ESTUDIO SOBRE EL CONOCIMIENTO Y LA APLICABILIDAD DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS MÉDICAS DE BOGOTA

Rosa María Zambrano Burbano

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

ESTUDIO SOBRE EL CONOCIMIENTO Y LA APLICABILIDAD DE LA SEGURIDAD INFORMÁTICA EN LAS EMPRESAS MÉDICAS DE BOGOTA

Rosa María Zambrano Burbano

Trabajo de grado presentado como requisito para optar al título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director
Yolima Mercado Palencia

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
PROGRAMA DE ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2018

Nota de aceptación:

_____
_____
_____
_____

Firma del presidente del jurado

Firma del jurado

Bogotá D.C (09, 08, 2018)

La preocupación por el hombre y su destino siempre debe ser el interés primordial de todo esfuerzo técnico. Nunca olvides esto entre tus diagramas y ecuaciones.

Albert Einstein

AGRADECIMIENTOS

A Dios, por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor. Un agradecimiento muy especial merece la comprensión, paciencia y el ánimo recibidos de mi familia y amigos, en los momentos más difíciles de mi vida, algunas están aquí conmigo y otras en mis recuerdos y en mi corazón, sin importar en donde estén quiero darles las gracias por formar parte de mí, por todo lo que me han brindado y por todas sus bendiciones.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

GLOSARIO

ACTIVOS: los activos son todos los elementos que requiere una empresa u organización para el desarrollo de sus actividades misionales y las que serán tratadas durante el proceso de análisis de riegos.

AMENAZAS: es la ocurrencia de cualquier tipo de evento o acción que puede provocar un daño, en el caso de la Seguridad Informática, los elementos de Información.

CONFIDENCIALIDAD: los datos sólo pueden ser precisos y trasformados por personas autorizados, tanto en el acceso a datos que son almacenados y durante la transferencia de ellos.

CIBERCRÍMEN: conjunto de actividades ilegales asociadas con el uso de las Tecnologías de la Información y las Comunicaciones, como fin o como medio.

DISPONIBILIDAD: el acceso a los datos debe ser asegurado en el momento necesario. Es importante proveer el acceso adecuado a la información y evitar fallas del sistema.

DATOS: es un grupo de sistemas lógicos que tienen como función manejar el software y el hardware.

EMPRESA MEDICA: establecimiento destinado a proporcionar todo tipo de asistencia médica, incluidas operaciones quirúrgicas y estancia durante la recuperación o tratamiento, y en el que también se practican la investigación y la enseñanza médica.

INTEGRIDAD: los datos son completos, no modificados y todos los cambios son reproducibles. Se debe conocer quién realizó el cambio y el momento que lo hizo.

SEGURIDAD: procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, con el fin de garantizar su confidencialidad, integridad y disponibilidad.

GESTION DE RIESGO: método para determinar, analizar, valorar y clasificar el riesgo, y así lograr implementar mecanismos de control.

VULNERABILIDAD: se considerada una debilidad del sistema informático, el cual puede ser utilizada para causar un daño en la capacidad, las condiciones y características del sistema mismo.

RESUMEN

Actualmente el desarrollo de la tecnología, hace que los administradores del sistema informático se preocupen más por la seguridad de la información, es por ello que ésta monografía permitió identificar las características, condiciones y factores de riesgo de la seguridad informática en empresas medicas; mediante el análisis crítico de distintas fuentes bibliográficas. Esta revisión permitió construir un marco teórico, en el cual se especifican las diferentes metodologías soportadas, su importancia y aplicabilidad. Posteriormente y después de las revisiones y análisis documentales, fue posible evaluar establecer que la metodología MAGERIT, es la mejor herramienta, que reconoce los riesgos asociados a autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad, a los cuales están sometidos los activos de la información en las empresas médicas de Bogotá. MAGERIT genera mayor confiabilidad en seguridad informática y además obtiene las mejores recomendaciones al momento de tomar decisiones ante un riesgo inminente. Finalmente se destaca que es de vital importancia que en las empresas médicas, se establezcan objetivos empresariales, políticas de seguridad que permitan controlar la realización de los procesos, y de esta manera mejorar el análisis de riesgos.

Palabras clave: Amenaza cibernética, información, telecomunicaciones, salud, sistemas

ABSTRACT

Currently the development of technology, makes the administrators of the computer system worry more about the security of information, which is why this monograph allowed to identify the characteristics, conditions and risk factors of medical companies; through the critical analysis of different bibliographic sources. This review allowed the construction of a theoretical framework, in which the different methodologies supported, their importance and applicability are specified. Subsequently and after the reviews and documentary analyzes, it was possible to assess that the MAGERIT methodology is the best tool, which recognizes the risks associated with authenticity, confidentiality, integrity, availability and traceability, to which the information assets are subject. In the medical companies. MAGERIT

generates greater reliability in computer security and also obtains the best recommendations when making decisions in the face of an imminent risk. Finally it is emphasized that it is of vital importance that in the medical companies, business objectives are established, security policies that allow to control the realization of the processes, and in this way improve the risk analysis.

Keywords: cyber threat, information, telecommunications, health, systems

INTRODUCCION

Sin duda alguna las telecomunicaciones en la historia y el desarrollo del mundo, merecen atención constante, debido a que estos medios reducen distancias, de forma que generan progreso en las empresas, siempre y cuando, se utilicen de manera positiva. Generalmente, las telecomunicaciones son una forma de comunicación electrónica a distancia, que satisface las necesidades de enlace rápido para el mundo, generando soluciones de problemas, además de entregar oportunamente el conocimiento, principalmente de ciencia, tecnología e innovación, hasta en lugares muy lejanos.

En Colombia, el impacto de las telecomunicaciones según Manchola[1]. Son de gran relevancia en el crecimiento de las empresas, ya que permiten el fluido de la información entre población-empresa-estado, y así agilizan distintos procesos jurídicos, de salud, educación, seguridad, entre otros (Ahora bien, este avance en las telecomunicaciones, ha traído como consecuencia la transferencia de datos e información confidencial, que generan dificultades en las empresas.

De acuerdo con Intel Security (2016), citado por El TIEMPO, el cibercrímen representa el 15% de los ilícitos cometido a empresas en Colombia y generó un daño económico cercano a 600 millones de dólares en el año 2016. Además señala que en la mayoría de las compañías, destinan bajo presupuesto para la seguridad informática, es decir, no supera el 10%, en el mejor de los casos. Igualmente, las amenazas cibernéticas se incrementan entre el 50 y 60% cada año.

Internamente en las organizaciones es importante llevar a cabo el desarrollo de políticas de seguridad, es por ello que en el desarrollo de esta monografía cabe destacar que es significativo la utilización de herramientas que permitan la seguridad de la organización, y en el trascurso del documento se presentarán metodologías de análisis de riesgos. La importancia y aplicabilidad en las empresas médicas de Bogotá en cuanto a la seguridad de los activos que posee. En consecuencia, éste estudio pretende conocer y analizar los elementos que se deben tener en cuenta, para lograr la mayor seguridad informática en las empresas médicas.

[1] MANCHOLA, Sandra. Investigación y sus posibles comienzos en la comunidad estudiantil. Caso Universidad Piloto de Colombia. In Telematics and information Systems (EATIS), 8th Euro American Conference on IEEE, 2016, 1-8 p.

TÍTULO

Estudio sobre el conocimiento y la aplicabilidad de la seguridad informática en las empresas médicas de Bogotá.

1. DESCRIPCIÓN DEL PROBLEMA

Es indispensable tener en cuenta que la seguridad informática, hace parte de la estructura de cualquier empresa o institución, ya que asegura que la información confidencial, bien sea material informático o programas de una organización estén utilizados de manera idónea y que el acceso a la información contenida, así como las modificaciones que se realicen, sólo sean posibles, por parte de personas autorizadas y que se encuentren capacitadas por la empresa. Así mismo, el constante desarrollo de la tecnología, hace que los administradores del sistema se preocupen más por la seguridad de la información, ya que dentro de las organizaciones, no se aplican sistemas de seguridad que permitan evaluar las amenazas y vulnerabilidades, tales como pérdida o fuga de información privada, amenazas de correo electrónico comercial o personal, y el ataque de virus; es por ello que se ve necesario el estudio de diferentes temáticas que ayuden a conceptualizar la importancia de la seguridad informática dentro de las organizaciones y evitar así la liquidación parcial o total de las mismas.

1.1 FORMULACIÓN PREGUNTA PROBLEMA

¿Las empresas médicas en Bogotá cumplen con los estándares de seguridad informática?

2. JUSTIFICACIÓN

Anteriormente dentro de las organizaciones médicas, se manejaba la información sobre bases de datos normales, es decir bases de datos no tan complejas con las que actualmente se manejan hoy en día, ya que en la actualidad las bases de datos tienen un estándar de seguridad que toda organización debe cumplir ya que esto garantiza confianza y credibilidad de la información que se está siendo almacenada, actualmente existe la Resolución N° 1441 de mayo 6 de 2013, expedida por el Ministerio de Salud y Protección Social, donde se muestra el Sistema Obligatorio de Garantía de Calidad de la Atención de Salud, aprobando que se acuerden los procedimientos y condiciones para la habilitación de los servicios de salud, de conformidad con el desarrollo del país y los avances del sector que permitan brindar seguridad a los usuarios frente a los potenciales riesgos asociados a la prestación de los servicios de salud, independiente de la especialidad prestada Ministerio de Salud y Protección Social. Es por ello que al realizar este proyecto se pone a prueba las metodologías que se podrían aplicar para lograr una disminución en las amenazas presentadas.

En la actualidad, se pueden presentar algunos factores de riesgo en el proceso de atención, dónde se pueden generar errores de digitalización, procedimientos entre otros, y para generar confianza en los pacientes es necesario que estos procesos se efectúen de mayor veracidad.

Entre las razones fundamentales de investigar los posibles factores de riesgo, asociados a la seguridad informática en las empresas médicas, se encuentran: el adecuado funcionamiento del servidor que permita dar soporte a la información personal del paciente, además apoye todos los procedimientos clínicos realizados, que se ejecuten de forma computacional y se digitalicen de forma idónea, para su posterior análisis y prescripción médica; cronograma de citas y atención de usuarios constantemente.

Es por ello que es necesario conocer y analizar la importancia de la seguridad informática en las empresas médicas, las características, las condiciones y los factores de riesgo y de esta forma generar la confianza suficiente a los pacientes, personal administrativo y médico, al momento de enfrentarse a la competencia, para mantener su seguridad y privacidad en medio del mundo globalizado.

3. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El desarrollo de la monografía se llevará a cabo con la revisión de diferentes fuentes bibliográficas que tengan correlación con la seguridad informática en las empresas médicas de Bogotá, tomando como límite desde el año 2015 hasta la actualidad, de esta manera se evalúa la evolución de la seguridad dentro de las organizaciones con el fin de determinar estrategias de seguridad en las empresas médicas, para minimizar los factores de riesgos que se presenten.

4. OBJETIVOS DE PROYECTO

4.1 OBJETIVO GENERAL

Realizar un estudio sobre la aplicabilidad de la seguridad informática en las empresas médicas.

4.2 OBJETIVOS ESPECÍFICOS

1. Revisar las fuentes bibliográficas que tengan relación con la seguridad informática en las empresas médicas de Bogotá, con el fin de encontrar información necesaria para el desarrollo de la monografía.

2. Describir los factores de riesgo, asociados a la información almacenada en las bases de datos, con el fin de conocer las vulnerabilidades existentes.

3. Describir la importancia de las técnicas de seguridad en empresas médicas de Bogotá, identificando los posibles riesgos a la infraestructura computacional, sistemas operativos, bases de datos, redes y sistemas de información.

4. Identificar la metodología de análisis de riesgo que puede utilizar una empresa médica de Bogotá, determinando así las vulnerabilidades que se pueden presentar.

5. MARCO REFERENCIAL

5.1 MARCO TEÓRICO

Una empresa médica, es un establecimiento destinado para la atención y asistencia a enfermos por medio de personal facultativo, enfermería, personal auxiliar y de servicios técnicos durante 24 horas. Tiene una estructura especialmente diseñada para cumplir las funciones de prevención, diagnóstico y tratamiento de enfermedades. En la Figura 1, se detalla la organización de una empresa médica, donde se encuentra los ejes de sistema asistencial, sistema contable, sistema gerencial, sistema de información, sistema técnico y sistema administrativo.

Figura 1. Diagrama organizacional de una empresa médica

Fuente: Del autor

En la actualidad las empresas se enfrentan a riesgos e inseguridades ocasionadas por una amplia variedad de amenazas, tales como: robo de información, suplantación de identidad, uso no autorizado de sistemas informáticos, virus informáticos o código malicioso, entre otros; los cuales pueden dañar de forma significativa los sistemas de información, así como también poner en peligro la continuidad del negocio. Por tal motivo, se recomienda a las organizaciones aplicar sistemas de seguridad para minimizar las amenazas o vulnerabilidades que están expuestos y de esta manera garantizar el fortalecimiento de las organizaciones.

A continuación, se muestran algunos tipos de seguridad informática.

- Como dice Arrieta[2] la seguridad organizacional: se implanta en el marco de seguridad que debe tener la organización, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, denotando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

- Según lo que indica Arrieta[3], la Seguridad Lógica trata de integrar y crear los procedimientos y mecanismos, que permitan monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, control de acceso a las aplicaciones, perfiles de seguridad y documentación sobre la gestión de soporte en sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso.

- Seguridad Física, definido por Arrieta[4], donde identifica los límites que se deben cumplir en cuanto a parámetros de seguridad, de forma que se puedan realizar transferencia de información, controles en el manejo de equipos, y control de los accesos a las distintas áreas con base en la importancia de los activos.

- Arrieta[5], presenta la Seguridad Legal, como los requerimientos de seguridad que deben cumplir todos los empleados y usuarios de la red institucional, bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos de la organización en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Dentro de la seguridad informática hay tres principios o aspectos fundamentales, que una organización debe poseer: confidencialidad, integridad y disponibilidad.

1. Confidencialidad, a veces denominada secreto o privacidad, es la condición, que asegura que la información no pueda estar disponible o ser descubierta por personas, entidades o procesos no autorizados.

[2] ARRIETA, Álvaro. Políticas y Normas de Seguridad Informática. gs-gestión de soporte en sistemas, 2011. 54p.
[3] Ibíd., p. 5.
[4] Ibíd., p. 7
[5] Ibíd., p. 9

2. García y Vidal[6], definen la Integridad, como una opción que garantiza que la información solo puede ser modificada, incluyendo su creación y borrado, por el personal autorizado. Es responsable que la información sea exacta y completa que el sistema no modifique o corrompa la información o que permita que alguien no autorizado al sistema lo haga

3. Disponibilidad, es la propiedad que certifica el acceso a los activos de información y la utilización de los recursos informáticos en cualquier instante por las personas autorizadas. Un sistema seguro debe proteger la información disponible para los usuarios. La disponibilidad significa que el sistema, tanto software como hardware, funcione de forma eficiente y que sea capaz de recuperarse velozmente en caso de fallo. El enfoque de la seguridad y de los mecanismos utilizados para su implementación está influido en cada caso por el más importante de esos tres aspectos en el lugar de que se trate.

Como lo indica García y Vidal[7], los términos de seguridad informática y seguridad de la información, se diferencian en que el primero contiene la seguridad en el ambiente informático, mientras que la información puede encontrarse en diferentes medios y formas y no solo en los medios informáticos.

5.2 MARCO CONCEPTUAL

Durante la ejecución del proyecto, se tendrán en cuenta algunos conceptos básicos tales como:

Seguridad de la información: se debe proteger la información de una organización de los daños causados por las herramientas informáticas o por personas mal intencionado que generen daños y quieran estropear la información y terminar con la continuidad de negocio.

Metodologías de análisis: ayuda a verificar cuales son los activos que hay dentro de una empresa y así ayuda a implementar estas metodologías para proteger los activos de la empresa ya sean de hardware o software.

Seguridad informática: es un área de la informática que se dedica a la protección de todo lo que compone un sistema informático conformado por: hardware, software y datos.

[6] GARCÍA PIERRAT, Gonzalo y VIDAL LEDO, María Josefina. La informática y la seguridad. Un tema de importancia para el directivo. Infodir Revista de Información para la Dirección en Salud, 2016, 12(22), 47-58p

[7] Ibíd., p. 58.

Finalmente dentro de esta clasificación de metodologías como se presenta en numeral 6 metodologías de análisis de riesgo se pueden evaluar diferentes metodologías y escoger la más apropiada, para lograr así minimizar los riesgos que se ocasionan dentro de una organización o empresa.

5.3 MARCO LEGAL

La Norma que establece sobre la gestión de seguridad informática es la norma ISO 27000, y 27001 que es establecida por la organización internacional para la estandarización, esta norma ayuda a facilitar el intercambio de información y contribuir a las trasparencia de tecnologías, y la norma 27001 ayuda a preservar la confidencialidad, integridad y disponibilidad.

Existen normas que rigen la seguridad de la información que pueden ser utilizadas en una organización, una de ellas puede ser: la norma ISO/IEC 27000, esta norma posibilita conocer la seguridad de la información ya que tiene implementado un Sistema de gestión de seguridad de la información que permite mantener la seguridad de la información. Norma ISO 27001 ayuda a garantizar la protección de los datos personales y privacidad, de acuerdo con la legislación y los reglamentos pertinentes. Norma ISO/IEC 27002 esta norma realiza todos los controles necesarios y así poder determinar el nivel en el que se tiene que implementar para minimizar los riesgos. Norma ISO/IEC 27005 es dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información.

6. METODOLOGÍA DE TRABAJO

En el desarrollo del trabajo de grado se utiliza la metodología de análisis explicativa la cual toma el análisis documental que permite conocer el estado de seguridad implementado en empresas médicas. Seguido del análisis de algunos casos específicos del tipo de seguridad que tienen las empresas y finalmente conocer la importancia que tiene aplicar las distintas metodologías de análisis de riesgos. Para el desarrollo de este proyecto, se identificaron diferentes metodologías de análisis de riesgos y de esta manera tener la técnica apropiada que permita lograr mejores resultados en cuanto a seguridad de la información.

Mediante las revisiones documentales, fue posible evaluar los riesgos a los cuales están sometidos los activos de la información en empresas médicas, bajo la metodología de análisis de riesgos. El desarrollo del proyecto se llevó a cabo en tres fases: la primera consistió en tener material necesario para el desarrollo; la segunda identificar que si se realizan procedimientos o métodos de control de seguridad en las organizaciones y la tercera es el análisis y evaluación de los resultados obtenidos.

La documentación recolectada permitió tener un amplio conocimiento de la seguridad de la información, todo esto se llevó a cabo con la utilización de trabajos previos, información y datos divulgados por medios impresos, audiovisuales y electrónicos.

7. TÉCNICAS DE ANÁLISIS Y PROCESAMIENTO DE DATOS

El análisis de las fuentes bibliográficas relacionadas con la seguridad informática en empresas médicas, se inició con un esquema de consulta bibliográfica, que incluyó identificar palabras clave, para su posterior búsqueda en línea en buscadores académicos: dichas palabras fueron: security of information, risk analysis, methodologies of analysis, entre otras. Posteriormente, mediante un esquema de observación y exploración de información en los buscadores académicos, se logró obtener numerosa información relacionada con el tema en diferentes años. En seguida se inició con la clasificación de la información obtenida, la cual ya fue filtrada desde el año 2010 hacia delante. Lo anterior permitió definir la importancia del conocimiento de la seguridad informática en empresas médicas, las características y los factores de riesgo. Por otro lado, con esta clasificación de documentos relacionados con el tema, se detalló el análisis de la información en organizaciones médicas, las cuales tienen o aplican técnicas de seguridad informática, dentro de este alcance se logró identificar si en las instituciones generan o llevan a cabo un plan de continuidad de negocio, en cuanto a la seguridad de los activos que tienen.

8. ESTUDIOS DESARROLLADOS SOBRE SEGURIDAD INFORMATICA EN EMPRESAS MEDICAS DE COLOMBIA

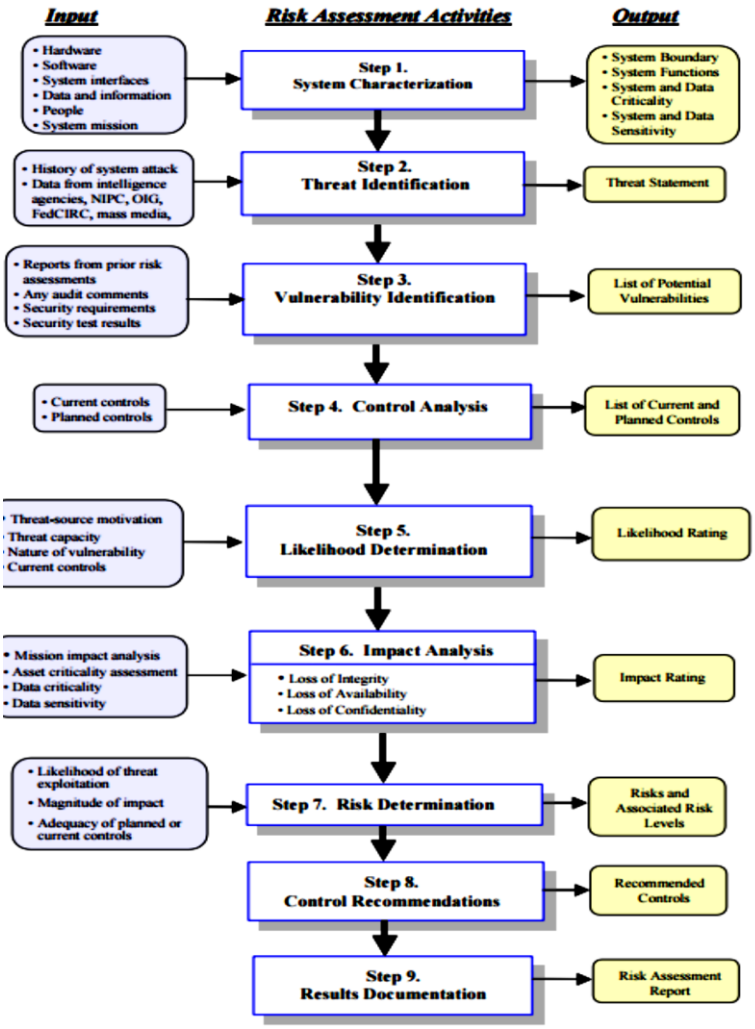
A continuación se muestran algunos estudios que se han desarrollado sobre seguridad informática para empresas médicas y la necesidad de salvaguardar la información, ya que al no tener las medidas adecuadas, las organizaciones se arriesgan a asumir la perdida de la información y posiblemente repercusiones legales.

Para fortalecer todo el sistema de seguridad en las empresas médicas se implementaron diversas certificaciones que garantizan mayor seguridad y respaldo de la información, tal como se muestra en los siguientes estudios.

- Los resultados del trabajo realizado por González y Parrado[8], en el análisis de gestión de incidentes de seguridad de la información para la oficina del ministerio de salud y protección social, indicó que la herramienta NIST (National Institute of Standards and Technology) NIST SP 800-30, Guía de Gestión de Riesgos para Sistemas de Tecnología de la Información, donde la SP 800, está enfocada a la seguridad de la información. El diagrama de proceso de esta metodología, se puede observar en la Figura 2.

[8] GONZÁLEZ, Andrés, y PARRADO Ángela. Guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación, 2016, 231p.

Figura 2. Diagrama de flujo NIST SP 800-30



Fuente: Tomado de González y Parrado (2016) p, 31.

Igualmente, tuvieron en cuenta la metodología Cramm., que consiste en el análisis de riesgos desarrollado por el Centro de Informática y la Agencia Nacional de Telecomunicaciones (CCTA) del gobierno del Reino Unido. El significado del acrónimo proviene de CCTARisk Análisis and Management Method. La primera versión es del año 1987 y la versión actual es la 5.2 basada en las mejores prácticas de la administración pública británica, por lo que es más adecuado para organizaciones grandes, tanto públicas como privadas, es lo que indica González y Parrado[9].

[9] GONZÁLEZ, Andrés, y PARRADO Ángela. Op. Cit., p. 56.

Con la realización de este trabajo, se logró obtener y desarrollar una metodología para la identificación de los incidentes de seguridad de la información que se presentan dentro del Ministerio de Salud y Protección Social (MSPS)., además según los niveles de impacto y las responsabilidades para la toma de acciones frente a los incidentes de seguridad de la información que se puedan presentar en el Ministerio de Salud y Protección Social, se definió el escalamiento que se debe tener en cuenta para informar o notificar los incidentes de seguridad de la información de los cuales se tenga conocimiento es lo que presenta González y Parrado[10]. Por otro lado, los autores recomiendan, realizar revisiones trimestrales del proceso de identificación de incidentes, para determinar la posible existencia de nuevos tipos de eventos de seguridad de la información, y un seguimiento, monitoreo y revisión continúa de todo el proceso de gestión del riesgo.

- En el estudio realizado por Amador[11] en su investigación de gestión del riesgo con base en ISO 27005 adaptando OCTAVE-S (2014), aquí se define el alcance del caso de estudio aplicando la metodología de la elipse al proceso de inscripciones y admisiones en DARCA e identificar los subprocesos con otros procesos dentro de la universidad del cauca y la interacción con otras entidades externas, adaptar la metodología de análisis y gestión del riesgo OCTAVE-S al caso de estudio cumpliendo con las directrices de la norma ISO/ IEC 27005 y finalmente efectuar el riesgo al caso de estudio con base en la adaptación de la metodología de análisis de riesgo OCTAVE-S, lo primero que se realizo fue la recolección de la información referente al proceso de inscripciones de y admisiones. Luego se procedió a crear la documentación del mismo debido a que no existía de manera detallada, obteniendo así siete procedimientos los cuales se presentan a continuación.

Definición del calendario de admisión, justificación del servicio de aplicación de la prueba, inscripciones, alistamiento para la aplicación de la prueba, aplicación de la prueba y evaluación de la prueba admisiones, y dentro de las organizaciones se pueda buscar las necesidades de seguridad de la información.

OCTAVE es una técnica de evaluación y planificación estratégica basada en el riesgo para la seguridad de la información esta metodología simplifica para las organizaciones más pequeñas que tienen estructuras jerárquicas planas y también una metodología llamada OCTAVE allegro que es utilizada es una versión más completa para la organización grandes o aquellos con estructuras de varios niveles.

[10] GONZÁLEZ, Andrés, y PARRADO Ángela. Op. Cit., p.36.
[11] AMADOR DONADO, Siler. Gestión del riesgo con base en ISO 27005 adaptando OCTAVE-S, Universidad internacional de la Rioja master universitario en seguridad informática, Popayán, Colombia, 2014. 21p.

Finalmente se concluye que dentro de la herramienta de la metodología OCTAVE se alinea con las directrices de la norma ISO 27005 de 2011, brindando una guía para identificar amenazas y estimar su impacto y probabilidad de manera cualitativa, sin embargo se considera conveniente adaptarla a un método cuantitativo que permitiera medir el riesgo y visualizar la reducción de este a medida que se ejecute la estrategia de tratamiento del riesgo.

- TORRES[12] en su investigación Modelo de Gestión de Riesgos Aplicando Metodología Octave Allegro en Entidades del Sector Fiduciario es una Herramienta Basada en el Método Mehari que mejora la productividad y la precisión de un enfoque de gestión de riesgos especialmente en contexto de medianas empresas, esta es una herramienta basada en el método MEHARI que mejora la productividad y la precisión de un enfoque de gestión de riesgos especialmente en contexto de medianas empresas. RISICARE define un perímetro de procesos claves para optimizar el proceso y los recursos sean internos o externos, apoyado en los siguientes parámetros, tales como: utilizar el método MEHAR, personalizar la base de conocimientos e incluso construir su propia base de conocimiento, relacionar la cuantificación de los escenarios de riesgo con una posible auditoría, desarrollar planes coherentes para optimizar la reducción de riesgos generales, todo esto con el fin de garantizar la seguridad de la información dentro de las organizaciones.

- Cruz, Parra y Ariza[13], en su trabajo de diseño de las políticas de seguridad para la institución social del estado hospital integrado san Antonio de puente nacional. Dentro de éste los autores realizaron un diagnóstico global de la seguridad de la información, con el fin de identificar los puntos críticos, además establecieron políticas de la organización, para aplicar las medidas necesarias; también diseñaron políticas de seguridad de la información para el hospital, de acuerdo con el diagnóstico y políticas actuales. Por lo tanto, identificaron diferentes áreas dentro de la organización, tales como: el área de contabilidad, área de facturación, área del sistema de información de atención al usuario SIAU, área de estadística, la gerencia; y así determinaron las amenazas y vulnerabilidades presentadas dentro del hospital, identificando los activos, como: aplicaciones de software y servicios. La metodología definida consistió en realizar un diagnóstico inicial donde detectaron vulnerabilidades en la administración de la información.

[12] TORRES MORALES. Modelo de Gestión de Riesgos Aplicando Metodología Octave Allegro en Entidades del Sector Fiduciario, Universidad Distrital Francisco José de Caldas, 2017.
[13] CRUZ VARGAS, German Alberto, PARRA Leonel y ARIZA Nancy. Diseño de las Políticas de Seguridad para la Empresa Social del Estado Hospital Integrado san Antonio de Puente Nacional. 2016.

Cruz, Parra y Ariza[14], frente a las vulnerabilidades existentes propusieron desarrollar metodologías que permitieran asegurar los activos de información del hospital San Antonio de Puente Nacional. Así mismo, plantearon diseñar políticas de seguridad de la información que estén de acuerdo con los lineamientos del gobierno en línea y así mantener la integridad, confiabilidad y disponibilidad de los activos de información del hospital.

La metodología que utilizaron los autores en el desarrollo del proyecto fue describir las fases de: Identificación, planeación, diseño y socialización cumpliendo así con el objetivo teniendo en cuenta la de referencia la norma ISO/IEC 27001.

Finalmente la generación de políticas de seguridad de información, a través de la metodología propuesta inició con la recolección de información para ello se usó el manual de procedimientos de la empresa social de estado hospital integrado San Antonio de Puente Nacional donde se ilustra de manera formal cada uno de los pasos para completar un procedimiento en cada área entre ellas las áreas SIAU (Sistema de Información y Atención al Usuario), contabilidad, estadística, facturación, gerencia; incluidas en la declaración de políticas de seguridad de la información.

Con el análisis del estado actual de la empresa se generó un documento con las incidencias encontradas, donde se describieron las vulnerabilidades, amenazas y riesgos a que los activos se exponen en las áreas.

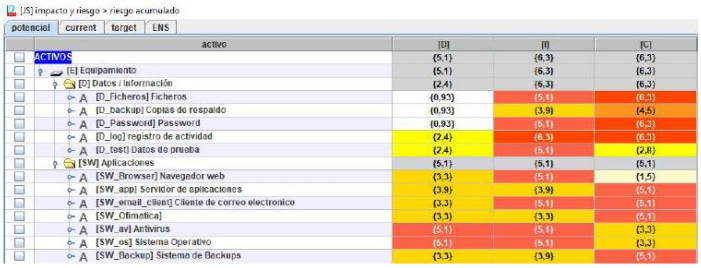
- Joya y Sacristán[15] en su tesis “Desarrollo de una Propuesta de Mitigación de Riesgos y Vulnerabilidades en Activos Lógicos para el hospital JAVESALUD I.P.S”, realizó un análisis de riesgos a los activos lógicos de JAVESALUD IPS, aplicado el modelo MAGERIT 3.0 y de esta forma se generó un informe de controles, normativas y buenas prácticas, enfocado a minimizar la probabilidad, la ocurrencia y el impacto de los riesgos más críticos.

También analizaron los diferentes datos de la entidad y de esta manera identificaron los activos lógicos y su impacto en JAVESALUD; además, desarrollaron un análisis de riesgos y vulnerabilidades de la entidad JAVESALUD basado en el modelo MAGERIT 3.0, con el fin de medir el impacto y criticidad. Igualmente, evaluaron los riesgos más críticos según el modelo realizado para construir el informe de controles y finalmente diseñaron un plan de capacitación en cuanto a políticas de seguridad informática, para incrementar los conocimientos de los colaboradores de la entidad.

[14] CRUZ German, PARRA Leonel y ARIZA Nancy. Op. Cit., p.25.
[15] JOYA CRUZ Javier y SACRISTÁN HERNANDEZ Carlos. Desarrollo de una propuesta de mitigación de riesgos y vulnerabilidades en activos lógicos para la empresa Javesalud I.P.S, Universidad Católica De Colombia, 2017.

Para el desarrollo y cumplimiento de los objetivos propuestos, realizaron entrevistas a los diferentes líderes de los procesos y así recolectar información relevante para poder cumplir con los objetivos propuestos; después se clasificó la información obtenida, mediante la metodología de MAGERIT, en la Figura 3, se presentan los activos que tiene la empresa JAVESALUD.

Figura 3. Activos de JAVESALUD


[5] impacto y riesgo > riesgo acumulado

potencial | current | target | ENS

activo	[D]	[I]	[C]
ACTIVOS	{5,1}	{6,3}	{6,3}
[E] Equipamiento	{5,1}	{6,3}	{6,3}
[D] Datos / Información	{2,4}	{6,3}	{6,3}
[D_Ficheros] Ficheros	{0,93}	{5,1}	{6,3}
[D_backup] Copias de respaldo	{0,93}	{3,9}	{4,5}
[D_Password] Password	{0,93}	{5,1}	{6,3}
[D_log] registro de actividad	{2,4}	{6,3}	{6,3}
[D_test] Datos de prueba	{2,4}	{5,1}	{2,8}
[SW] Aplicaciones	{5,1}	{5,1}	{5,1}
[SW_Browser] Navegador web	{3,3}	{5,1}	{1,5}
[SW_app] Servidor de aplicaciones	{3,9}	{3,9}	{5,1}
[SW_email_client] Cliente de correo electronico	{3,3}	{5,1}	{5,1}
[SW_Ofimatica]	{3,3}	{3,3}	{5,1}
[SW_av] Antivirus	{5,1}	{5,1}	{3,3}
[SW_os] Sistema Operativo	{5,1}	{5,1}	{3,3}
[SW_Backup] Sistema de Backups	{3,3}	{3,9}	{5,1}

Fuente: Joya y Sacristán (2017)

Dentro de la organización se determinaron algunas políticas de seguridad, todo esto con el fin de mejorar el nivel de seguridad de la información de JAVESALUD tanto para la información, el recurso humano, los accesos, la seguridad física y del entorno, las comunicaciones y las operaciones. Al realizar esta metodología se logró determinar que el la empresa JAVESALUD IPS, no cuenta con un proceso de gestión de riesgos informáticos para garantizar la seguridad informática del sistema.

Ya que fue posible encontrar y listar los activos lógicos que tiene el hospital donde se detectaron las amenazas relacionadas a cada activo y el impacto que se generaría en caso de materializarse y también se generaron controles necesarios a implementar.

AL finalizar el proyecto se identificación los riesgos y vulnerabilidades de JAVESALUD IPS, la observación de identificación de los riesgos de mayor impacto a través de las matrices correspondientes. Se emitió un informe donde se detallaron las posibles validaciones de procesos, protocolos y tareas que permitirán mitigar los riesgos de mayor impacto en la entidad.

- Bolívar[16] diseñó un sistema de gestión de seguridad de la información en la intranet del policlínico del Sur Olaya Bogotá, bajo la norma ISO 27001. Dicho

[16] BOLIVAR LEON, Jenny Andrea Diseño de un sistema de gestión de seguridad de la información En la intranet del policlínico del sur Olaya Bogotá, bajo la Norma ISO 27001,2015

estudio realizó un análisis preventivo y correctivo, con el fin de llevar una mejora en la administración y gestión de la Intranet conforme a la Norma ISO 27001 identificando las vulnerabilidades presentes en la organización.

Bolívar[17] estableció que la metodología MAGERIT es la norma que permite implementar un sistema de gestión y análisis de riesgos de los sistemas de información de forma organizada y que bajo esta herramienta es posible realizar las siguientes actividades:

- Identificación de activos
- Determinación de amenazas
- Estimación de impactos
- Determinación del riesgo
- Determinación de las medidas de seguridad necesarias

En la Figura 4 se observa el impacto acumulado por cada uno de los activos del Policlínico del Sur Olaya Bogotá.

Figura 4. Impacto acumulado

ACTIVO	D	I	C	A	T
Código fuente	9	9	9		
Documentación del proyecto	9	9	9		
Servidor	7	7			
Servidor DNS	7	7			
Servicio Directorio	6				
Servidor de correo electrónico	4				
Servidor web	10	8	8		
Software firewall		8	8		
Sistema de informacion de proyectos	10	9	9	8	
Software de sistema Operativo	10	9	9	8	
Servidores de Base de datos	10	7	8		
Firewall externo	10	6	7		
Firewall interno	10	6	7		
Router	10	6	7		
Red telefonica basica o RSDI	8				
Red Wan	9	6	7		
Red Lan	9	6	7		
UPS	10	3	8		
Servicios de Energía	10	3	8		
Cableado	10	3	8		
Muebles	3				
Internet	10	8	7		
EDIFICIO	10	8	8		
Administrador de Seguridad	5				

Fuente. Tomado de Bolívar (2015).

[17] BOLIVAR LEON, Jenny Andrea. Op. Cit., p. 24.

Así mismo, la Figura 5 muestra el riesgo acumulado, lo cual indica la medida en que las amenazas afectan los activos de orden superior al igual a los que depende de dicho activo.

Figura 5. Riesgo acumulado

ACTIVO	D	I	C	A	T
Código fuente	{7,2}	{7,1}	{7,5}		
Documentación del proyecto	{7,2}	{7,1}	{7,5}		
Servidor	{5,4}	{5,9}			
Servidor DNS	{5,4}				
Servicio Directorio	{5,4}				
Servidor de correo electrónico	{3,3}				
Servidor web	{6,8}	{6,3}	{6,3}		
Software firewall		{6,3}	{6,3}		
Sistema de información de proyectos	{6,8}	{6,9}	{6,9}	{5,7}	
Software de sistema Operativo	{6,8}	{6,9}	{6,9}	{5,7}	
Servidores de Base de datos	{7,2}	{5,0}	{5,7}		
Firewall externo	{7,2}	{4,4}	{5,1}		
Firewall interno	{7,2}	{4,4}	{5,1}		
Router	{7,2}	{4,4}	{5,1}		
Red telefónica básica o RSDI	{6,6}				
Red Wan	{7,2}	{4,4}	{5,1}		
Red Lan	{7,2}	{4,4}	{5,1}		
UPS	{7,4}	{2,7}	{5,7}		
Servicios de Energía	{7,4}	{2,7}	{5,7}		
Cableado	{7,4}	{2,7}	{5,7}		
Muebles	{3,3}				
Internet	{7,2}	{6,5}	{5,1}		
EDIFICIO	{6,8}	{5,7}	{5,7}		
Administrador de Seguridad	{3,8}				

Fuente. Riesgo acumulado. Tomado de Bolívar (2015).

Con la información anteriormente detallada, se logró dar a conocer a los empleados del policlínico que la política de seguridad es muy importante, para evitar minimizar los errores de los empleados. Además, permitió realizar un control de la utilización de la información, con el fin de evitar posibles consecuencias a nivel legal. Por otro lado, Bolívar[18] manifiesta que lo esencial a tener en cuenta para evitar los accesos de tipo no autorizado y los diferentes daños en el sistema es generar las distintas medidas de protección.

[18] BOLIVAR LEON, Jenny Andrea Diseño de un sistema de gestión de seguridad de la información En la intranet del policlínico del sur Olaya Bogotá, bajo la Norma ISO 27001,2015

9. TIPO DE AMENAZAS Y VULNERABILIDAES EN EMPRESAS MÉDICAS

Según Juntamay y Carrasco[19].Las amenazas a las cuales se ve afectado los sistemas de información de una empresa médica, está relacionada directamente con factores humanos, fallas en los sistemas de procesamiento de información, desastres naturales y actos mal intencionado y maliciosos. La seguridad de las bases de datos se ve afectada por la configuración de los procesos de conexión, hoy en día las bases de datos están accesibles al público desde internet y compartidas con los proveedores, aumentando la amenaza. Por lo tanto, es necesario proteger todos los niveles de vulnerabilidad.

A continuación se presentan algunos ataques que se pueden presentar en una base de datos, seguridad en redes, seguridad en páginas web y sistemas operativos.

- Descubrimiento de la información: las técnicas de inyección SQL, un atacante puede modificar consultas para acceder a los registros.

- Elevación de privilegios: todos los sistemas de autenticación que utilicen contraseñas almacenados en motores de base de datos, estos hacen que una vulnerabilidad de inyección SQL pueda permitir a un atacante acceder a la identificación de usuario.

- Denegación del servicio: la modificación de comandos SQL puede llevar a la ejecución de acciones destructivas como es el borrado de los datos.

- Suplantación de usuarios: al poder acceder al sistema sin contraseñas es posible que un atacante obtenga las contraseñas de otro usuario y pueda realizar modificación.

- Bases de datos sin actualizar: es necesario ir actualizando la versión de la base de datos con las últimas versiones lanzadas al mercado, ya que en ellas se solucionan aquellos problemas de seguridad detectados, ya que esta es una forma de controlar a los intrusos que quieran acceder a las bases de datos.

- Ataque por fuerza bruta: describe un estilo de programación primitiva, en el que el programador se basa en la potencia de procesamiento de la computadora en lugar de utilizar la inteligencia para simplificar el problema, los programadores de fuerza bruta, se escriben de una manera tediosa, llena de repeticiones,

[19] JUNTAMAY, MACAS. Estudio y aplicación de procedimientos de análisis forense en servidores de base de datos SQL Server y MYSQL, Caso práctico: DESITEL-ESPOCH, Escuela superior politécnica de Chimborazo, Riobamba. Ecuador, 2011.

cualquier intento criminal para acceder a un sistema informático por la ejecución repetida de una acción.

- Juntamay y Carrasco[20] define el desbordamiento de búfer: como la forma más conocida de las vulnerabilidades del software en cuanto a la seguridad, el desbordamiento de búfer es debido al error de técnicas expuestas, los desbordamientos de búfer no son fáciles de descubrir y si se descubre uno es muy difícil de explotar. Un desbordamiento de búfer ocurre cuando los datos que se describen en un búfer corrompen aquellos datos en direcciones de memoria adyacentes a los destinados para el búfer debido a una falta de validación de los datos de entrada.

- Seguridad en redes: es un nivel de seguridad que certifica que la puesta en marcha de todos los equipos y maquinas que estén dentro de una organización, la red que se encuentre configurada sea optima y que todos los usuarios de estas máquinas poseen los derechos que les han sido concedidos, para evitar así que personas no autorizadas intervengan en el sistema con fines malignos, y evitar que realicen operaciones involuntarias que puedan causar daño al sistema.

  Todos los sistemas informáticos conectados en red poseen identificadores para poder enviar y recibir la información desde otros sistemas. Esta identificación se conoce como la dirección IP (Internet Protocol), de esta manera un sistema pueda acceder a Internet, necesita tener una dirección IP única, que no se repita o que no posea otro sistema en la red. Para situaciones normales como envío de correo ofensivo, navegación, descarga de archivos, conversación con otros usuarios, es posible encontrar el rastro dejado por el computador utilizado, y en algunos casos logar detectar su ubicación física.

- Seguridad en páginas web: se considera que el filtrado que la seguridad de una aplicación, no se debe confiar en las entradas proporcionadas por los usuarios, para evitar ataques es necesario ejecutar validaciones utilizando JavaScript tanto para el cliente como para el servidor, es importante tener la validación de los datos del servidor ya que las validaciones del lado del cliente pueden ser sobrepasadas o incluso desactivarse, es necesario utilizar listas blancas para evitar datos erróneos en el ingreso de la aplicación y así poder implementar los datos proporcionados por el usuario del lado del servidor.

- El propósito del sistema operativo radica en gestionar los recursos de localización y protección del hardware, hoy en día la mayoría de dispositivos electrónicos utilizan microprocesadores para funcionar, llevan incorporado un sistema operativo. El objetivo de los sistemas operativos es ejecutar programas y resolver problemas del usuario de manera fácil y sencilla, haciendo que la

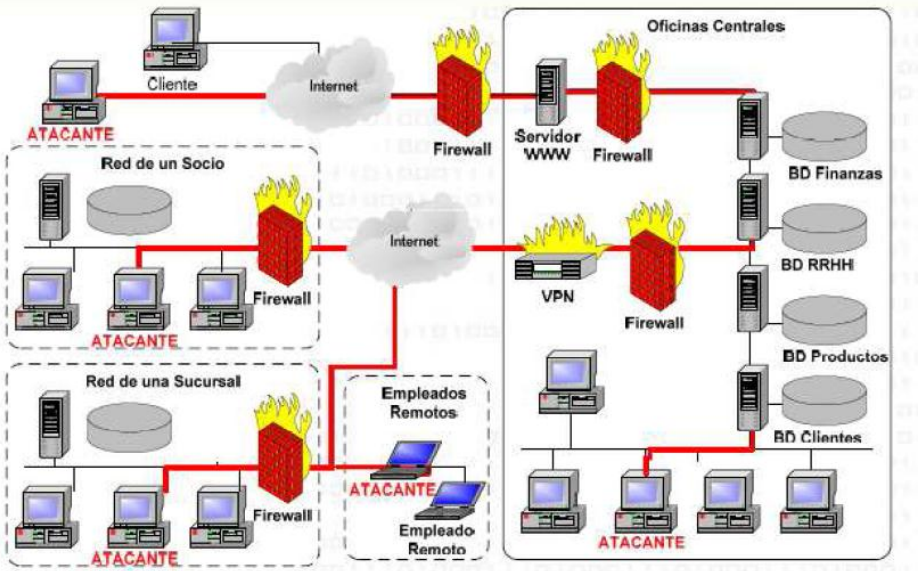
[20] JUNTAMAY. Op. Cit., p.40.

computadora sea cómoda y útil de usar, es importante proteger estos sistemas operativos ya que si se afecta la parte física y lógica de un sistema se vería afectada la información de una organización.

- Es necesario utilizar sesiones para la implementación de consultas ya que permite dar seguimiento al usuario, esto consiente en conservar valores de variables a través del sitio sin tener que emplear campos ocultos en formularios, logrando restringir el acceso a determinados elementos. Es significativo dar seguimiento a la sesión, así como iniciarla y terminarla de forma correcta, evitando infracciones y establecer el uso de sesiones en el lugar en el que el usuario comienza la interacción limitada con la aplicación

Finalmente en la Figura 6, se muestra un esquema de ataques a las base de datos, donde las vulnerabilidades inician desde el ingreso de un usuario a internet, aunque se observa que las bases de datos parecen estar seguras, no lo están porque los usuarios no están directamente conectados a ellas, sino a través de un servidor web, pero en realidad las bases de datos son frecuentes de ataque ya que usuarios que ingresan lo hacen a través de la red de datos o vía web.

Figura 6. Ataques a las bases de datos



Fuente. Recuperado de: http://dspace.espoch.edu.ec/handle/123456789/1425

10. IMPORTANCIA DE APLICAR TECNICAS DE SEGURIDAD EN LAS EMPRESAS MEDICAS DE COLOMBIA

En un entorno corporativo, complejo y progresivo es importante que una institución tome conciencia de aplicar continuamente una metodología de análisis de riesgo para garantizar el rendimiento de los sistemas y procesos dentro de la organización.

Entre las características más importantes a tener en cuenta, cuando se realice una aplicación de seguridad de la información es:

- Detallar visiblemente los activos y las políticas de seguridad ya que a partir de esto se podrían tomar decisiones y hacer mejoras en los procesos internos de la organización, para garantizar así la continuidad de negocio ya que permite tener en cuenta componentes y factores tanto internos como externos que intervienen en los objetivos misionales de la organización.

- Las técnicas de seguridad proporcionan herramientas que permiten mitigar los riesgos a los que está expuesta la información de una organización es por ello que se deben crea planes de contingencia y controles que aseguren y protejan los sistemas de información.

- Por medio de las técnicas de auditoria, de sistemas desarrollados por las empresas logren encontrar inconsistencias dentro del sistema, los cuales no han sido identificadas y no se sospechaba de su existencia. Existen, herramientas que son reconocidas por la Agencia Europea de Seguridad de las Redes y de la Información (ENISA) y promovida por el Consejo Superior de Administración Electrónica, la cual permite sistematizar el análisis de los riesgos que pueden presentar los activos de una organización. Éstas técnicas de seguridad son importantes porque el crecimiento de la tecnología dentro de las organizaciones se está dando de manera exponencial y, por lo tanto, es necesario minimizar los riesgos asociados al uso de los sistemas garantizando la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización.

Se debe tener en cuenta las siguientes tareas o actividades a desarrollar dentro de las organizaciones médicas para poder realizar así un buen desarrollo de técnicas de seguridad, tales como:

1. Caracterización de los activos: los activos son todos los elementos que requiere una empresa u organización para el desarrollo de sus actividades misionales y las que serán tratadas durante el proceso de análisis de riegos. Los activos se pueden

identificar ya sea como físicos, los cuales son: servidores, equipos, cableados, entre otros y lógicos como aplicaciones, bases de datos, sitios web, etc. Se debe determinar las dependencias entre los activos y finalmente la valoración de cada uno de los activos.

2. Caracterización de las amenazas: son todos aquellos hechos que pueden ocurrir en una empresa, perjudicando directamente los activos ya sea en el funcionamiento incorrecto o eliminación del mismo, dentro de esta caracterización se deben identificar las amenazas a las cuales están sometidos los activos. Dentro de esta fase se debe valorar las amenazas.

3. Caracterización de las salvaguardas: se identifica las salvaguardas pertinentes y la valoración de las salvaguardas

4. Estimación del estado del riesgo: son todas las debilidades de seguridad en la cual se encuentran los activos que se han identificado en el análisis y son susceptibles de amenazas para su daño o destrucción, se debe determinar la estimación del impacto y la del riesgo.

11. METODOLOGÍAS DE ANÁLISIS DE RIESGOS

Existen metodologías que permiten hacer un uso adecuado del análisis de riesgos y así asegurar los sistemas de información de las organizaciones. Entre las principales se tienen: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS, NIST SP 800:30.

En la Tabla 1 se hace referencia a las fases que componen cada una de las metodologías mencionadas anteriormente.

Tabla 1.Fases de las metodologías

FASES	1	1A	1B	2	3	4	5	6
caracterización del sistema	X	X	X	X	X	X	X	X
identificación de amenazas	X	X	X		X	X	X	X
Identificación de vulnerabilidades	X		X			X		X
Análisis de controles	X	X	X	X	X		X	X
determinación de la probabilidad								X
Análisis de impacto								X
Determinación del riesgo	X	X	X	X	X	X		X
Recomendaciones de control	X	X	X	X		X	X	X
Documentación de resultados	X			X				X
establecimiento de parámetros			X		X			
Necesidades de seguridad	X					X	X	

Fuentes: OCTAVE, (1A) OCTAVE S, (1B) OCTAVE ALLEGRO, (2) MEHARI, (3) MAGERIT, (4) CRAMM, (5) EBIOS, (6) NIST SP 800–30.

11.1 METODOLOGIA OCTAVE

La metodología OCTAVE (*Operationally Critical Threats Assets and Vulnerability Evaluation*), desarrollada por el Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), esta metodología ayuda a evaluar los riesgos de la seguridad de la información ya que OCTAVE propone un plan de mitigación dentro de las organizaciones que permiten reducir los riesgo de seguridad de la información para finalmente lograr una mayor protección de estos elementos dentro del sistema. OCTAVE ayuda a equilibrar aspectos de riesgos operativos, prácticas de seguridad y tecnología y a partir de estas características los entes basado en los principios de la seguridad de la información, esta

metodología propone dos objetivos específicos, uno de ellos y muy importante es dar a conocer que la seguridad de la información no solo depende de un técnico o personal encargado del sistema es una tarea de todas las personas que trabajan dentro de la organización y que pueden ayudar a proteger la información.

Hoy en día se han publicado tres metodologías de tipo OCTAVE y que han sido utilizadas para grandes organizaciones donde hay más de trecientos empleados, una de ellas es OCTAVE–S, esta metodología es utilizada en pequeñas empresas, por ejemplo, PYMES con veinte a ochenta empleados que tengan menor jerarquía y finalmente, OCTAVE ALLEGRO que permite analizar riesgos con mayor enfoque en activos de información, cada una de estas metodologías ejecuta las fases mencionadas con algunas variaciones dependiendo de las necesidades, OCTAVE ALLEGRO ayuda a establecer criterios de medición del riesgo, es te método se basa en la implementación de conjuntos de criterios cualitativos con lo cual se puede evaluar el efecto del riesgo contra la misión y objetivos de la empresa, también ALLEGRO ayuda a desarrollar un perfil de activos de información, se deben definir los activos que tengan valor dentro de la organización, ALLEGRO identifica contenedores de activos de información pertenecen a los repositorios o servidores donde esta almacenada la información y es aquí donde se debe tener más seguridad ya que los atacantes buscan estas partes para atacar. Con una metodología de análisis de riesgos como OCTAVE la empresa puede obtener beneficios como: dirigir y gestionar adecuadamente sus evaluaciones de riesgos, tomar decisiones basándose en los mismos, proteger los activos de información y, por último, comunicar de forma efectiva la información clave de seguridad, los cuales se derivan de las siguientes características: en primera medida, se establecen equipos auto dirigidos dentro de la organización con la finalidad de dar solución a las necesidades de seguridad que esta puede tener. Y por otro lado, se dice que este método es flexible ya que es adaptable a todo tipo de organización independientemente del entorno porque se basa en los riesgos, la capacidad de recuperación y la experiencia que se tenga en este tema.

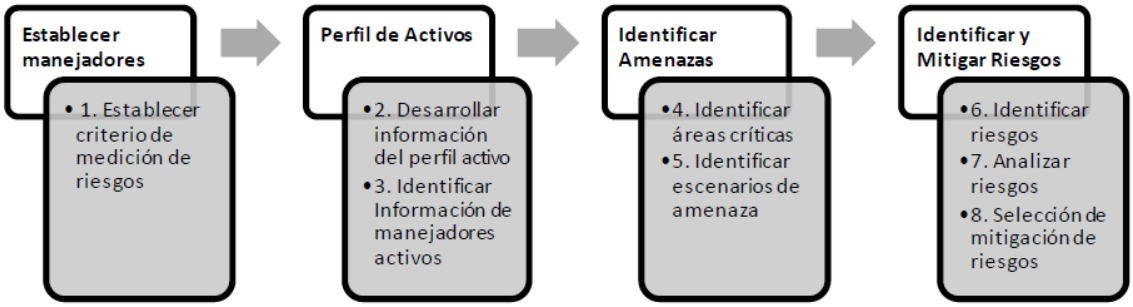
Finalmente el objetivo principal del OCTAVE es desarrollar una perspectiva de seguridad dentro de una organización teniendo en cuenta perspectivas de otros niveles para asegurarse que la implementación es fácil y es importante mencionar que OCTAVE busca asegurar la continuidad del negocio, identificar y medir riesgos, establecer controles para mitigarlos, conservar la información y los activos más importantes e intervenir en todas las dependencias de la organización, ya que de esta manera puede aprovechar al máximo el conocimiento de los distintos niveles de la empresa.

La metodología de OCTAVE clasifica los componentes de una empresa en activos y los ordena de acuerdo a su importancia en amenazas y vulnerabilidades la más clara decisión para desarrollar esta metodología se debe basar en una estructura que es la siguiente llevando un orden como primer paso la fase de visión organizativa, fase dos visión tecnológica y la fase tres y la más importante es

desarrollar una estrategia y plan de desarrollo para aplicar a las fases anteriormente mencionadas, a continuación se presenta el proceso que realiza el método de OCTAVE.

En la Figura 7 se muestra la manera de realizar el proceso de esta metodología es secuencialmente se realiza una tarea y después se continua con la siguiente es decir primeramente se establece manejadores, aquí se debe detallar los criterios de medición de riesgos, luego se realiza el perfil de activos, centro de este ítem se debe desarrollar información de los activos e identificar la información que maneja cada activo, seguidamente identifica las amenazas de las áreas críticas y se identifica los escenarios de amenazas y finalmente identifica los riesgos de tal forma que sirve para contrarrestar las amenazas a las cuales están siendo expuestos los activos de una organización.

Figura 7.Proceso de OCTAVE



Fuente: Propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del litoral

11.2 METODOLOGIA MEHARI MEHARI (METHOD FOR ARMONIZED ANALYSIS FRISK)

La organización Francesa define esta metodología como que suministra un conjunto de herramientas que permiten hacer un análisis de riesgos cualitativo y cuantitativo, cuando sea necesario para tener una adecuada gestión de seguridad. De lo anterior, se deduce que está diseñada para acompañar los procesos de análisis de riesgos empresariales tanto actuales como futuros. En la metodología MEHARI se hace un análisis de la seguridad basado en tres criterios básicos: confidencialidad, integridad y disponibilidad.

Esta metodología tiene como objetivo proporcionar procesos de evaluación y gestión de riesgos en el dominio de la seguridad de la información conforme a la norma ISO/IEC 27005.

11.3 METODOLOGIA MAGERIT

Descrita como la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, la cual es reconocida por ENISA (Agencia Europea de Seguridad de las Redes y de la Información) y promovida por el Consejo Superior de Administración Electrónica con el fin de sistematizar el análisis de los riesgos que pueden presentar los activos de una organización Molina[21]. Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los Sistemas de Información.

Según Camalo[22], MAGERIT se basa en analizar el impacto que pueda tener una organización la infracción de la seguridad de la información, buscando identificar las amenazas que pueden llegar a detectar la empresa y las vulnerabilidades que pueden ser utilizadas, esta metodología es importante ya que el crecimiento de la tecnología dentro de las organizaciones se está dando de manera exponencial y, por lo tanto, es necesario minimizar los riesgos asociados al uso de los sistemas garantizando la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización. MAGERIT presenta una guía de cómo llevar a cabo el análisis de riesgos y se divide en 3 libros, el primero describe la estructura del modelo de gestión de riesgos, el segundo presenta el inventario para enfocar el análisis de riesgos y el último compila una guía de técnicas de trabajo para dicho fin.

Igualmente está creada con el fin de cumplir con objetivos, tales como conocer el estado de seguridad de los sistemas de información e implementar medidas de seguridad, garantizar que no hayan elementos que queden fuera del análisis para que haya una profundidad adecuada en el mismo, mitigar las vulnerabilidades y asegurar el desarrollo del sistema en todas las fases. Estos objetivos han posicionado a MAGERIT como una de las metodologías más utilizadas en el ámbito empresarial ya que les permite prepararse para procesos de auditorías, certificaciones y acreditaciones y tener un nivel de alta calidad con los estándares establecidos.

Es necesario tener en cuenta que la metodología de MAGERIT persigue algunos objetivos tanto directos como indirectos algunos de ellos son:
Directos:

- Dar a conocer a todos los que hacen parte de las organizaciones que son responsables de los riesgos y amenazas que se están expuestos y que hay

[21] MOLINA MIRANDA, Mario, Fernando. Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. Espirales revista multidisciplinaria de investigación, 2017. 1-11p
[22] CAMALO, Luis. Gestión de riesgos. Recuperado de http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf, 2010.

formas de ayudar a evitarlos, eso dependería de cada empresa la forma como se maneja ese apoderamiento de la información.

- Ofrecer métodos que ayuden a analizar los riesgos que se derivan del uso inadecuado de las tecnologías de la información y comunicaciones (TIC).

- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

Indirectos:

1. Preparar a las empresas para ser evaluados y auditados para adquirir una certificación o acreditación.

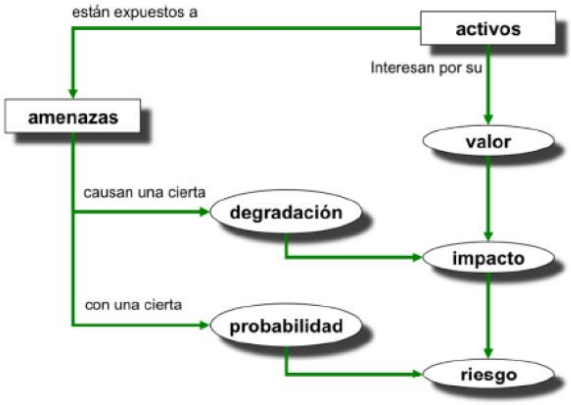
Con la implementación de MAGERIT según Molina[23]. Se puede describir la situación actual de la organización, luego a identificar los activos con sus respectivas amenazas, para proseguir a realizar la medición de riesgos existentes y sugerir las salvaguardas necesarias que podrían formar parte del plan de implantación, Para la evaluación se ha considerado la herramienta PILAR, la cual soporta el análisis y gestión de los riesgos de sistemas de información siguiendo la metodología MAGERIT. En la siguiente se presenta el modelo de MAGERIT.

La Figura 8 indica el modelo de la metodología de MAGERIT, donde se determina los activos valiosos que hay en la organización, su interrelación y su valor, estableciendo amenazas que están expuestos los activos anteriormente mencionados, buscar que salvaguardas hay dispuestas y cuán eficaces son frente al riesgo, también estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza. Y finalmente identificar cuál es el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

Esta metodología es una de las más opcionales para aplicar dentro de las organizaciones ya que les permite evaluar de manera detallada, y a cuales riesgos están siendo sometidos esos activos que hay en las empresas.

[23] MOLINA. Op. Cit., p. 35

Figura 8. Modelo MAGERIT



Fuente: Propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del litoral.

11.4 METODOLOGIA CRAMM CRAMM: (CCTA RISK ANALYSIS AND MANAGEMENT METHOD)

Es el método de análisis y control de riesgos de la Central Computer and Telecommunications Agency (CCTA) del gobierno británico, permite identificar, medir y reducir al mínimo los ataques a los que están expuestas las empresas día a día y es definida como una metodología que aplica los conceptos de manera formal, disciplinada y estructurada salvaguardando los principios de seguridad de la información de los activos de un sistema. Cabe resaltar que CRAMM realiza un análisis de riesgos cualitativo y cuantitativo por lo que se conoce como una metodología mixta, ésta se apoya de una herramienta de gestión, lo que permite a las organizaciones tener una visión clara y priorizada de las amenazas a las que está expuesta y que pueden afectar los recursos y la continuidad del negocio.

CRAMM es una metodología que sirve de apoyo para analistas de sistemas de información y esta metodología propone medidas eficaces para mejorar la seguridad de la información, esta metodología utiliza reuniones, entrevistas y cuestionarios para la recolección de datos, esta metodología ayuda a considerar el impacto de la perdida de confidencialidad, integridad y disponibilidad.

11.5 METODLOGIA EBIOS EBIOS

Novoa [24], define la metodología EBIOS como una Expresión de las Necesidades e Identificación de los Objetos de Seguridad, es una metodología francesa de

[24] Novoa Helena Alemán y Barrera Claudia. Metodología para el Análisis de Riesgos en los SGSI. Revista Especializada de Ingeniería.

gestión de riesgos, fue creada por la dirección Central de seguridad de los sistemas de Información de Francia DCSSI, con el fin de posibilitar la comunicación con los clientes internos y externos para contribuir al proceso de la gestión de riesgos de seguridad de los sistemas de información, de igual manera, ayuda a la empresa a tener un mayor reconocimiento en sus actividades de seguridad ya que esta tiene compatibilidad con las normas internacionales como la ISO.

Esta metodología tiene unas fases que ayudan a identificar bien los procesos de riesgos.

Fase 1. Análisis del contexto, se estudian cuáles son las dependencias de los procesos del negocio respecto los sistemas de información.

Fases 2 y 3: Análisis de las necesidades de seguridad y de las amenazas, se determina cuáles son los puntos de conflicto.
Fases 4 y 5: Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos secundarios.

11.6 METODOLOGIA NIST SP 800:30

La metodología NIST SP 800:30, según Avalos[25], está compuesta por nueve fases: caracterización del sistema, la cual permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la organización; identificación de amenazas, es donde se definen las fuentes de motivación de las mismas; identificación de vulnerabilidades, en esta fase desarrolla una lista de defectos o debilidades del sistema que podrían ser explotadas por una amenaza; análisis de controles; determinación de la probabilidad; análisis de impacto; fase de determinación del riesgo, ayuda a evaluar el riesgo en el sistema de información, recomendaciones de control en donde se proporcionan los controles que podrían mitigar el riesgo identificado disminuyéndolo hasta un nivel aceptable, finalmente está la documentación de resultados la cual genera un informe con la descripción de amenazas y vulnerabilidades, midiendo el riesgo y generando recomendaciones para la implementación de controles.

Esta metodología ayuda a optimizar la administración de riesgos a partir de los resultados en el análisis de riesgos, ayuda a proteger las habilidades de la organización para alcanzar su misión de las tic, el propósito de NIST SP 800:30es proveer una base de desarrollo de la gestión de riesgos, proveer información acerca de controles de seguridad en función de la productividad del negocio.

[25] AVALOS, Verónica. Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica NIST SP 800-30, 2013. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/2333/1/T-ESPE-021216.pdf, 2013.

Finalmente para proteger la seguridad de la información como un activo de la organización es necesario implementar metodologías apropiadas de identificación y análisis de riesgos que permitan gestionar acciones preventivas y tener contramedidas frente a las amenazas que se puedan presentar día a día.

12. METODOLOLOGÍA SUGERIDA PARA EL ANALISIS DE RIESGOS EN EMPRESAS MÉDICAS

Luego de la revisión de las diferentes metodologías orientadas al análisis de riesgo, tales como OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800:30, en donde se detallaba cada una de ellas y soportado en los estudios realizados sobre el análisis de riesgo en empresas del sector de la salud, se sugiere utilizar la metodología MAGERIT en las empresas médicas, teniendo en cuenta las características basadas en el análisis del impacto frente a una organización, especialmente en la infracción de la seguridad de la información. Además, busca y detecta las amenazas y vulnerabilidades a las cuales están expuestas las empresas médicas. Esta herramienta minimiza los riesgos asociados al uso de los sistemas, garantizando la autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad de los mismos, con la finalidad de generar confianza en los clientes tanto internos como externos de la organización. Así mismo, tiene algunos componentes fundamentales:

- Describe la estructura del modelo de gestión de riesgos.

- Enfoca el análisis de riesgos en el inventario.

- Compila una guía de técnicas de trabajo para dicho fin.

En consecuencia MAGERIT permite analizar de forma integral el riesgo, determinando la probabilidad, la ocurrencia de las amenazas y el impacto potencial en la organización, con el fin de mejorar la seguridad de la información.

Esta selección se ha basado en los estudios presentados en el numeral 9 en los cuales para ese tipo de empresas utilizaron la metodología de análisis de riesgos a determinar denominada MAGERIT.

- De acuerdo con los estudios presentados anteriormente, bajo la metodología MAGERIT por Cordero y García[26], los cuales lograron identificar todos los activos de información y de negocio de la institución, determinando las vulnerabilidades, amenazas y riesgos existentes en los sistemas de información, y así lograr establecer las posibles afectaciones al establecimiento. Los autores propusieron un plan de sensibilización, difusión y capacitación en políticas de seguridad informática para eliminar las vulnerabilidades existentes. Lo más relevante de esta investigación fue que la herramienta MAGERIT, a través del Software PILAR, determinaron los procesos críticos que maneja el E.S.E Hospital San Bartolomé de Capitanejo.

[26] CORDERO y GARCÍA. Op. Cit., p. 32.

- Por otro lado, Bastidas, López y Peña[27] investigaron la aplicabilidad de la herramienta en el hospital Susana López de Valencia de la ciudad de Popayán, a partir de la utilización EAR PILAR y enmarcado en la norma ISO 27001. Analizaron las vulnerabilidades y amenazas a la infraestructura tecnológica en la oficina de gestión de sistemas de información y telecomunicaciones del Hospital, diagnosticaron las vulnerabilidades y amenazas. Finalmente se determinó la probabilidad, ocurrencia de las amenazas y el impacto potencial en la Institución. eliminar

- Adicionalmente la tesis de Joya y Sacristán[28] realizó un análisis de riesgos a los activos lógicos de JAVESALUD IPS, aplicado el modelo MAGERIT 3.0 y obtuvieron la evaluación de los riesgos más críticos según el modelo realizado. Construyeron el informe de controles y finalmente diseñaron un plan de capacitación en cuanto a políticas de seguridad informática, para incrementar los conocimientos de los colaboradores de la entidad.

[27] BASTIDAS PARUMA, Henry y LÓPEZ ORTIZ, Iván. Análisis de riesgos y recomendaciones de seguridad de la Información al área de información y tecnología del hospital Susana López de valencia de la ciudad de Popayán, Universidad Nacional Abierta y a Distancia, 2014. 32p.
[28] JOYA y SACRISTÁN. Op. Cit., p. 25.

13. DOCUMENTACION DE LA METODOLOGÍA DE ANÁLISIS DE RIESGO EN UNA EMPRESA MEDICA EN BOGOTÁ

Teniendo conocimiento de los procesos desarrollados en una empresa médica oftalmológica de la ciudad de Bogotá que presta servicios de salud tales como medicina oftalmológica y exámenes diagnósticos, esta organización posee activos informáticos y sobre estos activos se propone realizar un ejercicio, empleando la metodología de análisis de riesgos MAGERIT, con la utilización de esta metodología se puede corregir las vulnerabilidades, amenazas y riesgos a los cuales está sometida la organización.

De acuerdo a lo establecido por la metodología de análisis de riesgos MAGERIT se desarrollaron las siguientes fases:

13.1 FASE DE DEFINICION DE ACTIVOS DE INFORMACIÓN

[D] Datos, es un activo abstracto que será almacenado en equipos de información.

[K] Claves criptográficas, la criptografía se emplea para proteger el secreto o autenticar a las partes, con el fin de proteger la información.

[S] Servicios, función que satisface una necesidad de los usuarios.

[SW] Software, son las aplicaciones informáticas, tales como aplicativos o programas, etc.

[HW] Hardware hace referencia a los equipos físicos que son utilizados dentro de la organización, como por ejemplo computadores, servidores, entre otros.

[COM] Redes de Comunicaciones, son los medios de transporte que llevan datos de un lugar a otro.

[Media] Soportes de información, son dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo, ejemplo discos duros, memorias, usb, etc.

[L] Instalaciones, donde se generan todos los procesos de servicios de la empresa.

[P] Personal, es el personal que está relacionado con los sistemas de información dentro de la organización.

13.2 FASE DE CLASIFICACION ACTIVOS DE LA ORGANIZACION

Se determina los activos relevantes, su interrelación y su importancia económica. En la Tabla 2 se presentan la clasificación de activos de la empresa médica oftalmológica de Bogotá.

Tabla 2. Activos de empresa médica

Tipos de Activos	**Descripción del Activo**
[D] Datos / Información	Reglamento interno de trabajo, procesos, formatos, Código Fuente: páginas web de la empresa Código Ejecutable: historias clínicas, agenda, programa contable, etc.
[K] Claves criptográficas	Claves de acceso a equipos de cómputo, software contable, etc.
[SW] Software	Programas, aplicativos, desarrollos: Historia Clínica, Agenda, Páginas Web, firewall, sistemas operativos (Windows), programa de control de acceso, Windows server 8 y programa contable, etc.
[HW] Hardware	Impresoras, teléfonos, datafonos, cito fonos, servidores, computadores, etc.
[COM] Redes de Comunicaciones	Modem de internet, Switch.
[Media] Soportes de información	Material impreso, memorias USB, discos duros
[L] Instalaciones	Edificio de empresa medica de oftalmología
[P] Personal	Personal que trabaja en la institución

Fuente el autor.

13.3 VALORACION DE LAS AMENAZAS

En la siguiente etapa se dimensiona la valoración de las amenazas a las cuales los activos están siendo expuestos, se pueden definir el origen de las amenazas, de origen natural como sismos que provoquen perdidas de las instalaciones de la empresa oftalmológica, puede presentarse también amenazas de tipo industrial ya que dentro de la empresa medica existen bajas de conexiones de corriente que

pueden causar daños en los equipos de cómputo y médicos, también pueden existir amenazas causadas intencionalmente por terceros.

La metodología de análisis de riesgos MARGERIT contempla dos tipos de valoraciones, cualitativa y cuantitativa. La primera hace referencia a calcular un valor a través de una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en la empresa oftalmológica su daño o perdida, en consecuencia la escala se refleja en:

- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (b)
- Muy bajo (MB)

En la Tabla 3 se presenta la valoración de los activos, describiendo los criterios de valoración

Tabla 3. Valoración de Activos

Valor	Criterio	Descripción
10	Daño muy grave a la organización	Muy alto (MA)
7-9	Daño grave a la organización	Alto (A)
4-6	Daño importante a la organización	Medio (M)
1-3	Daño menor a la organización	Bajo (b)
0	Irrelevante para la organización	Muy bajo (MB)

Fuente el autor.

13.4 VALORACION DE ACTIVOS

Dentro de esta fase se evalúa la valoración de los activos, de la empresa médica de Bogotá, teniendo en cuenta a que amenazas se enfrenta cada activo. En la Tabla 4 se presenta la calificación concreta de los activos de acuerdo al impacto que se podría tener dentro de la empresa.

Tabla 4. Valoración de activos de acuerdo al impacto

Activo	Amenaza	Impacto
Datos / Información	Robo de información	A
	Interceptación de información	A
	Destrucción de la información	A
Claves Criptográficas	Robo de claves y accesos	A
Servicios	Falla en servicios de comunicación	B
	Denegación del servicio	B
Software	Caídas en el sistema	B
	Fallo en los servicios de comunicación	B
	Fallas en los mantenimientos y actualizaciones	M
	Software dañino	M
	Fallas en la configuración	M
Hardware	Perdidas de equipos	A
	Robo	A
	Fallas en suministro eléctrico	B
	Desastres naturales	A
	Errores de mantenimiento (hardware)	A
	Errores de configuración	A
	Condiciones inadecuadas de temperatura	M
Redes de Comunicaciones	Errores de configuración	A
Soportes de Información	Disco con defectos de fabricación	B
Instalaciones	Falla en cableado de datos	M
	Fallas en red y tomas eléctricas	M
	Ingeniería social	A
Personal	Accesos no autorizados	M
	Errores de los usuarios	M
	Errores del administrador	M
	Abuso en los privilegios de acceso	M
	Ingreso de información falsa	M

Fuente el autor.

13.5 IDENTIFICACION DE LAS AMENAZAS

En la siguiente fase se identifican la valoración de las amenazas que pueden enfrentarse la empresa médica de Bogotá las cuales pueden ser:

AMENAZAS

- Desastres naturales: son los hechos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta, aquí se encuentran las amenazas de sismo de fuerte magnitud y daños por agua, etc.

- De origen Industrial: estos hechos se pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.

- Errores y fallos no intencionados: son los fallos no intencionales causados por las personas que trabajan dentro de la organización como errores de los usuarios, errores de los administradores, errores de configuración, descarga de software dañino, destrucción de la información, caídas del sistema, robo entre otros.

- Ataques intencionados: aquí se presentan los fallos causados por las personas, pueden ser la manipulación de la configuración, suplantación de la identidad del usuario, abuso de privilegios de acceso, difusión de software dañino, etc.

- Avería de origen físico o lógico: son problemas en el software y hardware de los equipos, se puede presentar debido a un defecto de fábrica o un desbordamiento en el funcionamiento del sistema.

- Corte del suministro eléctrico: son fallo que se presentan en la alimentación de energía, solo se cuenta con una fuente de respaldo para el servidor.

- Condiciones inadecuadas de temperatura o humedad: no se cuenta con áreas climatizadas, los equipos de cómputo se encuentran a temperatura ambiente, no existe ningún tipo de protección para evitar las condiciones naturales.

- Fallo de servicios de comunicaciones: Interrupción en la facultad de transmisión de datos de un punto de origen a un punto de llegada.

- Errores y fallos no intencionados. son los fallos no intencionales causados por las personas.

- Errores de los usuarios: errores humanos al momento de usar los servicios, datos, etc. Los usuarios ingresan de manera errónea datos al sistema, los cuales se pueden corregir solo parte del administrador del sistema informático.

- Errores del administrador: errores generados por personal con privilegios de administrador.

- Errores de configuración: introducción de datos de configuración erróneos que pueden ocasionar perdidas de los sistemas operativos

- Difusión de software dañino: propagación inocente de virus, gusanos, troyanos, bombas lógicas, etc. Los equipos, aunque cuentan con una versión free de antivirus, no están plenamente protegidos.

- Alteración accidental de la información: alteración accidental de la información. esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.

- Vulnerabilidades de los programas (software): defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos.

- Errores de mantenimiento / actualización de programas (software): defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante.

- Errores de mantenimiento / actualización de equipos (hardware): defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.

- Caída del sistema por agotamiento de recursos: la carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.

- Robo: pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad.

- Manipulación de la configuración: prácticamente todos los activos dependen de su configuración y ésta de la diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.

- Suplantación de la identidad del usuario: cuando un atacante consigue hacerse pasar por un usuario autorizado, disfruta de los privilegios de este para sus fines propios.

- Acceso no autorizado; el atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.

- Manipulación de programas: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

- Manipulación de los equipos: alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.

- Ingeniería social: Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.

13.6 CRITERIOS DE ACEPTACION DEL RIESGO

La descripción de los riesgos potenciales se relaciona en la tabla 5.

Tabla 5. Criterios de aceptación del riesgo

Rango	Descripción
Riesgo<=M	La empresa considera el riesgo poco identificable
Riesgo>M	La empresa considera el riesgo identificable y se debe ejecutar su respectivo procedimiento

Fuente el autor.

13.7 EVALUACION DEL RIESGO POTENCIAL A LOS ACTIVOS

En la Tabla 6 se muestra el análisis de riesgos de la empresa médica de oftalmología.

Tabla 6. Análisis de Riesgo

Análisis de Riesgos				
Activo	**Amenaza**	**Probabilidad**	**Impacto**	**Riesgo**
Datos / información	Robo de información	M	A	A
	Interceptación de información	M	A	A
	Destrucción de la información	M	A	A
Claves Criptográficas	Robo de claves y accesos	B	A	A
Servicios	Falla en servicios de comunicación	B	B	B
	Denegación del servicio	B	B	B
	Caídas del sistema	B	B	B
	Fallo en los servicios de comunicación	B	B	B
Software	Fallas en los mantenimientos y actualizaciones	B	M	M
	Software potencialmente dañino	M	M	M
	Fallas en la configuración	M	M	M
Hardware	Perdidas de equipos	B	A	A
	Robo	A	A	A
	Fallas en suministro eléctrico	B	B	B
	Desastres naturales	MB	A	M
	Errores de mantenimiento (hardware)	B	A	M
	Errores de configuración	B	A	A
	Condiciones inadecuadas de temperatura	M	M	M
Redes de Comunicaciones	Errores de configuración	M	A	A

Tabla 6. (Continuación)

Activo	Amenaza	Probabilidad	Impacto	Activo
Soportes de Información	Disco con defectos de fabricación	B	B	B
Instalaciones	Falla en cableado de datos	B	M	M
Instalaciones	Fallas en red y tomas eléctricas	B	M	M
Personal	Ingeniería social	B	A	A
Personal	Accesos no autorizados	MB	M	B
	Errores de los usuarios	B	M	M
	Errores del administrador	B	M	B

Fuente el autor.

13.7 POLITICAS DE SEGURIDAD PARA LA EMPRESA OFTALMOLOGIA DE BOGOTA

Al finalizar el ejercicio se presentan las siguientes políticas de seguridad, que se pueden practicar dentro de la organización tales como:

Políticas Generales

- Cada usuario al ingresar a un computador debe tener su usuario y contraseña.
- Los usuarios solo deben tener acceso a los servicios asignados y autorizados.
- Se debe restringir el acceso a internet para evitar que los usuarios descarguen o naveguen en páginas no autorizadas.
- Al usar el correo electrónico institucional los usuarios deben evitar abrir correo de remitentes desconocidos.
- Los usuarios de la organización deben utilizar los equipos de cómputo y médicos y si alguno de estas fallas, informar de manera inmediata al departamento de sistemas para así poder tomar las medidas necesarias.

Políticas de Seguridad a Nivel Físico

- Tener extintores contra fuego cerca del cuarto donde se encuentran el servidor y el archivo físico, se debe revisar anualmente para su respectivo mantenimiento.
- Se prohíbe el consumo de alimentos en los lugares de trabajo para evitar daños físicos en los equipos.
- Se debe tener control para el ingreso del personal al edificio para evitar así que personas que no son autorizadas ingresen y causen daños e inesperados y si hay personas que ingresen a las instalaciones o parte

Políticas de Seguridad a Nivel Lógico

- Todos los equipos con sistema operativo Windows debe tener instalado un software antivirus, el cual se actualizará manera automática, igualmente se realizará una revisión cada treinta (30) días, que incluya la actualización

general de la base de datos de firma de virus, análisis del equipo en busca de amenazas, eliminación de amenazas encontradas, etc.

- Los usuarios que están autorizados para el uso de dispositivos de almacenamiento externo están en la obligación de hacer uso del antivirus antes de ejecutar cualquier tipo de acción a fin de evitar que los equipos sean infectados.

- Las contraseñas contendrán al menos 3 de las siguientes condiciones: números, letras mayúsculas, letras minúsculas, símbolos; además poseer tenga mínimo 8 caracteres de longitud.

- Al finalizar cada trimestre del año se realizara cambio de contraseña para el acceso a las sesiones de Windows como a los programas que se usan en la organización.

Políticas de Respaldo y Recuperación de Información

- Las copias de respaldo de la información se realizaran diarias, semanal y mensualmente.

- Utilizando aplicaciones de software libre se podrán realizar copias automáticas de la información llevándolas a un disco externo.

- Se deben realizar respaldos de recuperación de la información y deben ser entregados al administrador de copias de seguridad.

- Deberá existir un administrador del sistema, que pueda verificar la correcta aplicación de los procedimientos de realización de las copias de seguridad y recuperación de los datos.

Políticas de Mantenimiento de Equipos

- Antes de encender el equipo de cómputo asegurarse de que este cuenta con las condiciones de ambiente adecuadas, verificación de corriente continúa etc.

- Al finalizar la jornada laboral se debe apagar el equipo de cómputo, verificando que este proceso se cumpla.

- Se deberá contar con protección ante fallas o interrupciones de energía mediante la utilización de UPS, en caso de una interrupción de energía se debe realizar apagado de los equipos de cómputo para evitar pérdidas de información.

- Se debe realizar mantenimiento preventivo físico a los equipos de cómputo, estos se realizarán cada 4 meses por personal capacitado.

- Toda actividad de mantenimiento realizada por el personal de sistemas contratado deberá estar documentada a fin de hacerle el seguimiento respectivo.

- Los mantenimientos preventivos físicos programados a los equipos de cómputo, se ejecutarán dentro de las instalaciones de la organización y bajo supervisión de una persona asignada por el departamento de sistemas.

Políticas de Uso de Software

- El administrador del sistema debe estar revisando que los equipos deben tener las últimas actualizaciones del sistema operativo Windows y parches de seguridad.

- Está prohibido el uso de programas sin licencias no autorizadas por la empresa. Solo el administrador o encargado del sistema puede instalar y verificar que los programas pueden ser instalados en los computadores.

- La Organización debe contar con un repositorio e inventario del software que hayan sido instalado en las diferentes áreas con el fin de que si se llegará a dañar algún computador se vuela a instalar las aplicaciones que esta tenia.

- Todo tipo de software adquirido por la empresa debe ser utilizado bajo los términos de licenciamiento.

- Los usuarios que utilicen los equipos de cómputo, manejará los programas de software solo con fines de trabajo y será responsable por el uso correcto de que se le da.

- El departamento de sistemas de la organización debe realizar revisiones periódicas por las diferentes áreas de servicio para identificar su correcto licenciamiento de software y así garantizar estabilidad y correcto funcionamiento de los equipos de cómputo.

13.8 SUGERENCIAS PARA LA EMPRESA OFTALMOLOGICA DE BOGOTA

Es necesarios capacitar al personal de la empresa oftalmológica, para el manejo de los equipos de cómputo y médicos con el fin de garantizar un buen uso de ellos y así evitar pérdidas de la información.

La ejecución de planes de actualización semanales, mensuales y de ser necesario diarios; pueden ayudar a los programas informáticos a contar con las últimas protecciones establecidas por sus mismos programadores. Lo anterior permitirá verificar que las fuentes de actualización son benignas, con el fin de evitar que los intrusos ingresen por páginas maliciosas.

Se sugiere que los sistemas de salud establezcan auditorías internas para los sistemas de seguridad de la información, ya que de esta manera se puede tener un control verídico de los activos que tienen las empresas médicas.

Implementar Software de Control: por software de control se hace referencia a cualquier aplicación o programa informático que ayude a identificar y mitigar cualquier tipo de amenaza. Entre estos programas se pueden encontrar los habituales antivirus, los cuales son bastante conocidos en la actualidad; aunque por sí solos tienen poca utilidad. Además de ellos se deben implementar Sistemas de Detección y Prevención de Intrusos IDS/IPS, Firewalls, Sistemas de Control de Acceso tanto físico como en el Sistema Operativo, entre otros.

CONCLUSIONES

Con el desarrollo de este proyecto se identifica que en su gran mayoría las empresas médicas no aplican sistemas de seguridad de la información, debido a la falta de conocimientos y de costos relacionados con el pago de servicios profesionales que implemente estándares de seguridad.

Con la elaboración de este proyecto, se puede definir un plan de continuidad de negocio dentro de las organizaciones médicas, ya que se implementarían metodologías de análisis de riesgos lo cuales se evaluarían todos los activos que hay dentro de la organización y de esta manera se podría identificar en que activos están más débiles y así emplear sistemas de seguridad para atacar a las amenazas que están siendo expuestos los activos de la empresas médicas.

En las empresas medicas la pérdida de información es ocasionada por la falta de seguridad, las cuales dan origen a muchas herramientas, modelos, metodologías, estándares o normas y soluciones para contrarrestar las amenazas informáticas y así evitar la pérdida o manipulación de datos en las organizaciones, y de este modo se establecen políticas de seguridad informática, con el fin de dar tener control en los sistemas de información internos en las empresas.

La revisión bibliográfica sobre la metodología MAGERIT y su aplicación en empresas médicas, permitió conocer los factores de riesgos asociados principalmente al uso de las bases de datos.

Se logró conocer la importancia de proteger los sistemas de información de vulnerabilidades que se pueden presentar, aunque es imposible de garantizar un 100% de seguridad al menos se puede evitar ser atacados utilizando métodos de encriptación o mecanismos de seguridad de la información.

RECOMENDACIONES

Uso de Credenciales de Usuario Fuertes: cuando se define el conjunto de normas para autenticar usuarios dentro de un Sistema de Información, se está hablando de las Credenciales de Usuario. En la mayoría de los casos, las credenciales suelen ser un nombre de usuario y contraseña; sin embargo, existen variantes donde pueden comprender el uso de huellas dactilares, medición de la retina del ojo y otros recursos biométricos. Cual sea el caso que se presente en las organizaciones, es altamente recomendado definir algunos requerimientos para el manejo de credenciales que resistan las diferentes amenazas de red.

Todas las metodologías de análisis de riesgos que se presentan en el trabajo son de gran importancia para que puedan ser estudiadas o evaluadas dentro de una organización ya que de esta forma se podría proteger la información y así se podría llevar un control interno de los activos que tiene las empresas.

Se recomienda que toda organización cumpla con estándares de seguridad utilizando alguna metodología de análisis de riesgos, y de esta manera se puede identificar las posibles vulnerabilidades en las que se encuentra el sistema de la organización, cuáles son las amenazas y las casusas, así mismo se puede observar los controles que se tienen y los que se necesita implementar para dar una confianza a la organización.

Se recomienda que dentro de las organizaciones se revisen constantemente la escala de riesgos, según la clasificación de activos que se haya realizado en la metodología de análisis de riesgos MAGERIT, y así identificar más fácilmente las amenazas y vulnerabilidades y de esta manera resolver de forma rápida cualquier tipo de intrusión de la información.

BIBLIOGRÁFIA

ARRIETA, Alvaro. Políticas y Normas de Seguridad Informática. gs-gestión de soporte en sistemas, 2011. 54p.

AVALOS, Verónica. Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica NIST SP 800-30, 2013. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/2333/1/T-ESPE-021216.pdf, 2013.

ANÁLISIS Y EVALUACIÓN DEL RIESGO DE LA INFORMACIÓN: caso de estudio Universidad Simón Bolívar. Recuperado de: http://www.scielo.org.ve/scielo.php?script=sci_arttext&pid=S1690-75152009000100004, 2014.

AMUTIO GOMEZ, Miguel. MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. (M. de H. y A. Públicas, Ed.). Madrid. Recuperado de http://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf, 2012.

AUDITORIA DE SISTEMAS, control interno informático. Recuperado de: https://noris14.wordpress.com/2011/06/10/control-interno-informatico/, 2011.

AMADOR DONADO, Siler. Gestión del riesgo con base en ISO 27005 adaptando OCTAVE-S, Universidad internacional de la Rioja master universitario en seguridad informática, Popayán, Colombia, 2014. 21p.

BALDEON, Mauricio y CORONEL, Christian. Plan maestro de seguridad informatica para la UTIC DE LA ESPE con lineamientos de la norma ISO /IEC 27002, Obtenido de http://repositorio.espe.edu. ec/bitstream/21000/6026/1/AC-GS-ESPE-034491.pdf, 2012.

BASTIDAS PARUMA, Henry y LÓPEZ ORTIZ, Iván. 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, Universidad Nacional Abierta y a Distancia, 2014. 32p.

BOLIVAR LEON, Jenny Andrea Diseño de un sistema de gestión de seguridad de la información En la intranet del policlínico del sur Olaya Bogotá, bajo la Norma ISO 27001,2015.

CAMALO, Luis. Gestión de riesgos. Recuperado de http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI-2010-Introduccion.pdf, 2010.

CORDERO MORENO,José y GARCÍA REYES, Yadimyr. Análisis de riesgos y recomendaciones de seguridad de la información del hospital E.S.E. San Bartolomé de Capitanejo, Santander, Universidad Nacional Abierta y a Distancia, 2016.

CONGRESO DE LA REPÚBLICA. MANUAL DE ESTRATEGIA DE GOBIERNO EN LÍNEA. Congreso de la República de Colombia. Disponible en: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf, 2014.

CÓRDOBA R., N. Evaluación de Riesgos, Amenazas y Vulnerabilidades. Recuperado de http://sisbib.unmsm.edu.pe/bibvirtualdata/tesis/basic/Cordova_RN/Cap5.2PDF

CRUZ VARGAS, German, PARRA Leonel y ARIZA Nancy. Diseño de las Políticas de Seguridad para la Empresa Social del Estado Hospital Integrado san Antonio de Puente Nacional. Institución Universitaria Politécnico Grancolombiano Facultad de Ingeniería y Ciencias Básicas Especialización en Seguridad de la Información. 2016.

DÍAZ, Ricardo, PÉREZ del Cerro y PROENZA-Pupo. Sistema para la Gestión de la Información de Seguridad Informática en la Universidad de Ciencias Médicas de Holguín. Ciencias Holguín, 2014. 13-26p.

DUSSAN Clavijo, Ciro Antonio. Políticas de seguridad informática. Entramado, 2006. 2(1) p.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA, Procedimientos e Impulso de la Administración Electrónica. MAGERIT – versión 3.0 Catalogo de Elementos para Análisis de Riesgos. Libro 3. España: Ministerio de Hacienda y Administraciones Públicas, 2015.

DANIEL P.F Análisis y Modelado de Amenazas. Recuperado de: https://radiosyculturalibre.com.ar/biblioteca/INFOSEC/Analisis-y-Modelado-de-Amenazas.pdf.

EL TIEMPO. (2016). Cibercrimen generó pérdidas por US$ 600 millones en Colombia .Bogotá – Colombia, Tomado de: http://www.eltiempo.com/archivo/documento/CMS-16493604, 2015.

FERRERO, Ernesto. Análisis y gestión de riesgos del servicio IMAT del sistema de información del I.C.A.I. Madrid, Universidad Pontificia Comillas. Obtenido de http://www.iit.upcomillas.es/pfc/resumenes/44a527ea231.pdf, 2006.

FREITAS, Vidalina. Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Caracas: Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10623695&p00=analisis+y+evaluacion+de+riesgos, 2009.

FERREIRO, Luisa. El Gobierno en Línea de Colombia. Universidad del Rosario. Disponible en: http://repository.urosario.edu.co/bitstream/handle/10336/4919/TESGOBIERNO_ELECTRONICO.pdf?sequence=1, 2015.

GARCÍA PIERRAT, Gonzalo y VIDAL LEDO, María Josefina. La informática y la seguridad. Un tema de importancia para el directivo. Infodir Revista de Información para la Dirección en Salud, 2016, 12(22), 47-58p.

GALLARDO, María. Análisis de riesgos informáticos y elaboración de un plan de continegencia TI para la empresa eléctrica Quito S.A: Obtenido de http://bibdigital.epn.edu.ec/bitstream/1500/3790/1/CD-3510.pdf, 2013.

GÓMEZ, Rafael. Metodología y gobierno de la gestión de riesgos de tecnología de la informacion. Obtenido de: http://www.scielo.unal.edu.co/scielo.php?script=sci_arttex&pid=SO121-4993201000012&lng=es&nrm=, 2010.

GONZÁLEZ AGUDELO, Daniel Felipe. El riesgo y la falta de políticas de seguridad informática una amenaza en las empresas certificadas BASC. Bachelor's thesis, Universidad Militar Nueva Granada, 2014.

GUTIÉRREZ, Camilo. Metodología MAGERIT: metodología práctica para gestionar riesgos, Obtenido de http://www.elsemanario.com/noticias/tecnologia/85028-magerit-metodologia-practica-para-gestionar-riesgos.html, 2013.

GONZÁLEZ, Andres, y PARRADO Angela. Guía de gestión de incidentes de seguridad de la información para la oficina de tecnología de la información y la comunicación–OTIC del ministerio de salud y protección social, tomando como base la norma ISO 27001:2013 Universidad Piloto de Colombia, Facultad de Postgrados, Especialización en Seguridad Informática, 2016, 231p.

ISO 27001. El estándar de seguridad de la información. Recuperado de: http://www.mondragon.edu/eps/jor/seguridad/JornadaSeguridadMCC-MU_archivos/Nextel.pdf

ISO 27001. El modelo de madurez de la seguridad de la información. Recuperado de: http://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de-madurez-de-la-seguridad-de-la-informacion/

ISO 27002.ES, Portal de soluciones técnicas y organizativas de referencia a los CONTROLES DE ISO/IEC 27002. Recuperado de: http://www.iso27000.es/iso27002.html

JOYA CRUZ Javier y SACRISTÁN HERNANDEZ Carlos. Desarrollo de una propuesta de mitigación de riesgos y vulnerabilidades en activos lógicos para la empresa Javesalud I.P.S, Universidad Católica De Colombia, 2017.

JUNTAMAY, MACAS. Estudio y aplicación de procedimientos de análisis forense en servidores de base de datos SQL Server y MYSQL, Caso práctico: DESITEL-ESPOCH, Escuela superior politécnica de Chimborazo, Riobamba. Ecuador, 2011.

LA SEGURIDAD DE LAS TELECOMUNICACIONES Y LAS TECNOLOGÍAS DE LA
INFORMACIÓN. Unión internacional de telecomunicaciones. Recuperado de: https://www.itu.int/dms_pub/itu-t/opb/hdb/T-HDB-SEC.03-2006-PDF-S.pdf

MANCHOLA, Sandra. Investigación y sus posibles comienzos en la comunidad estudiantil. Caso Universidad Piloto de Colombia. In Telematics and information Systems (EATIS), 8th Euro American Conference on IEEE, 2016, 1-8 p
PEÑA, Eduardo. Metodologías y normas para el análisis de riesgos: ¿cúal debo aplicar? Obtenido de http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgo%20TI.pdf, 2013.

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.We6wYXZrzIU.

MAGERIT-Versión 3.0 Metodología de análisis y gestión de riesgos de los sistemas de información. Recuperado de: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WiQBwnlrzIU

MAGERIT – versión 2, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: http://www.pilar-tools.com/doc/magerit/v2/meth-es-v11.pdf

MOLINA MIRANDA, Mario. Fernando. Análisis de riesgos de centro de datos basado en la herramienta pilar de Magerit. Espirales revista multidisciplinaria de investigación, 2017. 1-11p.

MAGERIT Versión 1.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Recuperado de: http://dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES MINTIC. Decreto número 2573 de 2015. Congreso de la República de Colombia. Disponible en: http://www.mintic.gov.co/portal/604/articles-14673_documento.pdf. Diciembre, 2014.

MINISTERIO DE JUSTICIA Y DEL DERECHO MINJUSTICIA. Estrategia de Gobierno en Línea, Manual 3.1. Congreso de la República de Colombia. Disponible en: http://www.minjusticia.gov.co/Portals/0/Ministerio/Planeacion_gestion_y_control/informe_de_GEL/Informe_de_Gobierno_en_L%C3%ADnea_2013_-_OIJ_ver_web.pdf, 2015.

Ministerio de Hacienda y Administraciones Públicas, MAGERIT: Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información., España. Ministerio para las Administraciones Públicas, 2015.

Novoa Helena Alemán y Barrera Claudia. Metodologia para el Analisis de Riesgos en los SGSI. Revista Especializada de Ingenieria.

PINTO, Ernesto. Análisis de seguridad para el manejo de la información médica en telemedicina. Ciencia e Ingeniería Neogranadina, 2011.

POVEDA, Jose. ANÁLISIS Y VALORACIÓN DE LOS RIESGOS, MÓDULO 8. Recuperado de: https://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-8.pdf, 2011.

Resolución N° 1441 de 6 de mayo. Definen los procedimientos y condiciones que deben cumplir los prestadores de servicio de salud para habilitar los servicios y se dictan otras disposiciones, 2013, 209p.

RÍOS, Luis Hernando. Importancia de las telecomunicaciones en el desarrollo universal. Ciencia e Ingeniería Neogranadina, 2016.

RONDEROS, Mario Fernando. Legislación informática y protección de datos en Colombia, comparada con otros países, revista Inventum, 2014, 17p.

REVISTA CIENCIA, INNOVACION Y TECNOLOGIA (RCIYT) Diciembre, vol. 1 no. 40, p. 39-53. ISSN 2390-058X. Ciencia, innovación y tecnología, V1, 2013, 39-53.

SEGURIDAD DE LA INFORMACIÓN COLOMBIANA. Recuperado de: http://seguridadinformacioncolombia.blogspot.com.co/2010/02/marco-legal-de-seguridad-de-la.htmlDownload, 2010.

TORRES MORALES. Modelo de Gestión de Riesgos Aplicando Metodología Octave Allegro en Entidades del Sector Fiduciario, Universidad Distrital Francisco José de Caldas, 2017.

YAÑEZ DE LA MELENA, Carlos y IBSEN MUÑOZ, Sebastián. Enfoque metodológico de auditoría a las tecnologías de información y comunicaciones. XIV Concurso Anual de Investigación,. Recuperado de http://www.olacefs.com/wp-content/uploads/2014/08/1erlugar.pdf, 2011, 1–82p.