UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN INGENIERÍA DE SISTEMAS CON MENCIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN

Gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de Información

AUTOR:

Ampuero Herrera, Renato Mario (ORCID: 0000-0002-2339-6023)

ASESOR:

Dr. Martínez López, Edwin Alberto (ORCID: 0000-0002-1769-1181)

LÍNEA DE INVESTIGACIÓN:

Auditoría de Sistemas y Seguridad de la Información

LIMA - PERÚ

2022

DEDICATORIA

Esta investigación está dedicada a mis hijas Marjorie y Xiomara, por ser mi motor y motivo para alcanzar mis metas; de igual forma a mis amistades que brindan el impulso y estímulo necesario.

AGRADECIMIENTO

Agradecido a Dios por la vida, así como el incondicional apoyo de la familia, amistades y otras personas que facilitaron su apoyo, conocimientos y experiencia profesional para la presente investigación.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

La presente investigación: Gestión de riesgos de la información basada en la metodología Magerit para una notaría de la Región Lima, tuvo como objetivo general proponer un modelo de gestión de riesgos de los sistemas de información que administran las notarías y pueda aplicarse en las notarías de la Región Lima y en los despachos notariales del país.

Esta investigación es de enfoque cualitativo, para profundizar los conocimientos sobre la gestión de riesgos de los sistemas informáticos en el ámbito notarial. En el aspecto metodológico, el tipo de investigación es básica y el diseño es investigación-acción. Como técnicas se utilizaron entrevistas semi estructuradas, observación y análisis documental, mientras que como instrumento de recolección de datos se emplearon la guía de entrevista, guía de observación y ficha de análisis documental.

Se concluye que la metodología Magerit es una herramienta práctica y documentada que permite gestionar adecuadamente los riesgos mediante el análisis y tratamiento respectivo, que será plasmado en un plan de seguridad, con la finalidad de garantizar la continuidad de los sistemas o procesos que se realizan en las notarías y de esta forma ayudar a los oficios notariales en mejorar y resguardar la seguridad de la información que gestionan.

Palabras clave: Gestión de riesgos, sistemas de información, Magerit, notaría

Abstract

The present research: Information risk management viiiillviiisis the Magerit methodology for a notary's office in the Lima Region, had the general objective of proposing a risk management model for the information systems administered by notaries and can be applied in notaries' offices in the Lima Region and in the notarial offices of the country.

This research has a qualitative approach, to deepen the knowledge about risk management of computer systems in the notarial field. In the methodological viiiillviiisi, the type of research is basic and the design is action research. Semi-structured interviews, observation and documentary viiiillviiisis were used as techniques, while the interview guide, observation guide and document viiiillviiisis sheet were used as a data collection instrument.

It is concluded that the Magerit methodology is a practical and documented tool that allows risks to be adequately managed through the respective viiiillviiisis and treatment, which viiiill be reflected in a security plan, in order to guarantee the continuity of the systems or processes that are carried out in notaries and thus help notary offices in improving and safeguarding the security of the information they manage.

Keywords: Risk management, information systems, Magerit, notary

I. INTRODUCCIÓN

La tecnología de la Información (TI), es una poderosa fuerza para propiciar el cambio en nuestro mundo globalizado. El uso de las TI un elemento importante en la evolución de las personas y organizaciones. Najar (2016), manifiesta la importancia que las organizaciones cuenten con tecnología de punta para mantenerse activas y facilitar su rápida identificación en el mundo competitivo, así como gestionar los datos mediante los sistemas de información.

Según Laudon y Laudon (2017), manifiestan que, desde el enfoque empresarial, los sistemas de información son fundamentales en los procesos que agregan valor para la adquisición, transformación y distribución de la información que los líderes de las empresas pueden aplicar para desarrollar mejoras en la toma de decisiones, las cuales son procesos diarios en una empresa y que deben ser más eficaces, de igual manera ayuda al desenvolvimiento de la organización y, en última instancia, al incremento de los índices de rentabilidad empresarial.

Desde la perspectiva organizacional actual, dentro de los elementos más importantes en todo tipo de organización se encuentra la información y, en consecuencia, requiere mecanismos que garanticen su adecuada protección. Precisamente, los sistemas son cada vez más vulnerables a diversos ataques, en las que se pretende acceder, manipular o dañar la información que gestionan las organizaciones. En este contexto, si la información no se administra y protege adecuadamente, estará expuesta a riesgos que pudiera poner en peligro el desarrollo de sus actividades. Esto significa que las organizaciones deben saber cómo aplicar la gestión relacionado a los riesgos de los sistemas informáticos y asegurar los tres elementos fundamentales de la seguridad: confidencialidad, integridad y disponibilidad, conforme a la norma internacional ISO/IEC 27001.

Asimismo, Aquino et al. (2020) señalaron que las organizaciones, públicas o privadas, con distintos números de trabajadores, desarrollan diversos tipos de información importante para las mismas. Estos datos, usualmente se almacenan en diversos medios, tanto físicos como electrónicos o digitales, por lo que se enfrentan, a problemas como: fraude informático, espionaje, virus, ataques de intrusión y denegación de servicios, así como sabotajes, vandalismo, incendios e incluso catástrofes naturales como terremotos, inundaciones, entre otros.

Efectivamente, las organizaciones están expuestas a diversos riesgos y amenazas, internas o externas, que aprovechan las vulnerabilidades no detectadas de los sistemas para vulnerar la información que gestionan. Según Gil (2018), el Perú es el segundo país de Latinoamérica en ser víctimas de ciberataques, lo que demuestra la falta de preparación frente a esta problemática.

De acuerdo con el estudio de Fuentealba & Cruz (2018), analizaron la responsabilidad civil del Estado derivada de los daños ocasionados a las personas por incidentes de seguridad de los datos personales o procesamiento de datos en Chile. Asimismo, analizaron los estándares de ciberseguridad que el Estado debe observar como responsable del procesamiento de datos personales, el estándar de diligencia requerido en caso de incidentes que afecten los sistemas informáticos utilizados para la prestación de los servicios públicos. Y, como resultado, causa daños a los titulares de los datos personales.

La Organización para la Cooperación y el Desarrollo Económicos – ODEC (2020), señaló la importancia de la identificación de los sectores vulnerables que pudieran conllevar a incidentes de seguridad, debido al incremento del uso de servicios y sistemas que podrían generar perjuicios económicos y sociales para las instituciones. Al respecto, Jimeno (2017) conceptualizó la ciberseguridad como el conjunto de acciones desarrolladas para la protección de la información en el ciberespacio o en un sistema informático, que incluye la infraestructura que lo soporta. Destacó que los riesgos tecnológicos, ocasionados por ciberataques y robos de información, afectan a diversos países, en particular tienen una especial relevancia en las economías más importantes como: EE. UU., Japón, Alemania, Singapur, Suiza, Malasia, Países Bajos, entre otros.

Según The Global Risk Report o informe de riesgos globales (2019) revelaron que los ciberataques maliciosos provocaron violaciones masivas de información personal en el año 2018, siendo la más colosal en la India, donde la base de datos de identificación del gobierno, Aadhaar, presuntamente sufrió múltiples violaciones que comprometieron los registros de los 1.100 millones de ciudadanos registrados. En enero del año 2019, se informó que los delincuentes estaban vendiendo el acceso a la base de datos a una tasa de 500 rupias durante 10 minutos, mientras que en marzo una filtración en una empresa de servicios públicos de propiedad estatal permitió a cualquiera descargar nombres y números

de identificación. En otros lugares, violaciones de datos personales afectó a alrededor de 150 millones de usuarios de la aplicación MyFitnessPal, y alrededor de 50 millones de usuarios de Facebook.

En tal sentido, una de las organizaciones que administran información relevante para nuestra sociedad, es el notariado, cuya función es desempeñada por el notario. El sistema notarial data de muchos años y sigue vigente en diferentes lugares del mundo. En el contexto nacional, según el Decreto Legislativo 1049, indica que el notario es el profesional del derecho, elegido por concurso público, quien está autorizado para dar fe de los actos y contratos que ante él se ejecuten o celebren. Para ello, custodia, certifica y da fe en acuerdos; formaliza la voluntad de las personas que participan en dichos actos, redacta los documentos (instrumentos protocolares) a los que se le otorga autenticidad, conserva los originales y expide los traslados correspondientes a otras instancias, como los registros públicos.

Por tanto, los despachos notariales gestionan cuantiosa información en físico como en digital, por lo que sin duda están expuestos a riesgos en la seguridad de dicha información. Al respecto, la Ley N° 29733, Ley de protección de datos personales, aprobada el 02 de julio de 2011 y su respectivo reglamento aprobado con Decreto Supremo N° 003-2013-JUS el 21 de marzo de 2013, garantiza el derecho fundamental a la protección de los datos de tipo personal, conforme a la Constitución Política del Perú.

Bajo este contexto, las notarías como institución de origen privado pero que brindan un servicio público, deben contar con los controles, medidas y procedimientos de seguridad para resguardar la información, tales como documentos, software, dispositivos físicos, personas, imágenes y servicios. Es interesante que Van Dijk et al. (2018), refirieron que la idea de incorporar salvaguardas para la privacidad en los sistemas de TIC fue introducido recientemente en la legislación de la UE como "Data Protection by Design ".

Ante la situación planteada, se formula la siguiente pregunta general: ¿En qué consiste la gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima?, siendo los problemas específicos: ¿Cómo se debe analizar los riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima?, ¿En qué consiste el tratamiento de

los riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima?, ¿en qué consiste el plan de seguridad de la información basado en la metodología Magerit para una Notaría de la Región Lima?.

La presente investigación se justifica en lo social, porque como señaló Mallqui (2015) el derecho notarial se ha convertido en los últimos tiempos en primordial en nuestra sociedad y es un eje para el desarrollo social y económico de la comunidad. Sin embargo, el autor refiere que, por las características de nuestro ordenamiento jurídico, algunas personas aprovechan ciertas debilidades del sistema notarial y registral para su conveniencia. La investigación tiene una justificación tecnológica porque pretende asegurar la confidencialidad, integridad, autenticidad y trazabilidad de la data que gestionan los despachos notariales.

La presente investigación tiene justificación teórica, porque frente a la ausencia de reglas regulatorias estrictas, los notarios deben integrar continuamente tecnologías en sus actividades profesionales. De igual manera, tiene una pertinencia aplicada, puesto que el análisis de los resultados permitirá evaluar, conocer los beneficios y dificultades encontradas al aplicar la metodología para la gestionar los riesgos de los sistemas informativos en la actividad notarial.

El objetivo general del proyecto investigativo es proponer un modelo para la gestión de riesgos basado en la metodología Magerit para una Notaría de la Región Lima, siendo sus objetivos específicos: a) Analizar los riesgos de la información basado en la metodología Magerit para una Notaría Pública de la Región Lima, b) Determinar el tratamiento de los riesgos de la información basado en la metodología Magerit para una Notaría Pública de la Región Lima, c) Establecer el plan de seguridad de la información basado en la metodología Magerit para una Notaría Pública de la Región Lima.

En el Perú, la cultura organizacional desde el enfoque de la seguridad de la información no se ha desarrollado a plenitud, y en menor grado en las notarías. La presente tesis, propone un modelo o plan para la gestión de riesgos de la información a través del análisis y tratamiento de los riesgos, como la fase inicial para la implementación de un sistema de gestión de seguridad de información para una notaría pública. Dicha propuesta servirá de base para que otros oficios notariales puedan aplicar esta metodología, para resguardar la información física y digital que gestionan en el ejercicio de su función pública.

II. MARCO TEÓRICO

Respecto a investigaciones nacionales sobre la gestión de riesgos mediante la metodología Magerit, Aquino et al. (2021) refirieron que con la ayuda de dicha metodología en combinación con otras metodologías se logró una reducción en los riesgos de seguridad de los activos de información de la Dirección de Tecnologías de Información en la Universidad Nacional Micaela Bastidas de Apurímac (UNAMBA). De otro lado, Garay et al. (2020), desarrollaron una modelación de activos donde se empleó una metodología para la evaluación y análisis de los riesgos basado en la metodología Magerit, logrando disminuir significativamente los esfuerzos para dicho modelado. Esta investigación fue orientada a las pequeñas y medianas empresas (PYMEs) en el Perú, para que estas puedan identificar de forma simple los activos y riesgos involucrados en sus actividades de negocio.

Por su parte Tarrillo (2016), en su estudio de posgrado sobre la influencia de la gestión de riesgo sobre la seguridad de activos de Información de la Superintendencia Nacional de los Registros Públicos, Sede Moyobamba, confirmando la importancia que tiene gestionar los riesgos en la seguridad de la información de dicha institución. Maquera (2015), mediante la metodología Magerit logró clasificar, valorar y determinar la dependencia de los activos de la Universidad Nacional del Centro del Perú, realizando el análisis de amenazas, salvaguardas, impactos y riesgos por categoría de activos, lo que sirvió para contar con una directiva de seguridad para salvaguarda de los activos de la universidad. Llontop (2018), en su tesis de maestría, demostró la eficiencia de una adecuada gestión del riesgo de información en las empresas de comercio y de servicio, considerando a Magerit como una metodología sencilla que facilita la tipificación y análisis de riesgos de los sistemas descritos.

Respecto a investigaciones realizadas en el extranjero sobre la gestión de riesgos, Vicente et al. (2014) señalaron que en España el Consejo Superior de Administración Electrónica estableció el método Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información) con el objetivo de implementar un marco común para el análisis y gestión de los riesgos en sistemas informáticos, sobre la base de los estándares ISO/IEC 27000 y otros. Para Garcia et al. (2018), en la actualidad, el uso de las Tecnologías de Información y la Comunicación (TIC),

así como de los Sistemas de Información (SI), constituyen un componente crítico para las organizaciones; por lo que, se requiere alinear los procesos del negocio con la forma en la que se gestionan los riesgos de la seguridad de la información.

De la misma forma Fernández & García (2016), en su investigación sobre enfoques de modelado de activos complejos versus simples para la evaluación de riesgos de seguridad de la información, señalaron que la metodología Magerit es utilizada como un método sencillo para la gestión de riesgos de acuerdo el estándar ISO/IEC 27001. Najar (2017), reflexionó respecto a los riesgos a los que se encuentra expuesta la información que gestionan las organizaciones y los mínimos estándares de seguridad que deben contar para el manejo, manipulación, cuidado y resguardo de la información, procesos y sistemas informáticos.

También Santos et al. (2016), manifestaron que entre las principales propuestas para el análisis y gestión de riesgos se puede destacar Magerit (desarrollado por el gobierno español), Octave (Operational Critical, Threat, Asset and Vulnerability Evaluation), desarrollado por el Centro de Coordinación del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon de Pensilvania (Estados Unidos) o Cramm (CCTA Risk Analysis and Management Method), desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico.

Respecto a la importancia del análisis, Buzdugan (2021) destacó que al comprender el impacto que tienen las amenazas cibernéticas en una infraestructura crítica, en esa misma proporción, el proceso de identificación de riesgos mejora considerablemente. Cárdenas-Solano et al. (2016), resaltó que las experiencias han demostrado que una buena gestión de la información, no sólo mejora el desempeño organizacional sino transforma los procesos, estructura y cultura de la organización. Según Daneshjo (2021), el principal motivo para la integración de los sistemas de gestión de riesgos debería ser incrementar la eficiencia de la producción disminuyendo las pérdidas debido a la superposición de recursos de sistemas de gestión individuales.

Al respecto Romero et al. (2010), manifestaron que la metodología Magerit categoriza los activos según una estructura jerárquica. También señalaron que un

activo puede pertenecer simultáneamente a diferentes tipos y es común que aparezcan nuevos activos en cada estudio. Además, la metodología Magerit establece que las dependencias entre activos se definen como la medida de cómo un activo de nivel superior puede verse comprometido por un problema de seguridad de algún activo inferior. Corda et al. (2017), en su artículo sobre gestión del riesgo tecnológico y bibliotecas, realizó una revisión de normas a nivel nacional e internacional respecto a la gestión del riesgo tecnológico, cuyos problemas son derivados por el acceso a la información, incrementando el peligro de pérdida, robo o adulteración.

Según Figueira (2019), Magerit calcula dos tipos de riesgo: riesgo potencial y riesgo residual. El riesgo potencial es un riesgo teórico, que se aplica a situaciones en las que no se han implementado salvaguardas, mientras que el riesgo residual es el riesgo después de la implementación de salvaguardas. Para los autores, varias normativas como Magerit (adaptación española de la ISO/IEC 27005) proporcionan un alto nivel de confiabilidad para el análisis de riesgos en las organizaciones. Asimismo, Toapanta et al. (2020) manifestaron que la metodología Magerit es utilizada con gran eficacia para analizar la gestión de riesgos, en instituciones como la NASA y el Centro Criptológico Nacional (CCN) de España.

A su vez Motaki (2016), señaló que Magerit se utiliza para la identificación, análisis y evaluación de los riesgos. Obtenido los resultados del análisis, se contará con los valores de las dependencias entre los elementos y el número de amenazas a las que se encuentran expuestas. Amutio et al. (2014), refirió que la metodología Magerit, determina el valor de los activos a partir de la integridad, trazabilidad, confidencialidad y autenticidad de la información, en diferentes niveles.

Por su parte Giménez (2015), manifiesta que la seguridad de la información debe realizarse siguiendo un método para el análisis y gestión de los riesgos, refiriendo que Magerit es una metodología sencilla que permite la evaluación del riesgo, por lo que cumple perfectamente con este propósito. Quintero (2015), desarrolló una investigación sobre la importancia del Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Superintendencia de Notariado y Registro de Colombia. Para el autor, la seguridad de los datos involucra tener en consideración múltiples alternativas de resguardo,

para que estas logren el aseguramiento de la información contra las diferentes situaciones que la hacen vulnerables. En su estudio también consideró los planteamientos y conceptualizaciones de los estándares internacionales de la ISO, específicamente las normas ISO/IEC 27001 e ISO/IEC 27002.

De otro lado, Selviyanti & Sardjono (2020), realizaron una investigación se para encontrar factores de riesgo del sistema de información y construir un modelo de evaluación de la gestión de riesgos del sistema de información para una empresa de televisión en Indonesia. Manifestaron que, para el logro de los objetivos comerciales de la empresa, los sistemas de información son la base que se utiliza como soporte de la estrategia comercial de la organización, con el fin de mejorar la calidad de los servicios y las operaciones comerciales. Concluyeron que el sistema de información y sus activos son vulnerables al riesgo de daños físicos y lógicos, por lo que, la gestión de riesgos requiere suma atención, puesto que su falta de cuidado pudiera ocasionar pérdidas financieras, merma de su reputación o incluso la desaparición del negocio.

En tal sentido, para Usländer (2014) la gestión de riesgos en términos generales constituye el conjunto de acciones preventivas integradas que se toman para abordar la identificación, el análisis y las medidas requeridas de los riesgos durante los desastres. Asimismo, Toapanta et al. (2020) concluyó que Magerit es una alternativa que permite mitigar las vulnerabilidades, amenazas y riesgos de los sistemas y procesos en los organismos públicos para la protección de su información, ante el incremento de los ataques informáticos junto con las amenazas externas, que pudieran causar robo de información y bases de datos.

En cuanto a Serrano et al. (2019), realizaron un análisis e identificación de los riesgos a los que se encuentra expuesto el Hospital Básico de Catacocha – Ecuador, a través de su Departamento de Tecnologías de la Información y Comunicaciones (TIC), para identificar las vulnerabilidades que pueden amenazar la seguridad de información de dicha institución, con la finalidad de contar con el plan de gestión para mitigar los riesgos.

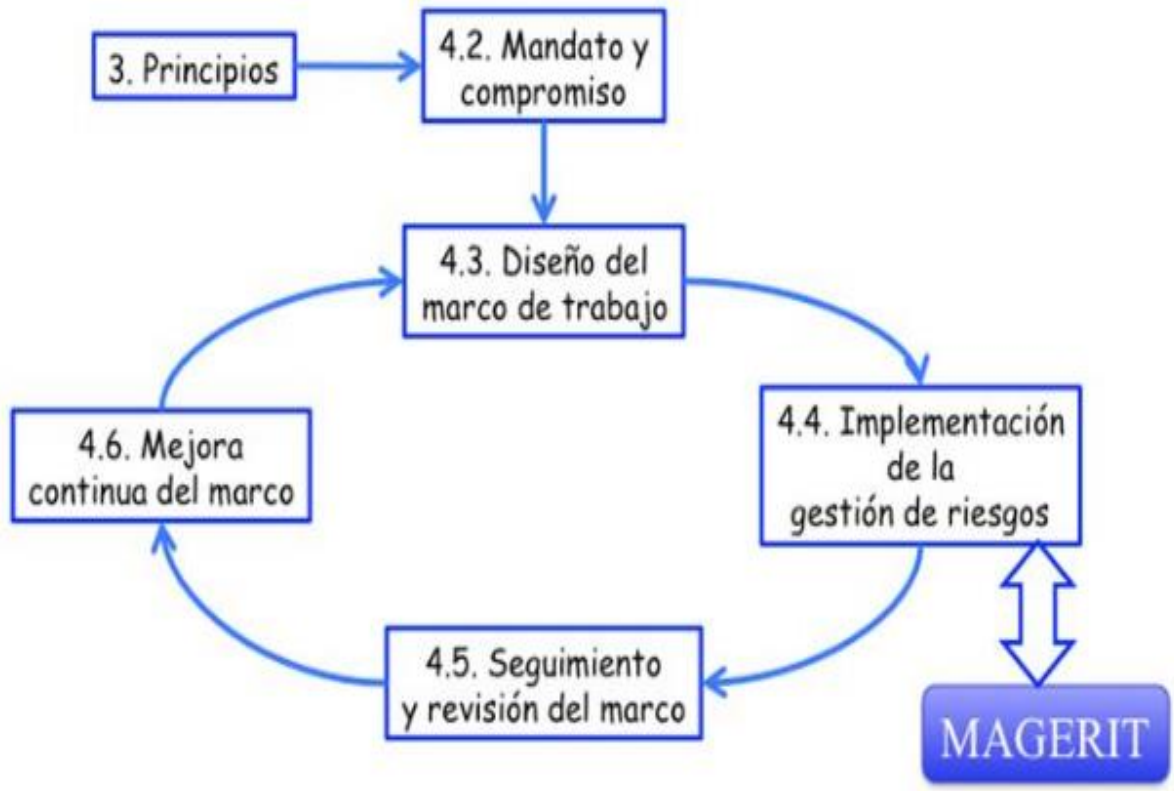
A continuación, se detallan conceptos básicos relacionados a la presente investigación. Resulta necesaria realizar una revisión de las teorías concernientes

al problema de estudio, iniciando con la metodología Magerit para la gestión de los riesgos de la información, el análisis y tratamiento de los riesgos, el plan de seguridad; asimismo, las teorías vinculadas con la función notarial y la normativa que regula el manejo de los datos personales en el Perú.

Referente a Magerit (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), Vicente et al. (2014) manifestaron que es un marco común para analizar y gestionar los riesgos de las aplicaciones informáticas, siendo de uso libre y promovido por el gobierno español, que se adapta a los estándares: ISO/IEC 27000/27001 (Sistemas de Gestión de la Seguridad de la Información), ISO/IEC 27005 (Gestión de riesgos de la Seguridad de la Información), ISO 31000 (Sistema de Gestión de riesgo) como se observa en la figura . La metodología está documentada en los libros siguientes: Libro I Método, Libro II Catálogo de elementos y Libro III Guía de técnicas.

Figura 1.

ISO 31000 – Marco de trabajo para la gestión de riesgos

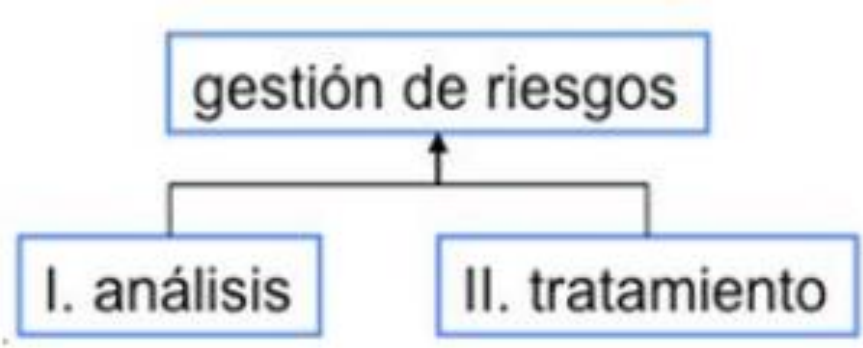


Fuente: Amutio et al, (2012)

Magerit se enfoca en el valor que tiene la información para las diferentes organizaciones y nace como respuesta a que las instituciones dependen cada vez más de las TI para cumplir su misión y objetivos correspondientes. Según Amutio et al. (2012), la gestión de riesgos con la metodología Magerit, requiere dos fases importantes: el análisis y tratamiento de los riesgos que soportan los sistemas de información, como se observa en la figura 2. La combinación del análisis y tratamiento, permitirá la gestión de los riesgos identificados.

Figura 2.

Gestión de Riesgos con Magerit



Nota: Amutio et al. (2012)

Para Amutio et al. (2014), para gestionar los riesgos en el manejo de información, se debe realizar el análisis de los riesgos. Es importante entender lo que implica el riesgo, el mismo está presente en todas las actividades que desarrollan las organizaciones públicas o privadas, lo que pudiera conllevar a problemas financieros y poner en riesgo la situación económica y la reputación de la organización. Existen casos específicos, como la quiebra y cierre de bancos o similares, debido a la mala administración del riesgo operativo, por lo que, el análisis de riesgos resulta fundamental para la gestión de la seguridad de los diversos sistemas. Garcia et al. (2018) precisan que Magerit propone etapas en el análisis de riesgos, de acuerdo a la figura 3.

Figura 3.

Pasos para el análisis de riesgos con Magerit

Nota: Garcia et al. (2018)

El referido autor, detalla la secuencia del análisis de esta manera: 1. Identificación de los activos a resguardar ; 2. Identificación de los componentes donde los ataques pueden generar daño o constituirse en una amenaza para la organización; 3. Determinar las medidas de seguridad o salvaguardas para protegerse frente a posibles ataques; 4. Estimación de los indicadores de la posición de riesgo para la toma de decisiones; 5. Estimación de los riesgos identificados que se refieren a la materialización de la amenaza.

Para el citado autor, la primera etapa corresponde a reconocer los activos y su clasificación en subgrupos. Seguidamente, es importante la formalización del árbol de dependencias entre todos los activos previamente definidos. Consecuentemente, cuando estén relacionados y definidos los activos se requiere asignar un valor a cada uno de ellos. Para ello, los activos deben estar descritos correctamente, para definir las potenciales amenazas y, utilizar su valoración de impacto, se puede determinar el riesgo correspondiente.

Luego de concretar el análisis de riesgos, conociendo los riesgos, amenazas y su impacto en la organización, se procede a establecer el tratamiento correspondiente, con la finalidad de prevenir, reducir o controlar los riesgos y

amenazas identificados, lo que permite disminuir su potencialidad de generar problemas para la continuidad de la institución; cuyo resultado es el plan de seguridad para la gestión de riesgos de la información. Según Chicano (2015), manifiesta respecto a la gestión, análisis y tratamiento de riesgos, que existe un estándar de la norma ISO (ISO 31000) que incluye distintas recomendaciones y actividades para que las organizaciones gestionen sus riesgos de una forma más adecuada y eficiente.

La información, para Did (2016), es el conjunto de datos alfabéticos, numéricos o alfanuméricos, articulados en forma significativa, los cuales son dispuestos en una secuencia lógica respecto a algún suceso importante. La información genera valor para tomar decisiones, siendo que mientras tenemos más información, nos resulta más fácil contar con decisiones correctas. Esa es fundamentalmente la finalidad de la información: reducir la incertidumbre, aumentar el conocimiento para incrementar las perspectivas de éxito.

Los sistemas de información, según Ros García (2018), basado en el libro de James Senn (1999), señala que se refiere al “conjunto de componentes que interactúan entre sí para lograr un objetivo común”. De acuerdo a ello, los sistemas de información procesan las entradas, mantienen la data de la organización a disposición, con los que producen continuamente información relevante, destacando la importancia de la gestión de esa información en las organizaciones, así como sus políticas de información. Asimismo, estos sistemas están constituidos por subsistemas como: mecanismos de almacenamiento, hardware y software, los cuales necesitan protección y resguardo pertinentes.

Cuando se hace referencia a vulnerabilidad de los sistemas de información, según SeguridadPC.Net (2016), se describe a una un punto débil de cualquier sistema que permite a un atacante vulnerar la confidencialidad de la información y de las aplicaciones, tomar el control del mismo, divulgar o comercializar la data por diferentes medios. Las vulnerabilidades son el resultado de continuos errores en el diseño o desarrollo de los sistemas de información. En ese sentido, el Departamento de Seguridad Informática (2016), señala que las amenazas nacen a partir de la presencia de vulnerabilidades, por lo que, una amenaza debe su

existencia a una vulnerabilidad que pudiera ser aprovechada. Es importante mencionar que las amenazas pueden ser internas o externas.

Por su parte, el riesgo tecnológico, según la Organización Internacional por la Normalización (ISO) es “la probabilidad que una amenaza se materialice, utilizando una o más vulnerabilidades de un activo o grupo de activos”, lo que pudiera generar pérdidas o daños para la organización. Entonces las amenazas pudieran propiciar un ataque informático u ocasionar un impacto negativo para la organización. El riesgo también involucra incertidumbre (si no se tiene la seguridad de que suceda) o pérdida potencial (por fallas, errores en sistemas o procesos).

La seguridad de la información, según Guzmán (2015) en su tesis de maestría, lo define como “el conjunto de metodologías, prácticas y procedimientos que buscan proteger la información como activo valioso”, con la finalidad de reducir las amenazas y riesgos expuestos, para asegurar el desarrollo del negocio, minimización de los daños a la organización y maximización del retorno de inversiones, así como las oportunidades del negocio. Por ende, comprende todas las medidas preventivas y de reacción que son tomadas por el hombre, las organizaciones y sistemas informáticos que permitan el resguardo y protección de la data, pretendiendo preservar la confidencialidad, la autenticidad e integridad de la misma.

Al respecto, McKinsey&Company (2018) estima que para el año 2025 existirán 300 millones de dispositivos conectados en México, lo que representa un 70% de crecimiento; sin embargo, la accesibilidad y disponibilidad de los sistemas informáticos incrementa los riesgos en los sistemas de información; por ejemplo, en el año 2017 más de 33 millones de personas fueron aquejadas por el cibercrimen en México. Sin duda, el crecimiento acelerado de las herramientas tecnológicas y comunicación han traído beneficios importantes para el sector público, privado, y la sociedad en general, promoviendo el intercambio cultural y comercial.

A continuación, es importante describir la función del notariado en la sociedad y la normativa que regula dicha actividad en el Perú. El TUO del Reglamento del D.L. 1049, Decreto Legislativo del Notariado, en su artículo 4° señala que “el notario es el profesional del derecho encargado de una función

pública consistente en recibir, interpretar y dar forma legal a la voluntad de las partes", plasmándola en un documento, con lo que le confiriere la autenticidad al mismo, debido a que conservan los originales y expiden copias en las que da fe de la veracidad del contenido. Para dicho autor, la misión fundamental del notario es documentar los acuerdos realizados entre las partes contratantes, concediéndole al contrato mismo, las calidades de certeza, veracidad, autenticidad y seguridad.

En el Perú, el Decreto Legislativo Nro. 1049 Ley del Notariado vigente desde junio del 2008 y modificatorias, promulgada en el marco de delegación de facultades otorgadas al ejecutivo para implementar el tratado de libre comercio entre el Perú y los Estados Unidos, introdujo modificaciones a la norma anterior, el Decreto Ley 26002, en cuanto a innovación tecnológica y el empleo de canales seguros que faciliten las transacciones comerciales. Dicha normativa establece, en el inciso i del artículo 16, que para ejercer la función notarial debe contar con una infraestructura tecnológica mínima, que propicie la interconexión del notario con el colegio de notarios correspondiente y a nivel nacional, así como a la informatización de sus registros que favorezcan la prestación de los servicios notariales en el intercambio comercial nacional o internacional.

En ese sentido, el derecho notarial es un elemento del derecho público y que, ejerce una función que es delegada por el Estado, la cual es dar fe pública de los actos, contratos y hechos que se le presentan, contando con un sistema organizativo que orienta y define el ejercicio de carácter autónomo y privado del notariado. En la actualidad, los despachos notariales se encuentran dotados de herramientas tecnológicas como soporte para el ejercicio de la función notarial. En este sentido dentro de uno de los tantos aspectos referidos a la informatización, la norma establece la posibilidad de que el archivo notarial, integrado por: los registros físicos, minutarios, documentos protocolizados y los índices, puedan estar contenidos en un soporte magnético. Como se aprecia, el notariado peruano ha venido adaptándose a las necesidades de la sociedad, así como el marco jurídico que la tutela.

A su vez Tambini (2014), mencionó que el notario no percibe una retribución económica de parte del Estado, debido a que el ejercicio de su función como profesional independiente, bajo el principio de rogación de las partes, por lo

que, solo recibe una compensación económica establecida para los servicios notariales que brinda a la comunidad. Asimismo, indicó que la fe pública notarial es la potestad que el Estado confiere al notario, para que proteja la verdad de hechos y actos jurídicos que le constan.

De acuerdo con la definición legal que recoge el Decreto Legislativo N° 1049, Decreto Legislativo del Notariado, el uso de las tecnologías de la información y comunicación son una excelente oportunidad para incrementar la transparencia, el acceso a la información y la comunicación con los usuarios, lo que indudablemente redunda en la optimización y mejora del servicio notarial. Sin embargo, el uso de las tecnologías de información y comunicación, también genera riesgos de pérdida, robo o adulteración de información sensible para las notarías y de sus usuarios. Precisamente, por este motivo, es importante identificar y analizar los riesgos o amenazas, para proponer una adecuada gestión de los mismos.

En el Perú, los despachos notariales están organizados en Distritos Notariales. Mediante Decreto Ley N° 26002, en su artículo 128°, se crearon inicialmente veinte distritos notariales; posteriormente, mediante Ley N° 27567 se incrementó en veintidós, como se indica en la tabla N° 1. Seguidamente se presenta el resumen de notarías ubicadas en el ámbito de la Región Lima, conformado por el Distrito Notarial de Callao, según se detalla en la tabla N° 2.

Tabla 1

Listado de Distritos Notariales en el Perú 2021

N°	Distrito Notarial
1	Distrito Notarial de Amazonas
2	Distrito Notarial de Ancash
3	Distrito Notarial de Apurímac
4	Distrito Notarial de Arequipa
5	Distrito Notarial de Ayacucho
6	Distrito Notarial de Cajamarca
7	Distrito Notarial de Callao
8	Distrito Notarial de Cusco y Madre de Dios
9	Distrito Notarial de Huancavelica
10	Distrito Notarial de Huánuco y Pasco
11	Distrito Notarial de Ica
12	Distrito Notarial de Junín
13	Distrito Notarial de La Libertad
14	Distrito Notarial de Lambayeque
15	Distrito Notarial de Lima
16	Distrito Notarial de Loreto
17	Distrito Notarial de Moquegua
18	Distrito Notarial de Piura y Tumbes
19	Distrito Notarial de Puno
20	Distrito Notarial de San Martín
21	Distrito Notarial de Tacna
22	Distrito Notarial de Ucayali

Nota: Minjusdh (Ministerio de Justicia y Derechos Humanos)

Tabla 2

Listado de Notarías del Distrito Notarial Callao, 2021

N°	Distrito	Cantidad
1	Barranca	2
2	Bellavista	2
3	Callao	5
4	Carmen de la Legua Reynoso	1
5	Chancay	1
6	Huacho	3
7	Huaral	3
8	Imperial	1
9	La Punta	1
10	Lunahuana	1
11	Mala	1
12	Matucana	1
13	Oyon	1
14	Paramonga	1
15	San Vicente de Cañete	2
16	Supe	1
17	Ventanilla	2
	Total	**29**

Nota: Minjusdh (Ministerio de Justicia y Derechos Humanos)

Como indica la tabla N° 2, son veintinueve (29) notarías ubicadas en la Región Lima, los cuales brindan sus servicios notariales a una población aproximada de más de 900,000 personas, según el censo poblacional ejecutado por el INEI en el año 2017. Asimismo, es importante mencionar que el Consejo del Notariado viene a ser la dependencia adscrita al Ministerio de Justicia y Derechos Humanos (Minjusdh), responsable de supervisar el Sistema Notarial peruano.

Por tanto, Magerit es una metodología que apoya a la norma ISO/IEC 27005 e ISO 30001, detectando las amenazas y la información crítica en las organizaciones. La utilización de Magerit consiste en ejecutar un estudio de los riesgos para asegurar la información, identificando y valorando sus activos, así también las amenazas que pudieran afectar sus actividades e implementar

salvaguardas para tratar, controlar y aminorar los riesgos identificados. Asimismo, la metodología Magerit permite medir el impacto que se generaría si la amenaza se concreta. Esto conllevará en la materialización del plan de gestión de riesgos de información, que servirá de base para implementar el Sistema de Gestión de Seguridad de la Información (SGSI).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Tipo de investigación

Según la finalidad de este trabajo el tipo es básico. Según Hernández (2018) este tipo de investigación se caracteriza porque busca producir o ahondar conocimientos y teorías. La investigación básica pretende acrecentar los conocimientos científicos, sin contrastarlos con algún aspecto práctico. En ese sentido, con la investigación se profundizan los conocimientos y principios científicos, respecto a las metodologías para gestionar los riesgos en los sistemas de información orientado a una notaría pública. Asimismo, se apoya en el enfoque cualitativo, que según Diaz (2017), la investigación cualitativa involucra recolectar una gran diversidad de materiales, experiencia personal, entrevistas, entre otros, que describan la costumbre o rutina, situaciones problemáticas, entre otros.

Diseño de investigación

Se utilizó el diseño de investigación - acción, consistente en diagnosticar la situación, formular el problema, recolectar los datos necesarios, realizar el trabajo de campo, analizar e interpretar los datos obtenidos, efectuar la discusión de resultados y las conclusiones o recomendaciones respectivas. Dicha metodología es apropiada para el estudio de una problemática social específica que amerita una solución, la cual afecta a un grupo de personas, comunidad, sociedad, escuela u organización. Para Blaxter, Hughes y Tight (2002), constituye un método idóneo para emprender cambios en las organizaciones. Para los referidos autores, se centra en la exploración de un limitado pero escrupuloso número de casos que se consideran esclarecedores, cuya meta es lograr la profundidad de estudio.

Con esa misma línea, según Bell (2005) resulta apropiada para aquellos investigadores que identifican un problema en su espacio de trabajo y quieren analizarlo para favorecer al proceso de mejora continua. Para Creswell (2019) este tipo de proyectos tienen parecimiento a las técnicas de investigación mixtas, debido a que en esta se ejecutan una serie de datos cuantitativo, cualitativo o ambos; diferenciándose al enfocarse en la solución del problema de forma específica y práctica. El referido autor clasifica dos tipos de investigación acción: práctica y

participativa. Con dicho diseño se determinan las causas y consecuencias de la problemática analizada y posibles soluciones.

3.2. Categorías, Subcategorías y matriz de categorización:

La categorización correspondiente se detalla en la tabla 3.

Tabla 3

Categorías y sub categorías

Categorías	Subcategorías
Análisis	Determinar los activos
	Determinar las amenazas
	Determinar las salvaguardas
	Estimar el impacto
	Estimar el riesgo
Tratamiento	Eliminación
	Mitigación
	Compartición
	Financiación
Plan de seguridad	Identificación de proyectos de seguridad
	Plan de ejecución
	Ejecución del plan

Nota: Elaboración propia

Las categorías descritas: identificación, análisis y evaluación; corresponden al tipo deductiva, las cuales se han establecido en base a la teoría y conocimientos previos sobre el tema de investigación.

3.3. Escenario de estudio

Tuvo lugar en el área de soporte tecnológico de la Notaría Nieves Chen, ubicada en el distrito y provincia de Barranca, Región Lima, cuyo despacho notarial inició sus actividades en el año 1998. En la actualidad, brinda sus servicios notariales en un edificio de cuatro pisos, que se encuentra frente a la plaza de armas de la ciudad. Cuenta con un área de soporte tecnológico, responsable de la administración de red, soporte técnico y sistemas informáticos que está a cargo de un especialista en Sistemas.

3.4. Participantes

En la investigación participaron el notario, el responsable del área de soporte tecnológico y colaboradores que laboran en dicha organización, en las áreas de instrumentos protocolares, actas y certificaciones extra protocolares y asuntos no contenciosos. Asimismo, se contará con la participación de especialistas en tecnologías de información con experiencia en la gestión de riesgos para las organizaciones públicas y/o privadas.

3.5. Técnicas e instrumentos de recolección de datos

De acuerdo con Hernández y Mendoza (2018), señalaron que la finalidad de la técnica es precisamente obtener datos, que pueden ser emociones, creencias, experiencias o pensamientos que se convertirán en información importante para el investigador y permitirá responder a las preguntas iniciales del presente estudio. Para la investigación se utilizará la entrevista semi estructurada porque se utilizarán preguntas abiertas con el objeto de obtener respuestas descriptivas.

En ese sentido, Folgueiras (2016) destacó que el objetivo principal de la entrevista es la obtención de información en forma oral y sobre todo personalizada, respecto a las experiencias y opiniones de las personas, con lo que se genera una interacción sobre el tema de estudio. Según el citado autor, en la entrevista semi estructurada se dispone con anticipación sobre la información que es requerida y sobre ello se establece una guía de preguntas. Sin embargo, las preguntas son elaboradas de forma abierta, permitiendo recolectar información más enriquecedora que en la entrevista estructurada.

Además, se utilizará la técnica de observación a fin de observar los hechos y situaciones que ocurren en el escenario de estudio. Teniendo en cuenta la emergencia sanitaria y distanciamiento social por el COVID-19, Hernán-García et al. (2020) manifestaron que la disponibilidad de Internet y entornos virtuales representa un gran potencial documental observacional y conversacional para los investigadores. Finalmente, la técnica de análisis documental se enfocará principalmente en la finalidad del estudio. Sánchez et al. (2021), señalaron que los instrumentos proporcionan una mayor profundidad de búsqueda por lo que, en esta investigación se empleó la guía de entrevista semi-estructurada, guía para la observación, así como una ficha para el análisis documental.

3.6. Procedimientos

Para la validación de los datos cualitativos se ha considerado la credibilidad, transferibilidad, constancia interna y fiabilidad. En este sentido, se coordinó y entrevistó a dos especialistas en tecnologías de información, con experiencia en sistemas y gestión de riesgos digitales. Se formularon a los entrevistados diversas preguntas, teniendo como soporte la guía de entrevista, relacionado a la gestión de riesgos y su importancia para las organizaciones, así como el método para su implementación. Luego se procedió a recopilar y procesar las entrevistas realizadas, con la finalidad de realizar la triangulación y conclusión de los resultados obtenidos.

3.7. Rigor científico

La solidez científica lleva implícita la valoración de los contextos para que la investigación puede ser distinguida como verdadera; por lo que, es fundamental buscar argumentos fiables de acuerdo con el proceso que se pueda comprobar los resultados del estudio realizado. El rigor científico se condice en la investigación de la realidad, la experiencia acumulada, evidencias disponibles y el conocimiento de los valores. Asimismo, la presente investigación está respaldada en artículos científicos publicados en revistas indexadas, así como libros de bases de datos electrónicas reconocidas en el ámbito científico.

3.8. Método de análisis de la información

Según Hernández y Mendoza (2018), indicaron que el éxito de una investigación científica depende que “el especialista decida indagar acerca de un problema formulado adecuadamente; por el contrario, el fracaso se producirá si hay un problema mal formulado”. De igual importancia es la elección del método científico que dependerá del planteamiento del problema, lo que implica que cada problema puede tener formas distintas de resolver. Asimismo, es necesario el uso de técnicas adecuadas para la recolección y el análisis de los detalles obtenidos, su correcta explicación y discusión de resultados. En tal sentido, Escudero et al. (2018) señalaron que, “para medir y verificar la exactitud de los resultados, existen técnicas como la triangulación de datos” para estudiar el mismo fenómeno.

3.9. Aspectos éticos

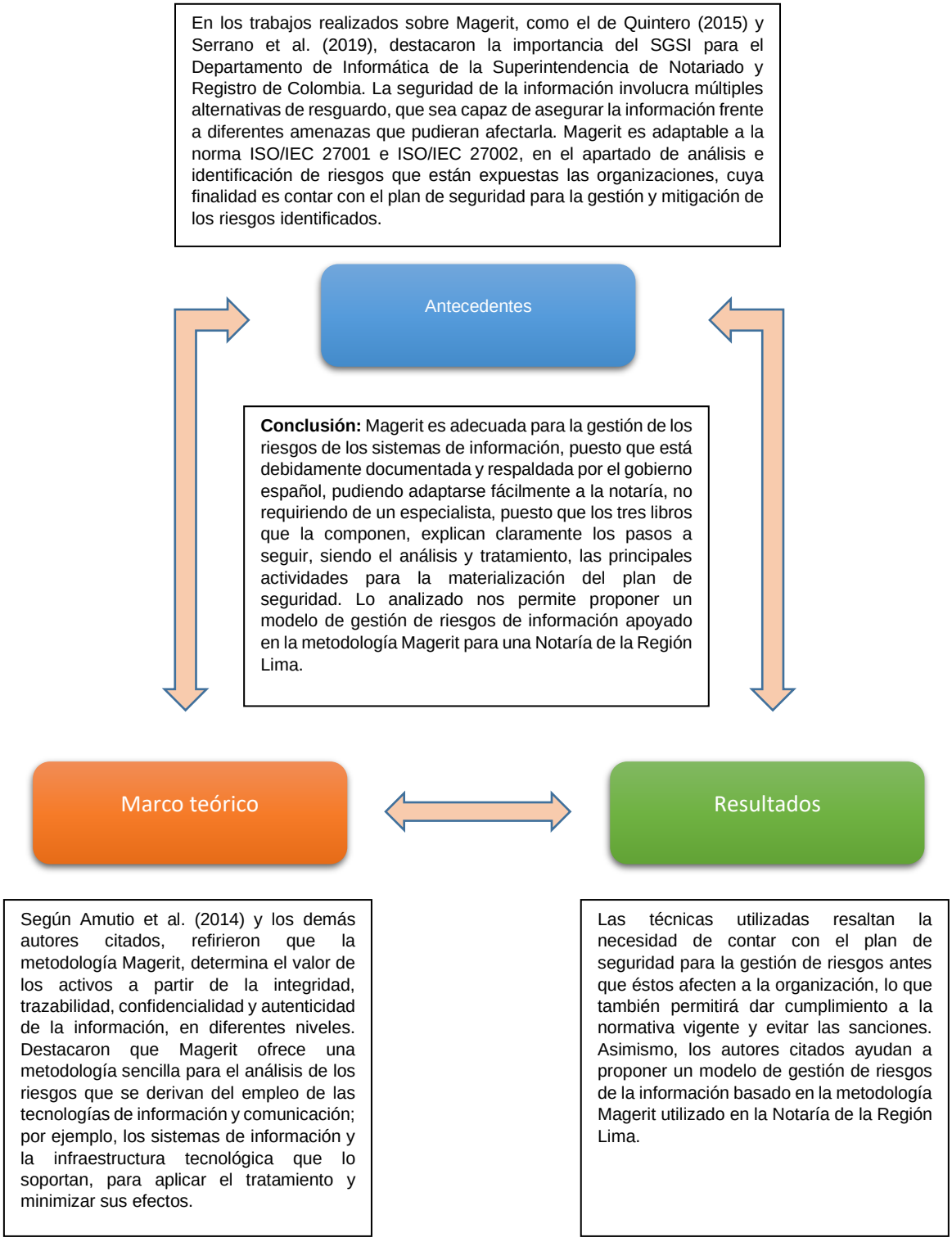
La presente investigación se sustenta en valores, como: claridad, veracidad y discreción de los datos obtenidos de la organización, conservando en el anonimato a los colaboradores. Asimismo, se consideró la Resolución del Vicerrectorado de Investigación N° 011-UCV, el Código de Ética de la Escuela de Posgrado de la UCV; asimismo se ha utilizado las Normas APA en su 7ma. versión para la redacción del presente documento, así como el uso del aplicativo Turnitin, para determinar el porcentaje de similitud con otras investigaciones.

IV. RESULTADOS Y DISCUSIÓN

Los resultados de esta investigación se obtuvieron utilizando diferentes técnicas para recolección de datos, entre los que se destaca: la entrevista semi-estructurada, la observación y el análisis documental, para lo cual, se elaboraron los instrumentos, para conseguir los objetivos establecidos. En ese sentido, se presenta a continuación las conclusiones a los que se llegó, aplicando las siguientes triangulaciones.

Figura 4

Triangulación de los antecedentes, del marco teórico y los resultados



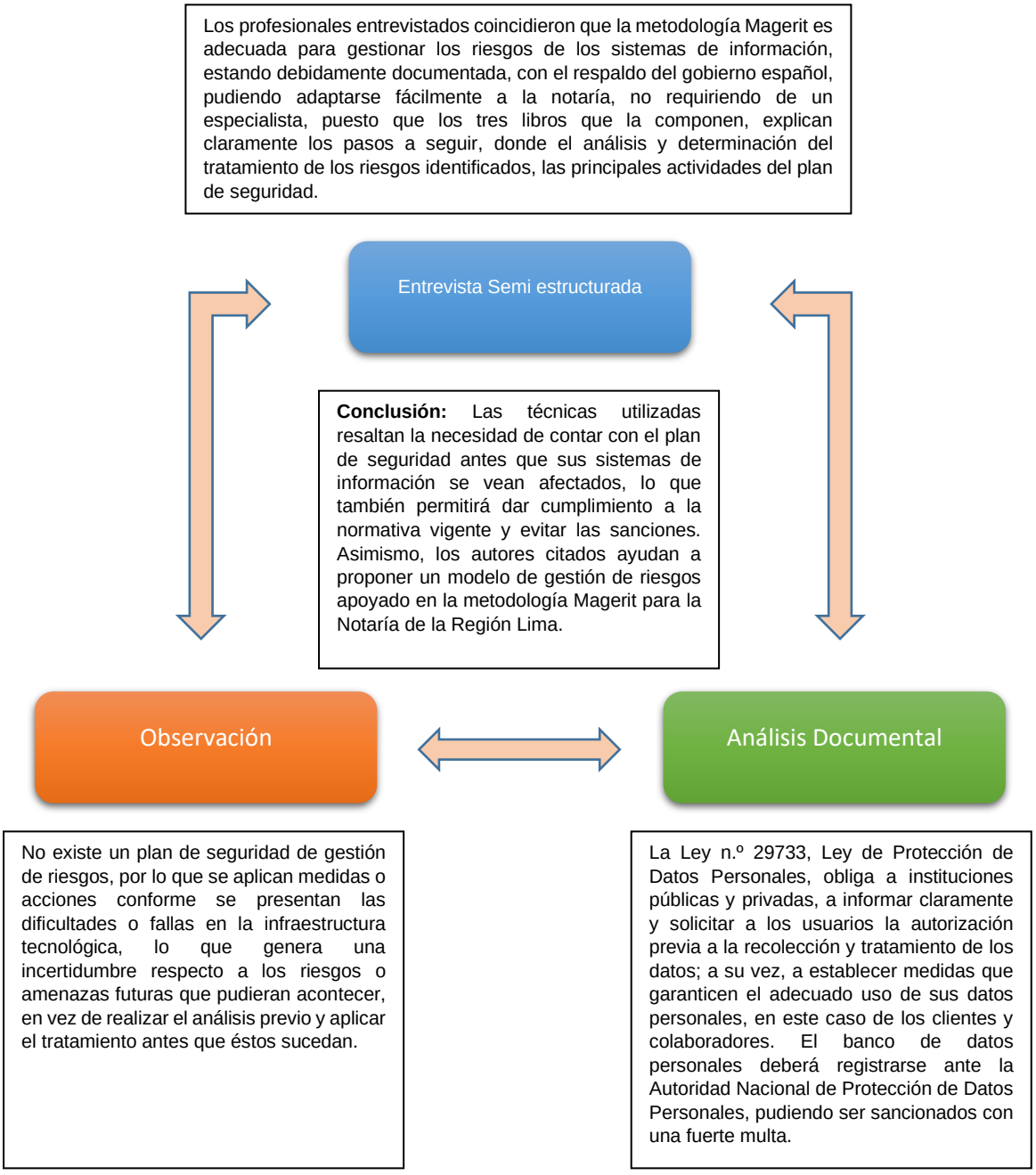
La figura 4 muestra la triangulación de los antecedentes, el marco teórico y resultados, que responde al objetivo general, indicando que Magerit es adecuada

para gestionar los riesgos en los sistemas de información, por estar debidamente documentada y respaldada por el gobierno español, pudiendo adaptarse fácilmente a la notaría.

Esto concuerda con la investigación de Amutio et al. (2014), quien indicó que Magerit ofrece una técnica ordenada para analizar aquellos riesgos que se derivan de la utilización de las tecnologías de información y comunicación. A su vez, Toapanta et al. (2020) señaló que Magerit es una alternativa que permite aminorar las vulnerabilidades, riesgos y amenazas en los organismos públicos, ante el constante incremento de los ataques informáticos junto con las amenazas internas o externas, que pudieran ocasionar el robo de información y otras problemáticas.

Figura 5

Triangulación de las técnicas utilizadas



La figura 5, muestra la triangulación de las tres técnicas utilizadas, como la entrevista semi-estructurada, observación y análisis documental, obtenidos mediante sus instrumentales correspondientes, donde se concluye que es sumamente importante contar con el plan de seguridad para la gestión de riesgos de los sistemas y prevenir la aparición de fallos que afecten la infraestructura

tecnológica de la notaría y perjudique la información o servicios. A su vez, esto permitirá dar cumplimiento a la normativa vigente, respecto a la forma cómo se deben tratar los datos personales en organizaciones públicas y privadas. En consecuencia, las técnicas indicadas demuestran que es factible proponer un modelo de gestión de riesgos de la información apoyado en Magerit para una Notaría de la Región Lima.

De acuerdo a la triangulación realizada, teniendo en cuenta los trabajos previos (antecedentes), el marco teórico y los resultados de las técnicas utilizadas, se concluye que la metodología Magerit se adapta a diferentes organizaciones públicas o privadas para gestionar los riesgos a través del analizar y tratar los mismos. Estos resultados están acordes con los objetivos específicos de la investigación, al señalar que es una herramienta sencilla que permite analizar los riesgos de la información apoyado en Magerit para la Notaría Pública de la Región Lima. Asimismo, permite determinar el tratamiento adecuado de los riesgos detectados antes que pueda afectar los sistemas o servicios de una notaría. Las actividades señaladas en la metodología Magerit permiten establecer el plan de seguridad para una Notaría Pública de la Región Lima.

Como parte de la discusión, se ha realizado la comparación de los resultados obtenidos, contrastándolo con la documentación incluida en la presente investigación, que conforman la realidad problemática, los trabajos previos o antecedentes, diversos artículos de revistas indizadas, indagación del marco teórico, los cuales están relacionados con los objetivos trazados. El principal objetivo del presente trabajo fue proponer un modelo de gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, utilizando tres técnicas para recopilar datos, como: entrevista semi-estructurada, observación y análisis documental; con sus respectivos instrumentos. La metodología utilizada es de tipo básica y su diseño es de investigación-acción, de enfoque cualitativo.

Referente a ello, los especialistas entrevistados señalaron que Magerit es adecuada para la gestión de los riesgos de los sistemas que administran información, puesto que está debidamente documentada y respaldada por el gobierno español, pudiendo adaptarse fácilmente al oficio notarial, además no

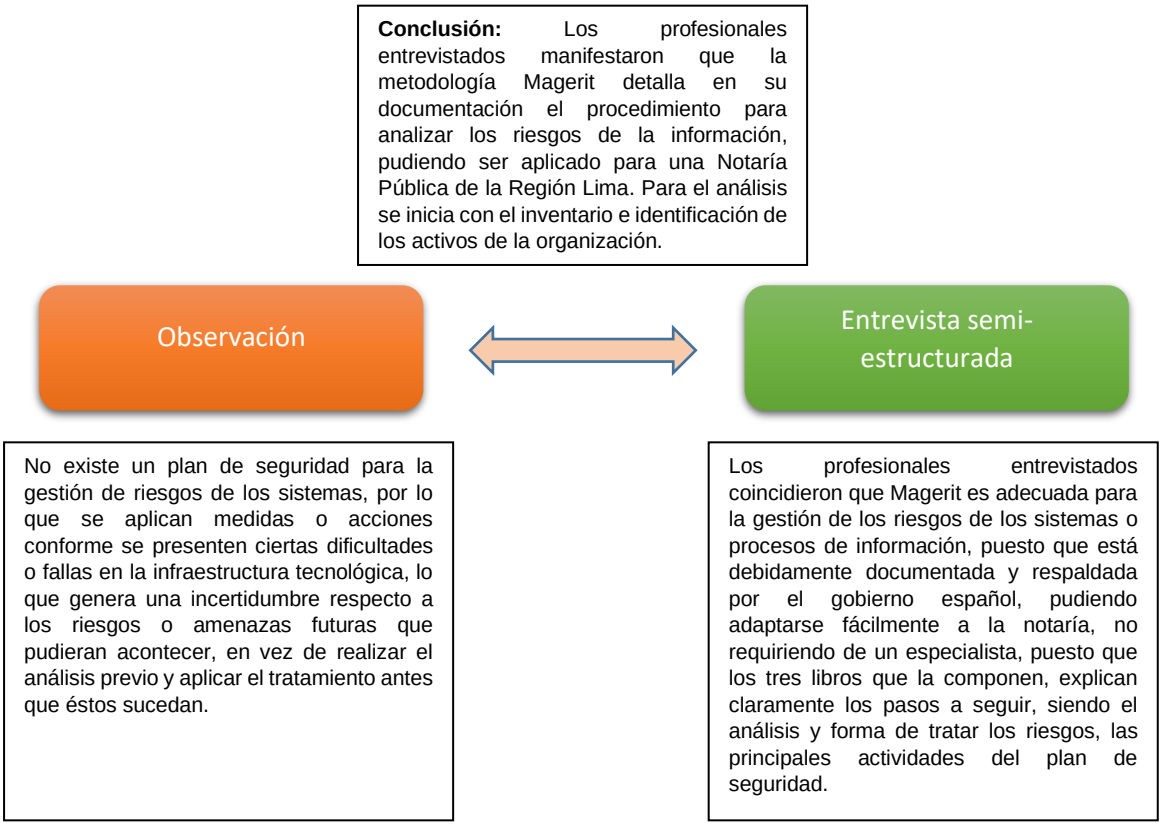
requiere contratar a un especialista, puesto que los tres libros explican claramente los pasos a seguir, coincidiendo que el análisis y tratamiento de riesgos, son las principales actividades para la materialización del plan de seguridad.

Los autores, como Amutio et al. (2014), miembro del equipo que elaboró la metodología de análisis de riesgos de TI “Magerit”, versión 1 y versión 2 y jefe de proyecto de Magerit versión 3, manifestaron que a través de dicha metodología se pretende también concientizar a los encargados de las instituciones, la presencia de diferentes riesgos en los sistemas y procesos de información, así como la exigencia de su adecuada gestión para minimizar el impacto negativo para la organización.

Con las técnicas utilizadas, se evidenció la importancia de contar con el plan de seguridad para la gestión de riesgos de los sistemas de información, con la finalidad de prevenir la aparición de fallos que pudieran afectar la infraestructura tecnológica de la notaría, perjudicando la información o los servicios que prestan a sus clientes. Asimismo, su implementación permitirá dar cumplimiento a la normativa vigente, respecto a la forma de cómo deben tratarse o administrarse los datos personales en las organizaciones públicas y privadas. Por tanto, las técnicas indicadas demuestran que es factible proponer un modelo de gestión de riesgos de información apoyado en Magerit para la Notaría de la Región Lima.

Figura 6

Triangulación de entrevistas y observación



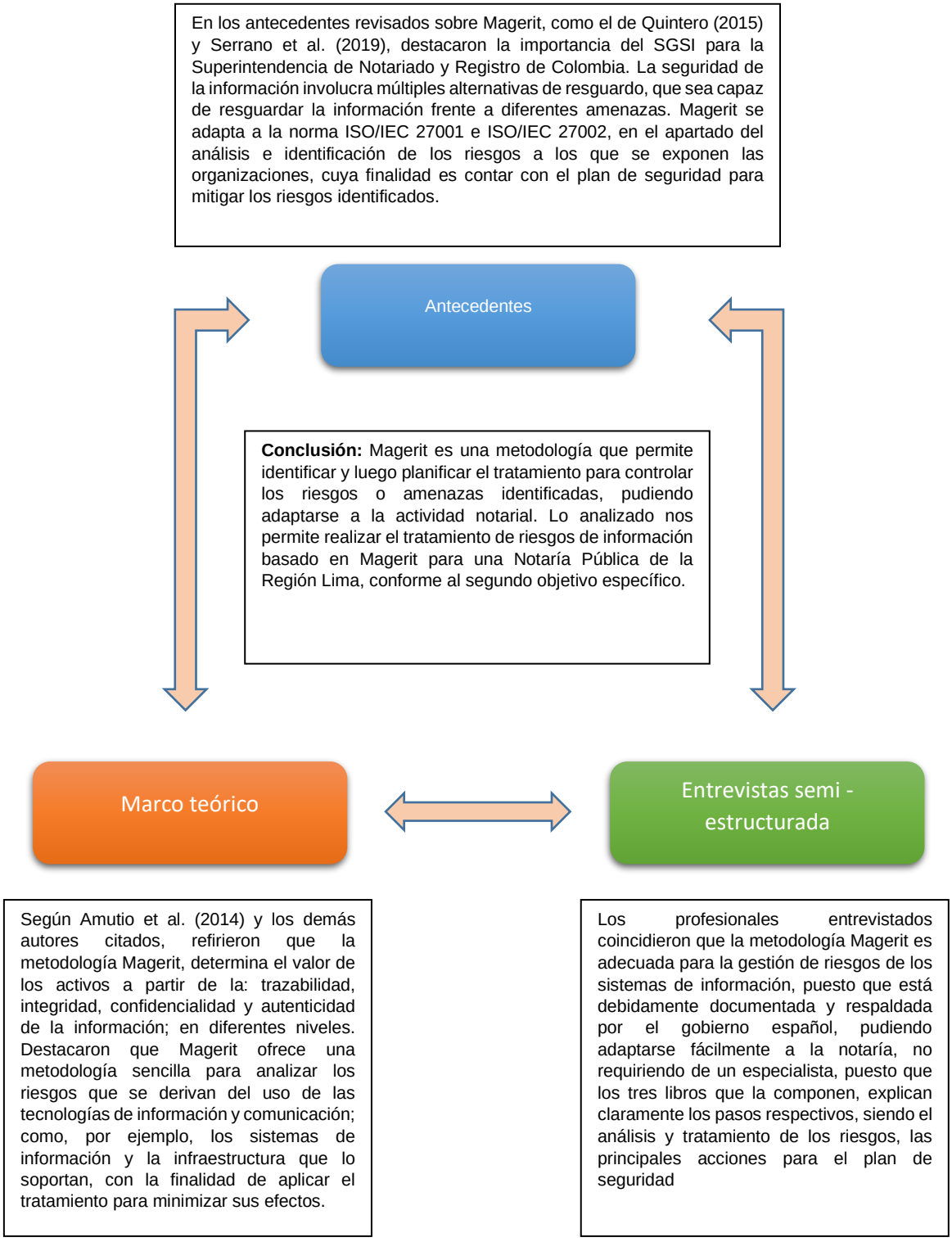
La figura 6, muestra la triangulación de las entrevistas efectuadas a los profesionales especializados en sistemas y riesgos digitales, así como la observación que se realizó a la unidad estudiada, concluyendo que para la gestión de los riesgos se debe realizar su análisis respectivo, partiendo de la identificación y valorización de los activos con los que cuenta la organización, lo que permitirá cumplir el primer objetivo específico del presente trabajo. Emutio et al. (2014) señalaron que al analizar los riesgos se proporciona un modelo de activos, amenazas y salvaguardas. Asimismo, la fase de tratamiento, abarca las acciones tomadas para resguardar la seguridad correspondiente.

Esto coincide con Romero et al. (2010), quienes manifestaron que Magerit categoriza los activos según una estructura jerárquica. De otro lado, los profesionales entrevistados señalaron que Magerit establece cinco pasos para analizar los riesgos: 1) Identificar sus activos, es decir, cualquier componente o funcionalidad del sistema de información que pueda ser atacado 2) Determinar las

amenazas, identificando lo que pudiera afectar los sistemas de información 3) Determinar las salvaguardas, estableciendo los mecanismos de protección para los sistemas de información 4) Estimar el impacto de materializarse una amenaza que pudiera afectar los sistemas de información y, 5) Estimar su riesgo, estimando la perspectiva de materializarse dicha amenaza.

Figura 7

Triangulación de los antecedentes, el marco teórico y las entrevistas



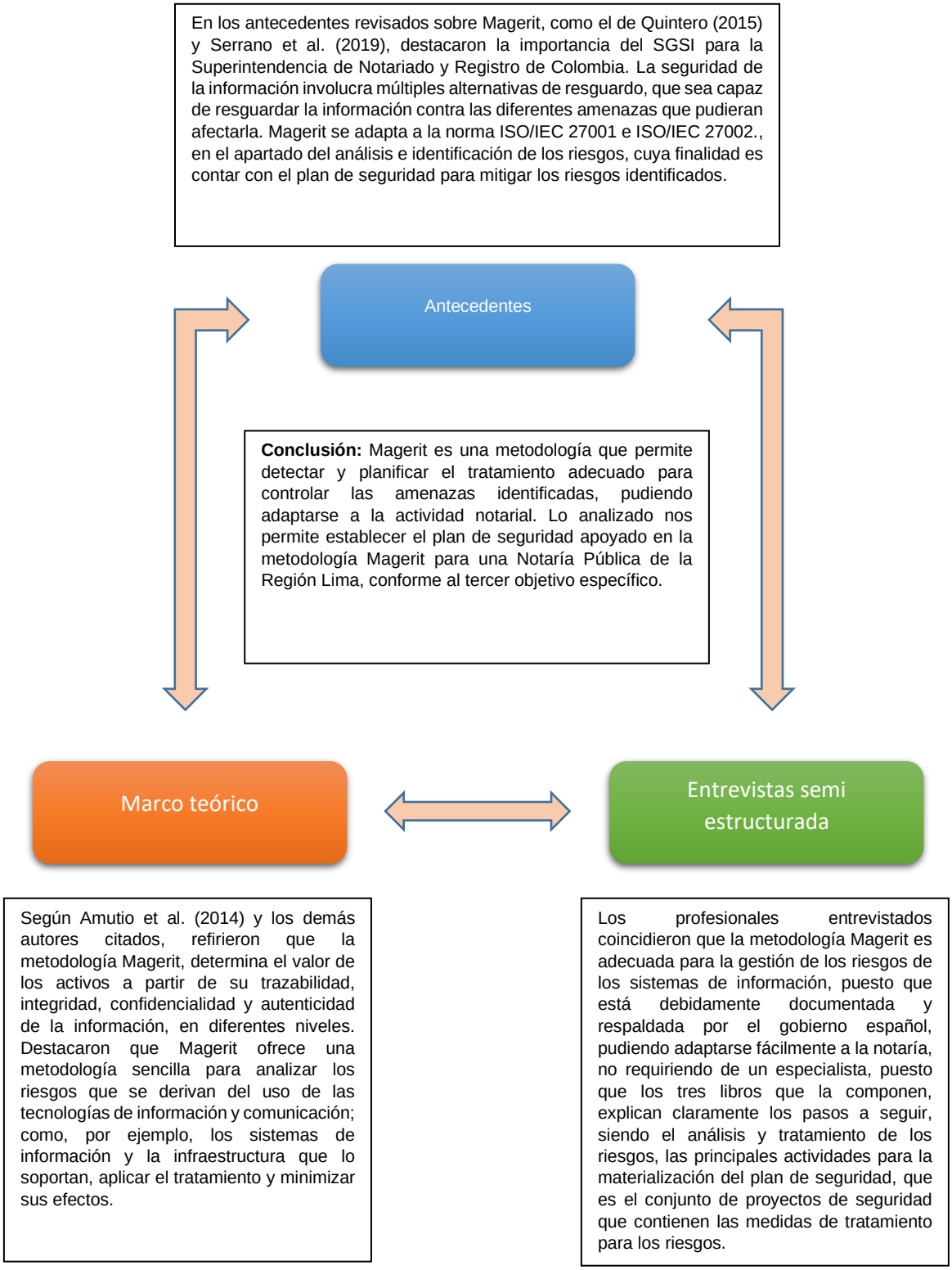
La figura 7 muestra la triangulación de los antecedentes, marco teórico y entrevistas semi estructuradas realizados a profesionales con experiencia en gestión de

riesgos, responde al segundo objetivo específico de la investigación, concluyendo que la metodología Magerit permite determinar el tratamiento de riesgos de información para una Notaría Pública de la Región Lima.

Como señaló Amutio et al. (2014), que la metodología pretende establecer y planificar el tratamiento para conservar los riesgos detectados bajo una vigilancia adecuado y de esa forma minimizar o controlar sus efectos para la organización. Esto implica evaluar la eficacia de los tratamientos que existen relacionados al riesgo que los mismos soportan. Los autores refirieron que a través del tratamiento de riesgos se pretende establecer la defensa necesaria para que no ocurra algo perjudicial y prepararlos para contener las ocurrencias negativas, superar los incidentes que pudiera perjudicar la continuidad de sus operaciones o servicios; sin embargo, cuando no se puede eliminar completamente, éste se aminora a nivel residual, el cual se asume sin mayor dificultad.

Figura 8

Triangulación de los antecedentes, el marco teórico y las entrevistas



Dicha figura 8, muestra la triangulación de los antecedentes, marco teórico y entrevistas semi-estructuradas realizados a profesionales con experiencia en

gestión de riesgos, responde al tercer objetivo específico de la investigación, concluyendo que la metodología Magerit permite establecer el plan de seguridad de información para una Notaría Pública de la Región Lima.

Como señaló Motaki (2016), la metodología Magerit se utiliza para la identificación, análisis y evaluación de los riesgos. Con el resultado de analizar los riesgos, se contará con los valores de las dependencias entre los elementos y el número de amenazas a las que se encuentra expuesta. De igual forma, los profesionales entrevistados coincidieron que el plan de seguridad es el compendio del análisis realizado en la organización y las acciones o tratamiento definido para una adecuada gestión de los riesgos. Para su elaboración se establecen los objetivos, las estrategias de seguridad y la política corporativa de seguridad de tecnologías de información para la institución.

V. CONCLUSIONES

PRIMERA:

Se concluye que el empleo de las tecnologías de información y comunicación (TIC) ha producido enormes ventajas para la sociedad; pero a su vez, se incrementan los riesgos que deben tratarse adecuadamente con disposiciones de seguridad que respalden la confianza de sus usuarios o clientes. En ese sentido, la metodología Magerit es apropiada como modelo de gestión de riesgos de la información apoyado en el uso de la metodología Magerit para una Notaría de la Región Lima, el cual se describe en el Anexo 8.

SEGUNDA:

Se concluye que el análisis de riesgos establece los impactos y riesgos, independientemente de que sea más o menos probable que sucedan. A partir del análisis realizado, se tendrá información importante para la toma de decisiones, sabiendo claramente lo que queremos proteger. El análisis de riesgos puede desarrollarse basado en los pasos establecidos en la metodología Magerit para una Notaría Pública de la Región Lima.

TERCERA:

Se concluye que el tratamiento del riesgo está referido a las actividades destinadas para modificar el riesgo y el proceso de selección e implantación de las salvaguardas necesarias para la continuidad de los sistemas o servicios. El tratamiento implica seleccionar e implantar salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados: Siendo así, se puede determinar el tratamiento de los riesgos basado en la metodología Magerit para una Notaría Pública de la Región Lima.

CUARTA:

Se concluye que el plan de seguridad es el conjunto de acciones que contienen las decisiones para la gestión de riesgos y seguridad de la información. Dicho plan está acorde con los objetivos, estrategia y política de la organización. Asimismo, el plan de seguridad permitirá plasmar las decisiones señaladas para el tratamiento de

riesgos. El plan de seguridad incluye la documentación de políticas que debe comunicarse a todo el equipo de trabajo para su conocimiento y aplicación en lo que les corresponda. Es necesario además que se estipule un tiempo determinado para que se realicen las revisiones cada cierto tiempo a fin de mantenerlas actualizadas. Por tanto, luego del análisis y tratamiento de los riesgos identificados se establece el plan de seguridad de la información apoyado en la metodología Magerit para una Notaría Pública de la Región Lima.

VI. RECOMENDACIONES

PRIMERA

Se sugiere que el encargado del soporte tecnológico recomiende al Notario, la pronta implementación de la metodología Magerit para la adecuada gestión de los riesgos en los sistemas de información utilizados en la Notaría, permitiendo proteger su activo principal que es la información que custodian. Asimismo, se sugiere como siguiente paso, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001/27002.

SEGUNDA

Recomendar al responsable de soporte tecnológico realizar periódicamente el análisis de riesgos, con la finalidad de identificar nuevas amenazas en igual proporción del avance de la tecnología. En ese sentido, es necesario que la notaría realice el proceso de actualización de riesgos a los que pudieran estar en exposición los activos y seleccionar las salvaguardas adecuadas.

TERCERA

Recomendar al responsable de soporte tecnológico realizar la revisión habitual del tratamiento de los riesgos, con la finalidad de aplicar salvaguardas a las nuevas amenazas que pudieran presentarse. En ese sentido, es necesario que la notaría realice el proceso de actualización de riesgos a los que se encuentran expuestos sus activos con la finalidad de aplicar las salvaguardas adecuadas.

CUARTA

Recomendar la revisión del plan de seguridad para la gestión de los riesgos, con la finalidad de identificar nuevas amenazas en igual proporción del avance de la tecnología. En ese sentido, es necesario que la notaría realice el proceso de actualización e identificación de sus activos y consecuentes riesgos, a fin de seleccionar salvaguardas adecuadas. Asimismo, es recomendable la aplicación de nuevos estándares en la contratación de personas es importante para evitar la fuga de información, por lo cual se recomienda agregar cláusulas de confidencialidad en los contratos de trabajo.

REFERENCIAS

Amutio, M., Candau, J. & Mañas, J. (2014). *MAGERIT- V3, methodology for information systems risk analysis and management. Book I - The Method, Ministerio de Administraciones Públicas*. Recuperado de: https://bit.ly/3DMbw9u

Aquino M., Huallpa J., Huillcen H., Carpio E., Palomino F. (2021). *Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division*. Advances in Emerging Trends and Technologies. Advances in Intelligent Systems and Computing. doi.org/10.1007/978-3-030-63665-4_21

Baca G., Solares P., Acosta E. (2014). Administración Informática I: Análisis y Evaluación de Tecnologías de Información. México: Grupo Editorial Patria. ISBN 9786074388626.

Bell, J. (2005). *Cómo hacer tu primer trabajo de investigación*. México: Gedisa.

Blaxter, L.; Hughes, C.; y Tight, M. (2002). *Cómo se hace una investigación.* 2da edición. Barcelona: Gedisa.

Botto-Tobar, M., S. Gómez, O., Rosero Miranda, R., & Díaz Cadena, A. (Eds.). (2021). *Advances in Emerging Trends and Technologies. Advances in Intelligent Systems and Computing*. doi:10.1007/978-3-030-63665-4

Buzdugan, A. (2021). Model for Cyber Security Maturity Assessment in Critical Infrastructures. Buletin Stiintific, 154–156.

Cárdenas-Solano, L.-J., Martínez-Ardila, H., & Becerra-Ardila, L.-E. (2016). Gestión De Seguridad De La Información: Revisión Bibliográfica. El Profesional de La Información, 25(6), 931–948. https://doi.org/10.3145/epi.2016.nov.10

Chicano, E. (2019). *Auditoría de seguridad informática. IFCT0109*. España: IC Editorial. ISBN 9788416433230

Corda, M. C., Viñas, M., & Coria, M. K. (2017). *Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje*. Palabra Clave (La Plata), 7(1), e032. https://doi.org/10.24215/18539912e032

Creswell, J. (2019). *Educational research. Planning, conducting and evaluating quantitative and qualitative research. [Investigación educativa. Planeación, conducción y evaluación en investigación cuantitativa y cualitativa]*. (4ª ed). USA: Pearson.

Daneshjo, N., Malega, P., Kóňa, J., & Barilová, B. (2021). Integrated Management System and Corporate Risk Management. TEM Journal, 10(4), 1686–1693. https://doi.org/10.18421/TEM104-26

David Sutton. (2014). *Information Risk Management: A Practitioner's Guide*. BCS, The Chartered Institute for IT.

Díaz C. (2017). *Investigación cualitativa y análisis de contenido temático. Orientación intelectual de revista Universum*. Revista General de Información y Documentación - Chile. ISSN: 1132-1873. doi: 10.5209/RGID.60813

Escudero, C. & Cortez, L. (2018). *Técnicas y métodos cualitativos para la investigación científica*. Editorial UTMACH, Ecuador. ISBN: 978-9942-24-092-7.

Fernandez, A., & Garcia, D. F. (2016). *Complex vs. simple asset modeling approaches for information security risk assessment: Evaluation with MAGERIT methodology. 2016 Sixth International Conference on Innovative Computing Technology (INTECH)*. doi:10.1109/intech.2016.7845064

Figueira, P. T., Bravo, C. L., & López, J. L. R. (2019). *Improving information security risk analysis by including threat-occurrence predictive models*. Computers & Security, 101609. doi: 10.1016/j.cose.2019.101609

Folgueiras, P. (2016). *Técnica de recogida de información: La entrevista*. Diposit Digital de la Universitat de Barcelona, España. Disponible en http://hdl.handle.net/2445/99003

Fuentealba, N. & Cruz, A. (2018). *Liability of the state administration for cybersecurity breaches [La responsabilidad de la Administración del Estado por incidentes de ciberseguridad]*. Revista Chilena de Derecho y Tecnología. doi: 10.5354/0719-2584.2021.58776

Garay, D. F. C., Carbajal Ramos, M. A., Armas-Aguirre, J., & Molina, J. M. M. (2020). *Information security risk management model for mitigating the impact on SMEs in Peru*. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI). doi:10.23919/cisti49556.2020.9140980

Garcia, F. Y. H., & Moreta, L. M. L. (2018). *Maturity Model for the Risk Analysis of Information Assets based on Methodologies MAGERIT, OCTAVE y MEHARI*; focused on Shipping Companies. 2018 7th International Conference On Software Process Improvement (CIMPS). doi:10.1109/cimps.2018.8625848

Gil Mena, F. (2018). Redacción. Ciberseguridad: El 70% del valor de una empresa puede ser afectado tras un ataque informático. Gestión [online]. 27 septiembre 2018. [Accesado 27 octubre 2021]. Disponible: https://gestion.pe/tecnologia/ciberseguridad-70-empresa-afectadoataque-informatico-245430-noticia/

Giménez, J. (2015). *Seguridad en equipos informáticos. IFCT0109*. España. IC Editorial. ISBN: 9788416433247.

Global Risk Landscape (2019). *Global Risks Report*, World Economic Forum. Disponible en https://www.weforum.org/reports/the-global-risks-report-2019

Guzmán, G. (2015). *Metodología para la seguridad de tecnologías de información y comunicaciones en la Clínica Ortega*. (Tesis de posgrado, Magíster en Ingeniería de Sistemas con mención en Gerencia de Tecnología de Información y Comunicación). Universidad Nacional del Centro del Perú. Perú. Disponible en: http://hdl.handle.net/20.500.12894/1478

Hernán-García, M., Lineros-González, C., Ruiz-Azarola, A. (2020). *Cómo adaptar una investigación cualitativa a contextos de confinamiento*. Gaceta Sanitaria, Volume 35, España. doi: 10.1016/j.gaceta.2020.06.007

Hernández, R. & Mendoza, C. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. México: Mc Graw Hill Educación. Disponible en http://repositorio.uasb.edu.bo/handle/54000/1292

Jimeno, J. (2017). *La responsabilidad civil en el ámbito de los ciberriesgos*. Madrid: Fundación Mapfre. Disponible en https://www.fundacionmapfre.org/publicaciones/todas/responsabilidad-civil-ciberriesgos/

Laudon, K. C., & Laudon, J. P. (2017). *Sistemas de información gerencial* (Décimo cuarta edición). México D.F.: Pearson Educación.

Llontop Díaz, G. C. (2018). *Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks* (Tesis de Maestria). Lima. Disponible en: https://repositorio.ucv.edu.pe/handle/20.500.12692/17596

Maquera, H. (2015). *Diseño de seguridad para salvaguardar activos de información en el campus de la UNCP*. Revista Ciencia & Desarrollo de la Universidad Nacional Jorge Basadre Grohmann. Tacna, Perú. doi: 10.33326/26176033.2015.20.520

Mallqui, M. (2015). *Consideraciones generales sobre la importancia del derecho notarial en el Perú*. Número 09 Revista de Investigación Jurídica de la Universidad Católica Santo Toribio de Mogrovejo. Chiclayo, Perú. ISSN2222-9655

McKinsey&Company (2018). *Perspectiva de seguridad en México*. Ciberseguridad de COMEXI - Consejo Mexicano de Asuntos Internacionales, México. Disponible en https://consejomexicano.org/multimedia/1528987628-817.pdf

Motaki, K. (2016). *Risk Analysis and Risk Management in Critical Infrastructures (Tesis de maestría). University of Piraeus*. Recuperado de: http://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/9741/Motaki_Katerina.pdf?sequence=1&isAllowed=y

Najar, J. (2017). *Exposición del activo más valioso de la organización, "la información".* Visión Electrónica. Colombia. doi: 10.14483/22484728.12345

OCDE, Organización para la Cooperación y el Desarrollo Económicos (2020). Perspectivas económicas de América Latina 2020: *Transformación digital para una mejor reconstrucción*. Disponible en bit.ly/3dbPt0Z

Quintero, L (2015). *Sistema de Gestión de Seguridad de la Información para el Departamento de Informática de la Superintendencia de Notariado y Registro*. (Tesis de grado, especialista en seguridad informática). Universidad Nacional Abierta y a Distancia – UNAD. Colombia. Disponible en: https://bit.ly/3oxn3EW

Romero M., B. D., & Haddad, H. M. (2010). *Asset Assessment in Web Applications*. 2010 Seventh International Conference on Information Technology: New Generations. doi:10.1109/itng.2010.170

Ros García, J. (2018). Auge de los Sistemas de Información y Documentación en las Organizaciones (Acerca del libro de James A. Senn). Cuadernos de Documentación Multimedia, 2, 5-10. Recuperado 8 de diciembre de 2021, de https://revistas.ucm.es/index.php/CDMU/article/view/59337

Sanchez, M., Fernández, M., Díaz, J. (2021). *Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo*. Revista Científica UISRAEL, Vol. 8 Núm. 1, Ecuador. doi: 10.35290/rcui.v8n1.2021.400

Santos Olmo Parra, A., Sanchez Crespo, L. E., Alvarez, E., Huerta, M., & Fernandez Medina Paton, E. (2016). *Methodology for Dynamic Analysis and Risk Management on ISO27001*. IEEE Latin America Transactions, 14(6), 2897–2911. doi:10.1109/tla.2016.7555273

Selviyanti, E. & Sardjono W. (2020). *Risk management information systems assessment at the television broadcasting company*. Journal of Physics: Conference Series. 1465(1),012016. doi:10.1088/1742-6596/1465/1/012016

Serrano J., Salazar V., Ruiz, X., Guillén, C. (2019). ICT risk management in public hospitals [Gestión de riesgos de TIC en hospitales públicos]. Associacao Iberica de Sistemas e Tecnologias de Informacao. (E20), pp. 280-291. ISSN 16469895.

Tambini Avila, M. (2014). *Manual de derecho notarial*. Lima, Perú: Editorial Instituto Pacífico. ISBN: 9786124118876

Tarrillo, E. (2016). *Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015.* (Tesis de

maestría). Universidad César Vallejo, Lima, Perú. Recuperado de: https://bit.ly/3BMHW34

Toapanta, S. M. T., Maldonado, N. M. M., Gallegos, L. E. M., & Solis, M. P. (2020). *Security Prototype to Determine Critical Information and Improve the Management of a Public Organization. 2020 Asia Conference on Computers and Communications* (ACCC). doi:10.1109/accc51160.2020.9347902

Toapanta, S., Terán, Y., Naranjo, B., Mafla L. (2020). *Security and Privacy in Information Management in a Distributed Environment for Public Organizations*. Fuzzy Systems and Data Mining VI - A.J. Tallón-Ballesteros (Ed.). doi:10.3233/FAIA200716

Usländer, T. (2014). *Requirements and Open Architecture for Environmental Risk Management Information Systems.* Information systems for emergency management / p. 344–368. Print. ISBN: 0-7656-2134-7.

Van Dijk, N., Tanas, A., Rommetveit, K., & Raab, C. (2018). Right engineering? The redesign of privacy and personal data protection. International Review of Law, Computers & Technology, 32(2/3), 230–256. https://doi.org/10.1080/13600869.2018.1457002

Vicente, E., Mateos, A., & Jiménez-Martín, A. (2014). *Risk analysis in information systems: A fuzzification of the MAGERIT methodology. Knowledge-Based Systems*, 66, 1–12. doi:10.1016/j.knosys.2014.02.018

Constitución Política del Perú (1993).

Ley n.º 29733. Ley de Protección de Datos Personales (03 de julio 2011). Normas Legales, nº 445746. Diario Oficial El Peruano.

Ley n.º 27567. Ley que modifica los artículos 21° y 128° de la Ley del Notariado y crea los distritos notariales de Tacna; de Moquegua; de Huánuco y Pasco; y de Ucayali (29 de noviembre de 2001). Normas Legales, nº 35530. Diario Oficial El Peruano.

Decreto Legislativo nº 1049. Decreto Legislativo del Notariado (26 de junio de 2008). Normas Legales, nº 374811. Diario Oficial El Peruano.

Decreto Supremo nº 010-2010-JUS. Aprueban Texto Único Ordenado del Reglamento del Decreto Legislativo Nº 1049, Decreto Legislativo del Notariado (23 de julio de 2010). Normas Legales, nº 422679. Diario Oficial El Peruano.

Decreto Supremo nº 003-2013-JUS. Reglamento de la Ley N° 29733 Ley de Protección de Datos Personales (22 de marzo de 2013). Normas Legales, nº 491320. Diario Oficial El Peruano.

Resolución Ministerial n.º 004-2016-PCM, Norma Técnica Peruana ISO 27001 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información (14 de enero de 2016). Normas Legales, nº 575410. Diario Oficial El Peruano.

Gobierno de España - Administración Electrónica (2012), *Magerit V3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Disponible en: https://bit.ly/3DMbw9u

Anexo 1

Matriz de Categorización

Título: Gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021 (1 y 2)
Autor: Ampuero Herrera Renato Mario

Problema General	Objetivo General	Categorías	Subcategorías	Técnicas	Instrumentos
¿En qué consiste la gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021?	Proponer un modelo de gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021	Análisis de riesgos (3)	▪ Determinar los activos ▪ Determinar las amenazas ▪ Determinar las salvaguardas ▪ Estimar el impacto ▪ Estimar el riesgo	Entrevista Semi estructurada	Guía de Entrevista
Problemas Específicos	**Objetivos Específicos**				
¿Cómo se debe analizar los riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021?	Analizar los riesgos de la información basado en la metodología Magerit para una Notaría Pública de la Región Lima, 2021	Tratamiento de riesgos (4)	▪ Eliminación ▪ Mitigación ▪ Compartición ▪ Financiación	Observación	Guía de observación
¿En qué consiste el tratamiento de los riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021?	Determinar el tratamiento de los riesgos de la información basado en la metodología Magerit para una Notaría Pública de la Región Lima, 2021	Plan de seguridad (5,6)	▪ Identificación de proyectos de seguridad ▪ Plan de ejecución ▪ Ejecución	Análisis documental	Ficha de análisis documental
¿En qué consiste el plan de seguridad de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021?	Establecer el plan de seguridad de la información basado en la metodología Magerit para una Notaría Pública de la Región Lima, 2021				

uente: Amutio et al. (2014).

ANEXO 2:

Gestión de riesgos de la información basado en la metodología Magerit para una Notaría de la Región Lima, 2021

Guía de entrevista semi estructurada

1. ¿Considera adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría pública de la Región Lima?
2. ¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información?
3. ¿Cómo analizar la gestión de riesgos de la información en dicha organización?
   a. ¿Cómo se determinan los activos?
   b. ¿Cómo se determinan las amenazas?
   c. ¿Cómo se determinan las salvaguardas de la información?
   d. ¿Cómo se estima el impacto de una amenaza detectada?
   e. ¿Cómo se estima el riesgo frente a una amenaza detectada?
4. ¿En qué consiste el tratamiento de riesgos de la información en tal organización?
   a. ¿Cómo se eliminan los riesgos y en qué casos?
   b. ¿Cómo se mitigan los riesgos?
   c. ¿En qué consiste la compartición del riesgo?
   d. ¿En qué consiste la financiación del riesgo?
5. ¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?

a. ¿Cómo se realiza la identificación de proyectos de seguridad?

b. ¿En qué consiste el plan de ejecución?

c. ¿Cómo se realiza la ejecución del plan de seguridad?

6. ¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría?

Anexo 3

Matrices de desgravación de las entrevistas

N°	Preguntas	**Entrevistado 1** – Especialista en seguridad y sistemas integrados de gestión
1	¿Es adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría de la Región Lima?	Si. Magerit es una metodología de origen del gobierno español que permite la gestión de riesgos de los sistemas de información de las organizaciones públicas o privadas. Esta metodología está explicada en tres libros, los cuales detallan los pasos secuenciales para la gestión de riesgos. Por ejemplo, el Libro I establece una serie de procedimientos que permitirán asegurar la información. En cuanto a las notarías si bien es cierto son de origen privado, pero brindan un servicio público; por ende, manejan información sumamente importante para el desarrollo de las actividades económicas de la comunidad y son parte de la seguridad jurídica.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información?	Las organizaciones deben asegurarse que la información que manejan no sea vulnerada y para ello deben invertir para salvaguardar sus sistemas informáticos cuya información constituye el activo más importante, con la finalidad de evitar el robo, sabotaje, adulteración o uso no autorizado por terceros o hackers que pueden provocar la desconfianza de los usuarios en dichas organizaciones y peligrar su continuidad. La metodología establece dos pasos fundamentales: primero el análisis y, segundo, el tratamiento de riesgos, los cuales constituyen la gestión de riesgos.
3	¿Cómo analizar la gestión de riesgos de la información en dicha organización?	El análisis de riesgos consta de cinco pasos: Determinar o identificar los activos, es decir, la información y los servicios que brinda la organización. Determinar las amenazas a las que está expuesta la notaría, es decir, las circunstancias que pueden ocurrir y afectar o causarle daño. Determinar las salvaguardas o mecanismos para reducir las amenazas frente a los riesgos identificados. Estimar el impacto de una amenaza detectada, que se define como la afectación sobre el activo generado por la materialización de la amenaza identificada. Estimar el riesgo frente a una amenaza detectada, lo que significa como el impacto ponderado con la probabilidad de que se materialice la amenaza.
4	¿En qué consiste el tratamiento de riesgos de la información en tal organización?	Implica que una vez identificado el riesgo que puede convertirse en amenaza para la organización, se debe establecer el tratamiento, es decir, la forma de eliminarlo, mitigarlo, compartir y los recursos financieros para llevarlo a cabo. Como parte del tratamiento de los riesgos de los sistemas de información se debería considerar las restricciones de acceso al sistema informático notarial mediante la determinación de perfiles de usuario, la protección del hardware, la identificación del software no autorizado y control de acceso a la red local. También se puede

		considerar la revisión periódica del antivirus, software autorizado instalado, como parte de la protección de aplicaciones informáticas.
5	¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?	Consiste en planificar las medidas oportunas para mantener los riesgos bajo control adecuado. Comprende la identificación de proyectos de seguridad, establecer un plan de ejecución y la ejecución misma del plan de seguridad elaborado para controlar los riesgos identificados. Se pudiera decir que el plan de seguridad es el compendio del análisis realizado en la organización y las acciones o tratamiento definido para una adecuada gestión de los riesgos de los sistemas de información.
6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría?	El plan de seguridad permite materializar las decisiones de la gestión de riesgos. Implica también en concientizar la colaboración de las personas involucradas en los sistemas de información, acerca de su importancia y pertinencia. El plan elaborado debe ser revisado anualmente para la mejora continua. Contar con un plan de seguridad para la gestión de riesgos, preparará a la organización para los procesos de evaluación, auditoría, certificación o acreditación, lo que constituye un valor agregado para la imagen y confianza en la organización.

N°	Preguntas	**Entrevistado 2** – Especialista en seguridad de sistemas de información
1	¿Considera adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría de la Región Lima?	En primer lugar, debo manifestar que las diferentes organizaciones almacenan su información de manera estructurada o no estructurada en sistemas de información, los cuales se enfrentan a diversos peligros, riesgos o amenazas. De allí radica la importancia que la información que gestionan tenga la debida protección. La metodología Magerit es adecuada para el análisis y gestión de riesgos de los sistemas informáticos, lo cual permitirá que las organizaciones como, por ejemplo, las notarías puedan gestionar los riesgos que afecten o vulneren sus sistemas de información. Magerit contiene métodos sencillos para realizar el diagnóstico sobre el estado de la seguridad de los sistemas de información y aquello que pudiera afectar su continuidad. Este análisis permitirá establecer la política o plan de seguridad para la gestión de los riesgos previamente detectados.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información en dicha organización?	Hay dos pasos básicos, consistente en el análisis de riesgos y luego el tratamiento o salvaguardas para reducir el impacto de los mismos en los sistemas de información. Eso significa que se tendría que analizar los sistemas de información que utiliza la notaría para brindar sus servicios a los usuarios. Magerit es práctica porque cuenta con tres libros que detallan el uso y aplicación de la metodología para la gestión de los riesgos, no siendo necesario contar con un especialista para su aplicación en la notaría u otra organización. Es importante mencionar que esta metodología se adapta a las normativas internacionales ISO 27001 e ISO 31000, siendo la parte inicial para la implementación de un sistema de gestión de seguridad de la información.

3	¿Cómo analizar la gestión de riesgos de la información en dicha organización?	Magerit establece el método de análisis de riesgos y los cinco pasos que deben seguirse que está contemplado en su primer libro: 1) Identificar los activos de la notaría, que se refiere a cualquier componente o funcionalidad del sistema de información que pueda ser atacado en forma deliberada o accidental 2) Determinar las amenazas, identificando lo que pudiera afectar los sistemas de información, que utiliza en este caso la notaría 3) Determinar las salvaguardas, estableciendo los mecanismos de protección para los sistemas de información, como puede ser protección de los equipos, copias de respaldo, entre otros 4) Estimar el impacto de materializarse una amenaza y el grado de perjuicio que una seguridad insuficiente pudiera afectar a la notaría 5) Estimar el riesgo, estimando la expectativa de materialización de la amenaza. Parte importante del análisis es la identificación de los activos y para mayor facilidad, Magerit lo clasifica en cinco categorías: primera, el entorno del sistema de Información, por ejemplo, equipamiento, suministros, personal e instalación física. Segunda, el sistema de información, referido al hardware, software y comunicaciones. En tercer lugar, la información datos, meta-información y soportes. En cuarto lugar, las funcionalidades de la organización, como objetivos y misión de la organización, los bienes y servicios que produce, el personal usuario/destinatario de los bienes o servicios que se produce. Finalmente, otros activos, que no se haya mencionado en las categorías anteriores.

4	¿En qué consiste el tratamiento de riesgos de la información en tal organización?	Consiste en establecer los procedimientos operativos para el tratamiento de los riesgos identificados, mediante la implantación de medidas o salvaguardas para la prevención, reducción o control de los riesgos que se identificaron en la organización. Es importante que en dicho tratamiento se seleccionen y apliquen las medidas más apropiadas para reducir el riesgo, evitarlo, eliminarlo o transferirlo. En ese sentido, se debe tener en cuenta la protección de los equipos informáticos, la protección de las comunicaciones, así como los sistemas de información utilizados como soporte en la gestión documental. Verificar el cumplimiento de las condiciones físicas donde se encuentran los servidores para verificar el cumplimiento de la normativa correspondiente. También debe establecerse los planes de contingencia frente a caídas del sistema o servicios informáticos de apoyo notarial y programar las copias de seguridad (backups) periódicamente en la nube.
5	¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?	Con la información recopilada luego del análisis de riesgos, se genera el plan de seguridad para la gestión de riesgos de los sistemas de información, donde es importante involucrar a los colaboradores en particular los que utilizan los sistemas informáticos. El plan de seguridad significa la materialización del estudio realizado mediante el análisis y tratamiento de los riesgos e incluye el cronograma y la ejecución del mismo, mediante acciones concretas.
6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría?	Magerit genera beneficios para las organizaciones puesto que permite analizar aquellos riesgos internos o externos que pueden convertirse en amenazas para los sistemas de información. Es importante reconocer que los riesgos no desaparecerán, sino que irán incrementándose con el avance y desarrollo tecnológico. El plan de seguridad para la gestión de riesgos de la información preparará a la organización para una certificación o acreditación que además de proteger sus activos también mejore su imagen tan importante en nuestra actualidad competitiva.

N°	Preguntas	**Entrevistado 3** – Especialista en gestión de riesgos
1	¿Considera adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría de la Región Lima?	De acuerdo a mi experiencia, Magerit es una metodología apropiada para investigar los riesgos que pudieran afectar los sistemas de información de cualquier organización, como las notarías, para luego recomendar las medidas para controlar los riesgos detectados. Dicha metodología es de uso gratuito y está bien documentada y respaldada por el gobierno español. En el caso de las notarías, gestionan información importante y en ocasiones confidencial de parte de sus usuarios. Por tanto, al brindar un servicio público están en la obligación de resguardar la información que almacenan, de conformidad con la normativa vigente.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información en una notaría?	Magerit tiene dos objetivos principales: estudiar o analizar los riesgos y recomendar las medidas para prevenir, impedir, disminuir o controlar tales riesgos.

3	¿Cómo analizar la gestión de riesgos de la información en dicha organización?	Debo resaltar que esta etapa constituye el núcleo principal de Magerit, por lo que de su correcta aplicación depende la validez de todo el proyecto. El objetivo principal es la evaluación del riesgo del sistema en estudio. Comprende seis etapas, como son el recojo de información, identificación y agrupación de los activos, identificación y evaluación de las amenazas, identificación y estimación de las vulnerabilidades, identificación y valoración de los impactos y la evaluación de los riesgos. En la primera etapa, el recojo de información del sistema y los factores que influyen en la seguridad, comprende preparar la información necesaria, realizar entrevistas y analizar la información recolectada. En la segunda actividad, se identifican los activos y cómo están relacionados, profundizando sus características en base a la información recogida e incluye identificar y agrupar activos, identificar los mecanismos de salvaguarda existentes y valorar los activos. La tercera actividad, consiste en identificar y agrupar las amenazas, así como establecer los árboles de fallos generados por las amenazas. En la cuarta actividad, se identifican las vulnerabilidades y estimar las vulnerabilidades. En la quinta actividad se identifican los impactos, tipifican los impactos y valoran los impactos. Mientras que, en la sexta etapa, se evalúa el riesgo intrínseco, analizan las salvaguardas y evalúa el riesgo efectivo y residual.
4	¿En qué consiste el tratamiento de riesgos de la información en tal organización?	En esta etapa se eligen los mecanismos de tratamiento o salvaguarda, tomando como base su efectividad. Se estudian sus tipos, costos y relaciones, analizando si existen contraindicaciones para su aplicación. Finalmente, se establece el orden para su implantación. Dentro del tratamiento se priorizan los mecanismos necesarios, evalúan los recursos, el cronograma y se integran los resultados. Es recomendable implementar un sistema para el registro de incidencias y alertas.

5	¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?	La gestión de la seguridad de los sistemas de información incluye analizar los requerimientos de seguridad y establecer un plan para satisfacer tales requerimientos. Todas las actividades anteriores se plasman en el plan de seguridad, que incluye el mantenimiento y administración de la seguridad. Para su elaboración se establecen los objetivos, las estrategias de seguridad y la política corporativa de seguridad de tecnologías de la información para la organización. Como parte de esta política de seguridad corporativa está la instauración de una estructura organizacional apropiada para asegurar que los objetivos definidos por la institución se puedan alcanzar. Asimismo, el propósito del Plan de Seguridad es brindar una visión general de los requerimientos de seguridad del sistema de información y determinar los controles necesarios para alcanzar dichos requerimientos. En dicho plan, se delimitan las responsabilidades de toda persona o usuario que tenga acceso al sistema informático. A través del Plan de Seguridad se establecen las salvaguardas para proteger la información y los recursos tecnológicos.
6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría	Contar con un plan de seguridad en la notaría, permitirá resguardar la Información, los sistemas informáticos e instalaciones que sirven de soporte. Al realizar la gestión de riesgos, en este caso, con la metodología Magerit, podrán reducir o minimizar los riesgos y amenazas a los activos de la organización. Sin embargo, dicho plan debe ser revisado periódicamente, puesto que las amenazas van incrementándose con el desarrollo de la tecnología, apareciendo amenazas más destructivas, por ello, es necesario siempre contar con un plan de seguridad actualizado y revisado periódicamente, capaz de gestionar las nuevas vulnerabilidades o amenazas para la seguridad de la institución.

Anexo 4

Matriz de codificación de entrevista

N°	Preguntas	**Entrevistado 1** – Especialista en seguridad y sistemas integrados de gestión	**Entrevistado 1 - Codificada**
1	¿Considera adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría de la Región Lima?	Si. Magerit es una metodología de origen del gobierno español que permite la gestión de riesgos de los sistemas de información de las organizaciones públicas o privadas. Esta metodología está explicada en tres libros, los cuales detallan los pasos secuenciales para la gestión de riesgos. Por ejemplo, el Libro I establece una serie de procedimientos que permitirán asegurar la información que gestionan diferentes organizaciones. En cuanto a las notarías si bien es cierto son de origen privado, pero brindan un servicio público; por ende, manejan información sumamente importante para el desarrollo de las actividades económicas de la comunidad. Toda organización debe asegurarse que la información que manejan no sea vulnerada, evitar el robo, sabotaje, adulteración o uso no autorizado por terceros o hackers	• Magerit permite la gestión de riesgos de los sistemas de información. • Consta de III Libros documentados. • El Libro I, establece cómo asegurar la información. • Las notarías brindan un servicio público. • Manejan información importante de los usuarios. • Se debe asegurar que la información no sea vulnerada, robo, sabotaje, adulteración o accesos no autorizados.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información en una notaría?	Primeramente, las organizaciones deben invertir para salvaguardar sus sistemas informáticos que almacenan la información que gestionan, lo cual constituye el activo más importante, con la finalidad de conservar la confianza de los usuarios y su permanencia en el mercado competitivo. La metodología establece dos pasos fundamentales: primero el análisis de riesgos y, segundo, el tratamiento de los riesgos, los cuales constituyen la gestión de riesgos.	• Análisis de riesgos. • Tratamiento de los riesgos.
3	¿Cómo analizar la gestión de riesgos de la información para una notaría?	El análisis de riesgos consta de cinco pasos: Determinar o identificar los activos, es decir, la información y los servicios que brinda la organización. Determinar las amenazas a las que está expuesta la notaría, es decir, las circunstancias que pueden ocurrir y	• Identificar los activos. • Identificar las amenazas. • Determinar las salvaguardas. • Estimar el impacto de la amenaza. • Estimar el riesgo frente a la amenaza.

		afectar o causarle daño. Determinar las salvaguardas o mecanismos para reducir las amenazas frente a los riesgos identificados. Estimar el impacto de una amenaza detectada, que se define como la afectación sobre el activo generado por la materialización de la amenaza identificada. Estimar el riesgo frente a una amenaza detectada, lo que significa como el impacto ponderado con la probabilidad de que se materialice la amenaza.	
4	¿En qué consiste el tratamiento de riesgos de la información para una notaría?	Implica que una vez identificado los riesgos que pueden convertirse en amenaza para la organización, se debe establecer el tratamiento, es decir, la forma de eliminarlo, mitigarlo, compartir y financiar el riesgo. Como parte del tratamiento de los riesgos de los sistemas de información se debería considerar las restricciones de acceso al sistema informático notarial mediante la determinación de perfiles de usuario, la protección del hardware, la identificación del software no autorizado y control de acceso a la red local. También se puede considerar la revisión periódica del antivirus, software autorizado instalado, como parte de la protección de aplicaciones informáticas.	• Establecer la forma de eliminar, mitigar, compartir y financiar los riesgos identificados. • Restricción al sistema informático. • Perfiles de usuario. • Protección de los equipos informáticos. • Identificación del software no autorizado. • Acceso restringido a la red local. • Revisión del antivirus. • Revisión del software instalado.
5	¿Cómo elaborar el plan de seguridad para la gestión de riesgos de la información?	Consiste en planificar las medidas oportunas para mantener los riesgos bajo control adecuado. Comprende la identificación de proyectos de seguridad, establecer un plan de ejecución y la ejecución misma del plan de seguridad elaborado para controlar los riesgos identificados. Se pudiera decir que el plan de seguridad es el compendio del análisis realizado en la organización y las acciones o tratamiento definido para una adecuada gestión de los riesgos de los sistemas de información.	• Planificar acciones. • Identificar proyecto de seguridad. • Establecer el plan de ejecución. • Comprende el análisis y tratamiento establecido para la organización.
6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la	El plan de seguridad permite materializar las decisiones de la gestión de riesgos permitiendo mejorar la seguridad de los sistemas de información. Implica también en concientizar la colaboración de las personas involucradas	• Mejora la seguridad de los sistemas de información. • Permite concientizar la colaboración y participación de los trabajadores.

	información en una notaría	en los sistemas de información, acerca de su importancia y pertinencia. El plan elaborado debe ser revisado anualmente para la mejora continua. Contar con un plan de seguridad para la gestión de riesgos, preparará a la organización para los procesos de evaluación, auditoría, certificación o acreditación, lo que constituye un valor agregado para la imagen y confianza en la organización.	• Genera un valor agregado como es en la imagen y confianza hacia la organización.

N°	Preguntas	**Entrevistado 2** – Especialista en seguridad de sistemas de información	**Entrevistado 2 - Codificada**
1	¿Considera adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría de la Región Lima?	En primer lugar, debo manifestar que las diferentes organizaciones almacenan su información de manera estructurada o no estructurada en sistemas de información, los cuales se enfrentan a diversos peligros, riesgos o amenazas. De allí radica la importancia que la información que gestionan tenga la debida protección. La metodología Magerit es adecuada para el análisis y gestión de riesgos de los sistemas informáticos, lo cual permitirá que las organizaciones como, por ejemplo, las notarías puedan gestionar los riesgos que afecten o vulneren sus sistemas de información. Magerit contiene métodos sencillos para realizar el diagnóstico sobre el estado de la seguridad de los sistemas de información y aquello que pudiera afectar su continuidad. Este análisis permitirá establecer la política o plan de seguridad para la gestión de los riesgos previamente detectados. Es importante mencionar que esta metodología se adapta a las normativas internacionales ISO 27001 e ISO 31000, siendo la parte inicial para la implementación de un sistema de gestión de seguridad de la información.	• Magerit es adecuada para el análisis y gestión de riesgos de los sistemas informáticos. • Magerit contempla métodos para diagnosticar el estado de la seguridad. • Permite establecer la política o plan de seguridad. • Se adapta a las normas ISO 27001 e ISO 31000.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información en dicha organización?	Hay dos pasos básicos, consistente en el análisis de riesgos y luego el tratamiento o salvaguardas para reducir el impacto de los mismos en los sistemas de información. Eso significa que se tendría que analizar los sistemas de información que utiliza la notaría para brindar sus servicios a los usuarios. Magerit es práctica porque cuenta con tres libros que detallan el	• Analizar los riesgos. • Aplicar el tratamiento o salvaguardas para los riesgos identificados.

		uso y aplicación de la metodología para la gestión de los riesgos, no siendo necesario contar con un especialista para su aplicación en la notaría u otra organización.	
3	¿Cómo analizar la gestión de riesgos de la información en dicha organización?	Magerit establece el método de análisis de riesgos y los cinco pasos que deben seguirse que está contemplado en su primer libro: 1) Identificar los activos de la notaría, que se refiere a cualquier componente o funcionalidad del sistema de información que pueda ser atacado en forma deliberada o accidental 2) Determinar las amenazas, identificando lo que pudiera afectar los sistemas de información, que utiliza en este caso la notaría 3) Determinar las salvaguardas, estableciendo los mecanismos de protección para los sistemas de información, como puede ser protección de los equipos, copias de respaldo, entre otros 4) Estimar el impacto de materializarse una amenaza y el grado de perjuicio que una seguridad insuficiente pudiera afectar a la notaría 5) Estimar el riesgo, estimando la expectativa de materialización de la amenaza. Parte importante del análisis es la identificación de los activos y para mayor facilidad, Magerit lo clasifica en cinco categorías: primera, el entorno del sistema de Información, por ejemplo, equipamiento, suministros, personal e instalación física. Segunda, el sistema de información, referido al hardware, software y comunicaciones. En tercer lugar, la información datos, meta-información y soportes. En cuarto lugar, las funcionalidades de la organización, como objetivos y misión de la organización, los bienes y servicios que	• Identificar los activos • Determinar las amenazas • Determinar las salvaguardas • Estimar el impacto • Estimar el riesgo. • Magerit clasifica los activos en 5 categorías: entorno, sistemas de información, información, funcionalidades y otros.

		produce, el personal usuario/destinatario de los bienes o servicios que se produce. Finalmente, otros activos, que no se haya mencionado en las categorías anteriores.	
4	¿En qué consiste el tratamiento de riesgos de la información en tal organización?	Consiste en establecer los procedimientos operativos para el tratamiento de los riesgos identificados, mediante la implantación de medidas o salvaguardas para la prevención, reducción o control de los riesgos que se identificaron en la organización. Es importante que en dicho tratamiento se seleccionen y apliquen las medidas más apropiadas para reducir el riesgo, evitarlo, eliminarlo o transferirlo. En ese sentido, se debe tener en cuenta la protección de los equipos informáticos, la protección de las comunicaciones, así como los sistemas de información utilizados como soporte en la gestión documental. Verificar el cumplimiento de las condiciones físicas donde se encuentran los servidores para verificar el cumplimiento de la normativa correspondiente. También debe establecerse los planes de contingencia frente a caídas del sistema o servicios informáticos de apoyo notarial y programar las copias de seguridad (backups) periódicamente en la nube.	• Son los procedimientos operativos y medidas implementadas para prevenir, reducir y controlar los riesgos identificados. • Incluye la protección de equipos, comunicaciones, sistemas de información. • Verificar el cumplimiento de las condiciones físicas y normativa. • Establecer planes de contingencia ante fallos.

5	¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?	Con la información recopilada luego del análisis de riesgos, se genera el plan de seguridad para la gestión de riesgos de los sistemas de información, donde es importante involucrar a los colaboradores en particular los que utilizan los sistemas informáticos. El plan de seguridad significa la materialización del estudio realizado mediante el análisis y tratamiento de los riesgos e incluye el cronograma y la ejecución del mismo, mediante acciones concretas.	• El plan de seguridad comprende la información obtenida luego del análisis y las medidas para el tratamiento de los riesgos detectados. • Incluye el cronograma de actividades para la ejecución del plan.
6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría?	Magerit genera beneficios para las organizaciones puesto que permite analizar aquellos riesgos internos o externos que pueden convertirse en amenazas para los sistemas de información. Es importante reconocer que los riesgos no desaparecerán, sino que irán incrementándose con el avance y desarrollo tecnológico. El plan de seguridad para la gestión de riesgos de la información preparará a la organización para una certificación o acreditación que además de proteger sus activos también mejore su imagen tan importante en nuestra actualidad competitiva.	• Permite reconocer los riesgos internos o externos que pueden significar una amenaza de seguridad. • Prepara a la organización para la certificación o acreditación correspondiente.

Matriz de codificación de entrevista

N°	Preguntas	**Entrevistado 3** – Especialista en gestión de riesgos digitales	**Entrevistado 3 - Codificada**
1	¿Considera adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría de la Región Lima?	De acuerdo a mi experiencia, Magerit es una metodología apropiada para investigar los riesgos que pudieran afectar los sistemas de información de cualquier organización, como las notarías, para luego recomendar las medidas para controlar los riesgos detectados. Dicha metodología es de uso gratuito y está bien documentada y respaldada por el gobierno español. En el caso de las notarías, gestionan información importante y en ocasiones confidencial de parte de sus usuarios. Por tanto, al brindar un servicio público están en la obligación de resguardar la información que almacenan, de conformidad con la Ley de protección de datos personales.	• Es una metodología apropiada para investigar los riesgos para los sistemas de información. • Magerit es de uso gratuito, está documentada y respalda por el gobierno de España. • Las notarías gestionan información importante de los usuarios. • Tienen la obligación de resguardar la información de acuerdo a la Ley de protección de datos personales.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información en una notaría?	Magerit tiene dos objetivos principales: estudiar o analizar los riesgos y recomendar las medidas para prevenir, impedir, disminuir o controlar tales riesgos.	• Estudiar o analizar los riesgos. • Recomendar medidas para prevenir, impedir, disminuir o controlar los riesgos.

3	¿Cómo analizar la gestión de riesgos de la información en dicha organización?	Debo resaltar que esta etapa constituye el núcleo principal de Magerit, por lo que de su correcta aplicación depende la validez de todo el proyecto. El objetivo principal es la evaluación del riesgo del sistema en estudio. Comprende cinco etapas, como son la identificación y agrupación de los activos, identificación y evaluación de las amenazas, identificación y estimación de las vulnerabilidades, identificación y valoración de los impactos y la evaluación de los riesgos. En la primera etapa, el recojo de información del sistema y los factores que influyen en la seguridad, comprende preparar la información necesaria, realizar entrevistas y analizar la información recolectada. En la segunda actividad, se identifican los activos y cómo están relacionados, profundizando sus características en base a la información recogida e incluye identificar y agrupar activos, identificar los mecanismos de salvaguarda existentes y valorar los activos. La tercera actividad, consiste en identificar y agrupar las amenazas, así como establecer los árboles de fallos generados por las amenazas. En la cuarta actividad, se identifican las vulnerabilidades y estimar las vulnerabilidades. En la quinta actividad se identifican los impactos, tipifican los impactos y valoran los impactos.	• La evaluación del riesgo comprende 5 etapas: identificar los activos, agrupar las amenazas, identificar y valorar vulnerabilidades, identificar y valorar el impacto y evaluar el riesgo.

		Mientras que, en la sexta etapa, se evalúa el riesgo intrínseco, analizan las salvaguardas y evalúa el riesgo efectivo y residual.	
4	¿En qué consiste el tratamiento de riesgos de la información en tal organización?	En esta etapa se eligen los mecanismos de tratamiento o salvaguarda, tomando como base su efectividad. Se estudian sus tipos, costos y relaciones, analizando si existen contraindicaciones para su aplicación. Finalmente, se establece el orden para su implantación. Dentro del tratamiento se priorizan los mecanismos necesarios, evalúan los recursos, el cronograma y se integran los resultados. El tratamiento que se determine debe resguardar los sistemas de información y la infraestructura tecnológica que lo soporta. Es recomendable implementar un sistema para el registro de incidencias y alertas.	• Se estudian tipos, costos y relaciones de los riesgos. • Priorizar mecanismos para evaluar los recursos, establecer el cronograma e integrar los resultados. • Resguardar los sistemas de información y la infraestructura tecnológica. • Se recomienda implementar un sistema para el registro de incidencias y alertas.

5	¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?	La gestión de la seguridad de los sistemas de información incluye analizar los requerimientos de seguridad y establecer un plan para satisfacer tales requerimientos. Todas las actividades anteriores se plasman en el plan de seguridad, que incluye el mantenimiento y administración de la seguridad. Para su elaboración se establecen los objetivos, las estrategias de seguridad y la política corporativa de seguridad de tecnologías de la información para la organización. Como parte de esta política de seguridad corporativa está la instauración de una estructura organizacional apropiada para asegurar que los objetivos definidos por la institución se puedan alcanzar. Asimismo, el propósito del Plan de Seguridad es brindar una visión general de los requerimientos de seguridad del sistema de información y determinar los controles necesarios para alcanzar dichos requerimientos. En dicho plan, se delimitan las responsabilidades de toda persona o usuario que tenga acceso al sistema informático. A través del Plan de Seguridad se establecen las salvaguardas para proteger la información y los recursos tecnológicos. El plan debe incluir los planes de contingencia y backups periódicas de los sistemas de información en la nube.	• Analizando los requerimientos de seguridad. • Incluye establecer el mantenimiento y administración de la seguridad e instauración de una estructura organizacional adecuada. • Delimitar responsabilidades de los usuarios internos y externos. • Elaborar el plan de seguridad teniendo en cuenta la protección de la información y recursos tecnológicos. • Debe incluir el plan de contingencia y backups en la nube.

6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría?	Contar con un plan de seguridad en la notaría, permitirá resguardar la Información, los sistemas informáticos e instalaciones que sirven de soporte. Al realizar la gestión de riesgos, en este caso, con la metodología Magerit, podrán reducir o minimizar los riesgos y amenazas a los activos de la organización. Sin embargo, dicho plan debe ser revisado periódicamente, puesto que las amenazas van incrementándose con el desarrollo de la tecnología, apareciendo amenazas más destructivas, por ello, es necesario siempre contar con un plan de seguridad actualizado y revisado periódicamente, capaz de gestionar las nuevas vulnerabilidades o amenazas para la seguridad de la institución.	• Se podrá resguardar la información, sistemas e instalaciones. • Reducción de los riesgos y/o amenazas. • El plan debe ser revisado periódicamente, para gestionar nuevas vulnerabilidad o amenazas.

Anexo 5

Matriz de entrevistados y conclusiones

N°	Pregunta	E_1 – Especialista en seguridad y sistemas integrados de gestión	E_2 – Especialista en seguridad de sistemas de información	E3 – Especialista en gestión de riesgos digitales	Similitud	Diferencias	Conclusión
1	¿Es adecuada la metodología Magerit para la gestión de riesgos de la información para una notaría pública de la Región Lima?	• Magerit permite la gestión de riesgos de los sistemas de información. • Consta de III Libros documentados. • El Libro I, establece cómo asegurar la información. • Las notarías brindan un servicio público. • Manejan información importante de los usuarios. • Se debe asegurar que la información no sea vulnerada, robo, sabotaje, adulteración o accesos no autorizados.	• Magerit es adecuada para el análisis y gestión de riesgos de los sistemas informáticos. • Magerit contempla métodos para diagnosticar el estado de la seguridad. • Permite establecer la política o plan de seguridad. • Se adapta a las normas ISO 27001 e ISO 31000.	• Es una metodología apropiada para investigar los riesgos para los sistemas de información. • Magerit es de uso gratuito, está documentada y respalda por el gobierno de España. • Las notarías gestionan información importante de los usuarios. • Tienen la obligación de resguardar la información, de acuerdo a la Ley de protección de datos personales.	• Magerit es una metodología apropiada para la gestión de riesgos de los sistemas de información de las organizaciones públicas o privadas. • Consta de tres libros y es de uso libre, respaldada por el gobierno español. • Las notarías si brindan un servicio público y manejan información importante para el desarrollo de las actividades económicas. • Las organizaciones almacenan y gestionan su información mediante sistemas de información. • Es importante que la información que gestionan tenga la debida protección, frente a riesgos o amenazas.	• Magerit se adapta a las normas ISO 27001 e ISO 31000. • El análisis permitirá establecer las políticas o plan de seguridad para la gestión de los riesgos. • Las notarías tienen la obligación de resguardar la información, según la Ley de protección de datos personales.	• Magerit si es una metodología adecuada para la gestión de riesgos de los sistemas de información y consta de tres libros de uso libre. • Magerit facilita a la notaría para realizar el análisis y tratamiento de riesgos, permitiendo establecer el plan de seguridad.
2	¿Cuáles son los pasos a seguir para la gestión de riesgos del sistema de información en una notaría?	• Análisis de riesgos. • Tratamiento de los riesgos.	• Analizar los riesgos. • Aplicar el tratamiento o salvaguardas para los riesgos identificados.	• Estudiar o analizar los riesgos. • Recomendar medidas para prevenir, impedir, disminuir o controlar los riesgos.	• Magerit establece dos pasos fundamentales: el análisis y el tratamiento de riesgos.	• Permite establecer medidas para prevenir, impedir, disminuir o gestionar los riesgos, procurando evitar el robo, sabotaje, adulteración o uso no autorizado de la información por terceros o hackers.	• Consta de dos actividades principales: análisis y tratamiento de riesgos. • A su vez, cada actividad requiere la ejecución de determinadas acciones.

3	¿Cómo analizar la gestión de riesgos de la información en dicha organización?	• Identificar los activos. • Identificar las amenazas. • Determinar las salvaguardas. • Estimar el impacto de la amenaza. • Estimar el riesgo frente a la amenaza.	• Identificar los activos • Determinar las amenazas • Determinar las salvaguardas • Estimar el impacto • Estimar el riesgo. • Magerit clasifica los activos en 5 categorías: entorno, sistemas de información, información, funcionalidades y otros.	• La evaluación del riesgo comprende 5 etapas: identificar los activos, agrupar las amenazas, identificar y valorar vulnerabilidades, identificar y valorar el impacto y evaluar el riesgo.	• El análisis consta de cinco pasos explicados en el Libro I de Magerit: Determinar o identificar los activos. Determinar las amenazas. Determinar las salvaguardas o mecanismos para reducir las amenazas. Estimar el impacto de una amenaza, por la materialización de la misma. Estimar el riesgo frente a la amenaza.	• Magerit clasifica los activos en cinco categorías: entorno, sistemas de información, información, funcionalidades y otros.	• El análisis abarca cinco pasos definidos en el Libro I de la metodología Magerit: Identificar los activos, identificar las amenazas, determinar las salvaguardas, estimar el impacto de la amenaza, estimar el riesgo frente a la amenaza. • Los activos se clasifican en cinco categorías: entorno, sistemas de información, información, funcionalidades y otros.
4	¿En qué consiste el tratamiento de riesgos de la información en tal organización?	• Establecer la forma de eliminar, mitigar, compartir y financiar los riesgos identificados. • Restricción al sistema informático. • Perfiles de usuario. • Protección de los equipos informáticos. • Identificación del software no autorizado. • Acceso restringido a la red local. • Revisión del antivirus. • Revisión del software instalado.	• Son los procedimientos operativos y medidas implementadas para prevenir, reducir y controlar los riesgos identificados. • Incluye la protección de equipos, comunicaciones, sistemas de información. • Verificar el cumplimiento de las condiciones físicas y normativa. • Establecer planes de contingencia ante fallos.	• Se estudian tipos, costos y relaciones de los riesgos. • Priorizar mecanismos para evaluar los recursos, establecer el cronograma e integrar los resultados. • Resguardar los sistemas de información y la infraestructura tecnológica. • Se recomienda implementar un sistema para el registro de incidencias y alertas.	• Implica establecer el tratamiento, para eliminarlo, mitigarlo, compartirlo, así como financiar el riesgo. Mecanismos de protección para salvaguarda. • Establecer restricciones de acceso al sistema informático notarial con perfiles de usuario, protección del hardware, identificación del software no autorizado y control de acceso a la red local. • Protección de aplicaciones informáticas, verificando y controlando las aplicaciones instaladas. • Protección de los equipos informáticos, protección de las comunicaciones. Verificación de las condiciones físicas de los servidores.	• Establecer planes de contingencia y backups periódicas de los sistemas de información en la nube. • Implementar un sistema para el registro de incidencias y alertas.	• Permite eliminar, mitigar, compartir y financiar los riesgos identificados. • Permite proteger las aplicaciones informáticas, los equipos informáticos, las comunicaciones, a través de la verificación de las instalaciones. • Establecer planes de contingencia y la programación de copias de seguridad periódicamente en la nube.

5	¿Cómo se elabora el plan de seguridad para la gestión de riesgos de la información?	• Planificar acciones. • Identificar proyecto de seguridad. • Establecer el plan de ejecución. • Comprende el análisis y tratamiento establecido para la organización.	• El plan de seguridad comprende la información obtenida luego del análisis y las medidas para el tratamiento de los riesgos detectados. • Incluye el cronograma de actividades para la ejecución del plan.	• Analizando los requerimientos de seguridad. • Incluye establecer el mantenimiento y administración de la seguridad e instauración de una estructura organizacional adecuada. • Delimitar responsabilidades de los usuarios internos y externos. • Elaborar el plan de seguridad teniendo en cuenta la protección de la información y recursos tecnológicos.	• Planificar las medidas oportunas para mantener los riesgos bajo control adecuado. • Comprende la identificación de proyectos de seguridad, establecer un plan de ejecución y la ejecución misma del plan de seguridad elaborado para controlar los riesgos identificados. • Se debe involucrar a los colaboradores. El plan de seguridad incluye el cronograma y la ejecución de las acciones determinadas.	• Instauración de una estructura organizacional adecuada. • Delimitar responsabilidades de los usuarios internos y externos.	• Documentación de las políticas y acciones identificadas. • Involucrar a los colaboradores.
6	¿Cuáles son los beneficios del plan de seguridad para la gestión de riesgos de la información en una notaría?	• Mejora la seguridad de los sistemas de información. • Permite concientizar la colaboración y participación de los trabajadores. • Genera un valor agregado como es en la imagen y confianza hacia la organización.	• Permite reconocer los riesgos internos o externos que pueden significar una amenaza de seguridad. • Prepara a la organización para la certificación o acreditación correspondiente.	• Se podrá resguardar la información, sistemas e instalaciones. • Reducción de los riesgos y/o amenazas. • El plan debe ser revisado periódicamente, para gestionar nuevas vulnerabilidad o amenazas.	• El plan de seguridad permite la gestión de riesgos lo que beneficia a la organización. • Implica concientizar la colaboración de las personas involucradas en los sistemas de información.	• El plan debe ser revisado periódicamente. • Prepara para los procesos de evaluación, auditoría, certificación o acreditación y contribuirá a mejorar su imagen y posicionamiento.	• Magerit permite la gestión de los riesgos que pudieran afectar e interrumpir los sistemas de información. • Contar con un plan de seguridad prepara a la organización para la certificación ISO y/o acreditación, mejorando la seguridad de su sistema de información e imagen de la organización.

CONCLUSIÓN: Los entrevistados coincidieron que la metodología Magerit es adecuada para la gestión de los riesgos de los sistemas de información, puesto que está debidamente documentada y respaldada por el gobierno español, pudiendo adaptarse fácilmente a la notaría, no requiriendo de un especialista, puesto que los tres libros que la componen explican claramente los pasos a seguir, siendo el análisis y tratamiento de los riesgos, las principales actividades para la materialización del plan de seguridad.

Anexo 6

Ficha de Análisis Documental

Ubicación:	Barranca – Lima
Área:	Notaría Nieves Chen
Observador:	Renato Mario Ampuero Herrera

Título de la publicación: Ley n.º 29733.

Autor(es): Congreso de la República.

Número de la publicación: 445746.

Fecha de publicación: 03 de julio de 2011.

Tipo de documento: Ley.

Lengua: Español.

Página inicial: 1

Página final: 31

Resumen: La normativa tiene como finalidad, garantizar el derecho fundamental a la protección de los datos personales, previsto en el artículo 2 numeral 6 de la Constitución Política del Perú, a través de su adecuado tratamiento, respetando el derecho fundamental que en ella se reconocen. Esta norma establece obligaciones para que las organizaciones aseguren un adecuado tratamiento de los datos personales de sus clientes o usuarios, proveedores, trabajadores y personas vinculadas. Asimismo, esta legislación y su reglamento reconocen los derechos de las personas a quienes pertenecen dichos datos.

Las obligaciones que establece dicha normativa, se detallan a continuación:

1. Inscribir ante la Autoridad Nacional de Protección de Datos Personales, el (los) Banco(s) de Datos Personales (BDP) que posean. De acuerdo con la definición de la Ley, un BDP se refiere al conjunto organizado de información de personas naturales. Esta información puede encontrarse almacenada en diversos soportes, como en Word, Excel, PDF, imágenes, audios, vídeos, entre otros; los cuales se encuentren registrados en equipos o servidores de la empresa.

2. Obtener un consentimiento informado de los titulares de los datos personales, a través de una autorización del titular de los datos personales para que la empresa pueda darles el tratamiento correspondiente. Dicho consentimiento debe cumplir con ser claro, libre y con anterioridad al tratamiento. En este aspecto, las empresas muestran mayores dudas, puesto que el consentimiento informado no puede ser genérico, más bien debe comunicarse todos los tratamientos de los datos personales que realizará la empresa. Por ejemplo, indicar a quiénes se transferirá o se compartirá la información (de ser el caso), precisar si se utilizarán los datos para remitir publicidad y expresar un plazo determinado de almacenamiento, entre otros aspectos.
3. Establecer las medidas de seguridad que sean eficaces, que involucra los aspectos técnicos, organizativos y legales para evitar la filtración o sustracción de los datos personales. Dentro de estas medidas incluye establecer protocolos de seguridad sobre archivos en soportes automatizados y no automatizados, elaboración de políticas de privacidad, aprobar manuales organizativos que asignen las responsabilidades en el tratamiento de los datos personales, compromisos de confidencialidad y cláusulas contractuales, entre otros.
4. Establecer un procedimiento de atención de los derechos de las personas naturales, donde puedan ejercer los siguientes derechos: a) Acceso, es decir, que toda persona puede requerir el acceso a la información que de ella tiene la empresa o finalidad para la cual sus datos fueron recopilados, razones que motivaron su recopilación y las transferencias realizadas o que se prevén realizar de dichos datos a terceros. b) Rectificación, referido a que toda persona pueda pedir que modifiquen los datos contenidos en el BDP, si estos son incompletos, erróneos o falsos. c) Cancelación, que implica que toda persona puede pedir la eliminación de sus datos personales cuando hayan dejado de ser necesarios respecto a la finalidad para lo cual fueron recopilados. d) Oposición, por la que toda persona puede pedir la eliminación de sus datos cuando se hayan obtenido sin su consentimiento.
5. El incumplimiento de la referida norma, contempla tres tipos de sanciones para las instituciones: a) leve, con una multa mínima desde cero coma cinco de una unidad impositiva tributaria (UIT) hasta cinco UIT b) grave, sancionable

con una multa que va desde más de cinco UIT hasta cincuenta unidades UIT c) muy grave, que puede ser sancionada con una multa desde más de cincuenta UIT hasta cien UIT.

Descriptores: Ley de protección de datos personales

Clasificación: Protección de datos

Conclusión del análisis documental:

De conformidad con la Ley n.º 29733, se salvaguarda la utilización de los datos personales de todo individuo, reconociendo que son propietarios de los mismos, y que las organizaciones deben solicitar su consentimiento expreso antes de utilizarlo o transferirlo a terceros, si fuera el caso. Dicho consentimiento debe estar claramente expresado y puede ser revocado posteriormente si la persona así lo requiere. Esta normativa obliga a las instituciones a implementar los mecanismos adecuados para el tratamiento de los datos personales que recopilan, por ejemplo, de sus clientes o empleados. En ese sentido, las notarías deben incorporar los mecanismos necesarios para el tratamiento de los datos personales, con la finalidad de cumplir con la normativa vigente y evitar las sanciones que pudieran imponerse.

Anexo 7

Guía de observación

Empresa:	Notaría Nieves Chen
Ubicación:	Barranca – Lima
Área:	Notaría Nieves Chen
Observador:	Renato Mario Ampuero Herrera

La guía contempla lo observado en la visita a la unidad de análisis, siendo NOT: el notario, SOT: responsable del soporte tecnológico, IPP: personal que labora en el área de instrumentos públicos protocolares y asuntos no contenciosos, ACE, personal que labora en el área de actas y certificaciones extraprotocolares, ARP. Personal que labora en el área de registros públicos.

NOT: Responsable de la fe pública en los actos jurídicos y otros, mediante la materialización del formalismo y voluntad de las partes, a través de la redacción de los instrumentos públicos protocolares adecuado al tipo de trámite que requiera el usuario, confiriéndoles autenticidad, conservando los originales (escrituras públicas) y expidiendo copias que dan fe del contenido (testimonio y partes). Asimismo, se gestionan actas y certificaciones extraprotocolares (legalización de libros, autorizaciones de viaje, entre otros). Para realizar su actividad, el notario cuenta con colaboradores, los cuales están asignados a las áreas de instrumentos públicos protocolares y asuntos no contenciosos, área de actas y certificaciones extraprotocolares, área de registros públicos, área de administración, que comprende archivo, contabilidad, caja y soporte tecnológico.

SOT: Responsable del soporte tecnológico, encargado de monitorear la red local, sistemas informáticos, base de datos, copias de seguridad, equipos de comunicaciones, software instalado, entre otros. También se encarga de la gestión de la página web corporativa, correos institucionales y redes sociales. Gestiona las contraseñas de los diferentes componentes de la red (módem, firewall, servidor, NAS, etc.) y sistema notarial.

IPP: Es el área encargada de preparar las escrituras públicas y demás actas que el notario incorporará a su registro notarial, para su conservación y expedir los traslados cuando se requiera. Entre éstos se encuentran los trámites de compra-venta, donación, hipoteca, transferencias vehiculares, entre otros. En esta área

laboran tres colaboradores, los cuales, verifican los requisitos presentados para el trámite, asignan un número de trámite (Kardex) y registran los datos del cliente y trámite en el sistema notarial, para la generación del documento respectivo a través de plantillas predeterminadas, según el trámite correspondiente. Luego, proceden a imprimir un borrador para la verificación de parte del cliente, corrigiendo las observaciones, si las hubiera. Posteriormente, se imprime la escritura pública en los formatos oficiales proporcionado por el colegio de notarios y se verifica la identidad del cliente a través del sistema de verificación biométrica del RENIEC y se toma la firma del cliente u otros que intervengan en el acto jurídico. El personal traslada el expediente al notario para su verificación y firma correspondiente. A continuación, se expide el testimonio y/o parte notarial al cliente, según lo requiera el trámite, para su inscripción en los registros públicos. Actualmente, la Superintendencia Nacional de los Registros Públicos (SUNARP), cuenta con el Sistema de Intermediación Digital (SID) siendo el medio para el envío electrónico de los partes notariales que incluye la firma digital del notario, para su correspondiente inscripción en SUNARP. En los registros públicos se le asigna un número de título y una vez inscrito el acto jurídico se comunica al cliente y entrega el título expedido por la SUNARP.

ACE: El área de actas y certificaciones extraprotocolares, se encarga de los actos, hechos o circunstancias que se presencie o conste al notario en mérito a su función, por ejemplo: certificaciones de documentos, autenticación de firma, autorizaciones de viaje de menores al interior o exterior del país, entre otros. En dicha área laboran tres trabajadores, los cuales orientan al público, indican los requisitos, costos, recepcionan, registran los datos del cliente y del trámite en el sistema notarial; luego derivan al notario para su verificación y firma correspondiente. Finalmente, entregan al cliente lo requerido con la firma del notario, sellos oficiales y otras medidas de seguridad.

ARP: El área de registros públicos, donde labora una persona, se encarga de registrar los trámites que serán derivados a la SUNARP a través del SID, para que luego de su verificación el notario remita los partes notariales, es decir, el archivo que contiene el documento correspondiente con su firma digital. Realiza el seguimiento del trámite y luego de la aprobación del título en SUNARP, informa y entrega al cliente el documento expedido por los registros públicos. Es preciso

indicar que el pago requerido por los registros públicos se realiza a través de un monedero digital habilitado por SUNARP.

En el primer piso, se atienden los trámites relacionados con las actas y certificaciones extraprotocolares y caja. En el segundo piso, se atienden los trámites relacionados con los instrumentos públicos protocolares y asuntos no contenciosos. En el tercer piso se encuentra el despacho del notario. El notario comenta que en la actualidad no se cuenta con un plan de seguridad de la información como tal, pero en coordinación con el responsable de soporte tecnológico se tomaron medidas para prevenir ciertos riesgos.

Asimismo, en un espacio del tercer piso de la oficina notarial, se observa el ambiente asignado para el área de soporte tecnológico, dividido en un espacio con aire acondicionado donde se encuentra un gabinete para el servidor de aplicaciones, que contiene la base de datos del sistema notarial y los documentos notariales generados organizados en carpetas, un equipo UPS en caso de corte de la energía eléctrica, un equipo firewall para protección de la red, un switch gigabit para administrar la red, un servidor NAS para copias de seguridad, un Módem-Router para el acceso a Internet. En otro espacio del referido ambiente, se encuentra el responsable de soporte tecnológico, monitoreando el correcto funcionamiento de la red, servidor y equipos, así como brindando la atención de las consultas o dificultades que informan los colaboradores. En el ambiente, también hay otros colaboradores, los cuales tienen acceso físico al servidor y equipos de red. Respecto a las medidas de seguridad, el responsable de soporte tecnológico comenta que actualmente no se cuenta con un plan de seguridad de la información; sin embargo, en coordinación con el notario se tomaron acciones para prevenir inconvenientes que pudieran perjudicar la infraestructura tecnológica y afecte la continuidad del servicio a los clientes. Por ejemplo, mencionó que se cuenta con un antivirus original para el servidor y equipos de cómputo, que permite actualizar automáticamente la seguridad contra ataques de virus maliciosos, malware, entre otros. De otro lado, en la base de datos del servidor se encuentran registrados los colaboradores que tienen acceso al sistema notarial, los cuales reciben sus credenciales al iniciar sus labores en la notaría, recibiendo también una capacitación previa; asimismo, se han tomado acciones para prevenir la pérdida de datos, por ejemplo, la programación de las

copias de seguridad del servidor al NAS, de forma automática y diaria en horas de la noche. Adicionalmente, indica que se cuenta en el ambiente con aire acondicionado y extintor para prevenir algún amago de incendio, pero no se observa un detector de humo. Al consultarle sobre alguna incidencia, comenta que en una oportunidad se dañó el servidor y sus discos duros, al parecer por una falla en la fuente de energía del mismo. Se tuvo que habilitar provisionalmente un equipo de cómputo común como servidor, mientras se gestionaba la adquisición de uno nuevo. Se procedió a restaurar los archivos que contenía el servidor, sin embargo, en ese momento no se contaba con una copia actualizada de los datos, perdiéndose la información de dos días, por lo que, se tuvo que identificar y redactar los archivos no recuperados. Frente a esta situación, sugirió la adquisición del servidor NAS para la automatización de las copias de seguridad de forma diaria y de esta forma salvaguardar la información respectiva. Asimismo, manifestó que se encuentra en proceso la adquisición de un servicio en la nube para el resguardo de los archivos notariales. Sin embargo, no se observa algún sistema o registro de incidencias.

En el cuarto piso, se encuentra el área de archivo y el responsable del control y mantenimiento respectivo.

Conclusión de la observación:

De lo observado se concluye que la notaría cuenta con una estructura organizativa, que permite asignar las tareas y responsabilidades, de acuerdo al perfil de los colaboradores. Existe un responsable de soporte tecnológico, con el perfil de especialista en sistemas informáticos, quien se encarga de administrar la infraestructura tecnológica de la organización. Dicho responsable reconoce que no se cuenta con un plan de seguridad de los sistemas de información, pero progresivamente se han venido implementado acciones para mejorar la seguridad de la información y sistemas, en ocasiones debido a ciertos fallos en el servidor lo que motivó adquirir un equipo NAS para la automatización de las copias de seguridad, para respaldar toda la información del registro notarial en caso ocurran fallos en el servidor principal, no siendo una buena práctica para la gestión de riesgos. Por tanto, el plan de seguridad permitirá identificar los activos y determinar anticipadamente las salvaguardas o tratamiento para gestionar los riesgos y

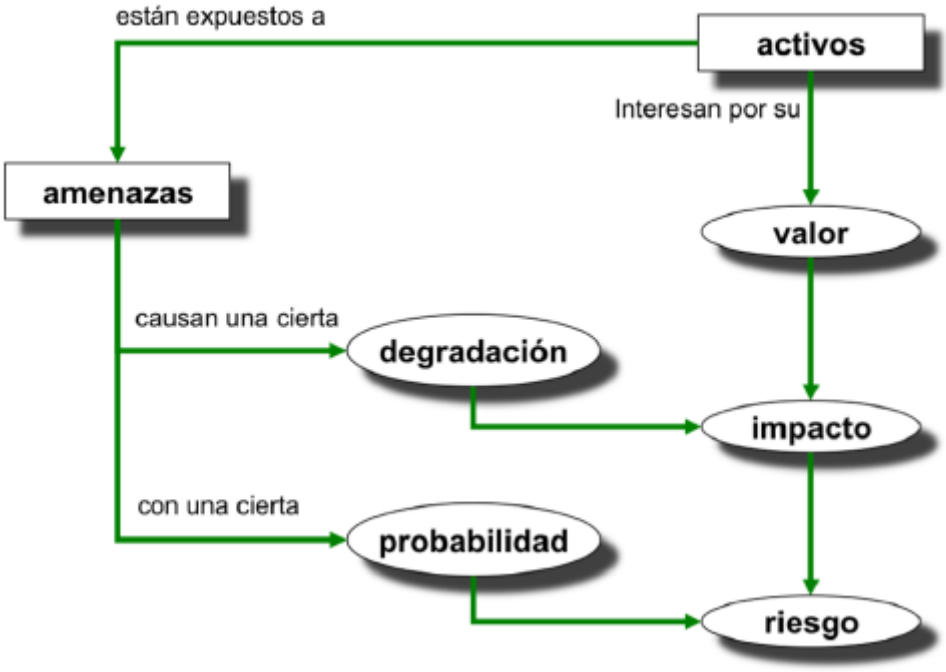
amenazas, según se requiera; con la finalidad de no esperar a que éstos ocurran para tomar alguna medida. Dicho plan, una vez aprobado, debe sensibilizarse con los colaboradores para que tengan en cuenta la importancia de la seguridad de la información.

Anexo 8

Modelo de gestión de riesgos basado en Magerit para una Notaría

1. Introducción

Magerit es una metodología de uso libre para el análisis y gestión de los riesgos de los sistemas de información, siendo desarrollada por el gobierno español como respuesta al creciente uso de las herramientas tecnológicas y comunicación por parte de las instituciones públicas y privadas. Magerit consta de tres libros, dentro de los cuales se encuentran su método (Libro I), catálogo de elementos (Libro II) y guía de técnicas a utilizar (Libro III). La metodología Magerit se resumen en el siguiente modelo:



El flujo de las actividades a seguir son los siguiente: 1. Determinar los activos relevantes para la organización, su interrelación y su valor, en el sentido de qué perjuicio o coste supondría su degradación.2.Determinar a qué amenazas están expuestos aquellos activos.3.Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.4.Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.5.Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia de la amenaza.

2. Gestión de riesgos

La gestión de riesgos, comprende dos actividades fundamentales: el análisis y tratamiento de los riesgos identificados. Magerit describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos a través de una serie de aspectos prácticos. La diferencia que tiene Magerit frente a otras metodologías, es que presenta una guía completa de cómo llevar a cabo paso a paso el análisis y tratamiento de riesgos, los cuales son descritos claramente en su documentación. El resultado de la gestión de riesgos es el plan de seguridad, el cual debe ser socializado entre los colaboradores de la organización y revisado periódicamente.

3. Análisis de riesgos

Permitirá determinar con qué cuenta la organización para luego estimar el impacto de diversos riesgos sobre los mismos, identificando aquello que pudiera afectar gravemente al rendimiento de los sistemas o procesos importantes. En ese sentido, se pretende establecer un umbral de riesgo deseable, que si es superado pasará a ser objeto de tratamiento. Es importante, considerar los siguientes elementos en esta etapa:

- **Activos**: Recursos del sistema de información o relacionados con este, necesarios para que funcione correctamente y alcance los objetivos propuestos por su dirección. El activo esencial es la información o dato, así como los procesos.
- **Amenazas**: Determinar las amenazas que pueden afectar a cada activo, hay que estimar cuán vulnerable es el activo en dos sentidos: Degradación: Como es de perjudicial y Frecuencia: Cada cuanto se materializa la amenaza.
- **Vulnerabilidades**: Potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.
- **Impactos**: Es el daño sobre el activo causado por la amenaza, conociendo el valor de los activos sería muy sencillo calcular el valor del impacto.
- **Riesgo**: Es la medida de la posibilidad que existe en que se materialice una amenaza. Conociendo el riesgo, podemos calcular la frecuencia.

- **Salvaguardas**: Es un mecanismo de protección frente a las amenazas, reducen la frecuencia de las amenazas y limitan el daño causado por estas.

3.1. Tipos de activos

Los activos son los elementos del sistema de información y que permiten la gestión de los sistemas o procesos de la organización. La tipificación de los activos es una información documental de interés como un criterio de identificación de amenazas potenciales y salvaguardas apropiadas a la naturaleza del activo. Los activos se clasifican dentro de una jerarquía, determinando para cada uno un código que refleja su posición jerárquica, un nombre y una breve descripción de las características. La pertenencia de un activo a un tipo no es excluyente de su pertenencia a otro tipo; es decir, un activo puede ser simultáneamente de varios tipos. Los activos se agrupan en:

[essential] Activos esenciales	Información y servicios. Establecen los requisitos de seguridad para los demás componentes del sistema
[arch] Arquitectura del sistema	Elementos que permiten estructurar el sistema, definiendo su arquitectura interna y sus relaciones con el exterior
[D] Datos / Información	La información es un activo abstracto que será almacenado en equipos o soportes de información
[keys] Claves criptográficas	Las claves criptográficas, combinando secretos e información pública, son esenciales para garantizar el funcionamiento de los mecanismos criptográficos
[S] Servicios	Función que satisface la necesidad de los usuarios y los servicios que utilizan. Incluyen los servicios que permiten altas y bajas de usuarios de los sistemas
[SW] Software / aplicaciones informáticas	Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación

	de la información para la prestación de los servicios
[HW] Equipamiento informático (hardware)	Medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
[COM] Redes de comunicaciones	Incluye las instalaciones dedicadas como servicios de comunicaciones contratados a terceros
[Media] Soportes de información	Dispositivos físicos que permiten almacenar información de forma permanente o durante largos periodos de tiempo
[AUX] Equipamiento auxiliar	Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos
[L] Instalaciones	Lugares donde se hospedan los sistemas de información y comunicaciones
[P] Personal	Personas relacionadas con los sistemas de información

3.1 Identificación de activos

Para el proceso de identificar los activos de la organización se recomienda el uso de los siguientes formatos:

A2.1. [info] Activos esenciales: información

[info] Información	
código:	**nombre:**
descripción:	
propietario:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.1.	

Valoración de la información, típicamente en las siguientes dimensiones de seguridad: [I] integridad [C] confidencialidad [A] autenticidad de los datos [T] trazabilidad de los datos.

Valoración		
dimensión	***valor***	***justificación***
[I]		
[C]		
[A]		
[T]		

A2.2. [service] Activos esenciales: Servicio

[service] Servicio	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.1.	

Valoración de los servicios que ofrece la Organización a otros, típicamente en las siguientes dimensiones: [D] disponibilidad [A] autenticidad de quién accede al servicio [T] trazabilidad de quién accede al servicio, cuándo y que hace.

A2.3. [D] Datos / Información

[D] Datos / Información	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.3.	

Las dependencias normalmente identifican equipos que los hospedan líneas de comunicación por las que se transfieren soportes de información personas relacionadas: usuarios.

A2.4. [K] Claves criptográficas

[K] Claves criptográficas	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.4.	

Las dependencias normalmente identifican equipos que las hospedan soportes de información personas relacionadas: operadores, administradores y criptocustodios.

A2.5. [S] Servicios

[S] Servicios	
código:	**nombre:**
descripción:	

A2.6. [SW] Aplicaciones (software)

[SW] Aplicaciones (software)	
código:	**nombre:**
descripción:	
responsable:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.6.	

A2.7. [HW] Equipamiento informático (hardware)

[HW] Equipamiento informático (hardware)	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.7.	

A2.8. [COM] Redes de comunicaciones

[COM] Redes de comunicaciones	
código:	**nombre:**

[COM] Redes de comunicaciones
descripción:
responsable:
ubicación:
número:
tipo (marque todos los adjetivos que procedan) Ver Sección 2.8.

A2.9. [Media] Soportes de información

[SI] Soportes de información	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan)	

A2.10. [AUX] Equipamiento auxiliar

[AUX] Equipamiento auxiliar	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.10.	

A2.11. [L] Instalaciones

[L] Instalaciones	
código:	**nombre:**
descripción:	
responsable:	
ubicación:	
número:	
tipo (marque todos los adjetivos que procedan) Ver Sección 2.11.	

A2.12. [P] Personal

[P] Personal	
código:	**nombre:**
descripción:	

[P] Personal
número:
tipo (marque todos los adjetivos que procedan) Ver Sección 2.12.

Ejemplo:

2.1. [info] Activos esenciales		**Valoración**		
código: I001	**nombre: Fichero Clientes**	**Dimensión**	**Valor**	**Justificación**
descripción:	Fichero de clientes con información personal	**[I]**	A	Incumplimiento regulatorio
propietario:	Responsable Administración	**[C]**	A	Incumplimiento regulatorio
responsable:	Gerente	**[D]**	M	Es replicable
tipo:	[or][per][M][classified][R]	**[A]**	A	Incumplimiento regulatorio
		[T]	A	Incumplimiento regulatorio
Dependencias				
Activos: [HW].HW001		**Grado:** Alto		
¿Por qué? El maestro de clientes se almacena en el servidor principal dentro del ERP				

3.2 Dimensiones de valoración

Las dimensiones se utilizan para valorar las consecuencias de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo se ve dañado en dicha dimensión.

[D] Disponibilidad	Característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren
[I] Integridad	Característica consistente en que el activo de información no ha sido alterado de manera no autorizada
[C] Confidencialidad	Característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados

[A] Autenticidad	Característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos
[T] Trazabilidad	Característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad

3.3 Criterios de valoración

Se utiliza una escala detallada de diez valores, dejando en valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo). Si se realiza un análisis de riesgos de poco detalle. Ambas escalas, detallada y simplificada se correlacionan como se indica a continuación:

10	(EX) Extremo	Daño extremadamente grave
9	(MA) Muy alto	Daño muy grave
6-8	(A) Alto	Daño grave
3-5	(M) Medio	Daño importante
1-2	(B) Bajo	Daño menor
0	(MB) Depreciable	Irrelevante a efectos prácticos

3.4 Amenazas

Se tiene en consideración el catálogo de amenazas posibles sobre los activos de un sistema de información. Para cada amenaza se presenta un cuadro como el siguiente:

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

A continuación, se agrupan las posibles amenazas:

[N.*] Desastres naturales	**[N.1]** Fuego, **[N.2]** daños por agua, **[N.3]** contaminación, **[N.4]** siniestro mayor, **[N.6]** fenómeno climático, **[N.7]** fenómeno sísmico, **[N.8]** fenómeno de origen volcánico, **[N.9]** fenómeno meteorológico, **[N.10]** inundación
[I] De origen industrial	**[I.1]** Fuego, **[I.2]** daños por agua, **[I.4]** siniestro mayor, **[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]** falla de servicios de comunicaciones, **[I.9]** interrupción de otros servicios y suministros esenciales **[I.10]** degradación de los soportes de almacenamiento, **[I.11]** emanaciones electromagnéticas
[E] Errores y fallos no intencionados	**[E.1]** Errores de los usuarios, **[E.2]** errores del administrador, **[E.3]** errores de monitorización, **[E.4]** errores de configuración, **[E.7]** deficiencias en la organización, **[E.8]** difusión de software dañino, **[E.9]** errores de encaminamiento, **[E.10]** errores de secuencia, **[E.14]** escapes de información, **[E.15]** alteración accidental de información, **[E.18]** destrucción de información, **[E.19]** fugas de información, **[E.20]** vulnerabilidad de los programas (software), **[E.21]** errores de mantenimiento o actualización de programas, **[E.23]** errores de mantenimiento o actualización de equipos (hardware), **[E.24]** caída del sistema por agotamiento de recursos, **[E.25]** pérdida de equipos, **[E.28]** indisponibilidad del personal

[A] Ataques intencionados	**[A.3]** Manipulación de los registros de actividad, **[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]** reencaminamiento de mensajes, **[A.10]** alteración de secuencia, **[A.11]** acceso no autorizado, **[A.12]** análisis de tráfico, **[A.13]** repudio, **[A.14]** interceptación de información, **[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

3.5 Estimación del impacto

Para calcular el impacto se tiene en consideración lo siguiente:

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

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

3.6 Estimación del riesgo

De otro lado, se modelan impacto, probabilidad y riesgo por medio de escalas cualitativas:

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

Puede combinarse impacto y frecuencia de la siguiente forma para calcular el 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

4. Salvaguardas o tratamiento

Las salvaguardas permiten hacer frente a las amenazas. En el tratamiento de riesgos se seleccionarán los mecanismos o acciones que se implementarán como soluciones seleccionadas en la actividad anterior La eficacia del 0% corresponde a aquellas salvaguardas inexistentes, mientras que un 100% a aquellas idóneas y en uso perfectamente implantadas, mantenidas, controladas

y conocidas. A continuación, se resumen las salvaguardas que pudieran utilizarse:

H Protecciones generales u horizontales	H Protecciones Generales. H.IA Identificación y autenticación. H.AC Control de acceso lógico. H.ST H.IR Segregación de tareas. Gestión de incidencias. H.tools Herramientas de seguridad. H.tools.AV Herramienta contra código dañino. H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión. H.tools.CC Herramienta de chequeo de configuración. H.tools.VA Herramienta de análisis de vulnerabilidades. H.tools.TM Herramienta de monitorización de tráfico. H.tools.DLP DLP: Herramienta de monitorización de contenidos. H.tools.LA Herramienta para análisis de logs. H.tools.HP Honey net / honey pot. H.tools.SFV Verificación de las funciones de seguridad. H.VM Gestión de vulnerabilidades. H.AU Registro y auditoría.
D Protección de la Información	D.A Copias de seguridad de los datos (backup). D.I Aseguramiento de la integridad. D.C Cifrado de la información. D.DS Uso de firmas electrónicas. D.TS Uso de servicios de fechado electrónico (time stamping).
K Protección de las claves criptográficas	K Gestión de claves criptográficas. K.IC Gestión de claves de cifra de información. K.DS Gestión de claves de firma de información. K.disk Gestión de claves para contenedores criptográficos. K.comms

	Gestión de claves de comunicaciones. K.509 Gestión de certificados.
S Protección de los servicios	S Protección de los Servicios. S.A Aseguramiento de la disponibilidad. S.start Aceptación y puesta en operación. S.SC Se aplican perfiles de seguridad. S.op Explotación. S.CM Gestión de cambios (mejoras y sustituciones). S.end Terminación. S.www Protección de servicios y aplicaciones web. S.email Protección del correo electrónico. S.dir Protección del directorio. S.dns Protección del servidor de nombres de dominio (DNS). S.TW Teletrabajo. S.voip Voz sobre IP.
SW Protección de las aplicaciones (software)	SW Protección de las Aplicaciones Informáticas. SW.A Copias de seguridad (backup). SW.start Puesta en producción. SW.SC Se aplican perfiles de seguridad. SW.op Explotación / Producción SW.CM Cambios (actualizaciones y mantenimiento). SW.end Terminación.
HW Protección de los equipos (hardware)	HW Protección de los Equipos Informáticos. HW.start Puesta en producción. HW.SC Se aplican perfiles de seguridad. HW.A Aseguramiento de la disponibilidad. HW.op Operación. HW.CM Cambios (actualizaciones y mantenimiento). HW.end Terminación HW.PCD Informática móvil. HW.print Reproducción de documentos. HW.pabx Protección de la centralita telefónica (PABX)

COM Protección de las comunicaciones	COM Protección de las Comunicaciones. COM.start Entrada en servicio. COM.SC Se aplican perfiles de seguridad. COM.A Aseguramiento de la disponibilidad. COM.aut Autenticación del canal. COM.I Protección de la integridad de los datos intercambiados. COM.C Protección criptográfica de la confidencialidad de los datos intercambiados. COM.op Operación. COM.CM Cambios (actualizaciones y mantenimiento). COM.end Terminación. COM.internet Internet (uso/acceso). COM.wifi Seguridad Wireless (WiFi). COM.mobile Telefonía móvil. COM.DS Segregación de las redes en dominios.
AUX Protección de los elementos auxiliares	AUX Elementos Auxiliares. AUX.A Aseguramiento de la disponibilidad. AUX.start Instalación. AUX.power Suministro eléctrico AUX.AC Climatización. AUX.wires Protección del cableado.
L Seguridad física – Protección de las instalaciones	L Protección de las Instalaciones. L.design Diseño. L.depth Defensa en profundidad. L.AC Control de los accesos físicos. L.A Aseguramiento de la disponibilidad. L.end Terminación.
PS Salvaguardas relativas al personal	Son aquellas que se refieren a las personas que tienen relación con el sistema de información. PS Gestión del Personal. PS.AT Formación y concienciación. PS.A Aseguramiento de la disponibilidad.
G Salvaguardas de tipo organizativo	Son aquellas que se refieren al buen gobierno de la seguridad. G Organización.

	G.RM Gestión de riesgos. G.plan Planificación de la seguridad. G.exam Inspecciones de seguridad.
BC Continuidad de operaciones	Se refiere a la prevención y reacción frente a desastres. BC Continuidad del negocio. BC.BIA Análisis de impacto (BIA). BC.DRP Plan de Recuperación de Desastres (DRP).

Existen diferentes tipos de salvaguardas que pudieran utilizarse, tal como se observa a continuación:

Efecto	Tipo	Descripción
Prevenir: Actúa sobre la probabilidad, reduciéndola	[PR] preventivas	Reduce las oportunidades de que la amenaza se produzca.
	[DR] disuasorias	Producen un efecto disuasorio ante los atacantes, antes de que se produzca.
	[EL] eliminatorias	Logra que el incidente se produzca actuando antes.
Limitar: Actúa sobre la degradación, acotándola	[IM] minimizadoras	Reduce el impacto acotando las consecuencias.
	[CR] correctivas	Actúan reparando el daño reduciéndolo, después de que se haya producido.
	[RC] recuperativas	Permiten retornar al estado anterior al incidente para reducir el daño.
Fortalecer: Complementan consolidando el efecto de las demás	[MN] de monitorización	Monitorizan lo que ocurre online o a posteriori sobre el incidente o estado del sistema. Permiten mejorar las salvaguardas o determinar impacto.
	[DC] de detección	Detectan y alertan de que un ataque se está produciendo, permitiendo reaccionar con otras medidas para pararlo o minimizar el impacto.
	[AW] de concienciación	Acciones de formación sobre las personas en contacto con el sistema. Reducen errores y potencian la eficacia de otras salvaguardas al mejorar el conocimiento de las personas que las operan.
	[AD] administrativas	Componentes y procesos de administración de la seguridad del sistema.

Para la aplicación de las salvaguardas debemos identificar los activos que obtuvieron un riesgo Alto/Muy Alto. De éstos, se analizan si es de aplicación alguna salvaguarda que ayude a reducir el grado de degradación o disminuir su

probabilidad, de forma que se altera para disminuir el impacto en la organización.

5. Plan de seguridad

El plan de seguridad debe atender los riesgos encontrados, se divide en tres áreas: identificación de proyectos de seguridad, el plan de ejecución y la ejecución. Sobre la identificación de proyectos de seguridad, se enfoca en la elaboración de un conjunto procedimientos de seguridad, que consta de una agrupación de tareas que se ordena por conveniencia, las cuales son las normativas de seguridad, la eliminación de fallos de seguridad y la clasificación de inventario. En el caso de las normativas de seguridad, se refieren a los documentos que deben existir para la autorización del uso del software, pues es importante que se considere como una grave falta que los colaboradores instalen programas en los equipos de la institución. Estas normativas deben aplicarse a fin de prevenir virus y malware.

Asimismo, dentro de la normativa debe incluirse la obligatoriedad de verificación de información y medios de almacenamiento, por lo cual deben ejecutarse un antivirus. Así como también la documentación del uso correcto de los equipos informáticos, a fin de asignar responsabilidad a cada colaborador. Seguidamente se encuentra la etapa de plan de ejecución, cuyo objetivo es la ordenación de forma temporal de las normativas de seguridad. Es importante que, para ejecutar este plan de manera óptima, se realice una clasificación adecuada y actualizada de los activos físicos y lógicos.

Finalmente, el plan de seguridad debe incluir la información obtenida del análisis y tratamiento de los riesgos, así como la documentación de políticas institucionales que debe comunicarse y sociabilizarse a todo el equipo de trabajo. Es necesario además que se estipule un tiempo determinado para que se realicen las revisiones periódicas de estas políticas a fin de mantenerlas debidamente actualizadas.