tecnica/cnpv-2018-presentacion-3ra-entrega.pdf

Dirección General de Modernización Administrativa de España. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (Vol. 1). Ministerio de Hacienda y Administraciones Públicas. http://administracionelectronica.gob.es/

Gede Wisnu A., N. L. (2019). *The Implementation of System Enterprise Risk Management Using Framework ISO 31000*. edsbas. https://doi.org/10.5281/zenodo.3256500

Gobierno de España. (2012a). *PAe - MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Portal de Administración Electrónica. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es#.XeCCEb97mRt

Gobierno de España. (2012b). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método: Vol. Vol.1*. Ministerio de Hacienda y Administraciones Públicas. https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html?idioma=es#.XeXbO797mRu

Gómez, R., Pérez, D. H., Donoso, Y., & Herrera, A. (2010). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, *31*.

http://www.redalyc.org/resumen.oa?id=121015012006

ICONTEC. (2006). *Norma Técnica Colombiana. NTC-ISO/IEC 27001. Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información. Requisitos*.

ICONTEC. (2008). *Norma Técnica Colombiana. NTC-ISO/IEC 27005. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información*.

ICONTEC. (2013). *Norma Técnica Colombiana. NTC-ISO/IEC 27002. Tecnología de la Información. Técnicas de Seguridad. Código de Prácticas para Controles de Seguridad de la Información*.

International Organization for Standardization. (2018). *ISO Survey 2018*. https://www.iso.org/the-iso-survey.html

International Organization for Standardization. (2020). *ISO - ISO 31000—Risk management*. ISO. https://www.iso.org/iso-31000-risk-management.html

Joint NEMA/COCIR/JIRA. (2007). *Information Security Risk Management for Healthcare Systems*. MITA (Medical Imaging & Technology Alliance). http://www.medicalimaging.org/wp-content/uploads/2011/02/Information-Security-Risk-Management-for-Healthcare-Systems.pdf

Melo Reyes, O. (2019). *Aspectos a tener en cuenta para el análisis de riesgos con base en las normas ISO/IEC 27001, ISO/IEC 27005 E ISO/ IEC 31000 ; Analisis de riesgos normas ISO*. edsbas. https://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.8EA261FF&lang=es&site=eds-

live&scope=site

Organisation for economic co-operation and development. (2019). *OECD Stat Health expenditure and financing*. https://stats.oecd.org/Index.aspx?DataSetCode=SHA

Pereira, S., Robinson, J. O., Peoples, H. A., Gutierrez, A. M., Majumder, M. A., Mcguire, A. L., & Rothstein, M. A. (2017). Do privacy and security regulations need a status update? Perspectives from an intergenerational survey. *PLoS ONE*, *12*(9), 1-11. a9h.

Prada-Ríos, S. I., Pérez-Castaño, A. M., & Rivera-Triviño, A. F. (2017). Clasificación de instituciones prestadores de servicios de salud según el sistema de cuentas de la salud de la Organización para la Cooperación y el Desarrollo Económico: El caso de Colombia. *Revista Gerencia y Políticas de Salud*, *16*, 51-65.

Restrepo, J. P. U. (2018). Estructura del gasto en Salud Pública en Colombia. *PAPELES EN SALUD No. 17*, *17*, 46.

Santos Olmo Parra, A. (1), Sanchez Crespo, L. E. (2), Alvarez, E. (3), Huerta, M. (4), & Fernandez Medina Paton, E. (5). (2016). Methodology for Dynamic Analysis and Risk Management on ISO27001. *IEEE Latin America Transactions*, *14*(6), 2897-2911. edselc. https://doi.org/10.1109/TLA.2016.7555273

Sittig, D. F., Belmont, E., & Singh, H. (2018). Improving the safety of health information technology requires shared responsibility: It is time we all step up. *Healthcare*, *6*(1), 7-12. https://doi.org/10.1016/j.hjdsi.2017.06.004

Sutton, J. (2013). Of Information, Trust, and ice cream: A recipe for a different perspective on the privacy of health information. *Arizona Law Review*, *55*(4), 1171-1200. lgs.

Tovino, S. A. 1. (2017). The HIPAA Privacy Rule and the EU GDPR: Illustrative Comparisons.

Seton Hall Law Review, *47*(4), 973-993. lgs.

Valencia-Duque, F. J., & Orozco-Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *22*, 73-88. ProQuest Central. https://doi.org/10.17013/risti.22.73-88

Verbano, C., & Turra, F. (2010). A human factors and reliability approach to clinical risk management: Evidence from Italian cases. *Safety Science*, *48*(5), 625-639. https://doi.org/10.1016/j.ssci.2010.01.014

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, *68*, 1-13. https://doi.org/10.1016/j.future.2016.08.011

Yusof, M. Mohd., Papazafeiropoulou, A., Paul, R. J., & Stergioulas, L. K. (2008). Investigating evaluation frameworks for health information systems. *International Journal of Medical Informatics*, *77*, 377-385. edselp.