ANÁLISIS DE LOS CONCEPTOS, ELEMENTOS Y TÉCNICAS DE LA GESTIÓN DE RIESGO ORIENTADO A LAS PYMES DEL SECTOR DE LAS TELECOMUNICACIONES BASADO EN MAGERIT V3.

DIEGO LEONARDO ANDRADE TALERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO
2021

ANÁLISIS DE LOS CONCEPTOS, ELEMENTOS Y TÉCNICAS DE LA GESTIÓN DE RIESGO ORIENTADO A LAS PYMES DEL SECTOR DE LAS TELECOMUNICACIONES BASADO EN MAGERIT V3.

DIEGO LEONARDO ANDRADE TALERO

Proyecto de Grado - Monografía presentada para optar al título
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Msc. Katerine Márceles Villalba
Directora de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍAS E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SOGAMOSO
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Bogotá., 27 de octubre de 2021

DEDICATORIA

Dedico este logro académico a mi madre y hermano que me apoyan siempre en todos los nuevos retos.

AGRADECIMIENTOS

Agradezco a la UNAD y al grupo de profesionales que me acompañó a lo largo de todo el proceso académico. De igual forma agradezco a mi familia por su ayuda incondicional.

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

ACTIVOS DE INFORMACIÓN: Se denomina así a cualquier elemento o información de valor o indispensable para el cumplimiento de los objetivos organizacionales.

AMENAZAS: Es cuando se produce alguna clase de suceso o actividad que influya de manera negativa en la organización causando un daño en la seguridad informática o en los activos de información.

CONFIDENCIALIDAD: Los datos deben ser exactos y modificados solo por personal autorizado, esto aplica tanto para almacenar, acceder y transmitir la información.

DISPONIBILIDAD: Los datos deben tener la posibilidad de ser requeridos y obtenidos en el momento que lo requieran, en lo posible evitando desperfectos en los sistemas.

DATOS: Es la información que tienen como propósito el análisis, control y medición de los procesos y tareas dentro de la organización.

INTEGRIDAD: Los datos deben ser absolutos y no deben ser modificados sin autorización. Adicionalmente los cambios realizados sobre los datos deben ser rastreables en todo momento para saber el tiempo exacto y la persona o proceso que lo realizó.

SEGURIDAD: Controles, procedimientos y labores que preservan las características de la información: disponibilidad, confidencialidad e integridad.

GESTION DE RIESGO: Método que precisa, evalúa, pondera y categoriza el riesgo para poner en práctica instrumentos de control.

VULNERABILIDAD: Es una flaqueza en el sistema informático y generalmente es explotada para ocasionar un perjuicio en los atributos o propiedades del sistema.

RESUMEN

Todas las organizaciones definen su sistema de gestión de seguridad de la información (SGSI) acorde a sus requisitos preestablecidos, recursos disponibles y el punto de vista de la gerencia en cuanto a los riesgos informáticos. De acuerdo a esto cada organización implementa los controles adecuados para mitigar, transferir o encarar los riesgos informáticos.

En la presente monografía se pretende dar solución al problema de cómo emplear la Metodología MAGERIT V.3 en organizaciones tipo Pyme del sector telecomunicaciones. MAGERIT V.3, fue elaborada por la Comisión de Estrategia TIC del Gobierno de España, antes conocida como El Consejo Superior de Administración Electrónica y es considerada como la más completa tanto para organizaciones públicas y privadas.

El objetivo principal que abarca la realización de este documento es acercar de una manera un poco más resumida la metodología MAGERIT V.3 a los profesionales en seguridad informática que estén interesados en implementar dicha metodología en pequeñas y medianas empresas del sector de las telecomunicaciones. La metodología consta de 3 libros: Método, Catálogo de Elementos y Guía de Técnicas. Finalmente se realizará una guía de la metodología empleada en pymes del sector de las telecomunicaciones.

Por lo tanto, se espera un documento que permita un acercamiento mucho más profundo a la metodología MAGERIT V.3 para precisar los beneficios al ejecutar el análisis y gestión de riesgos relacionados con las tecnologías de la información en Pymes.

Palabras Clave: Análisis, Gestión, Metodología, Riesgo y Vulnerabilidad.

ABSTRACT

All organizations define their information security management system (ISMS) according to their pre-established requirements, available resources and management's point of view regarding IT risks. According to this, each organization implements the appropriate controls to mitigate, transfer or address computer risks.

This monograph aims to solve the problem of how to use the MAGERIT V.3 Methodology in SME-type organizations in the telecommunications sector. MAGERIT V.3, was prepared by the ICT Strategy Commission of the Government of Spain, formerly known as the Higher Council of Electronic Administration and is considered the most complete for both public and private organizations.

The main objective covered by this document is to bring the MAGERIT V.3 methodology closer to professionals in information security who are interested in implementing this methodology in small and medium-sized companies in the telecommunications sector. The methodology consists of 3 books: Method, Catalog of Elements and Guide of Techniques. Finally, a guide will be made on the methodology used in SMEs in the telecommunications sector.

Therefore, a document is expected that allows a much deeper approach to the MAGERIT V.3 methodology to specify the benefits when executing the analysis and management of risks related to information technology in SMEs.

Keywords: Analysis, Management, Methodology, Risk and Vulnerability.

INTRODUCCIÓN

A través de la informática y la implantación de nuevas tecnologías en las organizaciones los procesos se desarrollan de forma ágil y efectiva garantizando la prestación de servicios y la satisfacción de los clientes. Es por esto, que la seguridad informática acompañada del análisis y gestión de riesgos cobran especial relevancia para asegurar dichos procesos y operaciones mediante la confianza en los componentes de la infraestructura de tecnología de cada organización.

El riesgo siempre se encuentra asociado a las amenazas y vulnerabilidades de la organización, que a su vez interfieren con la consecución de los objetivos puesto que suponen un factor negativo por las pérdidas económicas. Es por lo tanto bastante obvia la importancia que tiene conocer el estado real de riesgos a los que se encuentra sometida una organización. Con el fin de tomar medidas preventivas antes de que los riesgos pasen de ser hipotéticos a reales.

Dentro de las organizaciones es frecuente encontrar el análisis de riesgos muy ligado a las decisiones de la alta gerencia, justamente lo que se busca es prevenir que los riesgos se conviertan en amenazas que causen pérdidas económicas en la organización. Dicho análisis consiste en identificar los activos informáticos y los respectivos riesgos asociados estableciendo controles y acciones que logren mitigar sus efectos negativos en la consecución de los objetivos de las empresas.

Por lo anterior, este documento se centrará en realizar la descripción de los conceptos fundamentales de la metodología de análisis y gestión de riesgos MAGERIT V.3, en donde se definirán los elementos principales, se identificarán los elementos más relevantes del catálogo, se examinarán las técnicas específicas y generales y finalmente se propondrá una forma de implementación de la metodología de análisis y gestión de riesgos MAGERIT V.3 para Pymes del sector Telecomunicaciones.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

Según Quintero[1], en la economía Colombiana las pequeñas y medianas empresas (Pymes), generan un inmenso aporte para la economía local en cuanto al incremento de la producción y redistribución de bienes y servicios. Como es lógico apoyan su funcionamiento en las TICS para gestionar sus operaciones y los servicios ofrecidos a terceros. Al tener una dependencia directa del uso de la tecnología se hace necesaria la protección de la infraestructura y la información que es fundamental para alcanzar los objetivos organizacionales. Lo anterior, implica que las Pymes deben ser susceptibles a los cambios tecnológicos para que logren adaptarse a los tiempos modernos donde casi todos los procesos internos o externos se encuentran online, ya sea en la nube o en la intranet.

En la opinión de Crespo[2], en la actualidad las amenazas están siempre latentes en los sistemas informáticos y poseen una etapa temprana llamada riesgo que se puede definir como la eventualidad que obstaculiza el alcance de un objetivo en la organización y generalmente implica pérdidas económicas y se interpretan como un factor negativo, debido a sus consecuencias para las empresas. Para que el riesgo se materialice tienen que existir vulnerabilidades en los activos de información. Un riesgo implica varios elementos tales como: probabilidad, amenaza, vulnerabilidad, activos y finalmente impacto. Para Hasper[3], dentro de las organizaciones es frecuente encontrar el análisis de riesgos muy ligado a las decisiones de la alta gerencia, justamente lo que se busca es prevenir que los riesgos se conviertan en amenazas que causen pérdidas económicas en la organización. Dicho análisis consiste en identificar los activos informáticos y los respectivos riesgos asociados estableciendo controles y acciones que logren mitigar los efectos negativos en la consecución de los objetivos de las empresas.

Un análisis del riesgo es un proceso fundamental para que se tomen en serio los riesgos y las respectivas acciones creadas para reducir las vulnerabilidades en las plataformas tecnológicas de las empresas. Para llevar a cabo un análisis correcto se debe identificar los activos de información y sus vulnerabilidades, hacer cálculos de probabilidad y medir los posibles efectos de los riesgos encontrados. Es importante

[1]QUINTERO, Juan. Las pymes en Colombia y las barreras para su desarrollo y perdurabilidad. Bogotá: Universidad Militar Nueva Granada, 2018. p. 5.
[2]CRESPO, Paúl. Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES. Cuenca: Universidad de Cuenca. 2016. p. 22.
[3] HASPER, Joan, et al. Tendencias en la investigación sobre gestión del riesgo empresarial: un análisis bibliométrico. En: Revista Venezolana de Gerencia. Maracaibo, 2017. Vol. 22, No 79. p. 3.

mencionar que existen metodologías y normas reconocidas como MAGERIT[4], CRAMM, MEHARI[5], OCTAVE[6], NIST SP-800[7] e ISO/IEC 27005[8] que fueron especialmente diseñadas para estas labores al interior de las organizaciones. Según el autor Crespo[9], dichas metodologías y normas carecen de validez si no se concientiza a las organizaciones de la importancia del análisis de riesgos para preservar la información. Para Barrera[10], el análisis del riesgo visto de forma sencilla es considerar los peores escenarios que pueden afectar una plataforma tecnológica y desarrollar planes de prevención y contención que abarquen el ciclo de vida del proyecto a través de una gestión de los riesgos detectados.

1.2 FORMULACIÓN DEL PROBLEMA

Surge entonces una pregunta al relacionar los conceptos antes referidos: ¿Cómo aplicar la metodología MAGERIT V.3 en Pymes del sector de las telecomunicaciones para el análisis y gestión de riesgos de sistemas de la información?

Esta monografía pretende solucionar esta incógnita y se enfoca en la metodología MAGERIT versión 3, la cual es sin duda una de las más empleadas en diferentes clases de organizaciones.

[4]VICENTE, E, MATEOS, A y JIMÉNEZ-MARTÍN, A. Risk Analysis in Information Systems: A Fuzzification of the MAGERIT Methodology, Knowledge-Based Systems 66. 2014.p. 1.
[5]MIHAILESCU, Vladimir. Risk Analysis and Risk Management Using MEHARI . 2012. p. 3.
[6]WAGIU, Elmor; SIREGAR, Raminson y MAULANY, Raymond. Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method, Abstract Proceedings International Scholars Conference 7, No. 1. 2019. p. 1.
[7]SETIAWAN,Hermawan; PUTRA, Fandi y PRADANA Anggi. Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute, en 2017 International Conference on Information Technology Systems and Innovation (ICITSI), 2017. p. 4.
[8]GARCÉS, Oña. Gestión de riesgos informáticos utilizando NIST SP-800 e ISO/IEC 27005 en la empresa international forest products del Ecuador S.A. 2019. p. 7.
[9]CRESPO, Esteban y CORDERO, Geovanna. Estudio Comparativo entre las Metodologías CRAMM Y MAGERIT Para la Gestión de Riesgo de TI em Las MPYMES, 2016. p. 3.
[10]BARRERA. Ricardo; SÁNCHEZ, Maritza y ROJAS, William. Modelo de gestión del riesgo en proyectos informáticos Mogripi, I+D REVISTA DE INVESTIGACIONES 8, n.o 2. 2016. p. 3.

2. JUSTIFICACIÓN

De acuerdo a las tendencias de la actualidad como dice Ortegón[11], La tecnología es un factor determinante para las organizaciones, incluyendo obviamente a las Pymes que representan un alto porcentaje en la economía nacional, su activo más importante es sin duda alguna la información. Existen metodologías, recomendaciones y mejores prácticas que dan una guía de la importancia que tiene para las empresas el análisis y gestión de riesgos. Lo anterior, busca que clientes, proveedores, empleados y la alta gerencia no vean alterada su sinergia, debido a riesgos y vulnerabilidades asociados a las diferentes infraestructuras tecnológicas.

Según Alemán[12], Considerar el análisis y gestión de riesgos como una de las etapas más importantes dentro de la organización, supone descubrir, mitigar o controlar amenazas que sirvan para alcanzar los objetivos del negocio y efectuar una gestión dinámica de los recursos con los cuales dispone la organización. Lo más difícil casi siempre es cambiar la mentalidad un poco cerrada respecto al análisis de riesgos y de esta forma concientizar y recalcar los beneficios implícitos en dedicar recursos y personal para minimizar las amenazas y riesgos que rodean una infraestructura tecnológica. En la opinión de Tejena[13], cuando se implementan mecanismos de seguridad en conformidad con los riesgos y amenazas detectados se asegura la mitigación de los perjuicios que traen consigo los incidentes informáticos. Al estar preparados con este tipo de contingencias, una organización no solo previene la pérdida de datos o información; además, ahorra recursos económicos y reduce sobrecostos que desde el punto de vista del análisis y gestión de riesgos siempre son evitables.

Para Tejena[14], los documentos que hacen comparativas de las diferentes metodologías de análisis y gestión de riesgos como: OCTAVE, MEHARI, MAGERIT, CRAMM, EBIOS y NIST SP 800-30 generalmente son artículos cortos que aconsejan como mejor opción la metodología MAGERIT[15], pero carecen de la profundidad necesaria para resumir de manera acertada los conceptos tratados en dicha metodología y que se encuentran contenidos en Libro I: Método, Libro II Catálogo de Elementos y Libro III: Guía de

[11]ORTEGÓN, William; PINTO, Mario y PEROZO, Miguel. Diagnóstico Para La Mitigación de Riesgos Informáticos de La Empresa LYD COLOMBIA S.A.S. 2019. p. 19.
[12]ALEMÁN, Helena y RODRÍGUEZ, Claudia. Metodologías para el análisis de riesgos en los sgs, Publicaciones e Investigación 9. 2015. p. 3.
[13]TEJENA, Mayra. Análisis de riesgos en seguridad de la información, Polo del Conocimiento 3, n.o 4. 2018. p. 2.
[14]Ibid., p. 30.
[15]ABRIL, Ana, PULIDO, Jarol y BOHADA, John. Análisis de Riesgos en Seguridad de la Información. En: Revista Ciencia, Innovación y Tecnología (RCIYT). Tunja. 2013. Vol. 1, No. 1. p. 11.

Técnicas. Por lo tanto esta monografía será enteramente dedicada a definir de una manera consistente todos los términos y conceptos para los profesionales de la seguridad informática interesados en conocer la metodología MAGERIT como opción factible de implementación en una organización Pymes del sector de las telecomunicaciones.

Lo anterior, con el fin de servir de material de consulta y apoyo a nivel regional y nacional para una aproximación resumida y condensada de los temas intrínsecamente relacionados con la metodología MAGERIT y su puesta en funcionamiento en un entorno organizacional tipo Pymes para definir claramente sus beneficios como metodología de análisis y gestión de riesgos.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Análizar los conceptos, elementos y técnicas de la gestión de riesgo orientado a las Pymes del sector de las telecomunicaciones mediante una revisión sistemática de la metodología MAGERIT V.3., con el fin de prevenir y gestionar ataques.

3.2 OBJETIVOS ESPECÍFICOS

Establecer los conceptos, elementos y técnicas necesarios para la gestión de riesgo orientado a las Pymes del sector de las telecomunicaciones.

Examinar mediante una revisión sistemática de literatura la metodología MAGERIT V.3

Proponer una guía basada en un caso de estudio orientado a las Pymes del sector de las telecomunicaciones que permita gestionar el riesgo basado en Magerit V.3

4. MARCO REFERENCIAL

4.1 MARCO TEORICO

4.1.1**Importancia del Sistema de Gestión de la Seguridad de la Información con la gestión de riesgo**. Un concepto totalmente oportuno lo describe Nieves[16], la seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad; así como de los sistemas implicados en su tratamiento, dentro de una organización. Estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información. Por lo tanto, la Seguridad de la información es el punto de partida para el análisis y gestión de riesgos.

En la actualidad la seguridad informática es inherente a la organización según lo explica Parada[17], es el proceso donde las organizaciones deben contemplar para afrontar los eventos inesperados de seguridad; cuyo propósito es crear estrategias que permitan asegurar la información y el conocimiento de la organización (Saber- hacer) bajo la gestión de un proceso sistemático, lógico y continuo, que se muestre como un indicador positivo que da valor agregado a los procesos misionales. De la afirmación anterior, se puede concluir que sin el aseguramiento de la información las organizaciones pueden desintegrarse o fracturarse, debido a los riesgos y amenazas no analizados.

4.1.2. **Seguridad de la información y gestión de los riesgos en PYMES**. El aseguramiento de los datos es vital según Jácome[18], en el mundo corporativo generalmente la mayoría de actividades administrativas se desenvuelven alrededor del procesamiento de datos soportados en infraestructuras y sistemas, esto hace que las organizaciones consideren a la información como vital para la consecución de los objetivos del negocio. Es por eso que si se afectaran los datos, debido a que los atacantes tuvieran acceso a información sensible, sería considerado como una catástrofe para dicha organización. Entonces surge la necesidad de proteger este valioso recurso implementando medidas de seguridad en las TIC (Tecnologías de la información y comunicación). Basados en la afirmación anterior, se puede relacionar la seguridad informática directamente con el análisis y gestión de riesgos, puesto que tiene como función principal evitar escenarios desastrosos en los que la continuidad de la organización se ponga en duda. Ante un escenario de pérdida total de datos, es muy

[16]NIEVES, Arlenys. Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001:2013. 2017. p. 11.
[17]PARADA, Diego J. Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. Información tecnológica 29, n.o 1. 2018. p. 3.
[18]JÁCOME, José; PUSDÁ, Marco y IMBAQUINGO, Daisy. Fundamentos de Auditoría Informática basada en riesgos. 2017. p. 59.

poco lo que se puede hacer si los riesgos informáticos no fueron tenidos en cuenta.

En el presente se entiende que los riesgos están ligados inevitablemente a las empresas, como lo explica Correa[19], en esencia, esta revisión aborda la importancia de los sistemas de gestión de riesgos, partiendo de que el riesgo es inherente a la actividad empresarial. Por tal motivo el objetivo y propósito de este artículo es estudiar esos mecanismos, propuestas y las diferentes políticas de control que se incorporan en las organizaciones y que a través del tiempo se han ido integrando en las diversas áreas corporativas. Se concluye entonces que los riesgos están asociados a todas las áreas y procesos dentro de la organización, por lo tanto no son propiedad exclusiva del área de TI (Tecnología de la información) o la SI(Sistema de información).

El concepto de riesgos en las tecnologías de la información se define de la siguiente manera según Jácome[20], el tratamiento de riesgos es una expresión que se vale de procedimientos ordenados y lógicos que posibilitarán reconocer, examinar, valorar, manipular, supervisar y divulgar los riesgos relacionados con una tarea o proceso de forma que posibilité a las organizaciones minimizar sus pérdidas y maximizar sus utilidades. Como se puede observar, no es un proceso menor y eso hace que sea fundamental en las organizaciones que quieran garantizar su continuidad y más si se tienen servicios soportados en la infraestructura de TI.

Actualmente el análisis y tratamiento de riesgos son temáticas determinantes tal y como lo explica Caballero[21], se puede afirmar que el tratamiento de riesgos es una actividad sobre la cual se puede emplear procedimientos y medios para manejar los riesgos detectados en un proyecto y también desarrollar estrategias para su adecuada gestión. Adicionalmente proporciona un ambiente riguroso para tomar decisiones de una forma objetiva basados en la constante revisión e identificación de lo que puede ocasionar problemas; por lo tanto, la gestión de riesgos es importante porque ayuda a evitar inconvenientes. Este punto de vista enfatiza los objetivos de la temática abordada en cuanto a evitar pérdidas dentro de las organizaciones.

Se observa un escenario de riesgo especialmente en pequeñas y medianas empresas,

[19]CORREA, Gabriel; RÍOS, Eliana y ACEVEDO, Julio. Evolución de la cultura de la gestión de riesgos en el entorno empresarial colombiano: revisión y diagnóstico. Journal of Engineering and Technology 6, n.o 1. 2017.p. 5.
[20]JÁCOME, José; PUSDÁ, Marco y IMBAQUINGO, Daisy. Fundamentos de Auditoría Informática basada en riesgos. 2017. p. 63.
[21]CABALLERO, Sergio y KUNA, Horacio. Análisis y gestión de riesgo en proyectos software. 2018.p. 2.

tal como refiere Crespo[22], las PYMES (Pequeñas y medianas empresas), por lo general, se encuentran sumergidas en un entorno bastante riesgoso. A nivel nacional esto puede ocurrir por la economía y política inestable, a nivel regional es probable que a causa de las condiciones circundantes de cada ciudad. Este escenario se puede complicar si las Pymes consideran el área de informática exclusivamente como un área de soporte donde la máxima inversión en seguridad es un modesto antivirus. La desinformación y poca tenencia en cuenta del factor riesgo contribuyen a que el tratamiento de riesgos se convierta en un mito organizacional. Se logra interpretar de la anterior afirmación que las PYMES no están considerando el análisis y gestión de riesgos y por su misma naturaleza son más susceptibles que las grandes organizaciones.

Reforzando el párrafo anterior acerca de las PYMES también se encuentra el concepto de Inoguchi[23], la gran mayoría de Pymes desconocen la enorme problemática a la que se enfrentan día a día, esto hace que consideren la seguridad informática como algo prescindible y de menos importancia. Es por esto que no invierten en la contratación de personal capaz hacerse cargo de los incidentes de seguridad informática con consecuencias como destrucción de información, extorsión y finalmente filtración de información sensible a la competencia por nombrar solo algunos escenarios de ataque.

El concepto de análisis de riesgo ligado a la seguridad informática es definido según Jácome[24], el análisis y gestión de riesgos es una actividad formal con el objetivo de localizar los riesgos existentes dentro de un sistema de información, a través de un examen riguroso de sus componentes puede recomendar disposiciones adecuadas que deberían ser implementadas para poder mitigar los riesgos encontrados. El tratamiento de riesgos pretende definir la posibilidad de que sucedan los riesgos así como las repercusiones y consecuencias de su ocurrencia valiéndose de una evaluación del nivel de riesgo para definir las acciones a ejecutar para lograr una mitigación. El término análisis implica el estudio de las condiciones iniciales de los riesgos del sistema y el termino gestión se refiere a lo que se debe hacer en caso de que se presente una amenaza. En otras palabras es el antes y después de los riesgos convertidos en amenazas.

[22]CRESPO, Esteban. Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Enfoque UTE 8. 2017.p. 3
[23]INOGUCHI, Antonio y MACHA, Erika. Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016, Universidad San Ignacio de Loyola, 2017.p. 8.
[24]JÁCOME, José; PUSDÁ, Marco y IMBAQUINGO, Daisy. Fundamentos de Auditoría Informática basada en riesgos. 2017. p. 65.

Un modelo de riesgos también puede ser diseñado, tal como lo menciona Del Río[25], se plantea entonces que si un proyecto es administrado de forma ordenada y metódica, se encuentra un proceso cíclico del tratamiento de riesgos que se compone de siete fases: a) constitución de las variables del proyecto y la proyección del riesgo, b) reconocimiento de riesgos, c) análisis de riesgos tanto cualitativo como cuantitativo, d) estructuración de la respuesta al riesgo, e) seguimiento del riesgo, f) supervisión y g) robustecimiento del sistema mediante un proceso de mejora continua en cada una de las fases anteriores. Existen varios modelos para la gestión de riesgos, lógicamente pueden variar en número de etapas o fases, pero todas buscan el mismo objetivo dentro de la organización.

El impacto del riesgo cobra importancia dentro de la temática abordada y lo explica García[26], basado en la magnitud del impacto previsto y la posibilidad de ocurrencia del riesgo, se dispone la criticidad que podría tener la situación de acuerdo a cada riesgo. Este estudio permite definir el rango o preponderancia en tareas, equipos y sistemas para idear una táctica que favorezca el adoptar decisiones efectivas para redirigir los recursos y el esfuerzo en áreas que requieran mayor cuidado respecto a la seguridad organizacional. De acuerdo al impacto detectado se realizan prioridades en la forma de gestionar los riesgos.

La gestión de riesgos implica un proceso detallado, tal y como lo describe Álvarez[27], dentro de la identificación del riesgo se realiza una clasificación de los activos, se estable el nivel de importancia de cada uno de ellos, se identifican las amenazas, se identifican los controles y se identifican las vulnerabilidades y las posibles consecuencias o impactos que se darían en caso de que una amenaza explote una vulnerabilidad. En la estimación del riesgo se define la metodología, los criterios para la valoración de las consecuencias y la valoración de los incidentes. La gestión de riesgos tiene en el diseño de los controles su principal objetivo, ya que estos se encargaran de reaccionar de acuerdo a la amenaza materializada.

El análisis de riesgos es utilizado en casos concretos y llevados a la práctica tal y como

[25]DEL RÍO, Abel y CÁRDENAS, Beitmantt. Dinámica de sistemas: una forma de optimizar la gestión del riesgo. Magazine School of Business Administration. 2018.p. 5.
[26]GARCÍA, Gonzálo y VIDAL, María. La informática y la seguridad. Un tema de importancia para el directivo, Revista de Información científica para la Dirección en Salud. INFODIR 0, n.o 22. 2016. p. 11.
[27]ALVAREZ, Claudia; BARBOSA, Julia y ZAMBRANO, Leonardo. Análisis de Riesgos Informaticos de la Dependencia División de Sistemas Adscrita a la Subdirección Académica de la UFPSO, Basada en la Norma ISO/IEC 27005:2011. 2017.p. 24.

lo explica Santa Cruz[28], un problema principal al que se enfrentan las organizaciones en la actualidad es el inapropiado tratamiento de riesgos, especialmente cuando no se consideran riesgos a las situaciones que podrían afectar la estabilidad de las empresas. El análisis de riesgos es de gran utilidad para una organización interesada en seguir mejorando sus procesos.

Para la temática investigada no importa el sector económico de la organización, tal como lo manifiesta Acuña[29], el tratamiento del riesgo adquiere una mayor preponderancia en las organizaciones actuales, debido a la dinámica y evolución de las tecnologías, estas transformaciones presionan a las empresas a hacer frente a factores de internos y externos que posibilitan la incertidumbre al momento de la persecución de sus objetivos. La consecuencia de la incertidumbre dentro de la organización se conoce como riesgo. Independientemente del sector económico en el que se desenvuelva la organización, el análisis y gestión del riesgo siempre es pertinente para cumplir con los objetivos del negocio. Al proteger la información se protege también a los clientes.

El análisis y gestión de riesgos es una práctica común para conocer el estado actual de las organizaciones, como lo explica Ortegón[30], por el cual vio la necesidad de realizar un diagnóstico en seguridad informática que le permitiera identificar las posibles fallas en infraestructura tecnológica y riesgos a los que puede estar expuestos, de tal manera que les permitiera reestructurar y mejorar para que puedan seguir con su actividad económica con total normalidad y seguridad en la organización. Por lo anterior, se puede decir que la temática investigada es bastante actual, debido a que desde hace varios años todos los procesos de las organizaciones se soportan sobre las infraestructuras de tecnologías.

4.2 MARCO CONCEPTUAL

4.2.1 **PYMES**. Acerca de las organizaciones referidas en el presente documento se presenta según Díaz[31], las empresas clasificadas como pymes poseen atributos y cualidades comunes en lo referente a la utilización de la tecnología. Debido a su tamaño, se adecuan para instaurar tecnologías nuevas con rapidez, a pesar de que no continuamente lo pueden efectuar de forma segura y en circunstancias de garantía. Según su conformación, o a causa de que no

[28]QUIROZ, Santa y MILAGROS, Hilda. Implementación de gestión de riesgos de ti para obtener la certificación ISO 27001 en el Hospital Regional Lambayeque. Repositorio Institucional - USS. 2016. p. 7.
[29]ACUÑA, Tatiana y PEINADO, Yineth. Guía de Gestión de Riesgos Para el Departamento de Sistemas del Hotel Tarigua OCAÑA S.A.S, Basados en la Norma ISO/IEC 27001. 2019.p. 34.
[30]ORTEGÓN, Doncel; BARRETO, Pinto; LÉON, Perozo. Diagnóstico Para La Mitigación de Riesgos Informáticos de La Empresa LYD COLOMBIA S.A.S. 2019. p. 24
[31]DÍAZ, Juan. Esquema Director de Seguridad para Empresas pymes del sector Construcción. Alicante: Universidad de Alicante, 2020. p. 4.

tienen a disposición los elementos humanos y medios económicos suficientes, o por la posible ignorancia de las amenazas, acaban enfrentando riesgos desconocidos, que en vista de la dimensión de la empresa puede llegar a suponer una conmoción bastante importante.

4.2.2 **Gestión de Riesgos.** Para Díaz[32], el riesgo se define como la valoración del nivel de exposición para que una situación de amenaza se concrete en uno o diversos activos ocasionando detrimento en la Organización. Es por esto, que el análisis y tratamiento de riesgos es un paso fundamental para gestionar y para lograr la seguridad de la información, de tal modo que es importante llevar a cabo una gestión del riesgo asociado a amenazas humanas y tecnológicas relacionadas con cualquier tipo de activo de la información. Comprender y dominar los peligros que enfrentan los activos de información de los cuales depende la misión, objetivo y visión de la organización es fundamental para poder tratarlos.

4.2.3 **Magerit.** Respecto a la metodología escogida, Bravo[33], afirma que en la actualidad existen varias metodologías para tratar los riesgos: MAGERIT V.3, OCTAVE v.2 y NIST 800-30; esta monografía se enfoca en el análisis de la metodología de gestión de riesgos MAGERIT V.3 para identificar sus beneficios. Las dos primeras metodologías están articuladas con la ISO/IEC 27001:2013 y son las más usadas a nivel global. NIST 800-30 se origina en el National Institute of Standard Technology (Instituto Nacional de Estándares y Tecnología) con documentación en inglés y un marco de trabajo extenso de 9 pasos que la hace un poco complicada de implementar. MAGERIT posee documentación en español y lidera de forma consistente el análisis y tratamiento de los riesgos, mientras que OCTAVE posee una documentación bastante resumida y ocupa el segundo lugar.

Probablemente es la metodología más usada para el análisis de riesgos, y es definida según Ferruzola[34], MAGERIT es una metodología de análisis y tratamiento de riesgos, fue elaborada por el ministerio de hacienda y administraciones públicas para dar solución a la realidad de que la gran mayoría de entidades públicas y privadas dependen indudablemente y de forma progresiva de las TIC para lograr sus objetivos y cumplir su misión beneficiando a las propias empresas y a los usuarios de los servicios prestados.

Esta metodología se identifica plenamente con la temática escogida ya que es el método más empleado a nivel mundial para el análisis y gestión de riesgos en las organizaciones sin importar su sector económico o su carácter público o privado.

[32]Ibid., p. 30.
[33]BRAVO, María. Desarrollo de un Sistema de Gestión de Seguridad de la Información para bibliotecas basado en una metodología mejorada para análisis de riesgos compatible con la norma ISO/IEC 27001:2013. Quito: Escuela Politécnica Nacional, 2018. p. 21.
[34]FERRUZOLA, Enrique. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE 6, n.o 1. 2019. p. 2.

4.3 ANTECEDENTES.

Como fuentes referenciales que contribuyen con fundamentos principales para esta monografía se tienen:

Según el autor Jeysser Aurelio Palacios, el cual presentó el proyecto aplicado para optar al título de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia en el año 2020: Análisis de Vulnerabilidades de la Infraestructura Tecnológica en la Dependencia de Formación Profesional Integral del SENA Regional Guainía, para el Diseño de una Propuesta de Aseguramiento de la Información Basada en la Metodología Magerit[35]. El proyecto hace uso de la metodología Magerit para el análisis y gestión de riesgos a los que está expuesta la infraestructura tecnológica del SENA Regional Guainía con el objetivo de preservar la integridad, disponibilidad y confidencialidad de la información en todos los ámbitos de tecnologías de información de la regional. Por lo tanto es evidente la estrecha relación entre este proyecto y la presente monografía, puesto que comparten como base para el análisis y gestión de riesgos la misma metodología y todos los conceptos fundamentales.

De acuerdo al autor Juan Carlos Varón Quiroga, que presentó el trabajo de grado llamado Estudio de Análisis y Gestión de Riesgo al Sistema de Información de la Empresa Agesagro S.A.S. Utilizando la Metodología Magerit. Para optar al título de Especialista en Seguridad Informática en la Universidad Nacional Abierta y a Distancia en el año 2017[36]. Está monografía proporciona una visión global acerca del aseguramiento de los activos de información en una empresa empleando la metodología Magerit. Es por esta razón que el anterior trabajo se ve relacionado con esta monografía, debido a que suministra pasos para el análisis y gestión de riesgos dentro de una organización.

Según el autor Jair Hernando Vanegas Garzón, quien presento el trabajo de grado llamado Guía de Auditoria Basada en el Análisis de Riesgos a un Centro de Datos Aplicando la Metodología Magerit V3. Para optar al título de Especialista en Auditoria de

[35]PALACIOS, Jeysser Aurelio. Análisis de Vulnerabilidades de la Infraestructura Tecnológica en la Dependencia de Formación Profesional Integral del SENA Regional Guainía, para el Diseño de una Propuesta de Aseguramiento de la Información Basada en la Metodología Magerit. Proyecto aplicado para optar al título de Especialista en Seguridad Informática. Guainía: Universidad Nacional Abierta y a Distancia. 2020. 141p.

[36]VARÓN, Juan Carlos. Estudio de Análisis y Gestión de Riesgo al Sistema de Información de la Empresa Agesagro S.A.S. Utilizando la Metodología Magerit. Monografía para optar al título de Especialista en Seguridad Informática. Ibagué: Universidad Nacional Abierta y a Distancia. 2017. 91p.

Sistemas de Información de la Universidad Católica de Colombia en el año 2017[37]. El documento antes mencionado propone una guía para la realización de una auditoría interna a un centro de datos apoyándose en la metodología Magerit V3. El trabajo de investigación antes mencionado tiene relación con el presente documento dado que se identifican los activos de información, se evalúan los riesgos a los que estos se ven expuestos y finalmente se tratan los riesgos identificados a través de salvaguardas establecidas por la organización, todo lo anterior con la ayuda de la metodología de análisis y gestión de riesgos Magerit.

De acuerdo a los autores Fabián Paul Pazmiño Sánchez y Nelson Ismael Aldaz Calispa, quienes presentaron el trabajo de grado denominado Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de tecnología de información y comunicación de la Empresa Pública Municipal de residuos sólidos Rumiñahui-Aseo EPM empleando la metodología Magerit. Para optar al título de Ingenieros de Sistemas de la Universidad Politécnica Salesiana en el año 2021[38].El documento en mención tiene como objetivo el desarrollo de un plan que sirva para salvaguardar los activos de información de una empresa pública haciendo énfasis en los riesgos que afronten dichos activos y a la vez el tratamiento respectivo de los mismos. Es por esto que dicho proyecto se relaciona con este trabajo, ya que coincide en el empleo de la metodología Magerit como mecanismo efectivo para realizar el análisis y gestión de riesgos al interior de una organización.

4.4 MARCO LEGAL

La normativa legal que delimita este documento es la siguiente:

4.4.1 Ley 1273 del 2009**.**Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado, denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones[39]. Fue publicada el 5 de enero de 2009 y por medio

[37]VANEGAS, Jair Hernando. Guia de Auditoria Basada en el Análisis de Riesgos a un Centro de Datos Aplicando la Metodologia Magerit 3. Trabajo de grado para obtener el título de: Especialista en Auditoria de Sistemas de Información. Bogotá: Universidad Católica de Colombia. 2017. 168p.

[38]PAZMIÑO, Fabián y ALDAZ, Nelson. Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de tecnología de información y comunicación de la Empresa Pública Municipal de residuos sólidos Rumiñahui-Aseo EPM empleando la metodología Magerit. Trabajo de grado para obtener el título de: Ingeniero de Sistemas. Quito: Universidad Politécnica Salesiana. 2021. 150p.

[39]COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la

de esta ley el código penal fue modificado para la preservación de los sistemas de información y de igual forma penalizar con prisión y multas las conductas delictivas frente al manejo de las tecnologías de la información y las infraestructuras que las soportan.

4.4.2 Ley 1581 del 2012.Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma[40].Originalmente publicada el 18 de octubre de 2012 y con actualización el 4 de mayo de 2021, por medio de esta ley se reglamenta el uso apropiado al que deben ser sometidos todos los datos personales recopilados por parte de organizaciones públicas y privadas haciendo mención de las excepciones a dicha ley.

información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá D.C., 2009. No. 47223. p. 1-2.

[40]COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48.587. p. 1-5.

5. DESARROLLO DE LOS OBJETIVOS

5.1 ESTABLECER LOS CONCEPTOS, ELEMENTOS Y TÉCNICAS NECESARIOS PARA LA GESTIÓN DE RIESGO ORIENTADO A LAS PYMES DEL SECTOR DE LAS TELECOMUNICACIONES.

A lo largo del desarrollo de este capítulo del documento se abordaran en orden lógico los conceptos, elementos y técnicas necesarias para la gestión del riesgo orientado a las Pymes del sector de las telecomunicaciones, en conformidad con los objetivos propuestos. Lo anterior, con el fin de clarificar conceptos que se encuentran relacionados directamente con el análisis y gestión de riesgos, los cuales servirán de base para el desarrollo de la presente monografía.

De acuerdo a Santa María[41] pueden surgir aspectos relevantes al momento de realizar la gestión del riesgo en una organización, a continuación se incluyen las más relevantes como punto de partida para este documento. Posteriormente se abordarán los conceptos, elementos y técnicas.

5.1.1 Aspectos relevantes:

5.1.1.1 ¿Por qué se debe realizar una evaluación de riesgos? Una evaluación de riesgo proporciona la documentación necesaria para demostrar que se realiza la debida diligencia. Por su parte el resultado de los procesos de análisis y evaluación de riesgos se utilizará por lo general dos veces. La primera vez será cuando se tomen las decisiones; para el análisis de riesgos, eso significa decidir si se debe continuar con un nuevo proyecto y para la evaluación de riesgos, qué tipos de controles o salvaguardas deben implementarse. Para la evaluación de riesgos, el resultado identificará qué contramedidas deben implementarse o si la administración ha determinado que la mejor decisión es aceptar el riesgo. La segunda vez que se utilizarán los resultados es cuando se presenta un contratiempo, es decir, cuando surge un problema y la organización debe mostrar el proceso que utilizó para tomar las decisiones que tomó. La documentación surgida a partir de los procesos de gestión de riesgos permitirá a la organización mostrar quién estuvo involucrado, qué se discutió, qué se consideró y qué decisiones se tomaron de forma coordinada entre diferentes áreas de la empresa.
Un proceso de gestión de riesgos también favorece que una empresa tome el control de su propio futuro inmediato. Con un proceso de análisis de riesgos eficaz, solo se

[41]SANTA MARÍA, Wilber. Plan para Reducir los Riesgos Operativos de Tecnologías de la Información Basada en Metodologia Magerit en la Caja Piura de la Ciudad de Chiclayo. Tesis de grado para optar al título de Ingeniero de Sistemas. Chiclayo: Universidad de Lambeyeque. 2020. 110p.

implementarán aquellos controles y salvaguardas que sean considerados necesarios. Una empresa nunca más se enfrentará a tener que implementar un control obligatorio, excepto que se hayan efectuado cambios bastante drásticos en los procesos internos y en la forma de operar o prestar sus servicios a los clientes.

5.1.1.2 ¿Cuándo se debe realizar un análisis de riesgos? Se debe efectuar un análisis de riesgo siempre que se inviertan recursos económicos. Antes de comenzar una tarea, proyecto o proceso, se recomienda que la empresa debe realizar un análisis de las necesidades del proyecto. Por lo tanto se deben comprender los conceptos del análisis de riesgos y aplicarlos a las necesidades comerciales de la empresa, esto garantizará que solo se realicen los gastos necesarios. Evitando inversión en controles o salvaguardas poco efectivos. Adicionalmente, no será necesario implementar controles o salvaguardas a menos que sean completamente imperativos para la operación. Un proceso de gestión de riesgos adecuado garantizará que se necesiten controles de compensación para asegurar el cumplimiento de la misión de la empresa y el objetivo del negocio.

5.1.1.3 ¿Quién debe realizar el análisis de riesgos y la evaluación de riesgos? La mayoría de los proyectos de gestión de riesgos fracasan porque los expertos internos y los expertos en la materia no están incluidos en el proceso. El proceso de análisis y gestión de riesgos se beneficia de los expertos internos. Nadie mejor para conocer sus sistemas y aplicaciones o su negocio mejor que las personas que los desarrollan y ejecutan. El establecimiento de un equipo de expertos internos garantizará que el proceso de gestión de riesgos cuente con personas con un conocimiento profundo del verdadero funcionamiento de los procesos comerciales. Ninguna persona externa a la organización puede comprender los matices de sus operaciones mejor que las personas que deben trabajar con él y alrededor de él a diario.

5.1.1.4 ¿Quién dentro de la organización debe realizar el análisis de riesgos y la evaluación de riesgos? Si su organización tiene una oficina de gestión de proyectos, entonces los facilitadores de este grupo serían ideales para llevar a cabo los procesos de gestión de riesgos. Hay algunos grupos que, debido a sus reglamentos internos y responsabilidades, encontrarían un conflicto de intereses para liderar o facilitar estos procesos, por ejemplo: el personal de auditoría y las operaciones de sistemas.

5.1.1.5 ¿Cuánto tiempo debe tomar un análisis o evaluación de riesgos? Un análisis o evaluación de riesgos debe completarse en días (unas cuantas semanas), no en o meses, siempre tratando de reducir este tiempo. Para satisfacer las necesidades de una empresa, el proceso de gestión de riesgos debe completarse rápidamente con el menor impacto posible en la ya ocupada agenda de los trabajadores. El tiempo es un bien muy preciado y los procesos como la gestión de riesgos deben estructurarse para

que sean rápidos y eficientes. Si hay tiempo adicional disponible, las diferentes cosas que se pueden hacer parecen no tener fin. La mayoría de las organizaciones; sin embargo, tienen poco tiempo de sobra. Por lo tanto es importante recalcar esto en la organización.

5.1.1.6 ¿Qué puede analizar un análisis de riesgos o una evaluación de riesgos? Estos procesos se pueden utilizar para revisar cualquier tarea, proyecto o idea. Al aprender los conceptos básicos de la gestión de riesgos, la organización puede usarlos para determinar si se debe emprender un proyecto, si se debe comprar un producto específico, si se debe implementar un nuevo control o si la empresa está en riesgo de alguna amenaza.

5.1.1.7 ¿Qué puede obtener la organización de los resultados de una gestión de riesgos? El proceso puede identificar para la empresa cuáles son las amenazas y luego establecer una priorización de estos riesgos para permitir que la gerencia se concentre en las mayores preocupaciones. El mayor beneficio de un análisis de riesgo es la determinación de si es prudente proceder. Permite a la gerencia examinar todas las preocupaciones identificadas actualmente, priorizar el nivel de vulnerabilidad y luego seleccionar un nivel apropiado de control o de lo contrario aceptar el riesgo. El objetivo de la gestión de riesgos no es eliminar todos los riesgos. Es una herramienta que debe utilizar la dirección para reducir el riesgo a un nivel aceptable.

5.1.1.8 ¿Quién debe obtener los resultados de un análisis de riesgos? Rara vez se realiza un análisis de riesgo sin un visto bueno de la alta dirección. Los resultados están orientados a proporcionar a la administración la información que necesita para tomar decisiones comerciales bien informadas. Los resultados de una evaluación de riesgos normalmente se clasifican como confidenciales y se proporcionan solo a la alta gerencia y a quienes se considere apropiados para recibir esta información. Al trabajar los procesos de análisis de riesgos y evaluación de riesgos, será necesario recordar a todos los empleados que la información discutida en los procesos se clasifica como confidencial y no puede ser compartida fuera del foro de gestión de riesgos. Para cualquier tercero que participe en el proceso, será necesario suscribir un acuerdo de no divulgación o confidencialidad para asegurar la protección de la información discutida.

5.1.1.9 ¿Cómo se mide el éxito del análisis de riesgos? La forma tangible de medir el éxito es ver un resultado final más bajo desde el punto de vista de costos. La evaluación de riesgos puede ayudar en este proceso al identificar solo aquellos controles que deben implementarse. Otra forma en que se mide el éxito de un análisis de riesgos es si hay un momento en el que las decisiones de gestión se someten a

revisión. Al contar con un proceso formal que demuestre la debida diligencia de la gerencia en el proceso de toma de decisiones, este tipo de consultas se abordarán de manera rápida y exitosa comprobando la buena gestión no solo de la administración sino también del análisis y gestión de riesgos implementado.

Como afirma Santa María[42] el proceso de gestión de riesgos es un proceso empresarial que apoya a la dirección en la toma de decisiones. Permite a los propietarios de la administración de los activos cumplir con su responsabilidad de proteger los activos de la empresa de una manera razonable y prudente. El proceso no tiene por qué ser un asunto largo y prolongado. Para que sea eficaz, el análisis de riesgos y la evaluación de riesgos deben realizarse de forma rápida y efectiva.
Para el caso en particular de las Pymes del sector de las telecomunicaciones, no debe cambiar este enfoque, a pesar de la complejidad de la red de la organización, que por lo general abarca una o varias ciudades y municipios. Esta cobertura implica generalmente negociaciones con alcaldías municipales, bibliotecas públicas y colegios dentro de la cobertura de la red. También por supuesto se incluyen empresas privadas y personas naturales como clientes de estos proveedores de servicios de Internet (Internet Service Provider).

Un punto clave en la gestión de riesgos dentro de este tipo de Pymes es por lo tanto, hacer tomar conciencia a la empresa que al basar su servicio en tecnologías de la información se encuentran expuestos a una serie de amenazas que pueden causar un impacto leve o bastante notable en la prestación de su servicio, de acuerdo con esta afirmación, un análisis y gestión de riesgos en este tipo de empresas es un punto de partida sólido para la posible expansión y el futuro de la organización.

5.1.2 Seguridad informática. De acuerdo a Paredes[43] en los tiempos actuales, la dependencia de las organizaciones públicas y privadas de las tecnologías de la información va en aumento de una forma considerable, esto implica que el cumplimiento de los objetivos principales de dichas organizaciones; son ahora dependientes del aseguramiento de las infraestructuras de telecomunicaciones y la información almacenada y gestionada por las entidades. La afirmación anterior, convierte a la información, como el activo más importante para las organizaciones modernas, independientemente de su sector económico.

[42]Ibid., p. 12.
[43]PAREDES, Adriana. Análisis de Riesgos de la Seguridad de la Información Utilizando la Metodología Magerit en la Institución Educativa Domingo Savio en la Ciudad de Florencia – Caquetá. Proyecto de Grado para optar el título de Especialista en Seguridad Informática. Florencia: Universidad Nacional Abierta y a Distancia. 2018. 113p.

Como dice Paredes[44] tenemos seguridad informática y seguridad de la información, pueden parecer términos similares, pero existe una diferencia entre ambos, la cual se ve cuando enfocamos que se va a proteger con cada una de ellas. La seguridad informática se encarga de proteger los activos de información, en cuanto a los aspectos técnicos. Los activos pueden ser: equipos de cómputo, firewalls, servidores y todo este tipo de dispositivos físicos dentro de las redes organizacionales.

Como sugiere Pazmiño[45] la seguridad informática es una disciplina que involucra el esquema de técnicas, juicios, formas y estructuras para obtener sistemas de información seguros y confiables. Todas las compañías, excepto algunas poseen sistemas de información y métodos informáticos que apoyan el funcionamiento de la estrategia organizacional. La aplicación de normativas y procesos que permitan blindar dichos sistemas es central para proteger los activos al interior de la organización. Existen varios conceptos de seguridad informática dependiendo de lo que se esté tratando de proteger o la faceta en la que se realice la protección, algunas de ellas son:

5.1.2.1 Seguridad física. Enmarca todo lo concerniente a computadoras de escritorio, portátiles, servidores y equipos de red. Las amenazas más comunes a las que los equipos físicos están expuestos son los robos, desastres naturales como terremotos e inundaciones, fallos de energía entre otros.

5.1.2.2 Seguridad lógica. Cubre a los programas instalados que corren en los equipos físicos incluyendo por supuesto el sistema operativo. Las amenazas recurrentes que impactan en la seguridad lógica son las variantes de virus, esto incluye a troyanos, malware, spyware. Cualquier tipo de ataque que tome ventaja de una vulnerabilidad en aplicaciones, programas o sistemas operativos.

5.1.2.3 Seguridad activa. Son las medidas preventivas para reducir las posibilidades de ataques. Generalmente es la aproximación que se recomienda a las compañías que tienen una gran dependencia de las tecnologías de la información.

5.1.2.4 Seguridad pasiva. Son las medidas o procedimientos reactivos, después de recibir un ataque. Por lo tanto tiene un enfoque mucho más negativo para las organizaciones, solo tomar medidas posteriores a los ataques.

[44]Ibid., p. 17.
[45]PAZMIÑO. Op. cit,p. 28.

5.1.3 Seguridad de la información. Según Paredes[46] la seguridad de la información como su propio nombre lo indica será la encargada de proteger exclusivamente la información. En otras palabras no tanto lo que tenemos que proteger, sino cómo lo debemos proteger, ya que se está hablando de la información como un concepto general, por ejemplo bases de datos, contraseñas de equipos o servidores.

De conformidad con Pazmiño[47] la información se establece como el activo más trascendental en una organización, entonces se asume que posee un valor inestimable para las empresas y que adicionalmente demanda una protección de acuerdo a su importancia. La información se encuentra entonces relacionada a riesgos y amenazas que abarcan un amplio abanico de vulnerabilidades.

Tal como sugiere Pazmiño[48] la seguridad de la información está relacionada de forma directa con las previsiones aplicadas para proteger la información en sus tres pilares de la seguridad de la información: integridad, disponibilidad y confidencialidad. La confidencialidad de la información se debe garantizar con el acceso exclusivamente al personal autorizado, la integridad se alcanza cuando se garantiza que la información no se vea alterada de acuerdo a los requerimientos de los administradores de la misma. Finalmente para preservar la disponibilidad se debe asegurar el acceso a la información de parte de los usuarios en cualquier instante que se requiera. Cuando se quiere proteger los pilares de la seguridad de la información las organizaciones deben implementar procedimientos que aseguren la información, sin importar si el formato es físico o digital. A continuación se establecen las definiciones para vulnerabilidad, amenaza y riesgo.

5.1.4 Vulnerabilidades**.** Las vulnerabilidades se pueden entender como la posibilidad de que se materialice una amenaza informática sobre un activo de información. Existen diferentes tipos de amenazas implicadas en las vulnerabilidades, por ejemplo: un servidor puede afectarse por un fallo eléctrico o de hardware, mientras que los datos pueden ser accedidos, modificados o copiados por una persona no autorizada.

5.1.5 Amenazas**.** Son los ataques que se pueden perpetrar de forma interna o externa a los sistemas informáticos, tomando ventaja de las vulnerabilidades a las que se encuentran expuestos. Las amenazas pueden ser de tipo físico y lógico y pueden ser producidas por personas o máquinas que buscan que suceda algo en específico para

[46]PAREDES. Op. cit,p. 17.
[47]PAZMIÑO. Op. cit,p. 29.
[48]PAZMIÑO. Op. cit,p. 29.

efectuar algún daño en el sistema. Algunos ejemplos: pueden ser fallas de hardware, tormentas eléctricas, virus o software malicioso, sustracción de información o robo de equipos.

5.1.6 Riesgos**.** El riesgo es la viabilidad de que suceda o no una amenaza explotando las vulnerabilidades dentro del sistema. Es por esto que el riesgo existe si hay vulnerabilidades que puedan ser aprovechadas por amenazas en el momento de los ataques. El riesgo en otras palabras es la incertidumbre que se tienen en referencia al ataque potencial de acuerdo a las vulnerabilidades del sistema, por lo tanto puede ser medido y determinado.

De acuerdo a Pazmiño[49] si la organización no ha decidido medir e identificar los riesgos a los que se encuentra expuesta, se entiende que se encontrará en un estado de indeterminación e incertidumbre en el cual no puede protegerse adecuadamente. Solo hasta que la organización conoce sus riesgos, es cuando se puede proteger realmente de ellos y así garantizar el logro de los objetivos establecidos.

Como sugiere Palacios[50] autenticación, control de acceso, base de datos y activo de información, son elementos relevantes para el análisis y gestión de riesgos. Se presentan definiciones breves a continuación:

5.1.7 Autenticación**.** Es el procedimiento o servicio que verifica que la comunicación sea auténtica, tanto en su origen como en el destino. Se encarga de garantizar quién de los usuarios realizó el envío y en qué momento, esto también aplica para el proceso de recepción. Por lo tanto dicho servicio está ligado a la integridad de la información.

5.1.8 Control de acceso. Este servicio o control se encuentra relacionado a la confidencialidad de la información. Se usa generalmente para identificar y autenticar a los usuarios antes de acceder a la información. Si el proceso da conformidad se permite el acceso, de lo contrario se denegara el servicio.

5.1.9 Activo de información. Se suele pensar que solo se específica al hardware si se refiere a los activos de información, pero de hecho el software y la propia información sin tener en cuenta el medio en el que se está almacenando pueden ser considerados como activos. Al considerarse activo, se puede asumir que posee un valor

[49]PAZMIÑO. Op. cit,p. 30.
[50]PALACIOS. Op. cit,p. 20.

dentro de la organización, razón por la cual debe protegerse para que no se vean alteradas ni la integridad, ni la disponibilidad ni la confidencialidad de los activos.

5.1.10 Base de datos**.** Es un conjunto de datos interrelacionado entre sí. Suelen ser usadas para almacenar y gestionar gran cantidad de información de la organización y sus proveedores o clientes. Puede ser una sola base de datos general o diferentes bases de datos por dependencias o áreas dentro de la misma organización. Por lo tanto una base de datos es un activo de información.

5.1.11 Ataque informático**.** De acuerdo con Rodríguez[51]los ataques informáticos también conocidos como Ciberataques son las diferentes acciones que tienen como objetivo burlar o violar los procesos de seguridad de un sistema de información. Se puede afirmar entonces que un ataque informático se vale de alguna falla, debilidad o vulnerabilidad tanto en el hardware como en el software, las personas dentro de un entorno de tecnologías de la información también pueden ser parte del ataque de forma inconsciente; el ataque en última instancia busca un beneficio económico, provocando un resultado perjudicial en la seguridad del sistema, que impacta por supuesto de forma directa en los activos de información de la organización.

Como afirma Jiménez[52] la disponibilidad de servicios, el impacto de los ataques y su probabilidad también son conceptos relevantes al análisis y gestión de riesgos, independiente de la metodología escogida. A continuación definiciones breves de los conceptos antes referidos.

5.1.12 Disponibilidad de servicios. Enmarcada dentro de la estrategia de continuidad del negocio, trata de asegurar que los servicios prestados por la organización y que a su vez dependan de las tecnologías de la información no se vean afectados y continúen su funcionamiento planeado. Para esto se debe garantizar que la infraestructura de hardware, software y personal esté siempre presto a corregir imprevistos para de esta forma cumplir con las metas y objetivos organizacionales.

[51]RODRÍGUEZ, Hugo. Importancia de Controlar todas las Amenazas Detectadas a través de magerit v.3 e iso/iec 27002 Según Análisis de ataques informáticos en latinoamérica. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Barranquilla: Universidad Nacional Abierta y a Distancia. 2019. 115p.

[52]JIMÉNEZ, Giovanny. Análisis y Gestión de riesgos al Sistema de Información de la Empresa Textil Diseños y Dotaciones Osiris S.A.S Aplicando Metodología Magerit. Monografía para optar al título de Especialista en Seguridad Informática. Ibagué: Universidad Nacional Abierta y a Distancia. 2018. 86p.

5.1.13 Continuidad del Negocio. De acuerdo a Rojas[53] la continuidad del negocio consiste en identificar los sistemas o recursos informáticos que pueden sufrir un detrimento, daño o pérdida ocasionando graves perjuicios para el desarrollo normal de la organización, esto con el propósito de organizar, disponer y efectuar procedimientos y adjudicar responsabilidades que custodien y protejan la información, permitiendo con este actuar garantizar la disponibilidad, integridad y confidencialidad en el corto plazo y a unos costos apropiados.

Respecto a la continuidad del negocio y disponibilidad de servicios en las Pymes del sector de las telecomunicaciones se asume que el núcleo del negocio en este tipo de empresas es la prestación del servicio de internet a sus clientes, ya sean privados o públicos. Por lo tanto, el garantizar la disponibilidad del servicio ofrecido puede ser uno de los motivos para realizar un análisis y gestión de riesgos, ya que no solo los ataques informáticos pueden afectar el servicio entregado modificando de forma negativa la percepción de los clientes hacía los proveedores de internet locales en zonas geográficas desprovistas de la cobertura de los grandes operadores de Internet.

5.1.14 Contingencia. Como dice Rojas[54] es una eventualidad o fatalidad de la cual no se tiene la certeza de que suceda.

5.1.15 Plan de contingencia. Este plan debe cubrir todo lo necesario para afrontar una interrupción, puede incluir la puesta en marcha de un servicio alternativo, para lograr esto, se deben validar los procesos en el día a día. Incluyendo lo siguiente: hardware, software, recursos humanos, logística y documentación. Para establecer este plan se debe tener claro que procesos cruciales deben siempre estar en funcionamiento. Cada coordinador de área debe hacerse responsable de la puesta en marcha de este plan, con la ayuda de otras personas dentro del sistema y teniendo como base la preservación de la confidencialidad e integridad de la información. La vigencia del plan por lo tanto se verá influenciada por los cambios en las tecnologías de la información y equipos informáticos dentro de la empresa.

5.1.16 Impacto. Este concepto es clave, puesto que trata de determinar de qué manera se afectará la infraestructura en el caso de recibir ataques. Dependiendo del activo atacado y el propio tipo de ataque, los servicios o líneas de producción perjudicadas pueden ser fundamentales o insignificantes para la organización.

[53]ROJAS, Hernán. Aplicación de la Metodología Magerit para el Análisis de Riesgos de los Sistemas de Control en la Estación Tenay del Oleoducto. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Neiva: Universidad Nacional Abierta y a Distancia. 2019. 97p.
[54]Ibid., p. 32.

5.1.17 Probabilidad de ataques. Su objetivo es determinar los porcentajes de probabilidad de ataques que pueda sufrir la infraestructura tecnológica. Siempre teniendo en cuenta el riesgo inminente y las amenazas latentes dentro de los sistema de información y sus infraestructuras técnicas. De acuerdo a estas afirmaciones el riesgo se debe determinar al igual que su grado de complejidad para la organización.

5.1.18 Comparativa y Relaciones entre MAGERIT V.3 y otras Metodologías de Análisis y Gestión de Riesgos. Como dice Crespo[55] la norma ISO/IEC 27005:2011es acorde con las nociones comunes que se especifican en la norma ISO/IEC 27001; por lo tanto abarca el detalle de los procedimientos para el tratamiento del riesgo en la seguridad de la información, definiendo labores e instrucciones para gestionar el riesgo. Diferentes tipos de organizaciones que vean comprometida la seguridad de la información pueden implementar esta norma. La norma ISO 31000:2009 hace alusión al tratamiento de los riesgos, aportando fundamentos y directivas. Dicha norma suministra indicaciones acerca de cómo constituir y preservar un ámbito de gestión de los riesgos que pueda ser puesto en marcha en cualquier tipo de organización.

Según Crespo[56] la metodología MAGERIT acoge las buenas prácticas de la ISO 27001. Y en cuanto al tratamiento de riesgos se ajusta perfectamente con las exigencias de las ISO/IEC27005 e ISO 31000. MAGERIT tiene un ciclo que comienza con el reconocimiento de los activos de información, posteriormente determina las amenazas naturales y del contexto, evalúa la regularidad y el impacto para encargarse de las contramedidas y finalmente realizar la gestión del riesgo residual. Por lo tanto se aprecia una relación directa y se observa una dependencia de MAGERIT respecto a las normas ISO 27005 e ISO 31000.

De acuerdo a Crespo[57], que explica a la metodología CRAMM como realizada por la Agencia Central de Cómputo y Telecomunicaciones del Reino Unido en el año 1985, tiene como objetivos proteger las propiedades principales de un sistema de información y sus activos para hacer que la información sea confidencial, integral y disponible. Con los conceptos anteriores se dice que es una metodología para el análisis y tratamiento de riesgos que puede ponerse en práctica en diversas clases de sistemas. Para identificar los altos niveles de riesgo se precisa el estudio de factibilidad para determinar

[55]CRESPO, Esteban y CORDERO, Geovanna. Estudio comparativo entre las metodologías CRAMM y Magerit para la gestión de riesgo de TI en las Mpymes. Cuenca: Universidad del Azuay. 2016. p. 8.
[56]CRESPO. Op. cit., p. 9.
[57]CRESPO. Op. cit., p. 4.

las condiciones en la seguridad general, las contramedidas y los respectivos costos relacionados.

Para Crespo[58] la Metodología CRAMM posee un enfoque funcional y se encuentra sustentada en la ISO 27002, adicionalmente considera los cimientos de la ISO 27005 e ISO 31000. CRAMM a diferencia de MAGERIT está enfocada en su implementación en organizaciones grandes y posee un ciclo que comienza con el reconocimiento de los riesgos y posteriormente determina su periodicidad.

Como dice Hurtado[59] la metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) fue desarrollada en Estados Unidos a cargo del SEI (Software Engineering Institute). Goza de buena recepción a nivel global, aunque es catalogada por ser un poco más difícil comparada con el resto de metodologías debido a las fases que emplea. OCTAVE se focaliza menos en las tecnologías y más en el riesgo como tal, esa es una principal diferencia con las demás metodologías. Se debe tener en cuenta que fue ideada para ser utilizada en organizaciones de 300 empleados en adelante.

Como asegura Holguín[60] MEHARI es una metodología que se desarrolló en 1995 por el CLUSIF (Club de la Sécurité de l'Information Français) con el propósito de que los encargados de la seguridad informática realicen una valoración, tanto cuantitativa o cualitativa (dependiendo el escenario) de las fundamentales causas de riesgos que pueden detectar una organización en su respectivo ámbito económico. La valoración de forma cuantitativa o cualitativa es una diferencia principal de MEHARI respecto a MAGERIT que lo puede realizar de forma mixta al igual que CRAMM.

De acuerdo a Morocho[61] la metodología NIST SP 800-30 fue realizada por el Instituto nacional de Estándares y Tecnología (NIST), y está ideada para la valoración de los riesgos en la seguridad de la información de los sistemas TI. Teniendo en cuenta lo anterior, entonces provee una orientación para asegurar los esquemas de infraestructura desde un punto de vista netamente técnico. De igual manera suministra principios claros para la gestión y el manejo de los riesgos continuando con la

[58]CRESPO. Op. cit., p. 8.
[59]HURTADO, Martha. Gestión de Riesgo Metodologías OCTAVE y MAGERIT. Bogotá: Universidad Piloto de Colombia. 2018. p. 3.
[60]HOLGUÍN, Fresia. Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras. Samborondón: Universidad Espíritu Santo. 2018. p. 9.
[61]MOROCHO, Rodrigo y CUEVA, Irma. Diseño de un Plan para el Tratamiento de riesgos Tecnológicos utilizando la metodología NIST SP 800-30. Machala: Universidad Técnica de Machala. 2015. p. 5.

valoración y la atenuación de los mismos y de esta forma asistir a la organización en todos los aspectos relacionados a la tecnología. NISTP SP 800-30 posee un ciclo de 9 fases.

Las principales metodologías tienen como es de suponer bastantes elementos en común, especialmente en lo que se refiere a las fases, entre las metodologías más reconocidas se encuentran: MAGERIT, CRAMM, NIST SP 800-30, MEHARI y OCTAVE, en la tabla 1 se aprecian mejor las fases que constituyen cada una de las metodologías antes mencionadas.

Cuadro 1. Fases de las metodologías para el análisis de riesgos

Fases	METODOLOGÍAS					
	OCTAVE	**MEHARI**	**MAGERIT**	**CRAMM**	**EBIOS**	**NIST SP 800-3**
Caracterización del Sistema	**X**	**X**	**X**	**X**	**X**	**X**
Identificación de amenazas	**X**		**X**	**X**	**X**	**X**
Identificación de vulnerabilidades	**X**			**X**		**X**
Análisis de controles	**X**	**X**	**X**		**X**	**X**
Determinación de la probabilidad						**X**
Análisis de impacto						**X**
Determinación del riesgo	**X**	**X**	**X**	**X**		**X**
Recomendaciones de control	**X**	**X**		**X**	**X**	**X**
Documentación de resultados	**X**	**X**				**X**
Establecimiento de parámetros			**X**			
Necesidades de Seguridad	**X**			**X**	**X**	

Fuente: Universidad Técnica de Machala. Fases de las metodologías para el análisis de riesgos. 2015. Diseño de un Plan para el Tratamiento de riesgos Tecnológicos utilizando la metodología NIST SP 800-30. Machala, p. 5.

5.1.19 Herramientas y técnicas para análisis y gestión del riesgo. De acuerdo a Morí[62]una técnica se define como el conjunto de procesos dispuestos para alcanzar un

[62]MORI, Edinson. Técnicas Recomendadas para Análisis de Riesgo. Para optar al título profesional de Ingeniero de Sistemas e Informática. Iquitos: Universidad Nacional de la Amazonia Peruana. 2015. p. 51.

objetivo propuesto. Conforme a lo anterior, se puede encontrar las siguientes técnicas asociadas al análisis y gestión del riesgo, las cuales deben cumplir con su fácil implementación para que el proceso de análisis y gestión de riesgos sea ágil y oportuno en las pymes del sector de las telecomunicaciones:

5.1.19.1 Mapas de riesgos. Es una herramienta que ayuda a organizar la información sobre los riesgos empresariales y visualizar su dimensión, con el fin de diseñar estrategias apropiadas para su gestión. Los mapas de riesgo se pueden representar mediante gráficos o datos. Los gráficos corresponden a la calificación de riesgo con sus variables correspondientes y su valoración según el método empleado. Los datos se pueden agrupar en tablas, con información sobre los riesgos; su calificación, valoración, controles y demás datos necesarios para comprender la situación de la empresa y sus procesos, respecto a los riesgos que puedan afectarla y las medidas de tratamiento implantadas.

El mapa de riesgos es un instrumento metodológico a través del cual se identifica un conjunto ordenado y variable de factores que pueden dar lugar a eventos que contribuyan al logro de un objetivo, calificar la presencia de un riesgo y finalmente predecir sus posibles daños. Para los proyectos, el mapa de riesgos es un instrumento de control y seguimiento fundamental que posibilita la elección y toma de decisiones para alcanzar los objetivos específicos dentro del proyecto.

5.1.19.1.1Beneficios. Permite una mejor comprensión de la situación de riesgo de la empresa en su conjunto y de sus procesos o proyectos, proporcionando información de forma global o específica. Cuando la dirección no sea consciente de la necesidad de realizar la inversión respectiva en control de riesgos y en la capacitación y concientización del personal, la información de los mapas de riesgo puede servir para soportarla creación de programas de gestión de riesgos y para indicar las acciones a ejecutar definiendo prioridades y propuestas de medidas de tratamiento. A través del diseño y uso de los mapas de riesgo se promueve el trabajo en equipo, y se aumenta la comprensión de los procesos validados. El mapeo de riesgos también permite monitorear el desempeño de la organización en la gestión de sus riesgos, con el establecimiento de comparaciones anuales basadas en las evaluaciones de los distintos riesgos y el análisis de la efectividad de las medidas de control implementadas.

5.1.19.2 Técnicas analíticas. Se usan para entender y definir el contexto general de la gestión de riesgos. Pueden tener un enfoque cuantitativo y cualitativo; en al enfoque cuantitativo se emplean valores numéricos para asignar en la valoración de riesgos y

como su nombre lo índica, se debe cuantificar los aspectos validados. Por su parte el otro enfoque trata de identificar lo que existe dentro del proceso de gestión de riesgos.

5.1.19.3 Juicio de expertos. En este ambiente de incertidumbre respecto a los riesgos, es necesario acudir al juicio de expertos para diseñarla estrategia de tratamiento del Riesgo. Generalmente las personas con más experiencia y conocimiento de los procesos dentro de la empresa, deben estar al frente de la gestión del riesgo de los mismos, debido a su conocimiento a fondo de los procesos internos y de los factores que pueden afectar el desempeño de la organización.

5.1.19.4 Reuniones y entrevistas. Son técnicas comúnmente usadas dentro de las organizaciones, con el fin de identificar y comunicar aspectos claves dentro del proceso de análisis y gestión de riesgos con el personal al que le competen estas actividades.

Como se observa a lo largo del desarrollo del objetivo específico número 1, no son pocos los conceptos relacionados con el análisis y gestión de riesgos, es por lo tanto muy importante tener claridad en los aspectos antes abarcados, ya que sirven como punto de partida para el análisis y gestión de riesgos. Sería contraproducente no tener claros conceptos como riesgo, impacto, vulnerabilidad o amenaza, puesto que en el desarrollo del análisis y gestión de riesgos se podrían obviar factores clave que seguramente pueden repercutir de manera negativa en el óptimo desarrollo de los procesos internos de las Pymes prestadoras de servicios de telecomunicaciones; vale la pena recordar que este proceso de gestión de riesgos debe ser ágil y dinámico, en lo posible suele ejecutarse en un lapso de dos a tres semanas para que las decisiones de la gerencia empiecen a implementarse lo más rápido posible contemplando los escenarios analizados.

5.2 EXAMINAR MEDIANTE UNA REVISIÓN SISTEMÁTICA DE LITERATURA LA METODOLOGÍA MAGERIT V.3

En el transcurso de este capítulo del documento se examinará de forma sistemática la documentación oficial de Magerit en su versión 3, de conformidad con los objetivos propuestos. Lo anterior, con el fin de profundizar en los aspectos que comprende la metodología de análisis y gestión de riesgos, los cuales servirán de base para el siguiente paso de la presente monografía. Magerit está estructurada en su versión 3 con tres libros: Método, Catálogo de Elementos y Guía de Técnicas, los cuales se revisarán de manera ágil.

5.2.1 Libro I: Método. Magerit fue creada y desarrollada por el gobierno español específicamente el ministerio de hacienda y administraciones públicas para ofrecer una respuesta al uso creciente de las tecnologías de la información en los ámbitos públicos y privados para la consecución de los objetivos organizacionales. Magerit se encuentra entonces directamente relacionada con las medidas de seguridad para minimizar los riesgos intrínsecos de las tecnologías de la información.

5.2.1.1 Gobierno, confianza y gestión. Según el Ministerio de Hacienda y Administraciones Públicas[63] el buen gobierno, la confianza y la gestión son la base para el correcto desempeño de las organizaciones. La gestión de riesgos está relacionada con el gobierno o también llamada alta gerencia dentro de las organizaciones; a su vez lo riesgos están directamente relacionadas con las tecnologías de la información, por lo tanto deben ser tratados por las dependencias de gobierno. La confianza es la perspectiva que se tiene respecto a la previsión de lo pronosticado con anterioridad. Se puede afirmar entonces que la confianza es una cualidad de mucho cuidado en las organizaciones que prestan servicios. Los objetivos a cumplir dependen de los sistemas de información, es entonces cuando la seguridad se convierte en un tema importante y recurrente especialmente si los usuarios se ven afectados en caso de fallos, este hecho genera que lógicamente cuestionan la confianza en los sistemas. El entendimiento de los riesgos hace aumentar la seguridad y confianza, entonces el desconocimiento genera desconfianza. La gestión se divide en el análisis y tratamiento de los riesgos y la gestión, se encarga de minimizar los riesgos hasta niveles aceptables.

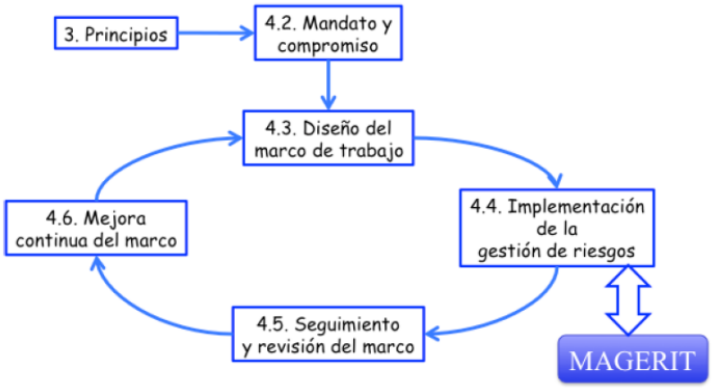
Se recomienda que el gobierno no gestione los riesgos TIC de forma separada de los demás riesgos de la organización. Esto con el fin de crear conciencia dentro de la

[63]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

gerencia respecto de los riesgos que conllevan las TIC (Tecnologías de la información y comunicación) para que de esta forma puedan ser sumados al marco general de la organización.

5.2.1.2 Magerit. En concordancia con el Ministerio de Hacienda y Administraciones Públicas[64] esta metodología enmarca el procedimiento de Gestión de Riesgos dentro de un ámbito de trabajo para que las dependencias de gobierno puedan tomar decisiones acertadas tomando en consideración los riesgos asociados al uso de la TIC. Por tanto, Magerit busca una aproximación estructurada que no dé lugar a la improvisación y que tampoco esté sometida al antojo del analista, tal como se observa en la figura 1.

Figura 1. Marco de trabajo para el manejo de riesgos



Fuente: Dirección General de Modernización Administrativa. Marco de trabajo para el manejo de riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid, p. 7

Magerit posee cuatro objetivos identificables, tres directos y uno indirecto, como se aprecia en la tabla 2. Los cuales se cumplen a cabalidad con una correcta implementación de la metodología.

Cuadro 2. Objetivos de Magerit

Objetivos de Magerit V.3	
Objetivos Directos	1. Concientizar a las organizaciones acerca de la necesidad de la gestión de los riesgos.

[64]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 7.

	2. Proporcionar una forma organizada de analizar los riesgos inherentes al empleo de las TIC.
	3. Asistir para proyectar y planificar el procedimiento que mantenga los riesgos controlados.
Objetivos Indirectos	1. Adiestrar a la Organización en procedimientos evaluativos, certificativos y de auditoría
Fuente: Elaboración propia	

De acuerdo al Ministerio de Hacienda y Administraciones Públicas[65] la metodología Magerit ha procurado mantener homogeneidad en los informes de descubrimientos y también en las conclusiones de las tareas de análisis y manejo de riesgos, tal como se observa en la tabla 3.

Cuadro 3. Homogeneidad de informes, descubrimientos y conclusiones en Magerit

Homogeneidad de informes, descubrimientos y conclusiones en Magerit	
Modelo de valor	Identificación de la importancia que tienen los activos dentro de la organización y así como las subordinaciones entre activos
Mapa de riesgos	Vínculo de las amenazas a las que están sujetas los activos
Declaración de aplicabilidad	En un grupo de salvaguardas se orienta si deben ser consideradas dentro del sistema de información en revisión, de lo contrario no se tienen en cuenta
Valoración de salvaguardas	Valorar la efectividad en las salvaguardas respecto a la amenaza que enfrentan
Condición de riesgo	Especificar los activos de acuerdo a su riesgo remanente, en otras palabras lo que puede acontecer, teniendo en cuenta las contramedidas empleadas
Informe de insuficiencias	Reunir las vulnerabilidades dentro del sistema, entendiendo estos como aspectos con débil protección en relación con las amenazas que podrían consumarse
Acatamiento de la legislación	Obedecer las condiciones requeridas. Determinar el ajuste y conformidad de acuerdo a la normativa pertinente

[65]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 8.

Programa de seguridad	Grupo de esquemas seguros que ayudan a concretar las determinaciones efectuadas para el de tratamiento de los riesgos
Fuente: Elaboración propia	

5.2.1.3 Seguridad. De acuerdo a lo sugerido por el Ministerio de Hacienda y Administraciones Públicas[66]la seguridad está definida como la capacidad que adquieren los sistemas de información o las redes para resistir con un determinado nivel de confianza los incidentes o ilícitos que afecten la integridad, disponibilidad y confidencialidad de los datos. La finalidad de la seguridad es la protección de la misión organizacional, considerando las facetas o propiedades de la seguridad y sus dimensiones derivadas como se aprecia en la tabla 4.

Cuadro 4. Propiedades principales y derivadas de la SI

Propiedades Principales y Derivadas de la seguridad de la información			**Consecuencias del incumplimiento de las propiedades**
Propiedades principales	Disponibilidad	Es la capacidad de los servicios o datos para ser empleados cuando se requieran.	La ausencia de la disponibilidad implica la suspensión del servicio e influye sin lugar a dudas en la producción de las organizaciones.
	Integridad	Sostenimiento de los atributos de entereza y corrección de los datos	Cuando se pierde esta propiedad la información puede mostrarse defectuosa, corrompida o alterada afectando el rendimiento en las labores de la organización.
	Confidencialidad	Cuando la información llega a personas no autorizadas	Pueden existir fugas o divulgaciones no autorizadas, esto implica que es una propiedad muy compleja en su restauración, lo que afecta la confianza de los terceros en la organización. Lo anterior puede infligir acuerdos contractuales referentes a los datos
Propiedades derivadas	Autenticidad	Característica en la cual un ente se encarga de garantizar la fuente de la procedencia de los datos	Cuando esta propiedad se pierde nos encontramos con adulteración en el origen y usurpación de identidad.

[66]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 9.

	Trazabilidad	Esta característica asegura que en cualquier momento se pueda definir quien efectuó acciones en los datos	Dicha propiedad está relacionada con los registros de las actividades ejecutadas y en caso de incidentes es fundamental para encontrar responsables
Fuente: Elaboración propia			

Estas propiedades pueden ser exigidas en algún momento y cuando esto suceda se deben asignar recursos para poder obtenerlas. A optimizar esta actividad es que se destinan las metodologías de análisis y tratamiento de los riesgos.

Riesgo se define así, según Magerit[67] valorar el nivel al que está expuesto un activo o varios para que una amenaza se concrete afectando a la organización. Por lo tanto, el riesgo expresa lo que podría suceder a los activos si no se protegen de forma correcta. En otras palabras se debe analizar el sistema para conocer en qué medidas de peligro se encuentran dichas características, en la tabla 5 se puede ver esto de manera más concreta.

Cuadro 5. Análisis del sistema

Análisis del Sistema	
Análisis del riesgo	Procedimiento metódico para valorar los atributos de los riesgos a la que una organización se encuentra expuesta Conociendo lo que podría llegar a suceder, se deben ejecutar decisiones

[67]Ibid., p. 9.

Tratamiento de los riesgos	Procedimiento dedicado a modificar o disminuir el riesgo. Existen diferentes maneras para el tratamiento de un riesgo, como por ejemplo: evitar las condiciones que lo causan, disminuir las probabilidades de que se manifieste, limitar sus consecuencias y finalmente aceptando dicho riesgo y reservando recursos para proceder cuando exista la necesidad. Cabe destacar que aceptar el riesgo es una opción totalmente válida y que la seguridad definitiva no existe. En ocasiones se aceptan riesgos en la operación sobre ciertas actividades que producen un beneficio que supera al riesgo y nos vemos en la obligación de confrontar. Es por esto que existen amplias definiciones de riesgo
Fuente: Elaboración propia	

Para el Ministerio de Hacienda y Administraciones Públicas[68] todo lo anterior, es un poco complejo, no es una situación netamente técnica, se deben agregar decisiones para aceptar diferentes grados de riesgos; por consiguiente, se hace imprescindible conocer las condiciones para modificar la confianza acorde al sistema. Para este proceso no hay nada mejor que un acercamiento metódico que soporte la toma de decisiones fundamentadas y explicadas razonablemente.

La gestión de riesgos es el proceso que permite a los gerentes comerciales equilibrar los costos operativos y económicos de las medidas de protección y lograr ganancias en la capacidad de la misión al proteger los procesos comerciales que respaldan los objetivos de la organización o la misión de la empresa. Sin embargo, la gestión de riesgos no se limita al ámbito de la seguridad y la tecnología de la información. Este es un proceso comercial que ayuda a la administración a cumplir con su deber fiduciario de proteger los activos de la organización.

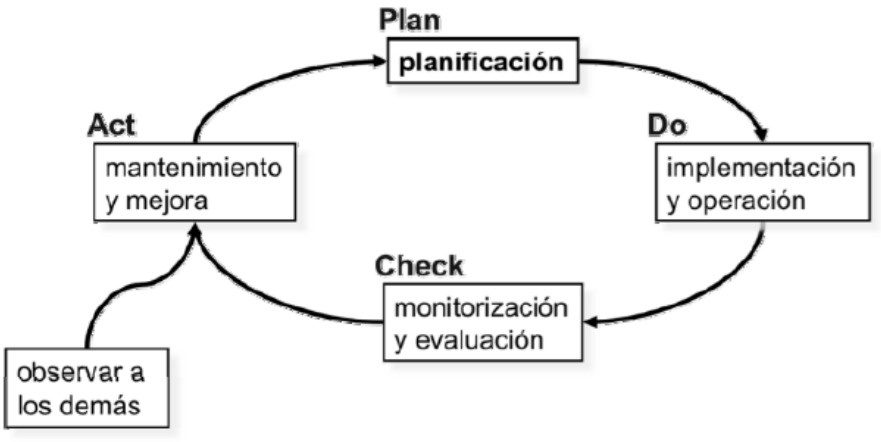
5.2.1.4 Entorno del análisis y gestión de riesgos. De acuerdo al Ministerio de Hacienda y Administraciones Públicas[69] el análisis y manejo de los riesgos van comprendidos dentro de la función del manejo de la seguridad. Está revisión o análisis permite conocer cuan protegido se encuentra el sistema. Es por esto que se deben coordinar los objetivos y la política estratégica de la organización. Las tareas para tratar

[68]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 10.
[69]Ibid., p. 10.

los riesgos favorecen la creación de un plan de seguridad que al ser implementado y ejecutado podrá satisfacer los objetivos planeados ajustados al nivel de riesgo aceptado por la dirección. Estas actividades agrupadas se conocen como el Proceso de Gestión de Riegos.

El Ministerio de Hacienda y Administraciones Públicas[70] afirma que a puesta en funcionamiento de las disposiciones de seguridad demanda una gestión y colaboración de todas las personas que estén interrelacionadas con el sistema de información, porque obviamente este personal es el encargado de la reacción frente a los incidentes y el seguimiento del sistema. Esta forma de trabajo debe ser cíclica, dado que los sistemas de información muy pocas veces son inalterables; por el contrario se encuentran en constante cambio, debido a activos nuevos y por supuesto a las nuevas amenazas, entonces se requiere una verificación periódica basada en la experiencia y con la adaptabilidad sobre las nuevas condiciones. El análisis de riesgos suministra una maqueta del sistema en lo que se refiere a activos, peligros y contramedidas y es fundamental para regular todos los procesos. Los sistemas de gestión de la seguridad de la información (SGSI) presentan cuatro etapas reiterativas como se observa en la figura 2.

Figura 2. Ciclo PDCA



Fuente: Dirección General de Modernización Administrativa. Ciclo PDCA. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid, p. 11.

Como afirma el Ministerio de Hacienda y Administraciones Públicas[71] el análisis de riesgos hace parte de la planeación, donde se adoptan decisiones para la

[70]Ibid., p. 10.
[71]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 11.

administración de la organización. Por tanto, las decisiones se ven concretadas en la instauración, donde se recomienda aplicar elementos de monitoreo de las actividades para medir la efectividad de las mismas y tomar decisiones según el caso. Todo lo anterior, enmarcado dentro de un proceso de mejora continua, incluyendo los conceptos relacionados a continuación en la tabla 6.

Cuadro 6. Contexto del análisis y gestión de riesgos

Contexto del análisis y gestión de riesgos	
Concientización y capacitación	Se requiere la generación de una cultura segura, que guiada por la alta gerencia concientice a todas las personas involucradas a cerca de los beneficios de estas acciones. Son tres las bases esenciales para la instauración de esta cultura: • Definición de unas medidas de seguridad organizacional, que la entiendan incluso los no expertos y que sea transmitida de forma efectiva con actualizaciones permanentes. • Definición de una normatividad de seguridad, aclarando el uso adecuado y las formas de incumplimiento. • Formación continua repasando las rutinas y los procesos especializados, de acuerdo a las diferentes responsabilidades en la organización.
	Para que estos procesos sean efectivos en la organización, es indispensable que la seguridad sea: • Poco intrusiva: que no complique sin necesidad las actividades y procesos diarios, y que tampoco ponga en duda los objetivos de producción organizacionales. • Debe ser natural: es decir que favorezca el acatamiento de las mejores prácticas propuestas. • Administrada por la dirección, esta debe dar ejemplo en las actividades del día a día y a la vez responder con prestancia tanto en las alteraciones e incidencias

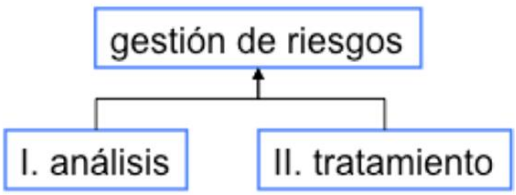
Incidentes y restauración	Se debe generar responsabilidad para cuando los futuros problemas puedan ser detectados por las personas en cercanía de los activos alterados, para de esa forma puedan ser enfocados hacia los centros de resolución. Al momento de ocurrir una incidencia, el tiempo se constituye como un enemigo del sistema, la sobrevivencia pasa a depender de la presteza con que se realicen los reportes y las reacciones. Una equivocación, confusión o ambivalencia en los momentos críticos se puede ver maximizado transformando un simple accidente en un desastre. Se recomienda asimilar tanto los aciertos como los errores y de esta forma añadir dichas experiencias dentro del proceso de gestión de riesgos
Fuente: Elaboración propia	

5.2.1.5 Perspectiva general. Según el Ministerio de Hacienda y Administraciones Públicas[72]se incluyen dos grandes tareas a ejecutar en la gestión de riesgos, tal como se observa en la tabla 7 y en la figura 3.

Cuadro 7. Tareas de la gestión de riesgos

Tarea	Descripción
1. Análisis de riesgos	Tarea en la cual se trata de anticipar lo que podría suceder, determinando con que cuenta la organización
2. Tratamiento de los riesgos	Esta tarea logra ordenar las defensas de una forma racional y consciente. La defensa pretende que no suceda nada malo y paralelamente estar atentos a las emergencias, para subsistir a los incidentes y lograr operar en condiciones óptimas. Como la perfección no existe se asume que la dirección puede enfrentar riesgos en niveles residuales
Fuente: Elaboración propia	

Figura 3. Gestión de riesgos



Fuente: Dirección General de Modernización Administrativa. Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid, p. 19.

[72]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 19.

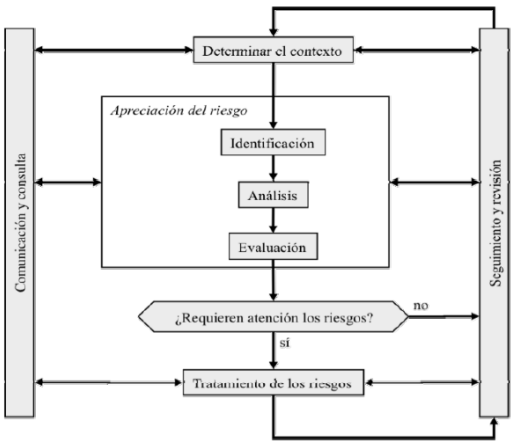
De acuerdo al Ministerio de Hacienda y Administraciones Públicas[73] el análisis de riesgos logra analizar los componentes de una manera procedimental para poder concluir las estimaciones con bases sólidas y posteriormente pasar a la fase del tratamiento, como se aprecia en la tabla 8.

Cuadro 8. Componentes y estimaciones del análisis del riesgo

Componentes del análisis de riesgos	Estimación
1. Los componentes o elementos (también llamados activos) del sistema de información, vinculados directamente con la organización y su misión.	1. El impacto, es decir lo que podría llegar a suceder 2. El riesgo, lo que probablemente suceda
2. Las amenazas, son situaciones que tienen la capacidad de afectar a los activos, causando pérdidas y daños a la Organización.	
3. Salvaguardas (se pueden conocer como contra medidas), son las disposiciones de seguridad extendidas para que las amenazas provoquen el menor daño posible.	
Fuente: Elaboración propia	

De acuerdo a Magerit[74] el proceso cíclico de gestión de riesgos que se propone se encuentra reflejado en el siguiente esquema de la figura 4 y más detallado en la tabla 9.

Figura 4. Proceso de gestión de riesgos



Fuente: Dirección General de Modernización Administrativa. Proceso de Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid, p. 20.

[73]Ibid., p. 19.
[74]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 20.

Cuadro 9. Proceso de gestión de riesgos

Proceso de gestión de riesgos	
Determinación del Contexto	Establece las variables junto con las delimitaciones internas y externas que posibilitan enmarcar la política que se implementará para gestionar los riesgos
Identificación de riesgos	Persigue la conexión entre las presumibles zonas de peligro. Lo que se reconozca será analizado en la siguiente etapa. Lo que no, pasará a ser un riesgo escondido u omitido
Análisis de riesgos	Busca evaluar los riesgos reconocidos, calculando sus repercusiones (análisis cuantitativo), clasificando su relevancia relativa (análisis cualitativo). De cualquiera de las dos formas el fruto del análisis corresponderá con una visión ordenada que logre enfocarse en lo más esencial
Evaluación de riesgos	Interpreta las consecuencias partiendo del análisis técnico enfocado en el negocio. La estrategia y la política definen que riesgos son aceptados y cuáles no
Tratamiento de riesgos	Compila los procesos encargados de alterar el estado del riesgo
Comunicación y consulta	Se debe recordar que el soporte de la productividad de las organizaciones se encuentra en los sistemas de información. Se debe procurar una equidad entre la productividad y la seguridad a través de varios interlocutores: • Usuarios que contribuyan de forma activa dentro de las variables de seguridad para resguardar la operación del sistema. • Proveedores externos para llevar a cabo los valores de servicio definidos. • Dependencias de la gerencia para diseñar conductos de comunicación que solidifiquen la confianza en el sistema de información
Seguimiento y revisión	Se debe recalcar que el proceso de análisis de riesgos es una labor de oficina y puede diferir con lo que se encuentre en la práctica, por lo tanto se debe proceder de acuerdo a las condiciones encontradas, especialmente al momento de reaccionar de manera acertada a los incidentes. Por último la mejora continua es imprescindible para ajustar la experiencia de acuerdo al entorno siempre cambiante de las organizaciones
Fuente: Elaboración propia	

5.2.2 Libro II: Catálogo de objetos. De acuerdo al Ministerio de Hacienda y Administraciones Públicas[75] el libro II posee los siguientes objetivos plasmados en la tabla 10.

Cuadro 10. Objetivos libro II

Objetivos Libro II	
1	1. Viabilizar el trabajo de las personas que estén interesadas en implementar la metodología de una forma en la que encuentran una estandarización fácil de asimilar, para enfocarse en el análisis del sistema
2	2. Lograr una uniformidad de los resultados en los análisis, impulsando un vocabulario y pautas homogéneas para cotejar y complementar análisis efectuados por diferentes equipos de personas
Fuente: Elaboración propia	

Como afirma el Ministerio de Hacienda y Administraciones Públicas[76]en la consecución de los objetivos antes mencionados y reconociendo la rápida evolución tecnológica a continuación se describe un catálogo que marca unas reglas para los siguientes ítems contenidos en la tabla 11.

Cuadro 11. Ítems catálogo de objetos

Ítems Catálogo de Objetos	
Tipos de activos	Pueden surgir nuevos tipos de forma continua
Dimensiones de valoración	En casos puntuales pueden surgir nuevas dimensiones, pero siempre se debe tener la confianza de haber analizado lo fundamental
Criterios de valoración	Tener presente la subjetividad del experto, la idea es estandarizar las dimensiones de valoración pero ideando relaciones entre dichas dimensiones
Amenazas	Reconociendo que hay amenazas con diferente peso específico según las organizaciones

[75]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.
[76]Ibid., p. 6.

Salvaguardas	Se deben manejar basándose en reconocer las necesidades. Cabe recalcar que implica cierto nivel de complejidad debido a las diferentes tecnologías y productos
Fuente: Elaboración propia	

5.2.2.1 Tipos de activos. De acuerdo al Ministerio de Hacienda y Administraciones Públicas[77]los tipos de activos están agrupados dentro de una jerarquía pero se especifica que un activo también puede pertenecer a diferentes tipos, tal como se observa en la tabla 12.

Cuadro 12. Tipos de activos

Tipos de activos	
Activos esenciales	En los sistemas se debe considerar 2 componentes esenciales: Información manejada y Servicios prestados. Los componentes esenciales definen los requerimientos en el aspecto de seguridad para las demás partes del sistema. Tienen particularidades si son de carácter individual y personal, también si poseen requisitos legales y si finalmente están controlados por clasificaciones de seguridad con propiedades reguladas Datos Personales: Para el tratamiento de los datos personales, según las condiciones que los rodeen existen leyes establecidas en cada país que definen medidas ineludibles para los sistemas de información. Por lo general esta reglamentación implica medidas de nivel básico, medio y alto
Estructura del sistema	Hace referencia a componentes que posibilitan la configuración del sistema, precisando su arquitectura interna y su nexo con el exterior
Datos / Información	Los datos son el núcleo de la organización que ayuda a suministrar sus servicios. La información será guardada en equipos y sistemas de información reuniendo bases de datos y archivos, será trasladada en diferentes lugares por diferentes medios de transmisión de datos. Entonces se puede considerar como un activo intangible

[77]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 7.

Claves criptográficas	Las claves criptográficas combinan información privada y pública, son primordiales para asegurar la operación de los instrumentos criptográficos. La criptografía sirve para resguardar el secreto y validar las partes implicadas en la transferencia de información
Servicios	Tarea o labor que solventa una necesidad de parte de los usuarios. Se tienen en cuenta servicios suministrados por el sistema
Software	Poseen diferentes designaciones: programas, aplicativos, etc. Se refiere por tanto a procesos desarrollados por un equipo informático para automatizar tareas. Los programas administran, examinan y cambian los datos permitiendo obtener provecho de la información encaminando todo lo anterior al suministro de servicios. El código fuente será tomado también como datos
Hardware	Se refiere a los instrumentos materiales y físicos encargados de sostener de forma directa o indirecta los servicios suministrados por la organización, en donde se almacenan de forma transitoria o definitiva los datos. Es también considerado como sostén de los programas y se encarga de procesar y transmitir datos
Redes de comunicaciones	Son los medios de transmisión de datos entre diferentes lugares y se incluye establecimientos destinados a funciones de comunicación tanto propio, como de terceros
Soportes de información	Se contemplan instrumentos físicos que puedan guardar información de manera estable, o por lo menos a lo largo de extensos periodos de tiempo
Equipamiento auxiliar	Se consideran instrumentos diferentes que apoyan a los soportes de información, pero no se encuentran ligados directamente con los datos
Instalaciones	Son los lugares donde se encuentran los sistemas de información y los sistemas de comunicación
Personal	Son las personas asociadas y vinculadas con los sistemas de información
Fuente: Elaboración propia	

5.2.2.2 Características de valoración. Como sugiere el Ministerio de Hacienda y Administraciones Públicas[78] son las propiedades o cualidades que logran hacer valorable un activo. Entonces la dimensión es un lado o rasgo del activo que es autónomo de otros lados. El análisis de riesgos se puede centralizar en una faceta sin

[78]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 15.

importar lo que suceda con otras. Las dimensiones son empleadas para determinar los resultados de la concreción de una amenaza. El valor asignado a la dimensión de un activo es el grado de daño en la organización cuando el activo se ve afectado en la dimensión. Las características de valoración se aprecian en la tabla 13.

Cuadro 13. Características de valoración

Características de valoración	
Disponibilidad	Particularidad o atributo del activo basado en que los individuos o procesos autorizados tienen entrada y acceso a los atributos en el momento que lo requieran
Precisión y coherencia de los datos	Particularidad o atributo del activo en el que se asegura que no ha sufrido modificaciones por individuos o procesos no autorizados
Reserva de la información	Particularidad o atributo en el que la información no ha sido revelada, ni puesto al alcance de individuos o procesos no autorizados
Autenticidad	Particularidad o atributo en el que los entes son quienes aseguran ser o las fuentes de las que proceden los datos son garantizadas
Trazabilidad	Particularidad o atributo en el que las acciones de un ente pueden ser responsabilizadas al ente antes mencionado
Fuente: Elaboración propia	

5.2.2.3 Criterios de valoración. Como afirma el Ministerio de Hacienda y Administraciones Públicas[79]en teoría para esta valoración se puede usar cualquier escala de valores. Pero para resultados prácticos se recomienda:

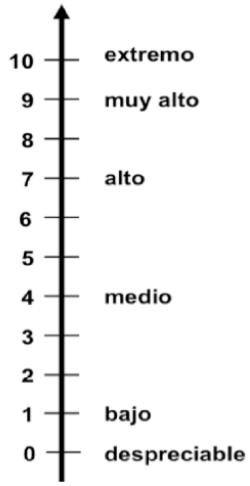
- Que todas las dimensiones empleen una escala en común para facilitar labores de comparación de los riesgos.
- Emplear una escala logarítmica, que no se centre en disparidades absolutas, sino por el contrario en disparidades relativas en el valor.
- Aplicar un juicio equilibrado para facilitar el contraste entre análisis efectuados en diferentes instancias

De acuerdo al Ministerio de Hacienda y Administraciones Públicas[80] la valoración cualitativa estará sujeta a juicios subjetivos, pero si la valoración es económica solo se

[79]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 19.
[80]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 19.

hablará de dinero. Se eligió una escala de diez valores, donde cero es un valor despreciable en cuanto al riesgo. Para análisis de riesgo con poco detalle se recomienda la tabla, Pero tanto la escala como la tabla se encuentran relacionadas. Se ha definido una escala con diez valores, el valor 0 como determinante de lo que sería un riesgo despreciable. Si se realiza una valoración de riesgos menos detallada, se puede elegir la tabla simplificada de menos niveles. Ambas escalas, la detallada y simplificada se muestran a continuación en la figura y la tabla.

Figura 5. Escala detallada de valores



Fuente: Dirección General de Modernización Administrativa. Escala detallada de valores. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Madrid, p. 19.

Cuadro 14. Tabla simplificada de valores

Valor	Criterio
Extremo	Daño extremadamente grave
Muy alto	Daño muy grave
Alto	Daño grave
Medio	Daño importante
Bajo	Daño menor
Despreciable	Irrelevante a efectos prácticos
Fuente: Dirección General de Modernización Administrativa. Escala detallada de valores. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Madrid, p. 19.	

5.5.2.4 Amenazas. Como asegura el Ministerio de Hacienda y Administraciones Públicas[81]el catálogo de amenazas informa posibles acciones que puedan influir negativamente en los activos de un sistema de información. Por lo general sus denominaciones serán auto explicativas, tal como se observa en la tabla 15.

Cuadro 15. Amenazas en Magerit

Amenazas	
Desastres Naturales	Se incluye acontecimientos que suceden sin que las personas causen o interfieran de forma directa o indirecta.
	Fuego: Se hace referencia a los incendios, puesto que el fuego puede destruir los recursos del sistema.
	Daños por agua: Pueden ser Inundaciones, generalmente causadas por aguas lluvias, que pueden generar destrozos en los recursos del sistema.
	Desastres Naturales: Se contemplan incidentes tales como: tormentas eléctricas, terremotos, tsunamis, ciclones, tornados, avalanchas, desprendimiento de tierras y erupciones volcánicas
De origen industrial	Fuego.
	Daños por agua: fugas, escapes o inundaciones.
	Desastres industriales, desastres causados por actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas.
	Contaminación mecánica: vibraciones, polvo, suciedad.
	Contaminación electromagnética: interferencias de radio, campos magnéticos.
	Avería de origen físico o lógico: puede ser una falla de origen o producirse durante el uso del sistema.
	Corte del suministro eléctrico: Cese de la alimentación de potencia.
	Condiciones inadecuadas de temperatura o humedad: Deficiencias en la refrigeración de equipos o instalaciones. Demasiado calor o frío o incluso humedad.
	Fallo de servicios de comunicaciones: Interrupción de la transmisión de datos debido a destrucción física de los medios.
	Interrupción de otros servicios y suministros esenciales.
	Degradación de los soportes de almacenamiento de la información: Generalmente causados por el paso del tiempo y el uso de los dispositivos.

[81]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 25.

	Emanaciones electromagnéticas: Poner datos al alcance de terceros vía radio.
Para todos los incidentes anteriores si el origen es el entorno se considera accidental y si el origen es humano, puede ser de forma accidental o deliberada	
Errores y fallos no intencionados	Como su nombre lo indica, se hace referencia a fallos causados por personas de forma no intencional
	Errores de los usuarios: Fallos de las personas en el uso de servicios o datos.
	Errores del administrador: errores causados por los encargados de la instalación y la operación.
	Errores de monitorización (log): Como su nombre lo indica errores u omisiones en los registros o tratamiento de registros.
	Errores de configuración: Configuración errónea.
	Deficiencias en la organización: cuando no existe precisión en cuanto a funciones y responsabilidades sobre los activos.
	Difusión de software dañino: virus, troyanos, gusanos, spyware y bombas lógicas.
	Errores de [re-]encaminamiento: errores en las rutas de transmisión de datos, lo que conlleva un error de entrega.
	Errores de secuencia: alteración no intencionada del orden en la transmisión de mensajes.
	Escapes de información: errores de entrega debido a que la información llega a personas que no deberían conocerla, lo anterior no implica alteración de datos.
	Alteración accidental de la información.
	Destrucción de información: Pérdida o daño accidental de la información.
	Fugas de información: Indiscreciones verbales, escritas y a través de medios digitales.
	Vulnerabilidades de los programas: Defectos de código fuente en las aplicaciones.
	Errores de mantenimiento / actualización de programas (software): Anomalías en controles y procesos.
	Errores de mantenimiento / actualización de equipos (hardware): Anomalías en controles y procesos.
	Caída del sistema por agotamiento de recursos: Recursos insuficientes provocando caídas del sistema debido a sobrecargas.
	Pérdida de equipos.
	Indisponibilidad del personal: Se puede dar por ausencias laborales, enfermedades y alteración del orden público.
Ataques	Son fallas causadas por las personas de forma intencional

intencionados	Alteración de los registros de actividad o logs: manipulación de registros para encubrir actividades.
	Alteración de la configuración: manipulación de privilegios de acceso, flujos de actividades y registros de actividad. Casi siempre a cargo de administradores.
	Suplantación de la identidad del usuario: suplantaciones de usuarios por parte de atacantes para uso no autorizado.
	Abuso de privilegios de acceso: Cuando los privilegios determinados son abusados o ignorados generalmente hay problemas.
	Uso no previsto: Uso personal de equipos corporativos.
	Propagación de software perjudicial: Difusión deliberada de gusanos, troyanos, virus, spyware y bombas lógicas.
	Cambio en la ruta de mensajes: Forzar un mensaje a usar una ruta incorrecta para que pueda ser visible o interceptado.
	Alteración de secuencia: con un mensaje alterado en su secuencia se compromete la integridad de los datos.
	Acceso no autorizado: Cuando los recursos son alcanzados por el atacante.
	Análisis de tráfico: Con el monitoreo de tráfico se puede sacar conclusiones de los datos analizados.
	Repudio: Negación de servicios ya empleados en el pasado. Repudio de origen, recepción y entrega.
	Interrupción de información: No implica alteración de la información pero si acceso a la misma sin autorización.
	Alteración de la información: para causar daños y perjuicios en la organización u obtener beneficios.
	Destrucción de información: destrucción de datos para causar daños y perjuicios en la organización u obtener beneficios.
	Divulgación de información: revelar información privada.
	Manipulación de programas: Modificación de programas para lograr un beneficio cuando alguien lo usa.
	Manipulación de los equipos: Manipulación de programas para lograr un beneficio cuando alguien lo usa.
	Denegación de servicio: Deficiencia de recursos cuando la carga de trabajo es sobrepasada.
	Robo: Hurto de equipos y si contienen datos puede implicar una fuga de información.
	Ataque destructivo: Se hace referencia a vandalismo, terrorismo o acción militar.
	Ocupación enemiga: Cuando se pierde dominio sobre los medios propios.

	Indisponibilidad del personal: Se habla de huelgas, absentismo y ausencias no justificadas. También se puede deber a bloqueos en las entradas de las instalaciones.
	Extorsión: Presión o amenazas del atacante sobre alguien para lograr una determinada acción.
	Ingeniería social (picaresca): Es cuando un tercero abusa de la inocencia de las personas y son conducidas a realizar una actividad en beneficio de dicho tercero.
Fuente: Elaboración propia	

5.5.2.4 Salvaguardas. Como afirma el Ministerio de Hacienda y Administraciones Públicas[82]las salvaguardas afrontan las amenazas. Las técnicas se ven afectadas por la evolución tecnológica debido a.

- Aparición de nuevas tecnologías.
- Obsolescencia de tecnologías antiguas.
- Modificación del tipo de activos en consideración.
- Evolución de las técnicas atacantes.
- Evolución de las salvaguardas existentes.

Como sugiere el Ministerio de Hacienda y Administraciones Públicas[83] el catálogo de salvaguardas es simplemente una clasificación de variadas manifestaciones materiales, tecnológicas y procedimentales que pueden ser aplicadas en un momento específico. Se observa el catálogo completo en la tabla 16.

Cuadro 16. Catálogo de salvaguardas

Catálogo de salvaguardas	Defensas generales y horizontales
	Defensa de los datos
	Defensa de las claves criptográficas
	Defensa de los servicios
	Defensa de los programas
	Defensa de los equipos
	Defensa de las comunicaciones
	Defensa en los puntos de interconexión con otros sistemas
	Defensa de los soportes de información
	Defensa de los elementos auxiliares
	Defensa de las instalaciones
	Contramedidas relativas al personal

[82]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 53.
[83]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 53.

	Contramedidas de tipo organizativo
	Constancia en las operaciones
	Tercerización
	Obtención y evolución
Fuente: Elaboración propia	

5.2.3 Libro III: Guía de técnicas. De acuerdo al Ministerio de Hacienda y Administraciones Públicas[84] el tercer libro tiene como objetivo la descripción de algunas técnicas empleadas en el análisis y gestión de riesgos. Se dividen principalmente en técnicas específicas y técnicas generales.

5.2.3.1 Técnicas específicas. Tal como afirma el Ministerio de Hacienda y Administraciones Públicas[85]se incluyeron técnicas tales como:

1. Tablas, para obtener resultados de manera simple.
2. Técnicas algorítmicas, para la obtención de resultados complejos.

5.2.3.1.1 Tablas. Tal como afirma el Ministerio de Hacienda y Administraciones Públicas[86]se ha demostrado basado en la experiencia el beneficio del uso de tablas, que a pesar de no tener precisión, si son efectivas al momento de la identificación de los activos y sus amenazas asociadas.

Se sugiere la siguiente escala para la calificación de: activos, dimensión del impacto y dimensión del riesgo:

- **MB**: muy bajo
- **B**: bajo
- **M**: medio
- **A**: alto
- **MA**: muy alto

La estimación del impacto puede realizarse de manera simple, empleando tablas de doble entrada como se aprecia en la tabla 17.

[84]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 4.
[85]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 5.
[86]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 6.

Cuadro 17. Estimación del impacto

Impacto		Degradación		
		1%	10%	100%
Valor	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

Fuente: Dirección General de Modernización Administrativa. Escala detallada de valores. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 6.

El impacto, probabilidad y riesgo se modelan a través de escalas cualitativas como se aprecia en la tabla 18.

Cuadro 18. Escalas de impacto, probabilidad y riesgo

Escalas		
Impacto	**Probabilidad**	**Riesgo**
MA: muy alto	MA: Prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: Bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

Fuente: Dirección General de Modernización Administrativa. Escala detallada de valores. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 7.

De esta forma se pueden combinar impacto y frecuencia, de acuerdo a la tabla 19.

Cuadro 19. Calculo de riesgo

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Dirección General de Modernización Administrativa. Escala detallada de valores. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 7.

5.2.3.1.2 Análisis algorítmico. Como dice el Ministerio de Hacienda y Administraciones Públicas[87]es la diferenciación y división de las partes de un todo para comprender sus fundamentos o elementos. Se tienen para lograr este objetivo, dos enfoques, uno cuantitativo y otro cualitativo, tal como se aprecia en la tabla 20.

Cuadro 20. Enfoques análisis algorítmico

Enfoques análisis algorítmico	
Modelo cuantitativo	En este tipo de análisis se desea saber qué es lo que existe realmente, con la respectiva cuantificación de todos los aspectos posibles. Se emplean diversas formulas y se emplean números positivos, modelo un poco complejo en su implementación. También se definen dependencias entre activos. Se emplean términos como: valor acumulado de un conjunto de activos, degradación de un activo, impacto acumulado de una amenaza sobre un activo, impacto repercutido de una amenaza sobre un activo, probabilidad de una amenaza, riesgo, riesgo acumulado y riesgo repercutido, paquete de salvaguardas, degradación residual, impacto residual, la probabilidad residual y riesgo residual.

[87]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 8.

Modelo cualitativo	En este tipo de análisis se desea saber qué es lo que existe realmente, sin necesidad de cuantificarlo precisamente. Se emplean diversas formulas y una escala discreta de valores, lo cual lo hacen un modelo un poco más complejo en su implementación. Se asignan valores a los activos dentro de una escala. También se definen dependencias entre activos. Se emplean términos como: valor acumulado de un conjunto de activos, degradación de un activo, impacto acumulado de una amenaza sobre un activo, impacto repercutido de una amenaza sobre un activo, probabilidad de una amenaza, riesgo, riesgo acumulado y riesgo repercutido, paquete de salvaguardas, degradación residual, impacto residual, la probabilidad residual y riesgo residual
Fuente: Elaboración propia	

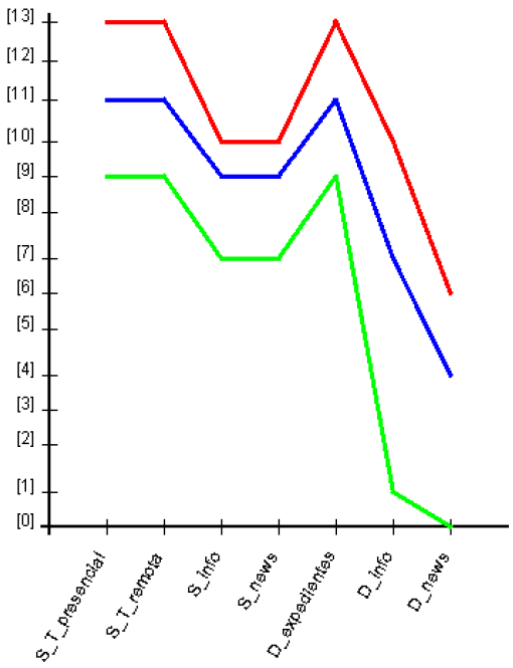
5.2.3.2 Técnicas generales. Como sugiere el Ministerio de Hacienda y Administraciones Públicas[88] se incluyeron técnicas tales como:

1. Técnicas gráficas. Que comprenden gráficas por puntos y líneas, barras, gráficos de radar, diagramas de pareto y diagramas de tarta.
2. Sesiones de trabajo. Que incluyen entrevistas, reuniones y presentaciones.

5.2.3.2.1 Técnicas gráficas. Como sugiere el Ministerio de Hacienda y Administraciones Públicas[89] a continuación se presentan ejemplos de las técnicas gráficas:

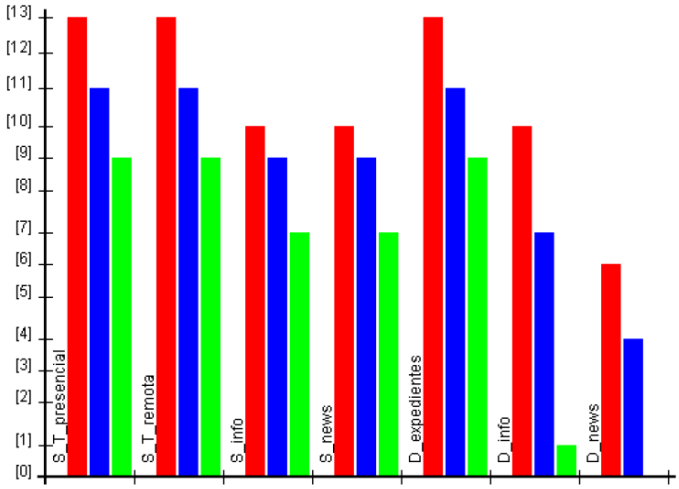
[88]MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Op. cit., p. 25.
[89]Ibid., p. 26.

Figura 6. Gráfico por puntos o líneas



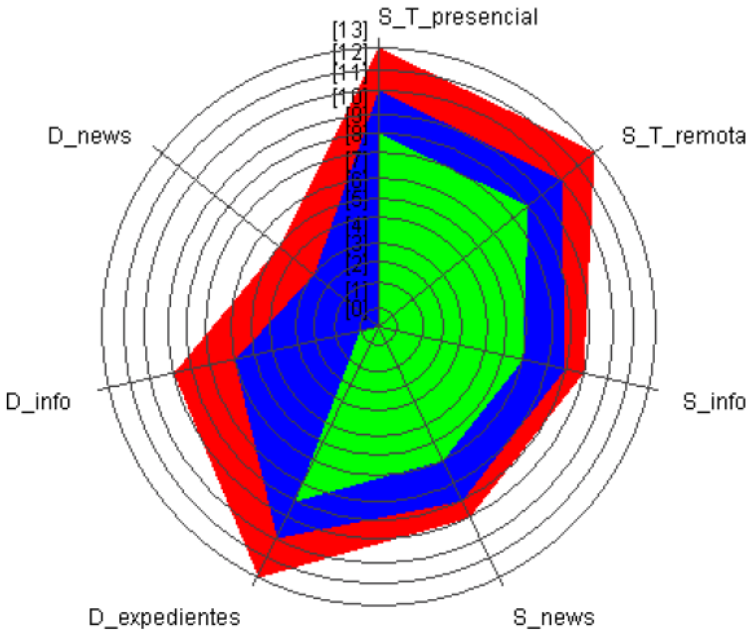
Fuente: Dirección General de Modernización Administrativa. Proceso de Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 27.

Figura 7. Gráfico por barras



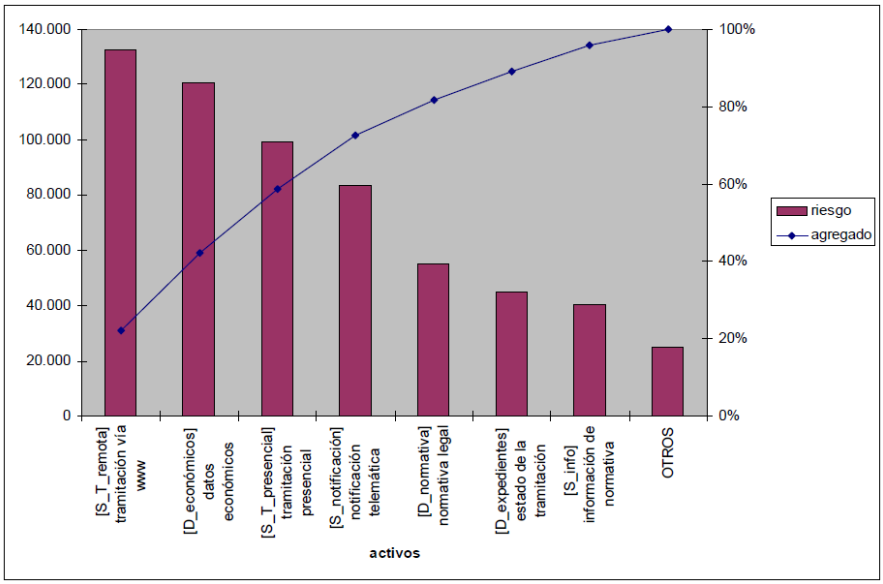
Fuente: Dirección General de Modernización Administrativa. Proceso de Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 28.

Figura 8. Gráfico de radar



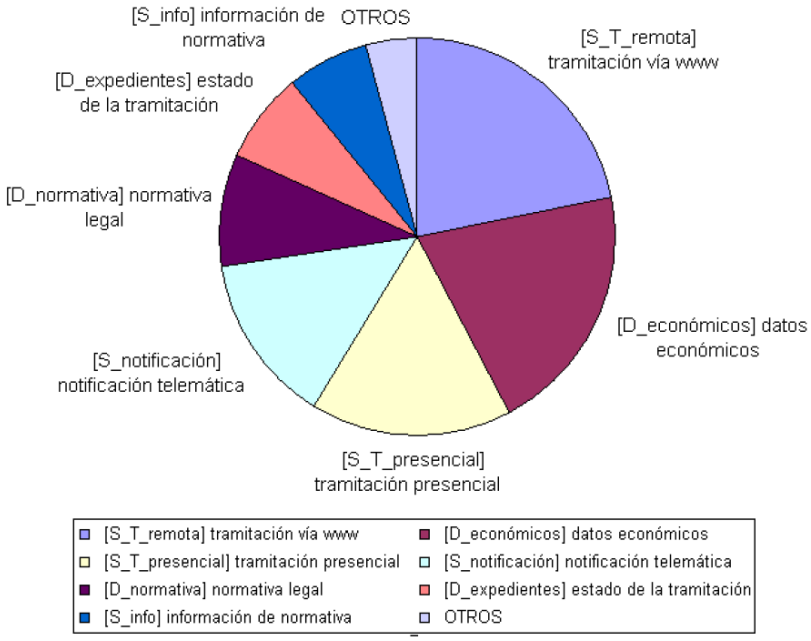
Fuente: Dirección General de Modernización Administrativa. Proceso de Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 29.

Figura 9. Gráfico de pareto



Fuente: Dirección General de Modernización Administrativa. Proceso de Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 32.

Figura 10. Gráfico de tarta



Fuente: Dirección General de Modernización Administrativa. Proceso de Gestión de Riesgos. 2012. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid, p. 33.

5.2.3.2.2 Sesiones de trabajo. Tal como afirma el Ministerio de Hacienda y Administraciones Públicas[90]las sesiones de trabajo pueden tener diferentes objetivos de acuerdo a su tipo. Los objetivos pueden ser los siguientes: obtención de información, comunicación de los resultados, disminución del tiempo en el desarrollo, fomentación de la participación de directivos y usuarios, por último mejorar la calidad en los resultados obtenidos. Dependiendo de las personas que participen, así como los objetivos perseguidos y la forma de realizarlas, las sesiones de trabajo pueden ser: entrevistas, reuniones y presentaciones. Esto se observa con un poco más de detalle en la tabla 21.

Cuadro 21. Tipos de sesiones de trabajo

Tipos de Sesiones de Trabajo	
Entrevistas	Se realizan de forma individual, con los roles definidos de entrevistador y entrevistado, para recopilar información.

[90]Ibid., p. 34.

Reuniones	Las reuniones pueden tener el mismo objetivo que las entrevistas, pero esta vez se hacen de forma grupal y se puede extraer información al igual que informar al grupo de personas involucrado.
Presentaciones	Su objetivo principal es comunicar e informar a un grupo de personas los avances, resultados y conclusiones de un proyecto en particular.
Fuente: Elaboración propia	

Como se puede apreciar a lo largo del desarrollo del objetivo específico número 2, el primer libro de la metodología contiene el método y a la vez conceptos relacionados con el análisis y gestión de riesgos enfocándose en la forma de realizar el proceso. El segundo y tercer libro contienen el catálogo de objetos y la guía de técnicas y ambos comprenden elementos que delimitan la gestión y el análisis de la gestión de riesgos de acuerdo al entorno Magerit. Los tres libros se abarcaron de forma ágil centrándose en los elementos determinantes para una gestión del riesgo rápida y efectiva.

5.3 PROPONER UNA GUÍA BASADA EN UN CASO DE ESTUDIO ORIENTADO A LAS PYMES DEL SECTOR DE LAS TELECOMUNICACIONES QUE PERMITA GESTIONAR EL RIESGO BASADO EN MAGERIT V.3

En el desarrollo de este último capítulo del documento se propondrá una guía basada en un caso de estudio, basado y orientado a las Pymes del sector telecomunicaciones, conforme al tercer objetivo propuesto. Lo anterior, con la intención de servir de medio de consulta para la implementación de la metodología de análisis y gestión de riesgos en su versión 3, enfocándose exclusivamente en las pequeñas y medianas empresas que proveen internet en municipios que requieren el servicio de conectividad y que a su vez están desprovistos del cubrimiento de los grandes operadores de Internet.

5.3.1 Caso de estudio. En el año 2004 y ubicada en la ciudad de Sogamoso en el departamento de Boyacá, comienza a operar una empresa de soporte de equipos de cómputo, impresoras y plotters. Con el fin de expandir su núcleo de negocio decidió apostar por ofrecer los primeros enlaces microondas punto a punto y punto multipunto con banda ancha para tratar de mejorar la conectividad de las empresas que por esos días solo contaban con la baja velocidad de la internet conmutada usando las líneas telefónicas tradicionales.

Como es de esperar, esta decisión tuvo una buena acogida en las empresas y el siguiente paso lógico fue expandir poco a poco la cobertura de la red empresarial para

de esta manera también ofrecer el servicio en el sector residencial en municipios aledaños a Sogamoso. Se empezó a trabajar también con las alcaldías, colegios públicos y bibliotecas municipales de los nuevos municipios que entraban dentro de la cobertura. Se ofrecieron también servicios de implementación y soporte de redes LAN, así como también instalación, soporte y monitoreo de servidores proxy para el control del ancho de banda y filtro de contenido dentro de los entes estatales para asegurar el uso adecuado de este recurso.

A medida que la red se expande y se vuelve un poco más compleja en su cubrimiento de más de 20 municipios en el departamento de Boyacá se hace más palpable la cantidad de amenazas y riesgos a que está expuesta la infraestructura de la empresa, no solo por la información propia y la de clientes estatales, empresariales y residenciales que maneja. Por este motivo la red de las Pymes del sector telecomunicaciones debe ser segura no solo para garantizar el servicio ofrecido, sino también para prevenir intrusiones o ataques a sus clientes.

5.3.2 Metodología de análisis y gestión del riesgo. Para el análisis y gestión del riesgo de los activos de información y la infraestructura tecnológica del caso de estudio en la Pymes ubicada en la ciudad de Sogamoso, en el departamento de Boyacá, se eligió la metodología MAGERIT, de la cual se pueden destacar las siguientes ventajas:

- Alcance completo dentro de la organización si así se requiere.
- Documentación en español de manera oficial con 3 módulos de consulta.
- Es libre y no requiere licenciamiento para su uso.
- Determina muy bien los activos para de esta forma realizar la valoración de riesgos en cada uno de ellos.

El objetivo principal de esta actividad es efectuar un inventario de activos, realizar un análisis de riesgos para establecer amenazas y vulnerabilidades a las que estén sometidos los activos y finalmente precisar las salvaguardas que posibiliten una mejora en la seguridad de los activos. En la tabla 22 se aprecian de forma separada las fases para la implementación de la metodología Magerit.

Cuadro 22. Fases metodología Magerit

Fase	Actividades Metodología Magerit	
1	Caracterización de los activos	Determinación de activos Relaciones de dependencia entre activos Estimación de activos

2	Caracterización de Amenazas	Reconocimiento de amenazas Ponderación de amenazas
3	Caracterización de las salvaguardas	Determinación de salvaguardas Estimación de salvaguardas
4	Estimación del estado de riesgo	Establecer impacto y riesgo acumulado Establecer impacto y riesgo residual Análisis de resultados
Fuente: Elaboración propia		

5.3.2.1 Alcance del análisis. El alcance dispuesto para la metodología Magerit respecto al caso de estudio está enfocado en la prestación del servicio de Internet a sus clientes, y cómo es lógico el punto de partida es la identificación de los activos, sus relaciones de dependencia y estimación de los riesgos a los que se encuentran expuestos dichos activos y la infraestructura empleada. Posteriormente se debe definir un plan de tratamiento del riesgo, que posibilite la implantación de medidas para asegurar los activos, las cuales deben minimizar o poner bajo control las vulnerabilidades y amenazas detectadas. Esto sin duda favorecerá la continuidad en la prestación del servicio principal de la Pyme del sector de las comunicaciones, asegurando los activos, servicios, aplicaciones y dispositivos empleados. En otras palabras esta monografía abarca las fases 1, 2 y 3. La Fase 4 ya implica una implantación real de salvaguardas y un seguimiento del sistema para determinar el estado actual del riesgo, específicamente el riesgo acumulado y el residual. Por lo tanto dicha fase no se encuentra contemplada en la elaboración de este documento.

5.3.3 Fase 1. Esta fase se relaciona con los activos y dividirá en cuatro numerales: Identificación y clasificación, descripción, dependencia y valoración de activos.

5.3.3.1 Clasificación e identificación de activos. De acuerdo a la metodología Magerit y a su primera fase y perteneciente al proceso de análisis y gestión del riesgo se procede a clasificar e identificar los activos del caso de estudio como se observa en la tabla 23.

Cuadro 23. Clasificación e Identificación de activos Magerit

Tipo de activo	Nombre del activo
[D] Datos e Información	1. [BD_CLIENTES] Base de datos clientes
[S] Servicios	3. [SERV_CLI] Servicio Internet Clientes

[SW] Aplicaciones	4. [SO_FW] Sistema operativo Servidor Proxy Firewall
	5. [SO_PC] Sistema operativo PC
	6. [HERR_OFI] Herramientas ofimática
	7. [SIST_CONT] Sistema contable y facturación
[HW] Equipos Informáticos	8. [SERV_FW] Servidor Proxy Firewall
	9. [PC] Computadora tipo escritorio
	10. [RAD_MAESTRO] Radio maestro
	11. [RAD_CLIENTE] Radio cliente
[COM]Redes de comunicaciones	12. [FIB_OP_PROV1] Canal fibra óptica Proveedor principal
	13. [FIB_OP_PROV2] Canal fibra óptica Proveedor respaldo
[AUX] Equipos auxiliares	14. [RED_CABLE] Red cableada
	15. [GABI_RED] Gabinete de red
[L] INSTALACIONES	16. [OF_ADMIN] Oficina administrativa
	17. [DATA_CENTER] Centro de datos
[P] Personal	18. [ADMIN_RED] Administrador de la red
	19. [MESA_SERV] Mesa de ayuda
	20. [ADMIN_FINAN] Administradora y financiera
	21. [COM_VEN] Comercial y ventas
	22. [SOP_TEC] Técnico de soporte en sitio e instalaciones
Fuente: Elaboración propia	

5.3.3.2 Descripción de activos. De acuerdo a la metodología Magerit y a su primera fase y perteneciente al proceso de análisis y gestión del riesgo se procede a describir los activos del caso de estudio como se observa en la tabla 24 incluyendo su responsable.

Cuadro 24. Descripción de activos Magerit

Activo	Descripción	Responsable
[D] [BD_CLIENTES] Base de datos clientes	Base de datos clientes en MySQL	Ingeniera electrónica encargada de la administración y facturación clientes.
[S] [SERV_CLI] Servicio Internet Clientes	Servicio principal de la empresa, prestación de servicio de Internet a clientes estatales, empresariales y residenciales.	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.
[SW] [SO_FW] Sistema operativo Servidor Proxy Firewall	Ubuntu Server 20.04 LTS 64 Bits corriendo aplicaciones de Proxy (ACL y filtro de contenido) y Firewall	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.
[SW] [SO_PC] Sistema operativo PC	Ubuntu Desktop 20.04.2.0 LTS 64 Bits	Técnicos de soporte en sitio.
[SW] [HERR_OFI] Herramientas ofimática	LibreOffice 7.1.4 64 Bits	Técnicos de soporte en sitio.

[SW] [SIST_CONT] Sistema contable y facturación	Ubuntu Desktop 20.04.2.0 LTS 64 Bits corriendo MySQL Community Server 8.0.25	Ingeniera electrónica encargada de la administración y facturación clientes.
[HW] [SERV_FW] Servidor Proxy Firewall	Servidor HPE ProLiant DL360 Intel Xeon Platinum 8160H 8th Gen 3.7 Ghz 256 Gb de RAM DDR4 4 SATA/ 2 SSD 20 TB SO Ubuntu Server 20.04 LTS 64 Bits Pantalla 24 pulgadas LCD	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.
[HW] [PC] Computadora tipo escritorio	Computador Tipo Clon con Procesador Intel i3 8va Generación 2.3 Ghz 8 Gb de RAM DDR4 y SSD 500 Mb. Pantalla 21 pulgadas LCD	Técnicos de soporte en sitio.
[HW] [RAD_MAESTRO] Radio Maestro	Ubiquiti LTU Rocket BaseStation 5.8 Ghz Antena Sectorial tipo panel	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.
[HW] [RAD_CLIENTE] Radio cliente	Ubiquiti LTU LR Subscriber Antena sectorial tipo grilla	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.
[COM] [FIB_OP_PROV1] Canal fibra óptica Proveedor principal	Canal Fibra óptica Movistar 1 Gb	Soporte Movistar
[COM][FIB_OP_PROV2] Canal fibra óptica Proveedor respaldo	Canal Fibra óptica Media Commerce 1 Gb	Soporte Media Commerce
[AUX] [RED_CABLE] Red cableada	Red cableada interconectando los elementos de red LAN y red WAN	Técnicos de soporte en sitio.
[AUX][GABI_RED] Gabinete de red	Switch 48 puertos, Patch Panel, UPS.	Técnicos de soporte en sitio.
[L] [OF_ADMIN] Oficina administrativa	Sede administrativa, Mesa de ayuda, administradora financiera y personal de ventas.	Ingeniera electrónica encargada de la administración y facturación clientes.
[L] [DATA_CENTER] Centro de datos	Servidor Proxy y Firewall, Administrador de red y equipos proveedores de Internet principal y respaldo.	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.
[P] [ADMIN_RED] Administrador de la red	Ingeniero de sistemas encargado del monitoreo y diseño de la red inalámbrica.	N/A
[P][MESA_SERV] Mesa de ayuda	Técnico de soporte remoto para recepción de PQRs.	N/A
[P][ADMIN_FINAN] Administradora y financiera	Ingeniera electrónica encargada de la administración y facturación clientes.	N/A
[P] [COM_VEN] Comercial y ventas	Administradora de empresas encargada de cotizaciones y ventas	N/A
[P] [SOP_TEC] Técnico de soporte en sitio e instalaciones	Técnicos de soporte en sitio.	N/A

Fuente: Elaboración propia

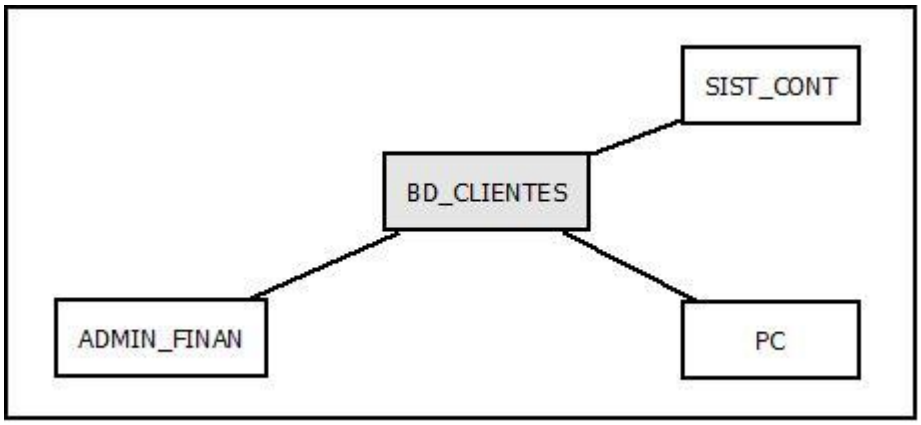
5.3.3.3 Dependencia y relaciones de activos. De acuerdo a la metodología Magerit y a su primera fase y perteneciente al proceso de análisis y gestión del riesgo se procede a describir la dependencia y relaciones entre activos del caso de estudio.

5.3.3.3.1 Dependencia y relaciones de activos tipo datos e información. Se define la dependencia para los activos tipo datos e información.

5.3.3.3.1.1 Base de datos clientes [BD_CLIENTES]. Se define la dependencia el activo Base de datos clientes en la figura 11, basado en:

- El software con el que interactúa
- El hardware con el que interactúa
- Persona que lo emplean

Figura 11. Dependencia activo [BD_CLIENTES]



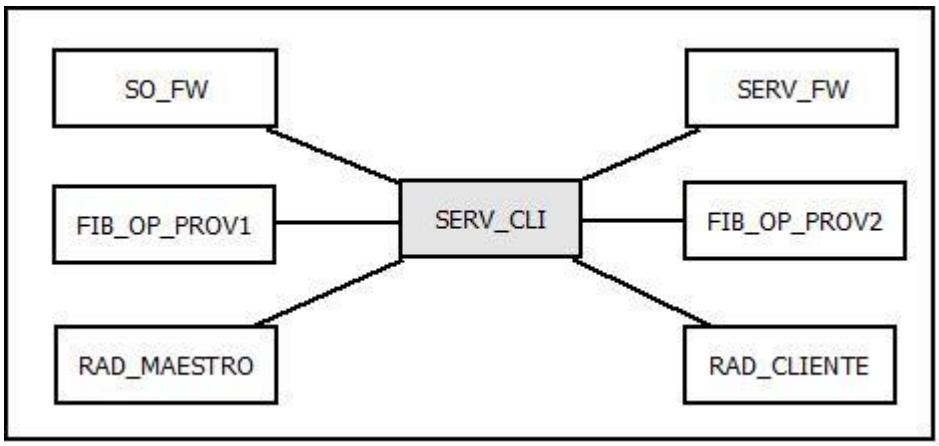
Fuente: Elaboración Propia.

5.3.3.3.2 Dependencia y relaciones de activos tipo servicios. Se define la dependencia para los activos tipo servicios.

5.3.3.3.2.1 Servicio clientes [SERV_CLI]. Se define la dependencia del activo servicio cliente en la figura 12, basado en:

- El software con el que interactúa
- El hardware con el que interactúa
- Los activos de redes y comunicaciones de los que depende.

Figura 12. Dependencia activo [SERV_CLI]



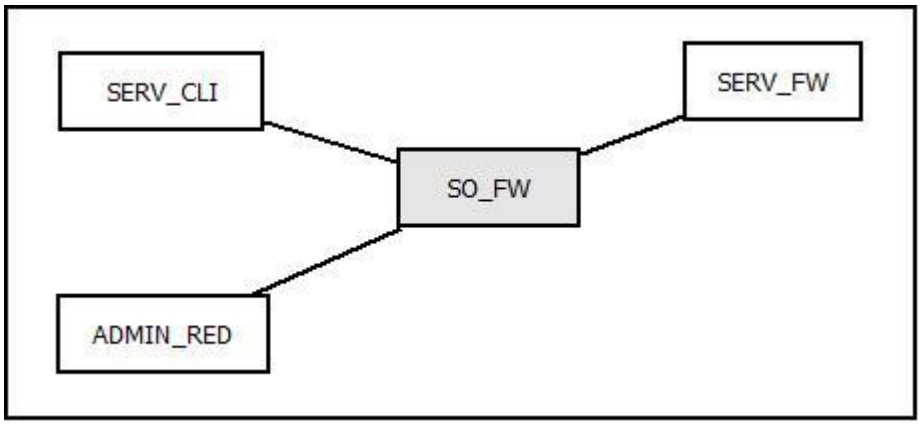
Fuente: Elaboración Propia.

5.3.3.3.3 Dependencia y relaciones de activos tipo aplicaciones. Se define la dependencia para los activos tipo aplicaciones (software).

5.3.3.3.3.1 Sistema operativo servidor Proxy y Firewall [SO_FW]. Se define la dependencia del activo sistema operativo servidor proxy y firewall en la figura 13, basado en:

- El hardware con el que interactúa.
- Los activos de servicios que dependen de dicho activo.
- La persona que lo emplea.

Figura 13. Dependencia activo [SO_FW]



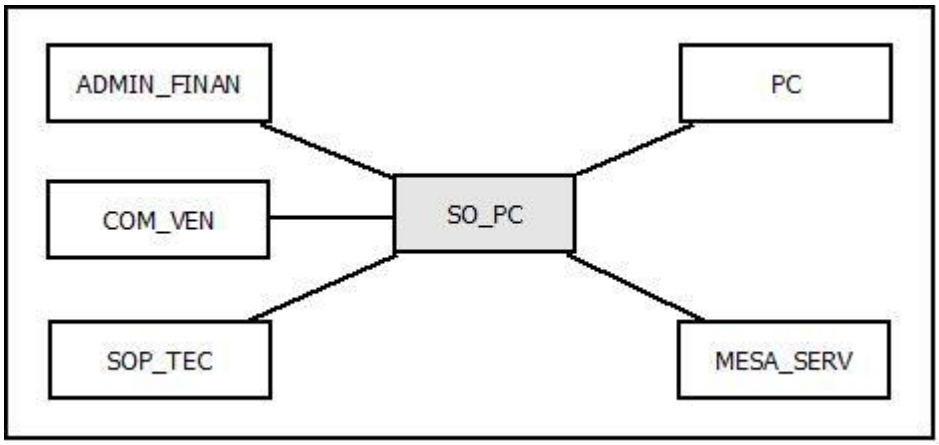
Fuente: Elaboración Propia.

5.3.3.3.3.2 Sistema operativo PC [SO_PC]. Se define la dependencia del activo sistema operativo PC en la figura 14, basado en:

- El hardware con el que interactúa.

- Las personas que lo emplean.

Figura 14. Dependencia activo [SO_PC]

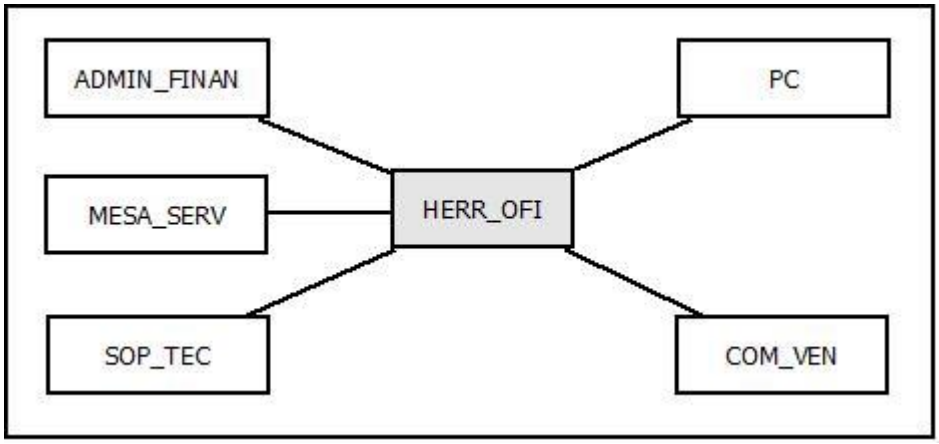


Fuente: Elaboración Propia.

5.3.3.3.3.3 Herramienta ofimática [HERR_OFI]. Se define la dependencia del activo herramienta ofimática en la figura 15, basado en:

- El hardware con el que interactúa.
- Las personas que lo emplean.

Figura 15. Dependencia activo [HERR_OFI]

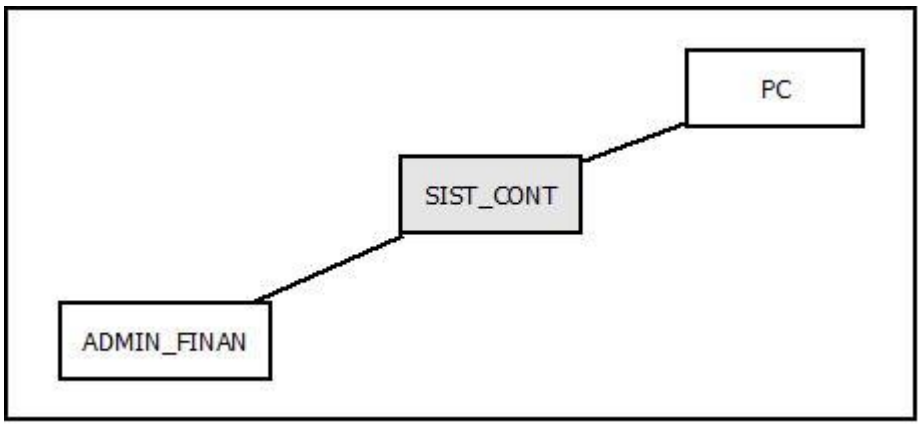


Fuente: Elaboración Propia.

5.3.3.3.3.4 Sistema contable [SIST_CONT]. Se define la dependencia del activo sistema contable en la figura 16, basado en:

- El hardware con el que interactúa.
- La persona que lo emplea.

Figura 16. Dependencia activo [SIST_CONT]



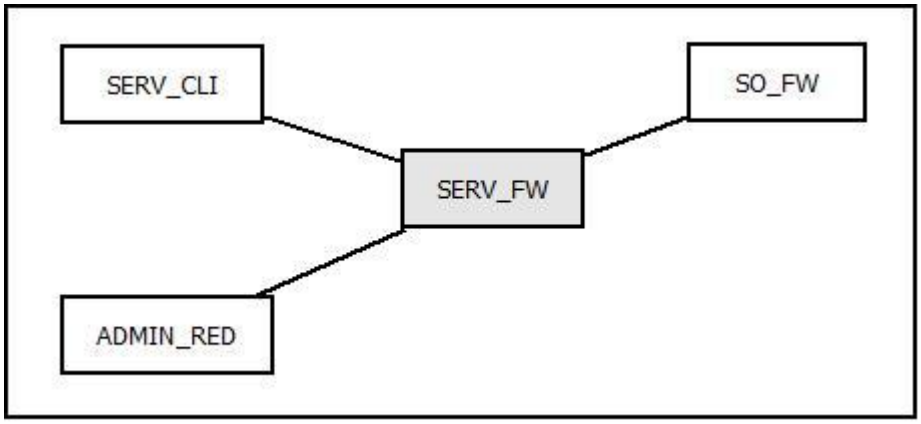
Fuente: Elaboración Propia.

5.3.3.3.4 Dependencia y relaciones de activos tipo aplicaciones. Se define la dependencia para los activos tipo equipos informáticos (hardware).

5.3.3.3.4.1 Servidor proxy firewall [SERV_FW]. Se define la dependencia del activo servidor proxy firewall en la figura 17, basado en:

- El software con el que interactúa.
- El activo de servicio con el que se relaciona.
- La persona que lo emplea

Figura 17. Dependencia activo [SERV_FW]

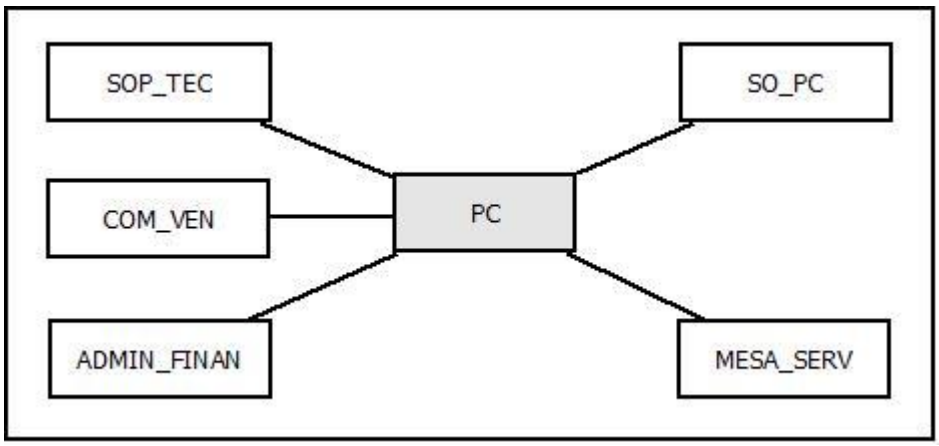


Fuente: Elaboración Propia.

5.3.3.3.4.2 Computadora de escritorio [PC]. Se define la dependencia del activo computadora de escritorio en la figura 18, basado en:

- El software con el que interactúa.
- Las personas que lo emplean.

Figura 18. Dependencia activo [PC]

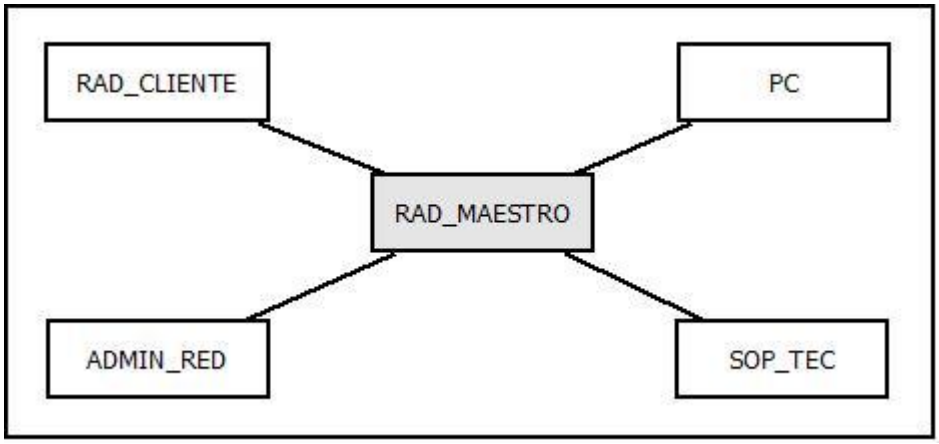


Fuente: Elaboración Propia.

5.3.3.3.4.3 Radio maestro [RAD_MAESTRO]. Se define la dependencia del activo radio maestro en la figura 19, basado en:

- El activo de equipos informáticos con el que se relaciona.
- El hardware con el que interactúa.
- Las personas que lo emplean.

Figura 19. Dependencia activo [RAD_MAESTRO]

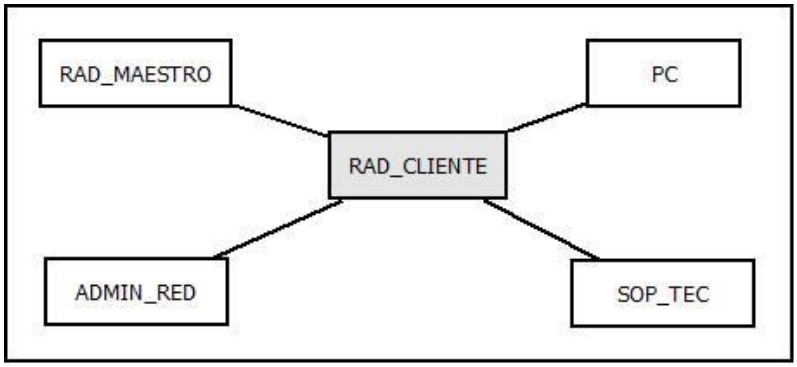


Fuente: Elaboración Propia.

5.3.3.3.4.4 Radio cliente [RAD_CLIENTE]. Se define la dependencia del activo radio cliente en la figura 20, basado en:

- El activo de equipos informáticos con el que se relaciona.
- El hardware con el que interactúa.
- Las personas que lo emplean.

Figura 20. Dependencia activo [RAD_CLIENTE]



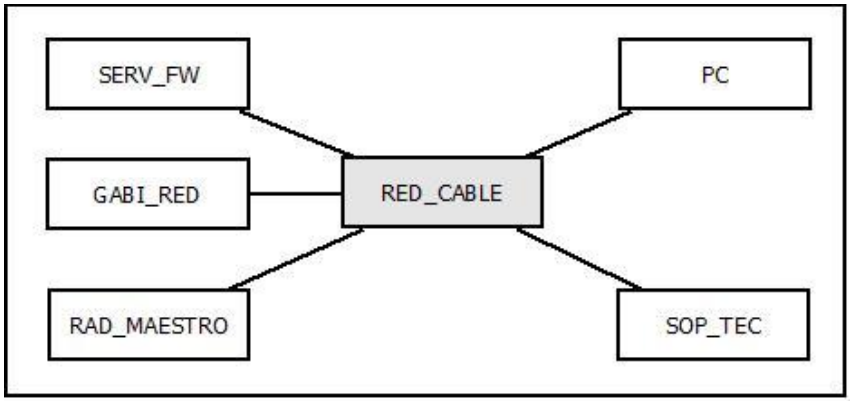
Fuente: Elaboración Propia.

5.3.3.3.5 Dependencia y relaciones de activos tipo equipos auxiliares. Se define la dependencia para los activos tipo equipos auxiliares.

5.3.3.3.5.1 Red cableada [RED_CABLE]. Se define la dependencia del activo red cableada en la figura 21, basado en:

- El hardware con el que interactúa.
- El activo con el que se relaciona.
- El personal que le da soporte.

Figura 21. Dependencia activo [RED_CABLE]

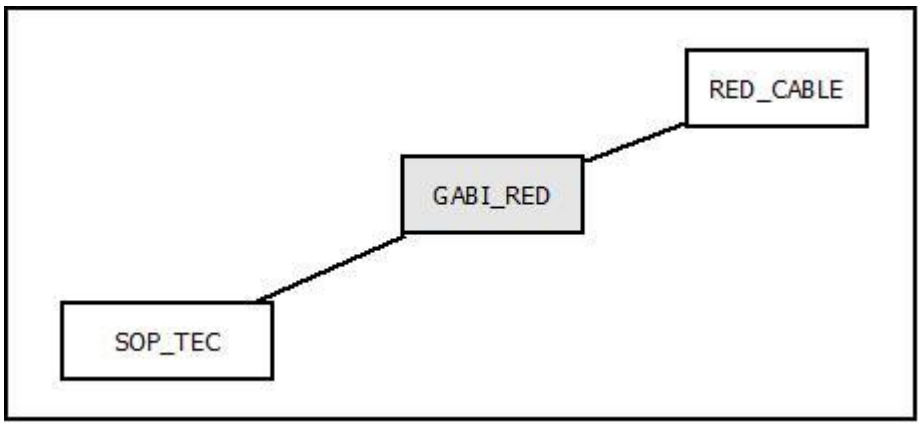


Fuente: Elaboración Propia.

5.3.3.3.5.2 Gabinete red [GABI_RED]. Se define la dependencia del activo gabinete red en la figura 22, basado en:

- El activo con el que se relaciona.
- El personal que le da soporte.

Figura 22. Dependencia activo [GABI_RED]



Fuente: Elaboración Propia.

5.3.3.4 Valoración de activos. De acuerdo a la metodología Magerit y a su primera fase y perteneciente al proceso de análisis y gestión del riesgo se deben tener en cuenta las dimensiones de valoración y los criterios de valoración en la organización de acuerdo a las tablas 25 y 26.

Cuadro 25. Dimensiones de valoración Magerit

Dimensiones de valoración
[D] Disponibilidad
[I] Integridad de los datos
[C] Confidencialidad de los datos
[AU] Autenticidad
[T] Trazabilidad
Fuente: Elaboración propia

Cuadro 26. Criterio de valoración Magerit

Valor			Daño a la organización
10	Muy alto	MA	Muy grave
7 -9	Alto	A	Grave
4 -6	Medio	MA	Importante
1 -3	Bajo	B	Menor
0	Despreciable	D	Irrelevante
Fuente: Elaboración propia			

A continuación en la tabla 27 se combinan las dimensiones y los criterios de valoración para los activos del caso de estudio de acuerdo a Magerit.

Cuadro 27. Valoración de activos Magerit

Tipo	Activo	Dimensiones de Seguridad				
		D	I	C	AU	T
[D] Datos e Información	1. [BD_CLIENTES] Base de datos clientes	8	10	10	8	8
[S] Servicios	2. [SERV_CLI] Servicio Internet Clientes	10	8	5	8	8
[SW] Aplicaciones	3. [SO_FW] Sistema operativo Servidor Proxy Firewall	10	8	8	8	7
	4. [SO_PC] Sistema operativo PC	7	7	7	7	7
	5. [HERR_OFI] Herramientas ofimática	7	7	7	7	7
	6. [SIST_CONT] Sistema contable y facturación	8	8	8	8	8
[HW] Equipos Informáticos	7. [SERV_FW] Servidor Proxy Firewall	10	9	8	9	10
	8. [PC] Computadora tipo escritorio	7	7	6	7	6
	9. [RAD_MAESTRO] Radio maestro	10	8	8	8	4
	10. [RAD_CLIENTE] Radio cliente	10	8	8	8	4
[COM]Redes de comunicaciones	11. [FIB_OP_PROV1] Canal fibra óptica Proveedor principal	10	7	5	5	5
	12. [FIB_OP_PROV2] Canal fibra óptica Proveedor respaldo	10	7	5	5	5
[AUX] Equipos auxiliares	13. [RED_CABLE] Red cableada	10	7	6	6	5
	14. [GABI_RED] Gabinete de red	10	7	6	6	5
[L] INSTALACIONES	15. [OF_ADMIN] Oficina administrativa	10	N/A	N/A	N/A	N/A
	16. [DATA_CENTER] Centro de datos	10	N/A	N/A	N/A	N/A

[P] Personal	17. [PERSONAL] Todo el personal que labora en la empresa	10	7	7	6	8
Fuente: Elaboración propia						

5.3.4 Fase 2. En esta fase se establecen riesgos, vulnerabilidades y amenazas en los activos de información del caso de estudio de acuerdo a Magerit.

5.3.4.1 Clasificación de amenazas. De acuerdo a Magerit se procede a enunciar las amenazas que pueden afectar la organización. en la tabla 28 se puede apreciar la clasificación de amenazas.

Cuadro 28. Clasificación de amenazas Magerit

Clasificación de amenazas	
[N] Desastres naturales	**[I] De origen industrial**
[N.1] Fuego [N.2] Daños por agua [N.3] Desastres naturales	[I.1] Fuego [I.2] Daños por agua [I.3] Contaminación mecánica [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [I.8] Fallo de servicios de comunicaciones [I.9] Interrupción de otros servicios y suministros esenciales [I.10] Degradación de los soportes de almacenamiento de la información [I.11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	**[A] Ataques intencionados**
[E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.7] Deficiencias en la organización [E.8] Difusión de software dañino [E.9] Errores de [re-]encaminamiento [E.10] Errores de secuencia [E.14] Escapes de información [E.15] Alteración accidental de la información	[A.3] Manipulación de los registros de actividad (log) [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.6] Abuso de privilegios de acceso [A.7] Uso no previsto [A.8] Difusión de software dañino [A.9] [Re-]encaminamiento de mensajes [A.10] Alteración de secuencia [A.11] Acceso no autorizado

[E.18] Destrucción de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas (software) [E.21] Errores de mantenimiento / actualización de programas (software) [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos [E.25] Pérdida de equipos [E.28] Indisponibilidad del personal	[A.12] Análisis de tráfico [A.13] Repudio [A.14] Interceptación de información (escucha) [A.15] Modificación deliberada de la información [A.18] Destrucción de información [A.19] Divulgación de información [A.22] Manipulación de programas [A.23] Manipulación de los equipos [A.24] Denegación de servicio [A.25] Robo [A.26] Ataque destructivo [A.27] Ocupación enemiga [A.28] Indisponibilidad del personal [A.29] Extorsión [A.30] Ingeniería social (picaresca)
Fuente: Elaboración propia	

5.3.4.2 Identificación de amenazas. De acuerdo a Magerit se procede a asociar las amenazas a los activos de información del caso de estudio. A continuación en la tabla 29 se puede observar dicha asociación.

Cuadro 29. Identificación de amenazas Magerit

Tipo	Activo	Amenaza
[D] Datos e Información	1. [BD_CLIENTES] Base de datos clientes	[E.4] Errores de configuración [E.15] Alteración accidental de la información [A.19] Divulgación de información
[S] Servicios	3. [SERV_CLI] Servicio Internet Clientes	[E.2] Errores del administrador [E.9] Errores de [re-]encaminamiento [E.24] Caída del sistema por agotamiento de recursos
[SW] Aplicaciones	4. [SO_FW] Sistema operativo Servidor Proxy Firewall	[I.5] Avería de origen físico o lógico [E.2] Errores del administrador [E.21] Errores de mantenimiento / actualización de programas (software) [A.11] Acceso no autorizado

[SW] Aplicaciones	5. [SO_PC] Sistema operativo PC	[I.5] Avería de origen físico o lógico [E.21] Errores de mantenimiento / actualización de programas (software)
[SW] Aplicaciones	6. [HERR_OFI] Herramientas ofimática	[I.5] Avería de origen físico o lógico [E.21] Errores de mantenimiento / actualización de programas (software)
[SW] Aplicaciones	7. [SIST_CONT] Sistema contable y facturación	[I.5] Avería de origen físico o lógico [E.2] Errores del administrador [E.21] Errores de mantenimiento / actualización de programas (software)
[HW] Equipos Informáticos	8. [SERV_FW] Servidor Proxy Firewall	[N.3] Desastres naturales [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware) [E.24] Caída del sistema por agotamiento de recursos
[HW] Equipos Informáticos	9. [PC] Computadora tipo escritorio	[I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.7] Condiciones inadecuadas de temperatura o humedad [E.23] Errores de mantenimiento / actualización de equipos (hardware)

[HW] Equipos Informáticos	10. [RAD_MAESTRO] Radio maestro	[N.3] Desastres naturales [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.2] Errores del administrador [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo
[HW] Equipos Informáticos	11. [RAD_CLIENTE] Radio cliente	[N.3] Desastres naturales [I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [E.2] Errores del administrador [E.23] Errores de mantenimiento / actualización de equipos (hardware) [A.25] Robo
[COM]Redes de comunicaciones	12. [FIB_OP_PROV1] Canal fibra óptica Proveedor principal	[I.8] Fallo de servicios de comunicaciones [E.24] Caída del sistema por agotamiento de recursos
[COM]Redes de comunicaciones	13. [FIB_OP_PROV2] Canal fibra óptica Proveedor respaldo	[I.8] Fallo de servicios de comunicaciones [E.24] Caída del sistema por agotamiento de recursos
[AUX] Equipos auxiliares	14. [RED_CABLE] Red cableada	[N.3] Desastres naturales [I.9] Interrupción de otros servicios y suministros esenciales [I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [I.7] Condiciones inadecuadas de temperatura o humedad

[AUX] Equipos auxiliares	15. [GABI_RED] Gabinete de red	[N.3] Desastres naturales [I.9] Interrupción de otros servicios y suministros esenciales [I.6] Corte del suministro eléctrico [E.23] Errores de mantenimiento / actualización de equipos (hardware) [I.7] Condiciones inadecuadas de temperatura o humedad
[L] INSTALACIONES	16. [OF_ADMIN] Oficina administrativa	[N.3] Desastres naturales
[L] INSTALACIONES	17. [DATA_CENTER] Centro de datos	[N.3] Desastres naturales
[P] Personal	18. [PERSONAL] Todo el personal que labora en la empresa	[E.28] Indisponibilidad del personal [A.30] Ingeniería social (picaresca)
Fuente: Elaboración propia		

5.3.4.3 Matriz de riesgos. De acuerdo a Magerit se procede a asociar las amenazas, vulnerabilidades y riesgos de los activos de información del caso de estudio. A continuación en la tabla 30 se puede apreciar dicha asociación.

Cuadro 30. Matriz de riesgos Magerit

Tipo de activo	Activo	Descripción	VULNERABILIDAD	AMENAZAS	RIESGO
[D] Datos e Información	[D] [BD_CLIENTES] Base de datos clientes	Base de datos clientes en MySQL	Falta de planes de copias de seguridad y configuración segura	[E.4] Errores de configuración	Divulgación de información
			Falta de planes de copias de seguridad	[E.15] Alteración accidental de la información	Adulteración de los registros
			Falta de seguridad en la base de datos	[A.19] Fugas de información	Divulgación de información
[S] Servicios	[S] [SERV_CLI] Servicio Internet Clientes	Servicio principal de la empresa, prestación de servicio de Internet a clientes estatales, empresariales y residenciales.	Falta de documentación en la configuración del servicio de los clientes	[E.4] Errores de configuración	Caída del servicio
			Falta de documentación en las rutas de los clientes	[E.9] Errores de [re-]encaminamiento	Caída del servicio
			Falta de recursos de hardware o software para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes

[SW] Aplicaciones	[SW] [SO_FW] Sistema operativo Servidor Proxy Firewall	Ubuntu Server 20.04 LTS 64 Bits corriendo aplicaciones de Proxy (ACL y filtro de contenido) y Firewall	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico
			Falta de planes de copias de seguridad	[E.2] Errores del administrador	Caída del servicio
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios
			Falta de seguimiento a logs de seguridad	[A.11] Acceso no autorizado	Información de la topología de red y clientes comprometida
	[SO_PC] Sistema operativo PC	Ubuntu Desktop 20.04.2.0 LTS 64 Bits	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios
	[SW] [HERR_OFI] Herramientas ofimática	LibreOffice 7.1.4 64 Bits	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios

	[SIST_CONT] Sistema contable y facturación	Ubuntu Desktop 20.04.2.0 LTS 64 Bits corriendo MySQL Community Server 8.0.25	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico
			Falta de planes de copias de seguridad	[E.2] Errores del administrador	Caída del sistema
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios
[HW] Equipos Informáticos	[HW] [SERV_FW] Servidor Proxy Firewall	Servidor HPE ProLiant DL360 Intel Xeon Platinum 8160H 8th Gen 3.7 Ghz 256 Gb de RAM DDR4 4 SATA/ 2 SSD 20 TB SO Ubuntu Server 20.04 LTS 64 Bits Pantalla 24 pulgadas LCD	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes
			Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes

			Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes
	[HW] [PC] Computadora tipo escritorio	Computador Tipo Clon con Procesador Intel i3 8va Generación 2.3 Ghz 8 Gb de RAM DDR4 y SSD 500 Mb. Pantalla 21 pulgadas LCD	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total de labores administrativas
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total de labores administrativas
	[HW] [RAD_MAESTRO] Radio Maestro	Ubiquiti LTU Rocket BaseStation 5.8 Ghz Antena Sectorial tipo panel	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes
			Falta de revisión del espectro electromagnético para verificar interferencias	[I.4] Contaminación electromagnética	Afectación del equipo microondas causando un bajo desempeño del servicio al cliente
			Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Afectación parcial o total del servicio prestado a los clientes

			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes
			Falta de documentación en la configuración de la red microondas	[E.2] Errores del administrador	Pérdida de gestión del elemento de red y afectación total del servicio prestado a los clientes
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes
			Falta de sistema de vigilancia en componentes red microondas y falta de stock de repuestos	[A.25] Robo	Afectación total del servicio prestado a los clientes
	[HW] [RAD_CLIENTE] Radio cliente	Ubiquiti LTU LR Subscriber Antena sectorial tipo grilla	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes
			Falta de revisión del espectro electromagnético para verificar interferencias	[I.4] Contaminación electromagnética	Afectación del equipo microondas causando un bajo desempeño del servicio al cliente
			Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Afectación parcial o total del servicio prestado a los clientes

			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes
			Falta de documentación en la configuración de la red microondas	[E.2] Errores del administrador	Pérdida de gestión del elemento de red y afectación total del servicio prestado a los clientes
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes
			Falta de sistema de vigilancia en componentes red microondas y falta de stock de repuestos	[A.25] Robo	Afectación total del servicio prestado a los clientes
[COM]Redes de comunicaciones	[COM] [FIB_OP_PROV1] Canal fibra óptica Proveedor principal	Canal Fibra óptica Movistar 1 Gb	Falta de planes de contingencia	[I.8] Fallo de servicios de comunicaciones	Afectación parcial o total del servicio prestado a los clientes
			Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes
	[COM][FIB_OP_PROV2] Canal fibra óptica Proveedor respaldo	Canal Fibra óptica Media Commerce 1 Gb	Falta de planes de contingencia	[I.8] Fallo de servicios de comunicaciones	Afectación parcial o total del servicio prestado a los clientes

			Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes
[AUX] Equipos auxiliares	[AUX] [RED_CABLE] Red cableada	Red cableada interconectando los elementos de red LAN y red WAN	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes
			Falta de mantenimiento y stock de repuestos	[I.9] Interrupción de otros servicios y suministros esenciales	Afectación parcial o total del servicio prestado a los clientes y a la red LAN
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes
			Falta de planes de mantenimiento de cableado	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos
	[AUX][GABI_RED] Gabinete de red	Switch 48 puertos, Patch Panel, UPS.	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes

			Falta de mantenimiento y stock de repuestos	[I.9] Interrupción de otros servicios y suministros esenciales	Afectación parcial o total del servicio prestado a los clientes y a la red LAN
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes
			Falta de planes de mantenimiento del gabinete de red	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos
[L] INSTALACIONES	[L] [OF_ADMIN] Oficina administrativa	Sede administrativa, Mesa de ayuda, administradora financiera y personal de ventas.	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes
	[L] [DATA_CENTER] Centro de datos	Servidor Proxy y Firewall, Administrador de red y equipos proveedores de Internet principal y respaldo.	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes
[P] Personal	[P] [PERSONAL]	Todo el personal que labora en la empresa	Falta de compromiso frente a las funciones	[E.28] Indisponibilidad del personal	Afectación parcial o total del soporte prestado a los clientes

			Falta de capacitaciones de seguridad de la información	[A.30] Ingeniería social (picaresca)	Robo de información por parte de terceros
Fuente: Elaboración propia					

5.3.4.4 Evaluación de riesgos. De acuerdo a Magerit se procede a la evaluación del riesgo después de haber realizado la asociación entre vulnerabilidades, amenazas y riesgos. Para esto se emplean a continuación la tabla 31 impacto del riesgo y 32 probabilidad en la ocurrencia del riesgo,

Cuadro 31. Impacto del riesgo Magerit

Impacto del riesgo		
Nomenclatura	**Categoría**	**Valoración**
MA	Muy alto	5
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy bajo	1
Fuente: Elaboración propia		

Cuadro 32. Probabilidad del riesgo Magerit

Probabilidad del riesgo		
Nomenclatura	**Probabilidad**	**Valoración**
MA	Casi seguro	5
A	Muy alta	4
M	Posible	3
B	Poco probable	2
MB	muy raro	1
Fuente: Elaboración propia		

Para realizar el cálculo del riesgo se emplea la siguiente fórmula, aplicada en la tabla 33:

Riesgo = Probabilidad * Impacto

Cuadro 33. Cálculo del riesgo Magerit

	Cálculo del riesgo					
Impacto	**MA**	5	10	15	20	25
	A	4	8	12	16	20
	M	3	6	9	12	15
	B	2	4	6	8	10
	MB	1	2	3	4	5
	Riesgo	**MB**	**B**	**M**	**A**	**MA**
		Probabilidad				
Fuente: Elaboración propia						

Finalmente se debe emplear la categorización del riesgo, tal como se aprecia en la tabla 34.

Cuadro 34. Categorización del riesgo Magerit

Valoración del riesgo		
Nomenclatura	Categorización	Valoración
MA	Crítico	21 a 25
A	Importante	16 a 20
M	Apreciable	10 a 15
B	Bajo	5 a 9
MB	Despreciable	1 a 4
Fuente: Elaboración propia		

Empleando las tablas 31, 32, 33 y 34 se procede a calcular la valoración del riesgo respecto a la probabilidad de ocurrencia y el impacto causado en el caso de estudio. Esto se observa en la tabla 35.

Cuadro 35. Valoración del riesgo Magerit

				Valoración del riesgo			
Activo	**VULNERABILIDAD**	**AMENAZAS**	**RIESGO**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**
[D] [BD_CLIENTES] Base de datos clientes	Falta de planes de copias de seguridad y configuración segura	[E.4] Errores de configuración	Divulgación de información	3	4	12	M
	Falta de planes de copias de seguridad	[E.15] Alteración accidental de la información	Adulteración de los registros	2	3	6	B
	Falta de seguridad en la base de datos	[A.19] Fugas de información	Divulgación de información	3	4	12	M

[S] [SERV_CLI] Servicio Internet Clientes	Falta de documentación en la configuración del servicio de los clientes	[E.4] Errores de configuración	Caída del servicio	4	5	20	A
	Falta de documentación en las rutas de los clientes	[E.9] Errores de [re-]encaminamiento	Caída del servicio	5	5	25	MA
	Falta de recursos de hardware o software para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M
[SW] [SO_FW] Sistema operativo Servidor Proxy Firewall	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	5	10	M
	Falta de planes de copias de seguridad	[E.2] Errores del administrador	Caída del servicio	4	5	20	A
	Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	3	5	15	M
	Falta de seguimiento a logs de seguridad	[A.11] Acceso no autorizado	Información de la topología de red y clientes comprometida	2	4	8	B

[SW] [SO_PC] Sistema operativo PC	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	3	3	9	B
	Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	3	3	9	B
[SW] [HERR_OFI] Herramientas ofimática	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	2	4	MB
	Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	2	2	4	MB
[SW] [SIST_CONT] Sistema contable y facturación	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	4	8	B
	Falta de planes de copias de seguridad	[E.2] Errores del administrador	Caída del sistema	2	4	8	B
	Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	2	4	8	B

[HW] [SERV_FW] Servidor Proxy Firewall	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B
	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	5	10	M
	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA
	Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	3	4	12	M
	Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M
	Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	4	5	20	A

[HW] [PC] Computadora tipo escritorio	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	2	4	MB
	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total de labores administrativas	5	2	10	M
	Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	1	2	2	MB
	Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total de labores administrativas	1	2	2	MB
[HW] [RAD_MAESTRO] Radio Maestro	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B
	Falta de revisión del espectro electromagnético para verificar interferencias	[I.4] Contaminación electromagnética	Afectación del equipo microondas causando un bajo desempeño del servicio al cliente	2	5	10	M
	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Afectación parcial o total del servicio prestado a	2	5	10	M

			los clientes				
	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA
	Falta de documentación en la configuración de la red microondas	[E.2] Errores del administrador	Pérdida de gestión del elemento de red y afectación total del servicio prestado a los clientes	2	5	10	M
	Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M
	Falta de sistema de vigilancia en componentes red microondas y falta de stock de repuestos	[A.25] Robo	Afectación total del servicio prestado a los clientes	1	5	5	B
[HW] [RAD_CLIENTE] Radio cliente	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B

	Falta de revisión del espectro electromagnético para verificar interferencias	[I.4] Contaminación electromagnética	Afectación del equipo microondas causando un bajo desempeño del servicio al cliente	2	5	10	M
	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M
	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA
	Falta de documentación en la configuración de la red microondas	[E.2] Errores del administrador	Pérdida de gestión del elemento de red y afectación total del servicio prestado a los clientes	2	5	10	M
	Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M
	Falta de sistema de vigilancia en componentes red microondas y falta de stock de repuestos	[A.25] Robo	Afectación total del servicio prestado a los clientes	1	5	5	B

[COM] [FIB_OP_PROV 1] Canal fibra óptica Proveedor principal	Falta de planes de contingencia	[I.8] Fallo de servicios de comunicaciones	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M
	Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M
[COM][FIB_OP_ PROV2] Canal fibra óptica Proveedor respaldo	Falta de planes de contingencia	[I.8] Fallo de servicios de comunicaciones	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M
	Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M
[AUX] [RED_CABLE] Red cableada	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B
	Falta de mantenimiento y stock de repuestos	[I.9] Interrupción de otros servicios y suministros esenciales	Afectación parcial o total del servicio prestado a los clientes y a la red LAN	2	5	10	M
	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a	5	5	25	MA

			los clientes				
	Falta de planes de mantenimiento de cableado	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M
	Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	2	5	10	M
[AUX][GABI_RED] Gabinete de red	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B
	Falta de mantenimiento y stock de repuestos	[I.9] Interrupción de otros servicios y suministros esenciales	Afectación parcial o total del servicio prestado a los clientes y a la red LAN	2	5	10	M
	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA
	Falta de planes de mantenimiento del gabinete de red	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M

	Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	2	5	10	M
[L] [OF_ADMIN] Oficina administrativa	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B
[L] [DATA_CENTER] Centro de datos	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B
[P] [PERSONAL]	Falta de compromiso frente a las funciones	[E.28] Indisponibilidad del personal	Afectación parcial o total del soporte prestado a los clientes	2	5	10	M
	Falta de capacitaciones de seguridad de la información	[A.30] Ingeniería social (picaresca)	Robo de información por parte de terceros	2	4	8	B
Fuente: Elaboración propia							

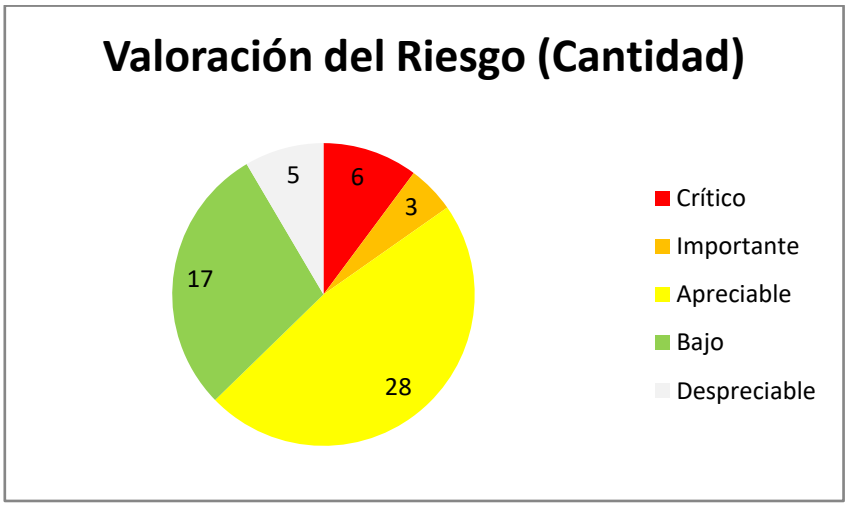
5.3.4.5 Análisis de resultados matriz de riesgos. De acuerdo a Magerit se procede a realizar el análisis de resultados de los riesgos: críticos, importantes y apreciables.

De acuerdo al caso de estudio, se encontraron para los activos de información 59 riesgos clasificados de la siguiente manera, de acuerdo a las tablas 36, 37 y las figuras 23 y 24.

Cuadro 36. Agrupación de riesgos según su valoración (Cantidad)

Valoración Riesgos	Cantidad
Crítico	6
Importante	3
Apreciable	28
Bajo	17
Despreciable	5
Total	59
Fuente: Elaboración propia	

Figura 23. Gráfico circular valoración del riesgo (Cantidad)

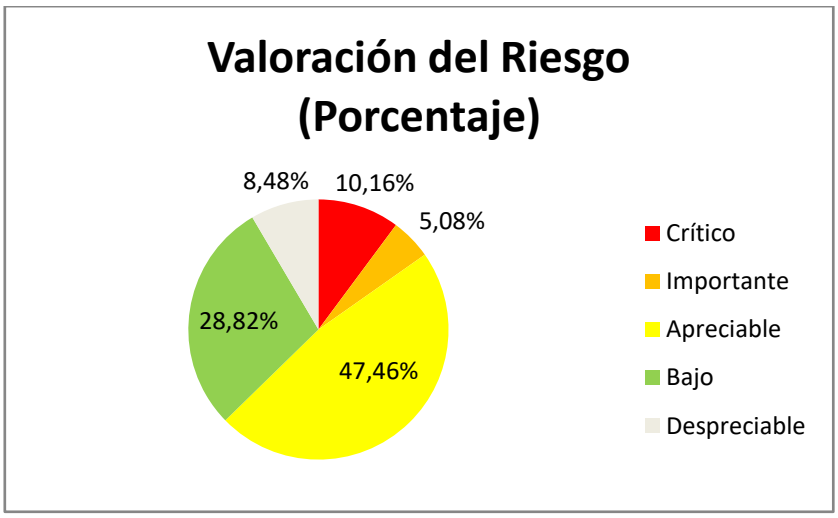


Fuente: Elaboración Propia.

Cuadro 37. Agrupación de riesgos según su valoración (Porcentaje)

Valoración Riesgos	Porcentaje
Crítico	10,16%
Importante	5,08%
Apreciable	47,46%
Bajo	28,82%
Despreciable	8,48%
Total	100,00%
Fuente: Elaboración propia	

Figura 24. Gráfico circular valoración del riesgo (Porcentaje)



Fuente: Elaboración Propia.

- Riesgos críticos.

De acuerdo a la tabla 36 y 37, se observa que los riesgos críticos corresponden a una cantidad de 6, equivalentes al 10,16% sobre activos tipo: servicios, hardware, y equipos auxiliares. Por lo tanto son los riesgos que más afectan la organización del caso de estudio, debido a que están directamente relacionados con el servicio de internet prestado a los clientes. Debido a su importancia son los riesgos que deben ser mitigados como prioridad dentro de la organización, puesto que están directamente ligados al núcleo del negocio de la empresa del caso de estudio. El correcto tratamiento de estos riesgos críticos repercutirá en el buen servicio prestado a los clientes de la empresa. Esto implica la protección de los activos implicados.

- Riesgos Importantes.

De acuerdo a las tablas 36 y 37, se observa que los riesgos importantes corresponden a una cantidad de 3, equivalentes al 5,08% sobre activos tipo: servicios, software y hardware. Son riesgos que también afectan indirectamente el servicio prestado a los clientes, pero debido a su cantidad y probabilidad un poco más baja que los riesgos críticos también deben ser atendidos al interior de la organización. El correcto tratamiento de estos riesgos importantes repercutirá en el buen servicio prestado a los clientes de la empresa. Esto implica la protección de los activos implicados.

- Riesgos apreciables.

De acuerdo a las tablas 36 y 37, se observa que los riesgos apreciables corresponden a una cantidad de 28, equivalentes al 47,46% sobre activos tipo: datos e información, servicios, software, hardware, redes de comunicaciones, equipos auxiliares y personal. Son riesgos que suman aproximadamente la mitad de la totalidad de riesgos en general, algunos de ellos afectan indirectamente el servicio prestado a los clientes y los demás afectan procesos internos, debido a su probabilidad un poco más baja que los riesgos importantes también deben ser atendidos al interior de la organización. El correcto tratamiento de estos riesgos apreciables repercutirá en el buen servicio prestado a los clientes de la empresa. Esto implica la protección de los activos implicados.

- Riesgos bajos.

De acuerdo a las tablas 36 y 37, se observa que los riesgos bajos corresponden a una cantidad de 17, equivalentes al 28,82% sobre activos tipo: datos e información, software, hardware, equipos auxiliares, instalaciones y personal. Son riesgos que suman aproximadamente la tercera parte de la totalidad de riesgos en general, algunos de ellos afectan indirectamente el servicio prestado a los clientes y los demás afectan procesos internos, debido a su probabilidad un poco más baja que los riesgos apreciables también deben ser atendidos al interior de la organización. El correcto tratamiento de estos riesgos bajos repercutirá en el buen servicio prestado a los clientes de la empresa. Esto implica la protección de los activos implicados.

- Riesgos despreciables.

De acuerdo a las tablas 36 y 37, se observa que los riesgos despreciables corresponden a una cantidad de 5, equivalentes al 8,48% sobre activos tipo: software y hardware. Como su nombre lo indica, no requieren tratamiento prioritario, debido a que su probabilidad e impacto es aún más baja que los riesgos bajos.

La empresa del caso de estudio al tener una infraestructura tecnológica con muchos componentes de red distribuidos en varias poblaciones del departamento de Boyacá, se ve influida por los riesgos: críticos, importantes, apreciables y bajos. Algunos afectan de forma directa e indirecta el servicio prestado a los clientes y los demás riesgos repercuten en los procesos internos de la organización. La protección de los activos implicados en la prestación del servicio es una prioridad de acuerdo a la característica de la Pymes del sector de las telecomunicaciones. Sin embargo los riesgos implicados en los procesos internos también deben ser atendidos, pero son una prioridad más baja en las necesidades de la organización.

5.3.5 Fase 3. En esta fase se propone un plan de tratamiento de los riesgos y vulnerabilidades encontrados en los activos de información del caso de estudio.

5.3.5.1 Plan de tratamiento de los riesgos. En esta última fase se diseña un plan de tratamiento de los riesgos y vulnerabilidades encontrados en los activos de información del caso propuesto: Pymes del sector telecomunicaciones. A cada activo, riesgo y vulnerabilidad detectada se propone una salvaguarda contemplada dentro del catálogo de objetos de Magerit. En la tabla 38 se documenta el plan de tratamiento de los riesgos.

Cuadro 38. Plan de tratamiento del riesgo Magerit

						Valoración del riesgo				Plan de tratamiento	
Tipo de activo	**Activo**	**Descripción**	**VULNERABILIDAD**	**AMENAZAS**	**RIESGO**	**Probabilidad**	**Impacto**	**Valoración**	**Nivel de Riesgo**	**Tratamiento**	**Salvaguarda**
[D] Datos e Información	[D] [BD_CLIENTES] Base de datos clientes	Base de datos clientes en MySQL	Falta de planes de copias de seguridad y configuración segura	[E.4] Errores de configuración	Divulgación de información	3	4	12	M	Mitigación del riesgo	D.A Copias de seguridad de los datos (back up)
			Falta de planes de copias de seguridad	[E.15] Alteración accidental de la información	Adulteración de los registros	2	3	6	B	Mitigación del riesgo	D.I Aseguramiento de la integridad

			Falta de seguridad en la base de datos	[A.19] Fugas de información	Divulgación de información	3	4	12	M	Mitigación del riesgo	D.C Cifrado de la información
[S] Servicios	[S] [SERV_CLI] Servicio Internet Clientes	Servicio principal de la empresa, prestación de servicio de Internet a clientes estatales, empresariales y residenciales.	Falta de documentación en la configuración del servicio de los clientes	[E.4] Errores de configuración	Caída del servicio	4	5	20	A	Mitigación del riesgo	S.A Aseguramiento de la disponibilidad
			Falta de documentación en las rutas de los clientes	[E.9] Errores de [re-]encaminamiento	Caída del servicio	5	5	25	MA	Mitigación del riesgo	S.A Aseguramiento de la disponibilidad
			Falta de recursos de hardware o software para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M	Mitigación del riesgo	S.A Aseguramiento de la disponibilidad
[SW] Aplicaciones	[SW] [SO_FW] Sistema operativo Servidor Proxy Firewall	Ubuntu Server 20.04 LTS 64 Bits corriendo	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	5	10	M	Mitigación del riesgo	SW.start Puesta en producción

		aplicaciones de Proxy (ACL y filtro de contenido) y Firewall	Falta de planes de copias de seguridad	[E.2] Errores del administrador	Caída del servicio	4	5	20	A	Mitigación del riesgo	SW.A Copias de seguridad (back up)
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	3	5	15	M	Mitigación del riesgo	SW.CM Cambios (actualizaciones y mantenimiento)
			Falta de seguimiento a logs de seguridad	[A.11] Acceso no autorizado	Información de la topología de red y clientes comprometida	2	4	8	B	Mitigación del riesgo	SW.CM Cambios (actualizaciones y mantenimiento)
	[SO_PC] Sistema operativo PC	Ubuntu Desktop 20.04.2.0 LTS 64 Bits	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	3	3	9	B	Mitigación del riesgo	SW.start Puesta en producción

			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	3	3	9	B	Mitigación del riesgo	SW.CM Cambios (actualizaciones y mantenimiento)
	[SW] [HERR_OFI] Herramientas ofimática	LibreOffice 7.1.4 64 Bits	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	2	4	MB	Aceptación del riesgo	SW.start Puesta en producción
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	2	2	4	MB	Aceptación del riesgo	SW.CM Cambios (actualizaciones y mantenimiento)
	[SIST_CONT] Sistema contable y facturación	Ubuntu Desktop 20.04.2.0 LTS 64 Bits corriendo MySQL	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	4	8	B	Mitigación del riesgo	SW.start Puesta en producción

		Community Server 8.0.25	Falta de planes de copias de seguridad	[E.2] Errores del administrador	Caída del sistema	2	4	8	B	Mitigación del riesgo	SW.A Copias de seguridad (back up)
			Falta de verificación de actualizaciones automáticas	[E.21] Errores de mantenimiento / actualización de programas (software)	Mal funcionamiento de aplicaciones o servicios	2	4	8	B	Mitigación del riesgo	SW.CM Cambios (actualizaciones y mantenimiento)
[HW] Equipos Informáticos	[HW] [SERV_FW] Servidor Proxy Firewall	Servidor HPE ProLiant DL360 Intel Xeon Platinum 8160H 8th Gen 3.7 Ghz 256 Gb de RAM DDR4 4 SATA/ 2	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	5	10	M	Mitigación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)

		SSD 20 TB SO Ubuntu Server 20.04 LTS 64 Bits Pantalla 24 pulgadas LCD	Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	3	4	12	M	Mitigación del riesgo	HW.op Operación
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M	Mitigación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)
			Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	4	5	20	A	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad

	[HW] [PC] Computadora tipo escritorio	Computador Tipo Clon con Procesador Intel i3 8va Generación 2.3 Ghz 8 Gb de RAM DDR4 y SSD 500 Mb. Pantalla 21 pulgadas LCD	Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Mal funcionamiento del sistema físico o lógico	2	2	4	MB	Aceptación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total de labores administrativas	5	2	10	M	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	1	2	2	MB	Aceptación del riesgo	HW.op Operación
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total de labores administrativas	1	2	2	MB	Aceptación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)

	[HW] [RAD_MAESTRO] Radio Maestro	Ubiquiti LTU Rocket BaseStation 5.8 Ghz Antena Sectorial tipo panel	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de revisión del espectro electromagnético para verificar interferencias	[I.4] Contaminación electromagnética	Afectación del equipo microondas causando un bajo desempeño del servicio al cliente	2	5	10	M	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad

			Falta de documentación en la configuración de la red microondas	[E.2] Errores del administrador	Pérdida de gestión del elemento de red y afectación total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)
			Falta de sistema de vigilancia en componentes red microondas y falta de stock de repuestos	[A.25] Robo	Afectación total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	HW.op Operación

	[HW] [RAD_CLIENTE] Radio cliente	Ubiquiti LTU LR Subscriber Antena sectorial tipo grilla	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de revisión del espectro electromagnético para verificar interferencias	[I.4] Contaminación electromagnética	Afectación del equipo microondas causando un bajo desempeño del servicio al cliente	2	5	10	M	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de mantenimiento preventivo y correctivo	[I.5] Avería de origen físico o lógico	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad

			Falta de documentación en la configuración de la red microondas	[E.2] Errores del administrador	Pérdida de gestión del elemento de red y afectación total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	HW.A Aseguramiento de la disponibilidad
			Falta de mantenimiento y stock de repuestos	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	HW.CM Cambios (actualizaciones y mantenimiento)
			Falta de sistema de vigilancia en componentes red microondas y falta de stock de repuestos	[A.25] Robo	Afectación total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	HW.op Operación

[COM] Redes de comunicaciones	[COM] [FIB_OP_PROV1] Canal fibra óptica Proveedor principal	Canal Fibra óptica Movistar 1 Gb	Falta de planes de contingencia	[I.8] Fallo de servicios de comunicaciones	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	COM.start Entrada en servicio
			Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M	Mitigación del riesgo	COM.A Aseguramiento de la disponibilidad
	[COM][FIB_OP_PROV2] Canal fibra óptica Proveedor respaldo	Canal Fibra óptica Media Commerce 1 Gb	Falta de planes de contingencia	[I.8] Fallo de servicios de comunicaciones	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	COM.start Entrada en servicio
			Falta de recursos de hardware o software o ancho de banda para asumir la carga requerida	[E.24] Caída del sistema por agotamiento de recursos	Afectación parcial o total del servicio prestado a los clientes	3	5	15	M	Mitigación del riesgo	COM.A Aseguramiento de la disponibilidad

[AUX] Equipos auxiliares	[AUX] [RED_CABLE] Red cableada	Red cableada interconectando los elementos de red LAN y red WAN	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	AUX.A Aseguramiento de la disponibilidad
			Falta de mantenimiento y stock de repuestos	[I.9] Interrupción de otros servicios y suministros esenciales	Afectación parcial o total del servicio prestado a los clientes y a la red LAN	2	5	10	M	Mitigación del riesgo	AUX.wires Protección del cableado
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA	Mitigación del riesgo	AUX.power Suministro eléctrico
			Falta de planes de mantenimiento de cableado	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	AUX.A Aseguramiento de la disponibilidad

			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	2	5	10	M	Mitigación del riesgo	AUX.AC Climatización
	[AUX][GABI_RED] Gabinete de red	Switch 48 puertos, Patch Panel, UPS.	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	AUX.A Aseguramiento de la disponibilidad
			Falta de mantenimiento y stock de repuestos	[I.9] Interrupción de otros servicios y suministros esenciales	Afectación parcial o total del servicio prestado a los clientes y a la red LAN	2	5	10	M	Mitigación del riesgo	AUX.wires Protección del cableado
			Falta de sistema de alimentación ininterrumpida	[I.6] Corte del suministro eléctrico	Afectación parcial o total del servicio prestado a los clientes	5	5	25	MA	Mitigación del riesgo	AUX.power Suministro eléctrico

			Falta de planes de mantenimiento del gabinete de red	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	Afectación parcial o total del servicio prestado a los clientes	2	5	10	M	Mitigación del riesgo	AUX.A Aseguramiento de la disponibilidad
			Falta de equipos de aire acondicionado	[I.7] Condiciones inadecuadas de temperatura o humedad	Falla por sobrecalentamiento o exceso de humedad en los equipos	2	5	10	M	Mitigación del riesgo	AUX.AC Climatización
[L] INSTALACIONES	[L] [OF_ADMIN] Oficina administrativa	Sede administrativa, Mesa de ayuda, administradora financiera y personal de ventas.	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a los clientes	1	5	5	B	Mitigación del riesgo	L.A Aseguramiento de la disponibilidad
	[L] [DATA_CENTER] Centro de datos	Servidor Proxy y Firewall, Administrador de	Falta de planes de continuidad del negocio	[N.3] Desastres naturales	Afectación parcial o total del servicio prestado a	1	5	5	B	Mitigación del riesgo	L.A Aseguramiento de la disponibil

		red y equipos proveedores de Internet principal y respaldo.			los clientes						idad
[P] Personal	[P] [PERSONAL]	Todo el personal que labora en la empresa	Falta de compromiso frente a las funciones	[E.28] Indisponibilidad del personal	Afectación parcial o total del soporte prestado a los clientes	2	5	10	M	Mitigación del riesgo	PS.A Aseguramiento de la disponibilidad
			Falta de capacitaciones de seguridad de la información	[A.30] Ingeniería social (picaresca)	Robo de información por parte de terceros	2	4	8	B	Mitigación del riesgo	PS.AT Formación y concienciación
Fuente: Elaboración Propia											

Cabe recordar que los elementos del catálogo de objetos no son obligatorios, pueden existir diferentes tipificaciones de activos, amenazas y por supuesto salvaguardas, entonces debe emplearse como punto de partida para la gestión de análisis de riesgos. Las salvaguardas sugeridas por Magerit son controles para aplicar dependiendo de la clase de activos que se está analizando. De su correcta implementación dependerá la protección de la disponibilidad, integridad y confiabilidad de los activos de información empleados para llevar a cabo las funciones internas así como de prestar el servicio de internet a los clientes de la Pyme del sector de las telecomunicaciones.

6. CONCLUSIONES

Con el desarrollo de esta monografía queda claro que antes de adentrarse en un tema técnico, debemos tener muy claros los conceptos que lo sustentan. Dichos conceptos y elementos relacionados con el análisis y gestión de riesgos no son pocos, es por eso que son fundamentales en la comprensión de las acciones propias a realizar en el desempeño de estas actividades. En la claridad de conceptos tales como: seguridad informática, riesgo, amenaza, vulnerabilidad, impacto, contingencia y continuidad del negocio reside el correcto desarrollo de una gestión de riesgos ágil a nivel de pymes del sector de telecomunicaciones, puesto que dicha gestión se requiere en el corto plazo para enfrentar de la mejor forma las amenazas a las que se ven sometidas las organizaciones.

En el libro I: Método, los conceptos que abarca la metodología MAGERIT en su versión 3, son sin lugar a dudas imprescindibles para poder entender y asimilar los fines del análisis y gestión de riesgos a nivel empresarial. Conceptos tales como gobierno, confianza y gestión son fundamentales para empezar a comprender los objetivos que persigue la metodología. Las dimensiones de la seguridad como: disponibilidad, integridad y confidencialidad son de suma importancia y su protección son la razón de ser de la metodología. El libro II: catálogo de objetos, es muy claro respecto a que no es una camisa de fuerza, sino una sugerencia de cuáles pueden ser los elementos a tener en cuenta, de acuerdo a cada escenario de la organización en estudio, seguramente pueden surgir nuevos elementos. El catálogo de elementos es por lo tanto muy dinámico debido a la evolución de las nuevas tecnologías. Finalmente el libro III: guía de técnicas, recoge la compilación de técnicas específicas y generales para la obtención de resultados de manera simple o compleja de acuerdo al tipo de organización.

La metodología Magerit es una alternativa viable para el análisis y gestión de riesgos en organizaciones tipo Pymes, debido a su método simple y a sus tres libros que sirven de guía en todo momento para la realización de las tareas con el objetivo de asegurar los activos de información luego de un análisis detallado de cada uno de ellos. Para este análisis se requiere un conocimiento detallado y profundo de los servicios ofrecidos por la empresa, sus procesos internos, los elementos que se puedan clasificar como activos basados en el catálogo de elementos y el personal responsable de los mismos. Con este conocimiento de punto de partida es relativamente sencillo realizar un análisis y gestión de riesgos en una pymes del sector de las telecomunicaciones, puesto que se reconoce como actividad principal y núcleo del negocio, la prestación del servicio de internet a sus clientes.

Basado en el caso de estudio se pudo apreciar luego de la implementación de las tres primeras fases de la metodología Magerit que existen riesgos críticos, importantes, apreciables e incluso bajos que están relacionados directamente o indirectamente con la prestación del servicio de Internet, por lo tanto se deben asegurar dichos activos de información con las salvaguardas sugeridas por Magerit para cada tipo de activo con el fin de garantizar la disponibilidad de dicho servicio, principalmente debido a que una empresa Pymes del sector de las telecomunicaciones posee una infraestructura de red distribuida en una región amplia. Y es por esta razón que principalmente los activos de información dentro de la categoría de Hardware se vean afectados por diversos riesgos que deben ser mitigados a través de las salvaguardas propuestas.

La implementación del plan de tratamiento incluye por supuesto a más áreas de la organización, y tiene que tener el visto bueno de la administración, porque implica generalmente gastos que no estaban previstos para asegurar la continuidad del negocio y la prestación del servicio a los clientes. La mayoría de los riesgos en el caso de estudio requieren un control para su mitigación debido a la implicación en el núcleo del negocio de la empresa y por lo general implican un alto costo, ya la decisión de la aplicación de los controles recae en el área administrativa. Muy pocos riesgos fueron aceptados, aunque incluso en ellos se pueden aplicar controles relativamente a bajo costo.

Como se explicó anteriormente la fase 4 no se tiene en cuenta en este documento, puesto que esa fase se encarga del cálculo del impacto del riesgo acumulado e incluye también el cálculo del impacto del riesgo residual, posterior a la implementación de las salvaguardas propuestas en el plan de tratamiento. Y tiene el objetivo de medir el estado real de los riesgos luego de la implementación de los controles propuestos para su respectiva mitigación.

7. RECOMENDACIONES

Desarrollar planes de continuidad del negocio para garantizar la prestación del servicio a los clientes de las pymes de telecomunicaciones, tratando de definir procedimientos en caso de afectaciones a la infraestructura técnica que soporta dicho servicio.

Implementar una política de seguridad informática, teniendo claro roles, funciones y responsabilidades dentro de la organización con el fin de la adopción de buenas prácticas que permitan un mayor control de la información y los activos de información que la sustentan, al igual que su infraestructura técnica.

Crear un plan de capacitación y concientización que involucre de forma dinámica a todos los empleados de la empresa de telecomunicaciones con el objetivo de que en el desarrollo de las actividades diarias siempre se tome la seguridad de la información como una prioridad para el beneficio de la propia organización, de sus empleados y clientes.

BIBLIOGRAFÍA

ABRIL, Ana, PULIDO, Jarol y BOHADA, John. Análisis de Riesgos en Seguridad de la Información. En: Revista Ciencia, Innovación y Tecnología (RCIYT). Tunja. 2013. Vol. 1, No. 1. p. 11.

ACUÑA, Tatiana y PEINADO, Yineth. Guía de Gestión de Riesgos Para el Departamento de Sistemas del Hotel Tarigua OCAÑA S.A.S, Basados en la Norma ISO/IEC 27001. 2019.p. 34.

ALEMÁN, Helena y RODRÍGUEZ, Claudia. Metodologías para el análisis de riesgos en los sgs, Publicaciones e Investigación 9. 2015. p. 3.

ALVAREZ, Claudia; BARBOSA, Julia y ZAMBRANO, Leonardo. Análisis de Riesgos Informaticos de la Dependencia División de Sistemas Adscrita a la Subdirección Académica de la UFPSO, Basada en la Norma ISO/IEC 27005:2011. 2017. p. 24.

BARRERA. Ricardo; SÁNCHEZ, Maritza y ROJAS, William. Modelo de gestión del riesgo en proyectos informáticos Mogripi, I+D REVISTA DE INVESTIGACIONES 8, n.o 2. 2016. p. 3.

BRAVO, María. Desarrollo de un Sistema de Gestión de Seguridad de la Información para bibliotecas basado en una metodología mejorada para análisis de riesgos compatible con la norma ISO/IEC 27001:2013. Quito: Escuela Politécnica Nacional, 2018. p. 21.

CABALLERO, Sergio y KUNA, Horacio. Análisis y gestión de riesgo en proyectos software. 2018.p. 2.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá D.C., 2012. No. 48.587. p. 1-5.

COLOMBIA. CONGRESO DE LA REPUBLICA. LEY 1273 (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá D.C., 2009. No. 47223. p. 1-2.

CORREA, Gabriel; RÍOS, Eliana y ACEVEDO, Julio. Evolución de la cultura de la gestión de riesgos en el entorno empresarial colombiano: revisión y diagnóstico. Journal of Engineering and Technology 6, n.o 1. 2017.p. 5.

CRESPO, Esteban y CORDERO, Geovanna. Estudio Comparativo entre las Metodologías CRAMM Y MAGERIT Para la Gestión de Riesgo de TI em Las MPYMES, 2016. p. 3.

CRESPO, Esteban y CORDERO, Geovanna. Estudio comparativo entre las metodologías CRAMM y Magerit para la gestión de riesgo de TI en las Mpymes. Cuenca: Universidad del Azuay. 2016. p. 8.

CRESPO, Esteban. Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Enfoque UTE 8. 2017.p. 3

CRESPO, Paúl. Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES. Cuenca: Universidad de Cuenca. 2016. p. 22.

DEL RÍO, Abel y CÁRDENAS, Beitmantt. Dinámica de sistemas: una forma de optimizar la gestión del riesgo. Magazine School of Business Administration. 2018. p. 5.

DÍAZ, Juan. Esquema Director de Seguridad para Empresas pymes del sector Construcción. Alicante: Universidad de Alicante, 2020. p. 4.

FERRUZOLA, Enrique. Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. Revista Científica y Tecnológica UPSE 6, n.o 1. 2019. p. 2.

GARCÉS, Oña. Gestión de riesgos informáticos utilizando NIST SP-800 e ISO/IEC 27005 en la empresa international forest products del Ecuador S.A. 2019. p. 7.

GARCÍA, Gonzálo y VIDAL, María. La informática y la seguridad. Un tema de importancia para el directivo, Revista de Información científica para la Dirección en Salud. INFODIR 0, n.o 22. 2016. p. 11.

HASPER, Joan, et al. Tendencias en la investigación sobre gestión del riesgo empresarial: un análisis bibliométrico. En: Revista Venezolana de Gerencia. Maracaibo, 2017. Vol. 22, No 79. p. 3.

HOLGUÍN, Fresia. Modelo de Madurez para el Análisis de Riesgos de los Activos de Información basado en las Metodologías MAGERIT, OCTAVE y MEHARI; con enfoque a Empresas Navieras. Samborondón: Universidad Espíritu Santo. 2018. p. 9.

HURTADO, Martha. Gestión de Riesgo Metodologías OCTAVE y MAGERIT. Bogotá: Universidad Piloto de Colombia. 2018. p. 3.

INOGUCHI, Antonio y MACHA, Erika. Gestión de la ciberseguridad y prevención de los ataques cibernéticos en las PYMES del Perú, 2016, Universidad San Ignacio de Loyola, 2017.p. 8.

JÁCOME, José; PUSDÁ, Marco y IMBAQUINGO, Daisy. Fundamentos de Auditoría Informática basada en riesgos. 2017. p. 59.

JÁCOME, José; PUSDÁ, Marco y IMBAQUINGO, Daisy. Fundamentos de Auditoría Informática basada en riesgos. 2017. p. 63.

JÁCOME, José; PUSDÁ, Marco y IMBAQUINGO, Daisy. Fundamentos de Auditoría Informática basada en riesgos. 2017. p. 65.

JIMÉNEZ, Giovanny. Análisis y Gestión de riesgos al Sistema de Información de la Empresa Textil Diseños y Dotaciones Osiris S.A.S Aplicando Metodología Magerit. Monografía para optar al título de Especialista en Seguridad Informática. Ibagué: Universidad Nacional Abierta y a Distancia. 2018. 86p.

MIHAILESCU, Vladimir. Risk Analysis and Risk Management Using MEHARI . 2012. p. 3.

MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 4.

MOROCHO, Rodrigo y CUEVA, Irma. Diseño de un Plan para el Tratamiento de riesgos Tecnológicos utilizando la metodología NIST SP 800-30. Machala: Universidad Técnica de Machala. 2015. p. 5.

NIEVES, Arlenys. Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001:2013. 2017. p. 11.

ORTEGÓN, Doncel; BARRETO, Pinto; LÉON, Perozo. Diagnóstico Para La Mitigación de Riesgos Informáticos de La Empresa LYD COLOMBIA S.A.S. 2019. p. 24

ORTEGÓN, William; PINTO, Mario y PEROZO, Miguel. Diagnóstico Para La Mitigación de Riesgos Informáticos de La Empresa LYD COLOMBIA S.A.S. 2019. p. 19.

PALACIOS, Jeysser Aurelio. Análisis de Vulnerabilidades de la Infraestructura Tecnológica en la Dependencia de Formación Profesional Integral del SENA Regional Guainía, para el Diseño de una Propuesta de Aseguramiento de la Información Basada en la Metodología Magerit. Proyecto aplicado para optar al título de Especialista en Seguridad Informática. Ibagué: Universidad Nacional Abierta y a Distancia. 2020. 141p.

PARADA, Diego J. Análisis de los Componentes de la Seguridad desde una Perspectiva Sistémica de la Dinámica de Sistemas. Información tecnológica 29, n.o 1. 2018. p. 3.

PAREDES, Adriana. Análisis de Riesgos de la Seguridad de la Información Utilizando la Metodología Magerit en la Institución Educativa Domingo Savio en la Ciudad de Florencia – Caquetá. Proyecto de Grado para optar el título de Especialista en Seguridad Informática. Florencia: Universidad Nacional Abierta y a Distancia. 2018. 113p.

PAZMIÑO, Fabián y ALDAZ, Nelson. Propuesta de un plan de contingencia para salvaguardar los activos de información en el Departamento de tecnología de información y comunicación de la Empresa Pública Municipal de residuos sólidos Rumiñahui-Aseo EPM empleando la metodología Magerit. Trabajo de grado para

obtener el título de: Ingeniero de Sistemas. Quito: Universidad Politécnica Salesiana. 2021. 150p.

QUINTERO, Juan. Las pymes en Colombia y las barreras para su desarrollo y perdurabilidad. Bogotá: Universidad Militar Nueva Granada, 2018. p. 5

QUIROZ, Santa y MILAGROS, Hilda. Implementación de gestión de riesgos de ti para obtener la certificación ISO 27001 en el Hospital Regional Lambayeque. Repositorio Institucional - USS. 2016. p. 7.

RODRÍGUEZ, Hugo. Importancia de Controlar todas las Amenazas Detectadas a través de magerit v.3 e iso/iec 27002 Según Análisis de ataques informáticos en latinoamérica. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Barranquilla: Universidad Nacional Abierta y a Distancia. 2019. 115p.

ROJAS, Hernán. Aplicación de la Metodología Magerit para el Análisis de Riesgos de los Sistemas de Control en la Estación Tenay del Oleoducto. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Neiva: Universidad Nacional Abierta y a Distancia. 2019. 97p.

SANTA MARÍA, Wilber. Plan para Reducir los Riesgos Operativos de Tecnologías de la Información Basada en Metodología Magerit en la Caja Piura de la Ciudad de Chiclayo. Tesis de grado para optar al título de Ingeniero de Sistemas. Chiclayo: Universidad de Lambeyeque. 2020. 110p.

SETIAWAN,Hermawan; PUTRA, Fandi y PRADANA Anggi. Design of information security risk management using ISO/IEC 27005 and NIST SP 800-30 revision 1: A case study at communication data applications of XYZ institute, en 2017 International Conference on Information Technology Systems and Innovation (ICITSI), 2017. p. 4.

TEJENA, Mayra. Análisis de riesgos en seguridad de la información, Polo del Conocimiento 3, n.o 4. 2018. p. 2.

TEJENA, Mayra. Análisis de riesgos en seguridad de la información, Polo del Conocimiento 3, n.o 4. 2018. p. 4.

VANEGAS, Jair Hernando. Guía de Auditoria Basada en el Análisis de Riesgos a un Centro de Datos Aplicando la Metodología Magerit 3. Trabajo de grado para obtener el

título de: Especialista en Auditoria de Sistemas de Información. Bogotá: Universidad Católica de Colombia. 2017. 168p.

VARÓN, Juan Carlos. Estudio de Análisis y Gestión de Riesgo al Sistema de Información de la Empresa Agesagro S.A.S. Utilizando la Metodología Magerit. Monografía para optar al título de Especialista en Seguridad Informática. Ibagué: Universidad Nacional Abierta y a Distancia. 2017. 91p.

VICENTE, E, MATEOS, A y JIMÉNEZ-MARTÍN, A. Risk Analysis in Information Systems: A Fuzzification of the MAGERIT Methodology, Knowledge-Based Systems 66. 2014. p. 1.

WAGIU, Elmor; SIREGAR, Raminson y MAULANY, Raymond. Information System Security Risk Management Analysis in Universitas Advent Indonesia Using Octave Allegro Method, Abstract Proceedings International Scholars Conference 7, No. 1. 2019. p. 1.

Fecha de Realización:	24/10/2021
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Gestión de sistemas
Título:	Análisis de los conceptos, elementos y técnicas de la gestión de riesgo orientado a las pymes del sector de las telecomunicaciones basado en Magerit v3.
Autor(es):	Diego Leonardo Andrade Talero
Palabras Claves:	Análisis, Gestión, Metodología, Riesgo y Vulnerabilidad.
Descripción:	Mediante el desarrollo de esta monografía se busca un acercamiento a la metodología de análisis y gestión de riesgos Magerit versión 3 y a los conceptos que la rodean, con el fin de proponer una guía de implementación de dicha metodología basada en un caso de estudio de una pymes del sector de las telecomunicaciones, haciendo uso de la documentación oficial Magerit y una recopilación de diferentes fuentes documentales.

Fuentes bibliográficas destacadas:

MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro I: Método. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro II: Catálogo de Elementos. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 6.

MODERNIZACIÓN ADMINISTRATIVA, DIRECCIÓN GENERAL DE. Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas. Madrid: Ministerio de Hacienda y Administraciones Públicas. 2012. p. 4.

QUINTERO, Juan. Las pymes en Colombia y las barreras para su desarrollo y perdurabilidad. Bogotá: Universidad Militar Nueva Granada, 2018. p. 5

CRESPO, Paúl. Metodología de seguridad de la información para la gestión del riesgo informático aplicable a MPYMES. Cuenca: Universidad de Cuenca. 2016. p. 22.

CRESPO, Esteban. Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs. Enfoque UTE 8. 2017.p. 3

ORTEGÓN, Doncel; BARRETO, Pinto; LÉON, Perozo. Diagnóstico Para La Mitigación de Riesgos Informáticos de La Empresa LYD COLOMBIA S.A.S. 2019. p. 24.

PALACIOS, Jeysser Aurelio. Análisis de Vulnerabilidades de la Infraestructura Tecnológica en la Dependencia de Formación Profesional Integral del SENA Regional Guainía, para el Diseño de una Propuesta de Aseguramiento de la Información Basada en la Metodología Magerit. Proyecto aplicado para optar al título de Especialista en Seguridad Informática. Ibagué: Universidad Nacional Abierta y a Distancia. 2020. 141p.

PAREDES, Adriana. Análisis de Riesgos de la Seguridad de la Información Utilizando la Metodología Magerit en la Institución Educativa Domingo Savio en la Ciudad de Florencia – Caquetá. Proyecto de Grado para optar el título de Especialista en Seguridad Informática. Florencia: Universidad Nacional Abierta y a Distancia. 2018. 113p.

Contenido del documento:	INTRODUCCIÓN 1. DEFINICIÓN DEL PROBLEMA 1.1 ANTECEDENTES DEL PROBLEMA 1.2 FORMULACIÓN DEL PROBLEMA 2. JUSTIFICACIÓN 3. OBJETIVOS 3.1 OBJETIVO GENERAL 3.2 OBJETIVOS ESPECÍFICOS 4. MARCO REFERENCIAL 4.1 MARCO TEORICO 4.1.2. Seguridad de la información y gestión de los riesgos en PYMES 4.2 MARCO CONCEPTUAL 4.2.1 PYMES 4.2.2 Gestión de Riesgos 4.2.3 Magerit 4.3 ANTECEDENTES 4.4 MARCO LEGAL 4.4.1 Ley 1273 del 2009 4.4.2 Ley 1581 del 2012 5. DESARROLLO DE LOS OBJETIVOS 5.1 ESTABLECER LOS CONCEPTOS, ELEMENTOS Y TÉCNICAS NECESARIOS

	PARA LA GESTIÓN DE RIESGO ORIENTADO A LAS PYMES DEL SECTOR DE LAS TELECOMUNICACIONES 5.2 EXAMINAR MEDIANTE UNA REVISIÓN SISTEMÁTICA DE LITERATURA LA METODOLOGÍA MAGERIT V.3 5.3 PROPONER UNA GUÍA BASADA EN UN CASO DE ESTUDIO ORIENTADO A LAS PYMES DEL SECTOR DE LAS TELECOMUNICACIONES QUE PERMITA GESTIONAR EL RIESGO BASADO EN MAGERIT V.3 6. CONCLUSIONES 7. RECOMENDACIONES BIBLIOGRAFÍA
Conceptos adquiridos:	Con el desarrollo de esta monografía se abordaron conceptos que permitieron precisar conocimientos relacionados a la implementación de la metodología Magerit, enmarcada en una pymes del sector de las telecomunicaciones. Se identificaron activos de información, amenazas y salvaguardas enmarcadas dentro del caso de estudio propuesto.
Conclusiones:	Con el desarrollo de esta monografía queda claro que antes de adentrarse en un tema técnico, debemos tener muy claros los conceptos que lo sustentan. Dichos conceptos y elementos relacionados con el análisis y gestión de riesgos no son pocos, es por eso que son fundamentales en la comprensión de las acciones propias a realizar en el desempeño de estas actividades. En el libro I: Método, los conceptos que abarca la metodología MAGERIT en su versión 3, son sin lugar a dudas imprescindibles para poder entender y asimilar los fines del análisis y gestión de riesgos a nivel empresarial. Conceptos tales como gobierno, confianza y gestión son fundamentales para empezar a comprender

	los objetivos que persigue la metodología. Las dimensiones de la seguridad como: disponibilidad, integridad y confidencialidad son de suma importancia y su protección son la razón de ser de la metodología. El libro II: catálogo de objetos, es muy claro respecto a que no es una camisa de fuerza, sino una sugerencia de cuáles pueden ser los elementos a tener en cuenta, de acuerdo a cada escenario de la organización en estudio, seguramente pueden surgir nuevos elementos. Finalmente el libro III: guía de técnicas, recoge la compilación de técnicas específicas y generales para la obtención de resultados de manera simple o compleja de acuerdo al tipo de organización. La metodología Magerit es una alternativa viable para el análisis y gestión de riesgos en organizaciones tipo Pymes, debido a su método simple y a sus tres libros que sirven de guía en todo momento para la realización de las tareas con el objetivo de asegurar los activos de información luego de un análisis detallado de cada uno de ellos. Para este análisis se requiere un conocimiento detallado y profundo de los servicios ofrecidos por la empresa, sus procesos internos, los elementos que se puedan clasificar como activos basados en el catálogo de elementos y el personal responsable de los mismos. Con este conocimiento de punto de partida es relativamente sencillo realizar un análisis y gestión de riesgos en una pymes del sector de las telecomunicaciones, puesto que se reconoce como actividad principal y núcleo del negocio, la prestación del servicio de internet a sus clientes.