FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

Desarrollo de un modelo de gestión de riesgos basado en la metodología MAGERIT para minimizar los riesgos de la implantación y uso de TI en una Municipalidad del Perú

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor:

Bach. Mogollon Garcia Manuel Esteban

ORCID: https://orcid.org/0000-0001-5814-7871

Asesor:

Mg. Bances Saavedra David Enrique

ORCID: https://orcid.org/0000-0002-7164-8918

Línea de Investigación:

Infraestructura, Tecnología y Medio Ambiente

Pimentel - Perú

2023

DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ

Aprobación del jurado

MG. MEJIA CABRERA HEBER IVAN

Presidente del Jurado de Tesis

MG. BRAVO RUIZ JAIME ARTURO

Secretario del Jurado de Tesis

MG. MINGUILLO RUBIO CESAR AUGUSTO

Vocal del Jurado de Tesis

Universidad
Señor de Sipán

DECLARACIÓN JURADA DE ORIGINALIDAD

Quien suscribe la **DECLARACIÓN JURADA**, soy Manuel Esteban Mogollon Garcia del Programa de Estudios de Ingeniería de Sistemas de la Universidad Señor de Sipán S.A.C, declaro bajo juramento que soy autor del trabajo titulado:

DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ

El texto de mi trabajo de investigación responde y respeta lo indicado en el Código de Ética del Comité Institucional de Ética en Investigación de la Universidad Señor de Sipán (CIEI USS) conforme a los principios y lineamientos detallados en dicho documento, en relación a las citas y referencias bibliográficas, respetando al derecho de propiedad intelectual, por lo cual informo que la investigación cumple con ser inédito, original y autentico.

En virtud de lo antes mencionado, firma:

(Apellidos y Nombres)	DNI: número	Firma
Manuel Esteban Mogollón García	00252937	

Pimentel, 02 de marzo de 2023.

Dedicatoria

Dedico esta tesis a mis hijos, a mi esposa y a toda mi familia por ser el soporte que tengo todos los días para seguir adelante en este proceso de aprendizaje llamado Vida. Y a todas las personas que me apoyaron y me siguen apoyando en seguir adelante y no decaer en el camino.

Agradecimientos

Agradezco a Dios por darme la salud para poder seguir adelante y a los docentes de la Escuela de Ingeniería de Sistemas de la Universidad “Señor de Sipán” por haberme formado con paciencia y dedicación en estos años de estudio.

Índice

Resumen

El presente trabajo tiene como objetivo, desarrollar un modelo de gestión de riesgos basado en la metodología MAGERIT para minimizar los riesgos de la implantación y uso de TI en una Municipalidad del Perú. Metodológicamente se desarrolló como una investigación de tipo cuantitativa y descriptiva, enmarcada en un diseño no experimental de corte transversal, utilizando una muestra de 201 activos que están integrados a la seguridad informática de la institución. El método propuesto se basa en la metodología MAGERIT, que se adhiere a dos (02) fases esenciales: (1) análisis y evaluación de riesgos y (2) gestión del riesgo. Como resultado del trabajo se obtuvo que los activos que están en un nivel *mayor* de exposición son los del tipo "persona", correspondiente al personal de la Unidad de Tecnologías de la Información (UTI), por ser el trabajador clave en el proceso de seguridad informática; los del tipo "instalaciones", específicamente el área inherente a la UTI, donde se acogen los equipos de transmisión de datos de la institución; y los activos inherentes del tipo "servicios", donde soporte técnico e internet resultaron ser los de *mayor* impacto y riesgo. Se concluye que, a partir del proceso de diagnóstico llevado a cabo, se pudo determinar que actualmente la Municipalidad carece de medidas de control para garantizar las de la seguridad informática, aun cuando posee 204 activos por proteger, y en función de ello, no se ha concretado una cultura organizacional al respecto, mucho menos, procesos y procedimientos documentados para protección de la información.

Palabras Claves: Gestión de riesgos, Análisis de riesgos, Metodología MAGERIT, Seguridad informática, TI.

Abstract

The present work aims to develop a risk management model based on the MAGERIT methodology to minimize the risks of the implementation and use of IT in the Municipality of Peru. Methodologically, it was developed as a quantitative and descriptive research, framed in a non-experimental cross-sectional design, using a sample of 201 assets that are integrated into the institution's computer security. The proposed method is based on the MAGERIT methodology, which adheres to two (02) essential phases: (1) risk analysis and evaluation and (2) risk management. As a result of the work, it was obtained that the assets that are at a higher level of exposure are those of the "person" type, corresponding to the ICU staff, as they are the key worker in the computer security process; those of the “facilities” type, specifically the area inherent to the Information Technology Unit (UTI), where the institution's data transmission equipment is housed; and the inherent assets of the “services” type, where technical support and the internet turned out to be the ones with the greatest impact and risk. It is concluded with from the diagnostic process carried out, it was determined that currently the Municipality lacks control measures to guarantee those of computer security, even though it has 204 assets to protect, and based on this, it has not been specified an organizational culture in this regard, much less, documented processes and procedures for information protection.

Keyword: Risk Management, Risk Analysis, MAGERIT Methodology, IT Security, IT.

I. INTRODUCCIÓN

1.1. Realidad problemática

Hoy en día, la gestión de riesgos en las esferas que envuelven la seguridad informática de las redes de comunicación, se ha convertido en el factor de mayor interés en las mejores empresas que van a la par con la globalización, principalmente para las que tienen intereses comerciales que se extiende a un edificio o región, e incluso a nivel internacional [1], que requieren en todo caso poder acceder a los espacios de procesamiento y registros de datos que se controlan a través de varios servidores y otras vías de conexión donde deben contar estratégicamente con una alta seguridad ante los posibles riesgos y amenazas, a partir de la adecuación de métodos que eviten que los sistemas inmersos sean vulnerados [2].

En función de ello, son varias las metodologías que se han desarrollado a nivel mundial para llevar acabo el análisis de riesgos en la seguridad informática (SI), siendo MAGERIT la pionera en las entidades gubernamentales (ministerios, gobernaciones, alcaldías, contralorías, entre otras), de países como España, donde fue desarrollada con ese especial propósito y atención de necesidades propias de ese tipo de organización, por cuanto su aplicación se lleva a cabo en el 87,6% de las administraciones públicas a lo largo de la distribución del espacio político de ese país [3]

Asimismo, en [1] aseveran, que MAGERIT maneja un excelente esquema de análisis y evaluación de riesgos, que conllevan a su efectivo tratamiento y por tanto es recomendada para las entidades estatales, motivo por el cual se ha aplicado bajo un volumen promedio en un 54% de los entes gubernamentales de Latinoamérica. Bajo esta misma idea, dado a su versatilidad, sencillez de aplicación y por su buen desarrollo documental en español, se ha extendido con éxito en su implementación para la gestión de riesgos en el 73,7% de los entes del gobierno de Chile, en un 59,8% en los de Ecuador, en un 90,5% en los de Colombia, en un 94,1% en los de Venezuela y un 81,9% en los de Perú [4].

Tal como se percibe, en las distintas instituciones que representan la administración pública de Perú, la gestión de riesgos de las tecnologías de la información (TI) no está exenta de alinearse a la gestión de la seguridad de la información, y así mantener de forma fiable las amenazas y peligros a los que se exponen, es decir, debe tener presente de forma clara, hasta qué grado está involucrado y las consecuencias que se pueden desprender de esa situación [5], por lo que muchos entes gubernamentales han adoptado la metodología MAGERIT para cumplir con la función de control de protección de información ante riesgos, medidas de seguridad y buenas prácticas establecidas en las leyes vigentes desde la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), a la cual están sujetas todas las instituciones del Estado [6]

Ante esta situación, son muchas las municipalidades concentradas en Lima-Perú, que por ser pequeñas se han alineado a poner en funcionamiento sistemas de SI bajo el enfoque de la metodología MAGERIT que en cuanto a seguridad de la información conlleva al fortalecimiento y garantía para que los activos tangibles e intangibles sean resguardados [7], y además los riesgos se puedan reconocer a través de procedimientos ya conocidos que se relacionan con herramientas de seguridad informática debido a que todas estas instituciones públicas se encuentran propensas a padecer transgresiones, por muy idóneo que sea su sistema de protección de infraestructura de TI, permaneciendo en un mundo donde la tecnología avanza a pasos agigantados y de esta manera se pueda dejar de infiltrar en las redes y sistemas de formas ilimitadas de todo tipo de virus en general [8].

De esta situación no escapa la Municipalidad Distrital de Papayal, en la Provincia de Zarumilla, Departamento de Tumbes, la cual está al servicio de atención de las necesidades de la comunidad, para lo cual cuenta en gran parte con un despliegue de mecanismos estratégicos de integración, en cuanto a controles administrativos, operativos y recurso humano, esto para mantener una estrecha relación con los diversos factores que le dan vida a la actividad institucional y organizacional; y ante esto, maneja una gran infraestructura informática, por medio de la cual gestiona gran cantidad de información que parten de

documentos de su labor diaria ante la ciudadanía [9].

Sin embargo, en la Gerencia de la citada Municipalidad, se pudo reconocer que hoy en día se encuentra presente un mal manejo de nuevos sistemas y equipos de telecomunicaciones adquiridos, cuyo desempeño no ha llegado a buen término durante su adecuación a los procesos de la institución, y ante esto han tenido que ser desincorporados después de haberse dispuesto de una gran inversión, ya sea por aversión del personal ante los cambios a otros sistemas; situación que de alguna manera también propicia a que la seguridad de la información de manera general sea crítica, al percibirse un manejo inadecuado de la misma, así como algunos recursos informáticos o de red institucional que evidentemente son ilícitos, causando una inapropiada regulación de acceso y perdida de información.

Aunado a esto, en [10] resalta que en situaciones similares se pueden distinguir las limitaciones de rango en el tiempo para tener acceso a la misma, las modificaciones no autorizadas, fallas con prolongaciones en la red, sistemas informáticos dañados por la exposición a virus, y de otras maneras de acceso remoto inseguros en puntos que no están monitoreados, además de un control exhaustivo de sus activos.

El contexto al que se hace mención, se debe a que la institución carece de lineamientos y políticas que se orienten a gestionar una óptima implementación y uso de la infraestructura tecnológica que se va incorporando a la Municipalidad, e igualmente, que puedan garantizar la disponibilidad, integridad y confidencialidad de la información ya que no se han dirigido métodos para examinar a primera instancia las necesidades de seguridad que el caso requiere bajo el marco de los riesgos que los caracteriza, identificando el más efectivo, y en efecto hasta ahora no se conoce que tan vulnerable se encuentra ante las amenazas de los riesgos a la que se ve propensa la información que se maneja a nivel operativo y administrativo en este organismo público, así como las acciones a decidir, o bien propiamente sus activos tangibles e intangibles.

Por lo tanto, es claramente esencial llevar a cabo un modelo de gestión de riesgos que evite los riesgos ante la implantación y uso de TI en la Municipalidad Distrital de Papayal, ya que estas son de gran apoyo en la labor de protección de activos que maneja la Municipalidad, permitiendo a su vez controlar los riesgos antes que estos mitiguen y vulneren la integridad de la infraestructura tecnológica de la organización, asimismo, se brinde eficiencia ante la ejecución de tecnologías futuras.

Ante lo expuesto, el presente trabajo de investigación se justifica ya que actualmente es de menester, que las instituciones públicas manejen la información en la mayoría de sus procesos operacionales y de gestión basadas en la implementación de sistemas informáticos y los fundamentos que incluyen. De esta manera es como ha ido tomando importancia la utilización de instrumentos que ayuden a visualizar la magnitud de los riesgos a los que se hacen ostentar el acceso a los datos, reconociendo las amenazas, debilidades e impactos en las operaciones de la institución, en donde el progreso continuo en gestión de la seguridad que enfocan las normas ISO 27001 en base de seguridad informática es equivalente a garantizar la prolongación y disposición de la eficiencia que pueda ofrecer en este sentido.

Desde este punto de vista, como la Municipalidad Distrital de Papayal, maneja un alto nivel de información en todos sus procedimientos que abarcan todos los datos en físico y electrónicos los cuales están enlazados a varios sistemas de tecnologías de la información, cuyo resguardo de estos activos es de vital importancia, recobra interés institucional la actual investigación, en la cual se analizan diferentes instrumentos que están orientados a la protección en base a la seguridad de la información, para poder reconocer su grado de eficacia, frente a su desempeño con la norma técnica ISO 27001.

Así mismo, en base a la percepción del instrumento más eficaz, a nivel metodológico es importante este trabajo, ya que la gestión de la Municipalidad Distrital de Papayal logrará tomar las medidas más enfocadas en relación con los métodos más favorables de seguridad y resguardo de los activos, y de esta manera garantizar la confidencialidad, integridad y

disponibilidad de la información en sus operaciones, y con ello reducir riesgos ante alguna amenaza.

Aunado a lo expuesto, la institución se beneficia a nivel legal, ya que se alinea a cumplir ordenanzas orientadas al cumplimiento de la Ley 29733 - Protección de Datos Personales del estado peruano, que establece en sus artículos la adopción de medidas que fortalezcan la seguridad para el resguardo adecuado de los datos personales; así como con la Ley 30096 - Delitos Informáticos, donde la ONGEI emite esfuerzos para la promoción de políticas de seguridad para proteger los datos informáticos y los sistemas en los entes públicos.

1.2. Formulación del problema

¿Cómo se pueden minimizar los riesgos de implantación y uso de TI en una municipalidad del Perú?

1.3. Hipótesis

El desarrollo de un modelo de gestión de riesgos puede minimizar los riesgos de la implantación y uso de TI en una Municipalidad del Perú.

a. Hipótesis Nula

El desarrollo de un modelo de gestión de riesgos no minimiza los riesgos de la implantación y uso de TI en una Municipalidad del Perú.

b. Hipótesis Alterna

El desarrollo de un modelo de gestión de riesgos si minimiza los riesgos de la

implantación y uso de TI en una Municipalidad del Perú.

1.4. Objetivos

1.4.1. Objetivo general

Desarrollar un modelo de gestión de riesgos basado en la metodología MAGERIT para minimizar los riesgos de la implantación y uso de TI en una Municipalidad del Perú.

1.4.2. Objetivos específicos

- Diagnosticar la situación actual de la institución, así como la identificación de su gestión de seguridad y los activos.
- Caracterizar la metodología MAGERIT, y así adaptar su método al análisis y tratamiento de los riesgos presentes en los activos de la institución, para su respectivo análisis de amenaza y vulnerabilidad.
- Diseñar el modelo de gestión de riesgos para la Municipalidad Distrital de Papayal, y así garantizar la implantación y uso de TI.
- Implementar el modelo de gestión de riesgos propuesto en la Municipalidad Distrital de Papayal.
- Validar por juicio de expertos el modelo de gestión de riesgos propuesto para la Municipalidad Distrital de Papayal.

1.5. Teorías relacionadas al tema

1.5.1. Seguridad de la información

Todos los datos que maneja una organización producto de su labor de servicio y labor

productiva se refieren a la información que esta engloba. La misma puede estar representada bajo escritura, figurativa, en forma de audio, entre otras modalidades que puedan ser almacenada en medios digitales con el fin de poder ser transmitidos por vía correo electrónico o sistemas telefónicos [11].

Considerando lo expuesto, la ISO 27001 dice, que la confidencialidad, integridad y disponibilidad, son parte de las garantías que pretende encaminar en toda empresa la seguridad de la información, unido a métodos que forman el esquema de gestión de TI para su proceso. De acuerdo con lo expresado, se detallan a continuación las características que según Zeña [2], dimensionan la seguridad de la información:

a. **Confidencialidad:** Es garantizar que la información, única y exclusivamente, esté a disposición de personas autorizadas y no sea revelada sin consentimiento.
b. **Integridad:** Se refiere a la exactitud, fiabilidad y tratamiento correcto de la información, sin presentar ningún tipo de error ni fallas.
c. **Disponibilidad:** Asegura que la información se obtenga de forma rápida y sencilla, cuando sea solicitada por el personal autorizado sin límite de acceso.

Estas premisas, son las consideradas como garantes de la eficacia en la gestión de seguridad de la información, es por esto por lo que las organizaciones tienen el compromiso de respaldar sus procedimientos informáticos y vincularlos con mecanismos de protección que ante riesgos les ayuden a exponerse y en todo caso impedirlos.

1.5.2. Seguridad informática

Para Oliván [3], comprende el conjunto de normas alineadas al efectivo logró del trabajo y rendimiento de un sistema de información sólido y protegido, que basado en técnicas

de seguridad también cubra sus demás elementos que lo conforman para alcanzar un buen servicio.

El mismo autor sobre esa base afirma que la seguridad informática se originó con los fundamentos y procedimientos técnicos que se desarrollaron con la finalidad de salvaguardar los activos tecnológicos institucionales. Tales aspectos que entran en el ámbito de resguardo se enmarcan en el contexto sobre: (a) lo que hay que proteger (hardware, software y datos), es decir, los activos que constituyen el sistema; (b) de quienes se debe proteger, que en este caso son de las potenciales amenazas del entorno, como son las personas, amenazas tecnológicas, y fenómenos propios del medio ambiente; y (c) como se puede proteger, es allí donde aplica la inserción de estrategias que consideran políticas y normas de seguridad, prácticas y herramientas. Todo ello, para evitar que los peligros de la seguridad de la información alcancen niveles que sean difíciles de mitigar [12].

1.5.3. Gestión de riesgos

Granadino [4], dice que un riesgo surge de un suceso imprevisible que podría tener un impacto negativo (amenaza) o positivo (oportunidad) en los objetivos de un proyecto. El riesgo se define como la posibilidad de exponer un sistema a la manifestación de un peligro en los activos de una institución, que es vulnerable ante desviaciones que impacten su integridad. Es decir que el riesgo indica lo que le podría pasar a los activos si no se protegen adecuadamente [5].

Se basa en una perspectiva mixta de enfoques cuantitativos y cualitativos que se representan en la cuantificación y valoración de los activos de la organización, donde estos se evalúan, se definen los peligros y debilidades para que se desarrollen, así como la posibilidad de que puedan ocurrir [1].

1.5.3.1. Etapas de la gestión de riesgos

En este aspecto, se logran distinguir las siguientes fases de la gestión de riesgos:

a. **Identificación de las amenazas y riesgos:** se centra fundamentalmente en la seguridad de los datos de información, estos peligros se pueden diferenciar de tres maneras:

   - **Entrada ilegal al sitio de los datos:** donde es adecuado examinar las adversidades que ocasionaría que fueran reveladas por personal que no posee autorización a su acceso (confidencialidad).
   - **Cambio no autorizado de los datos:** relacionado al daño causado al arruinarse o cambiarse de forma mal intencionada (integridad).
   - **Exclusión de los datos:** se refiere al daño que ocasiona no poseer la información solicitada en el instante requerido (disponibilidad). [6].

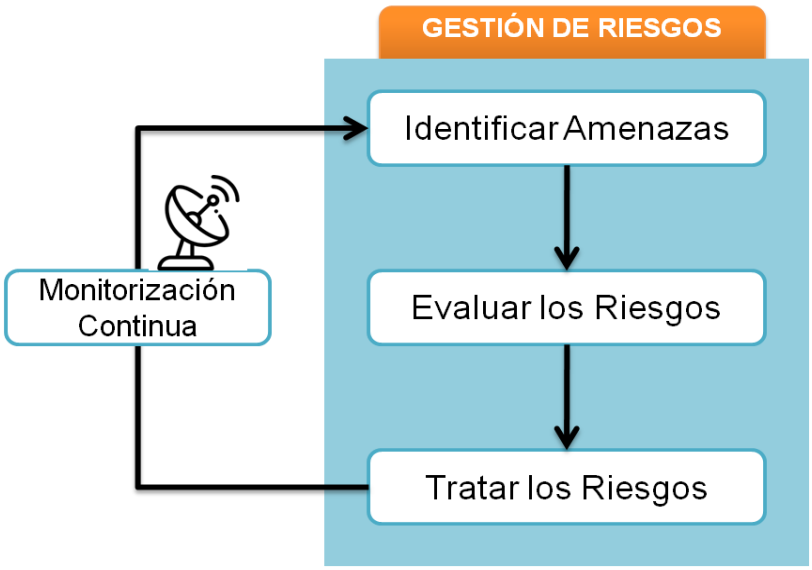
En este sentido, por lo general toda amenaza está relacionada a un riesgo sistematizado, por la cual el acto de tener identificados los riesgos siempre está ligado con tener definidos las causas que lo originaron.

b. **Evaluación de los riesgos**: está alineado a la valoración del daño a la que se encuentra exhibida la amenaza frente a la probabilidad de que esta se ejecute. Se puede resaltar, que el impacto se define en base a la falla detectada frente a la amenaza de un peligro, basándose en el potencial del suceso relacionado a esta es que se logra establecer el grado del riesgo [6].

c. **Tratamiento de los riesgos:** en esta fase finalizan los procedimientos de la gestión de riesgo, cuyas metas es encontrar las políticas de control que ayuden a disminuir y evadir el rango de exhibición de los activos frente a los continuos peligros [6].

Figura 1

Etapas de la Gestión de Riesgos



Nota: Adaptación de Agencia Española de Protección de Datos [6].

1.5.4. Metodologías para el análisis de riesgos y seguridad informática

Hoy por hoy, la seguridad informática y seguridad de la información, como tema base en predios de las tecnologías de la información se fundamentan en un conjunto de métodos de evaluación y gestión de riesgos, cuya selección se efectúa basada en la más apropiada perspectiva para ser aplicada de forma eficiente, de tal forma que se ejecute hasta el cumplimiento de sus metas.

No obstante, se puede resaltar que aun con metodologías muy avanzadas y

acreditadas, es complicado lograr la protección total referente a la gestión de riesgo, sin embargo, con el desarrollo de normas para el control se puede obtener la eficiencia en la calidad de resguardo, para disminuir los riegos como lo alega Alvarado [1].

De acuerdo con Alvarado [1] entre los métodos de gestión de riesgos más acreditados y adecuados al trabajo de los organismos de instituciones públicas, se pueden encontrar: OCTAVE, MEHARI, CRAMM, EBIOS y MAGERIT, de las cuales se suministra una introducción seguidamente:

- **OCTAVE (Operationally Critical Threat, Asset, And Vulnerability Evaluation)**, ha sido muy implementada para afrontar los riesgos de seguridad de la información adaptables a las TI en reconocidas instituciones con un número de trabajadores superior a los 300, concediendo el análisis y evaluación de cada capa de la estructura informática y sus escalas, para su siguiente técnica de remisión. Las cuales garantizan a las compañías normas frente a riesgos activos que perjudiquen al capital de la institución, y también dar seguimiento con un buen mecanismo de trabajo [7].
- **MEHARI**, fue llevada a cabo por CLUSIF (Club Francés de la Seguridad de la Información) en 1996 en Francia, abarca una técnica que vincula la evaluación con la gestión de riesgos para cualquier tipo de instituciones, y soliciten su inspección, administración y monitoreo, empleando metódicamente una distribución en módulos. Por lo tanto, es necesario un mecanismo de producción y accionamiento laboral capacitado [7].
- **CRAMM (CCTA Risk Analysis And Management Method)**, desarrollada por una institución pública de Inglaterra CCTA (Central Communication and Telecommunication Agency) opera dentro de su técnica de evaluación de riesgos más implementados en los países europeos por empresas reconocidas e instituciones públicas con un gran número de personal, tales como la OTAN, entre otras. Operan a gran nivel un plan de adaptación, esquemas de normas de protección ante amenazas,

después la evaluación de riesgos, y finalmente el análisis de control para moderarlos y en el mejor de los casos, erradicarlos [7].

- **EBIOS (Expresión de las Necesidades e Identificación de los Objetivos de Seguridad)**, de origen francés, este método está centrado en evaluar y administrar el riesgo de protección de un sistema de información de forma argumentada, bajo una política que ayuda a evidenciar su efecto en los procedimientos de la institución y a escala de sus finanzas [7].

1.5.5. MAGERIT como metodología de seguridad informática

MAGERIT, actualmente en su versión 3, es un método presentado por el Consejo Superior de Administración Electrónica para analizar y gestionar la situación de riesgos de los sistemas de información y así disminuirlos cuando son infiltrados en las organizaciones gubernamentales [1].

López [7], añade que es un método fácil de manejar, por ende, no es necesario tener instrucciones especializadas para su aplicación, en base a esto la puede manejar una o dos personas correspondientes a la institución, sin importa el tamaño de su agente humano.

Al estar alineada MAGERIT al mencionado contexto, es decir: (a) por ser diseñada explícitamente para ser aplicadas en instituciones del gobierno a disposición de un servicio público como lo es la Municipalidad Distrital de Papayal, (b) catalogada como una organización pequeña al contar solo con 51 funcionarios, y (c) con muy reducido personal en el área de TI (sólo una persona y un colaborador en ocasiones) para llevar a cabo el análisis y gestión del riesgo, en este informe de investigación se pretende poner en práctica dicha metodología ya que los aspectos detallados se identifican con los criterios de selección para ser aplicada en dicha institución. Siendo así, se destacan a continuación los aspectos que más resaltan de la metodología MAGERIT, aplicada al proceso de gestión del riesgo en los sistemas de información, en cuanto a la identificación, evaluación y tratamiento.

1.5.3.2. Principales características de MAGERIT

Ante esto, Alvarado [8] dice que entre las bondades que ofrece la metodología MAGERIT es que está en Español, aunque se coloca en primera instancia el conjunto de procedimientos metódicos y continuos para valorar y medir los riesgos a los que se ven expuestos las TIC, de manera de poder enfocar controles óptimos que sean eficientes en lo que a gestión de seguridad se refiere, identificando amenazas latentes en la organización ante las cuales se puedan adecuar las medidas preventivas y correctivas más eficaces.

1.5.3.3. Objetivos de MAGERIT

La metodología MAGERIT tiene como objetivos sensibilizar a los miembros de la organización a que se adecuen a los riesgos y amenazas existentes, y que, a su vez, estos sepan afrontarlos, así como poner a la orden un instrumento de trabajo que les permita analizar los riesgos que se desprenden de las TIC. Esto permitirá llevar a cabo planes y tratamiento en el momento requerido para controlar el índice de riesgos.

1.5.3.4. Elementos considerados en MAGERIT

Cuervo Álvarez [9], señala que la metodología MAGERIT toma los siguientes elementos para llevar a cabo la seguridad de la información:

- **Activos**: está representado principalmente por los datos y distintos recursos tecnológicos que componen una institución y constituye su sistema de información. Es la unidad principal que proteger. Integran toda la población de estudio.

- **Amenazas al activo**: son las amenazas a las que se exponen los activos de la empresa, frente alguna contingencia. Al conformarse pueden incidir en pérdidas de algunos activos de la institución, ya sean tangibles e intangibles.
- **Vulnerabilidad del activo**: es la posibilidad de que ocurra algún fallo o error poniendo en riesgo los activos.
- **Impacto de un activo**: son las secuelas de que se materialice un ataque sobre los activos.

1.5.3.5. Fases de la gestión de riesgos bajo la metodología MAGERIT

De acuerdo con Cuervo Álvarez [9], el método se adapta al siguiente modelo en dos (02) subprocesos principales:

a. **Análisis de Riesgos**: se acerca sistemáticamente a determinar el riesgo actual, así como se muestra a continuación:

- Determinación de los activos a resguardar.
- Estimación de activos.
- Determinación de peligros a los que están exhibidos los activos.
- Calcular el impacto basado en la valoración del daño a los que se ve expuestos un activo frente acontecimientos inseguros. El cual se puede calcular a través de la siguiente ecuación:

Impacto = Valor del activo x Porcentaje de Impacto

- Calcular el riesgo probable frente al impacto tomando en cuenta la continuidad en las que se puede presentar.

Riesgo = Frecuencia x Impacto

- Elegir apropiadamente el método para los riesgos reconocidos mediante funciones adecuadas.
- Disminuir el riesgo y los riesgos residuales debido que, al aminorarse cierto volumen de estos, se reduce su rendimiento, los cuales se denomina riesgos residuales.
- Valorar el riesgo, se define como el impacto por posibilidad.

Es de resaltar, que los parámetros de estimación de los activos, las debilidades, riegos y peligros, se consideran de “bajo” nivel cuando su valoración es igual a 1, se califican “medios” cuando la valoración es igual a 2 y se estiman que son de nivel “alto” cuando su valor es igual a 3.

b. **Tratamiento de riesgos**: etapa donde se proyectan las técnicas de inspección frente los acontecimientos de mala seguridad, y de esta manera poder certificar la secuencia de los procedimientos.

La aplicación, ofrece las funciones:

- R-Box: herramienta para analizar y evaluar riesgo bajo el marco de la

metodología MAGERIT.

- GxSGSI: herramienta para gestionar el desempeño del riesgo en función de la metodología MAGERIT.

Tal como se observa, MAGERIT se caracteriza por ser un instrumento para facilitar la implantación y aplicación del Esquema de Seguridad.

1.5.3.6. Modelo de gestión de riesgos basado en MAGERIT

Cuervo Alvarez [9], argumenta que su Sistema de Gestión de Riesgos (SGR) está centrado en las técnicas ISO 27001, y contienen:

Tabla 1

Contenido del Sistema de Gestión Bajo Metodología MAGERIT

Dominio	Descripción
Definición de la política de seguridad	Abarca los objetivos, el marco general, los requerimientos legales, los criterios de evaluación de riesgos.
Definición del alcance del SGR	Delimita hasta donde llega el plan de acción dentro de la organización considerando los activos, las TI, con sus respectivas descripciones.
Identificación de los riesgos	Describe las amenazas a las que están expuestos los activos de la organización, los responsables directos, a qué son vulnerables y el impacto en los activos en caso de que se vean afectada su confidencialidad, integridad y disponibilidad.
Análisis y evaluación de los riesgos	Corresponde a estimar el impacto de algunos de los riesgos si se llega a materializar. Se percibe allí la probabilidad de ocurrencia y cómo esto afectaría los controles implementados.
Tratamiento de riesgos	Se sugieren o aplican aquí los controles necesarios, de acuerdo a los riesgos identificados. También se clasifican los niveles de riesgo.
Políticas de Gestión para la seguridad en TI	Se define el tratamiento de los riesgos, vinculados a los controles, y ante esto se diseñan los indicadores para medir la eficiencia y eficacia de la gestión. Igualmente se plantea el plan de comunicación del SGR para promover la concientización y fomentar una cultura organizacional sobre el cumplimiento del mismo.
Monitoreo	Se lleva a cabo el diseño de estrategia de auditoría para la verificación y revisión periódica del SGR para determinar hasta qué nivel se está cumpliendo con la normativa.

Una vez concretado el análisis y evaluación de riesgos, será necesario desarrollar un sistema de gestión para garantizar la seguridad de la información, aplicando el esquema de elaboración del modelo de gestión planteado por MAGERIT, y con ello conllevar a la institución de administración pública a minimizar los riesgos a los cuales están expuestos todos sus activos.

1.5.6. Ley de Protección de Datos Personales

Tal fundamento legal distinguido con el N° 29733 sobre la Protección de datos personales (2013) establece que surge ante los requerimientos de regular la utilización de la información personal en todas la operaciones y transacciones en las que negocian las instituciones que cobran vida en el país. [10]. Según especifica la ley, que el objetivo de la norma se enfoca en la protección plena de la identidad personal del ciudadano, más aún a través de los canales que integran la TIC.

1.5.7. Normas Técnicas Peruanas de Seguridad de la Información

1.5.3.7. 2NTP- ISO/IEC 27001:2022

Esta metodología en su versión anterior 2005 y 2013, fue desarrollada para fortalecer los requerimientos principales en la aplicación, estructuración y conciliación de una distribución de gestión de riesgos de la seguridad de la información; dado que está basada en cubrir los requisitos de la organización, la seguridad y todas las operaciones propias de la institución [11].

La nueva ISO 27001:2022 [12], "Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos", que se publicó en octubre de 2022, señala que la ISO ejecuta de manera

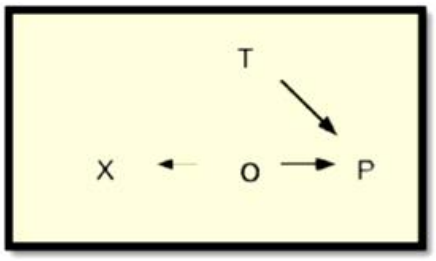
satisfactoria las principales etapas como lo son la programación, aplicación, acción y seguimiento que se consideran dentro del esquema de un sistema de gestión de riesgos. Se puede visualizar con antelación, que en la fase concluyente practica las normas del ciclo Deming, a través del cual se utilizan después de la evaluación los sistemas de gestión de seguridad informática (SGSI).

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación

La investigación es de tipo aplicada y descriptiva, dado que se orienta a detallar y cuantificar todas las variables que caracterizaron las situaciones que sobresalen en el caso de estudio, basándose a su vez en trabajos originales elaborados para obtener un nuevo conocimiento y aporte práctico, que en este caso fue en función de los riesgos latentes en los activos de la institución, como también los peligros a los que se exponen y sus debilidades frente a estos, y así conseguir un análisis con mayor certeza, vinculado a la circunstancia presente en el área de investigación [13].

Para la contrastación de la hipótesis se tomó como guía el documento de metodologías de la investigación de los autores Hernández, Fernández y Baptista [14], y en función de ello, se consideró este estudio como un diseño no experimental de corte transversal y propositivo. Es no experimental ya que no se manipuló sobre ninguna variable; transeccional o trasversal: debido a que se implementó en un momento dado y; propositivo, porque se desarrolló con una estructura referencial y luego se procedió a elaborar la valoración de la gestión de riesgo y el esquema del método, que permita mitigar las amenazas durante implantaciones y uso de TI en la Municipalidad Distrital de Papayal, en la Provincia de Zarumilla, Departamento de Tumbes, el mismo que al ser llevada a cabo, generó información de calidad y recomendaciones propuestas a los entes competentes para la toma de decisiones y ante soluciones de los eventos que suceden. En el siguiente esquema que se muestra se considera el vínculo de los elementos expuestos anteriormente:



Donde:

X: Realidad de la institución

O: Observación

T: Modelo teórico

P: Propuesta de soluciones y recomendaciones basadas en la norma ISO 27001.

2.2. Variables, Operacionalización

2.2.1. Variable independiente

Modelo de Gestión de Riesgos.

2.2.2. Variable dependiente

Riesgos de la implantación y uso de TI en una Municipalidad del Perú

Tabla 2

Operacionalización de variables

Variable de Estudio	Dimensiones	Indicadores	Técnicas e Instrumentos / Unid de Medida
Variable dependiente: Riesgos de la implantación y uso de TI en una Municipalidad del Perú	Diagnóstico de situación actual	- **Índice de frecuencia** = Tipo de riesgo × Cantidad de ocurrencias al año	Análisis Documental
	Eficacia de MAGERIT según su característica	- **Índice Usabilidad (AP Latinoamérica)** = Cantidad de instituciones AP que utilizaron MAGERIT en año 2018 / Cantidad total de instituciones AP que realizaron análisis de riesgos en año 2018 x 100	Registros históricos de la institución
		- **Índice Implementación (AP Latinoamérica)** = Cantidad de procesos de la metodología implementados / Cantidad de procesos de la metodología planificados x 100	Análisis Documental
	Valoración de activos (VA) por su disponibilidad, Integridad y Confidencialidad	- **VA de aplicaciones informáticas** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de equipos informáticos** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de redes de comunicaciones** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de instalaciones** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de servicios** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de personas** = 1 (Baja); = 2 (Media); = 3 (Alta)	Guías de observación (lista de registros)

Valoración de Amenazas de un activo (VAA) por su probabilidad de ocurrencia	- **VAA de aplicaciones informáticas** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VAA de equipos informáticos** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VAA de redes de comunicaciones** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VAA de instalaciones** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VAA de servicios** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VAA de personas** = 1 (Baja); = 2 (Media); = 3 (Alta)	Análisis Documental Ficha documentaria
Valoración de Vulnerabilidades de un activo (VVA) por el control de su seguridad	- **VA de aplicaciones informáticas** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de equipos informáticos** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de redes de comunicaciones** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de instalaciones** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de servicios** = 1 (Baja); = 2 (Media); = 3 (Alta) - **VA de personas** = 1 (Baja); = 2 (Media); = 3 (Alta)	Entrevista Guía de entrevista (La información y los riesgos)
Evaluación de amenaza y vulnerabilidad de los activos	- **Índice de Vulnerabilidad** = Promedio ∑ nivel de eventos - **Índice de Impacto** = Promedio ∑ nivel de eventos - **Índice de Riesgo** = Probabilidad × Impacto	

Tabla 2

(Cont.).

Variable de Estudio	Dimensiones	Indicadores	Técnicas e Instrumentos / Unid de Medida
Variable Independiente: Modelo de Gestión de riesgos	Eficacia del modelo propuesto (EFMO)	***% EFMO =*** *IAAP – IDAP x 100* / *IAAP*	Observación directa. ficha de observación
	Eficacia de controles en costos por incidentes (ECi)	**ECi** = Diferencia de costo de reparaciones de equipos entre años 2019 y 2020 / Costo de reparaciones de equipos año 2019 x 100	
	Nivel de coherencia y correspondencia	**IT1…IT(n)** = Muy Bueno, Bueno, Aceptable, Requiere atención y Crítico	Observación directa. Lista de chequeo

2.3. Población de estudio, muestra, muestreo y criterios de selección

La población está conformada por todos los activos de la Municipalidad Distrital de Papayal, es decir, 35 aplicaciones informáticas, 80 equipos informáticos, dos (02) redes de comunicaciones, 27 instalaciones, 6 servicios, 51 personas, para un total de 201 elementos. En este aspecto, la muestra está conformada por la población total, debido a que serán reconocidos los 201 activos que constituyen la función de administración de información de la Municipalidad.

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

Se emplearon los siguientes:

- Observación
- Análisis de documentos
- Entrevista informal

Instrumentos*:*

- Registros históricos de frecuencia de incidentes de SI ocurridos en el 2019, aplicado para el desarrollo del objetivo 1, el cual se utilizó para registrar los factores de riesgos y hallazgos suscitados (ver Anexo 1).
- Ficha documentaria para dar paso al Objetivo 2, con la cual se asentó los principales aspectos que caracterizan la metodología MAGERIT (ver formatos en anexo 2). Igualmente se utilizó este mismo instrumento para sustentar el capítulo 3, donde se desarrolló el modelo de gestión de riesgos tomando en cuenta dicha

caracterización.

- Matriz de observación: se contó una para el desarrollo de objetivo 1, con una lista de registros de activos identificados (ver anexo 3), para conocer los bienes asociados a la SI, de la institución. También se diseñó otra que permitió el desarrollo del objetivo 4, mediante las cuales se pudo recoger la perspectiva de los usuarios del área de informática para valorar activos identificados, amenazas y vulnerabilidades, aplicando a su vez las plantillas de análisis y evaluación (ver anexo 4).
- Guías de observación: Se utilizó como complemento del desarrollo del objetivo 4, contentivo de una lista de chequeo (checklist, en Anexo 5) que permitió hacer un diagnóstico general del estado de la seguridad informática y así verificar las actuales salvaguardas con los que cuenta la institución. También se elaboró una segunda lista de chequeo para el desarrollo del objetivo 5 (checklist, en Anexo 6) que permitió la validación del modelo de gestión de riesgo por parte de tres (03) especialistas en el tema de SI en TI.

Validez del instrumento:

No se consideró validación de instrumento porque todo estaban basado en la observación directa, es decir, ninguno se enfocó a estudiar la opinión de población o muestra alguna. Sin embargo, si entró en proceso de validación fue el modelo propuesto, en donde intervinieron tres (03) expertos en el área.

2.5. Procedimientos de análisis de datos

a. La *Entrevista* se dio con cada uno de los involucrados de manera individual, solo con

dos (02) Ingenieros de campo de la Municipalidad, donde la junta se realizó de forma grupal. En esta reunión se obtuvo el reconocimiento de los activos, la examinación de la estimación de los activos, los peligros y sus debilidades.

b. *La Observación* se dio del ejecutar continuo de los activos implicados, proporcionándose una representación de las circunstancias presentes de los inconvenientes de la gestión de riesgos en la seguridad informática y de esta manera conocer los procedimientos que fueron razón de análisis. Así mismo se implementó la valoración del modelo de gestión de riesgo por parte de tres (03) especialistas en el tema de SI en TI.

c. *Análisis de documentos*, que operan en todos los procedimientos de seguridad de la información y gestión de riesgo que ocurrieron en el transcurso del año.

d. Elaboración del modelo de gestión basado en todos los matices de seguridad física y de sistemas frente a los riesgos y peligros a la confiabilidad, integridad y la disponibilidad de la información, del mismo modo de las normas de protección por las se rige la metodología MAGERIT que para un mayor orden considera los objetivos de control de la ISO 27001.

- Precisión de la norma de seguridad.
- Determinación del efecto del SGR.
- Reconocimiento de los riesgos.
- Estudio y valoración de los riesgos.

- Métodos de riesgos.
- Administración.
- Supervisión (monitoreo).

2.6. Criterios éticos

El presente trabajo se basa en los criterios éticos establecidos en el Código de Ética en Investigación de la USS S.A.C., así como lo estipulado en la Declaración de Helsinki y el Reporte Belmont. Por lo que se resalta lo siguiente:

a) Es primordial respetar la privacidad de la información confidencial que la Municipalidad Provincial de Papayal proporciona para la investigación, así como también la que se recolecta de bases de datos incorporadas en plataforma TI en esta la institución. No obstante, frente a esto se necesitó una aprobación del organismo gubernamental a través de recursos escrito (ver anexo 7) para implementar su conocimiento general en esta investigación, y hacer uso de su denominación social.
b) Así mismo la seguridad de los datos de las personas involucradas en el estudio. En relación con esto, Se les exigió a los confidentes un comunicado de aprobación notificando (ver anexo 8), y de esta manera confirmar su consentimiento en la colaboración de esta investigación.

En este mismo orden de ideas, la credibilidad, la confirmabilidad y la transferibilidad también fueron tomadas como base para los criterios de rigor científico.

a. Credibilidad, se logra en el instante que los resultados obtenidos en la

investigación son acreditados por el autor de esta, como también por otros contribuyentes con quienes también se han deliberado las circunstancias percibidas. En el estudio actual se alcanzó el mencionado criterio debido a que las entrevistas fueron aplicadas como una conversación y no como un interrogatorio permitiendo así intercambiar ideas, indecisiones, observaciones que ayudaron a la evaluación y análisis de los activos, peligros y debilidades. Existiendo un ambiente de cordialidad en toda ocasión tanto como para el entrevistador como para el entrevistado.

b. La confirmabilidad, se percibe como la destreza que tiene otro autor de perseguir los pasos del investigador original obteniendo los mismos resultados; en la medida que todo se encuentre acreditado, tanto las técnicas de recolección de datos, soluciones, pensamientos, etc. Esto solo se obtiene teniendo enfoques iguales. En el actual estudio toda la información facilitada permitió que otro investigador pudiera proyectar una ruta semejante a la que se está efectuando, por esta razón obtener resultados parecidos o aproximados.
c. La transferibilidad, este criterio es el que accede a amplificar los resultados de la investigación a diferentes localidades, analizando en que dimensión los resultados se acercan a las diferentes situaciones. En el actual estudio se precisaron apropiadamente los resultados con fundamentos exactos, al tener ingreso a los datos de información por parte de las personas involucradas en esa labor.

III. RESULTADOS Y DISCUSIÓN

3.1. Resultados

Como resultado del primer objetivo de la investigación orientado a diagnosticar la situación actual de la institución, así como la identificación de su gestión de seguridad y los activos se pudo conocer que actualmente la Municipalidad, presenta muchas debilidades en la seguridad de la información dado que al no poseer el requerido control para la mitigación de incidentes antes las amenazas y vulnerabilidades, no toman acciones pertinentes cuando los mismos se manifiestan.

Lo antes señalado, genera como resultado un alto índice de situaciones subestándares reflejados en la tabla 3 y figura 2, según el tipo de riesgo (de acuerdo con la clasificación expuesta en las normas ISO 27001), que se presentaron a lo largo del año 2019 durante la gestión operativa y administrativa de la Municipalidad para su función social, en los activos de la institución.

Tabla 3

Incidentes de la gestión de seguridad informática ocurridos en el año 2019

Tipo de riesgo	Situación de riesgo	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total	Total riesgos
Institucional	**1.** Caída de los sistemas por corte eléctrico	2	1	3				5		1			1	**13**	62
	2. Daños en componentes de equipos	3	1	1				1		3				**9**	

	informáticos por corte eléctrico															
	3. Daños en aplicaciones informáticas por corte eléctrico	1	3							1					**5**	
	4. Desconexión de red por corte eléctrico	2	1	3			5			1			1		**13**	
	5. Recalentamiento de equipos informáticos por exceso de temperatura	3	4	2	2	3		1	1	2	2	1	1		**22**	
	6. Caída de los sistemas por falta de depuración	4	1		5			1		2	1	3			**17**	
Personas (por causa accidental)	**7.** Daños en aplicaciones informáticas por falta de actualización	2	1		1	1		1		1			1		**8**	58
	8. Pérdida de información por	2	1	1		2		1			1	1	1		**10**	

	mala restauración de los respaldos														

Tabla 3

(Cont.)

Tipo de riesgo	Situación de riesgo	Ene	Feb	Mar	Abr	May	Jun	Jul	Ago	Sep	Oct	Nov	Dic	Total	Total riesgos
Personas (provocadas intencionalmente)	**9.** Daños en equipos informáticos por falta de mantenimiento y actualización de software	3	2	1	3	1	0	5	1	2	1	2	2	**23**	84
	10. Hackeo de los sistemas por falta de políticas de control	1	1			2					1			**5**	
	11. Caída de los sistemas por agotamiento de los recursos ante su uso en equipos obsoletos	2	3	2							2	2	1	**12**	
	12. Distribución de virus en aplicaciones	5	2	3	1	2		3	1	2	2	2	1	**24**	

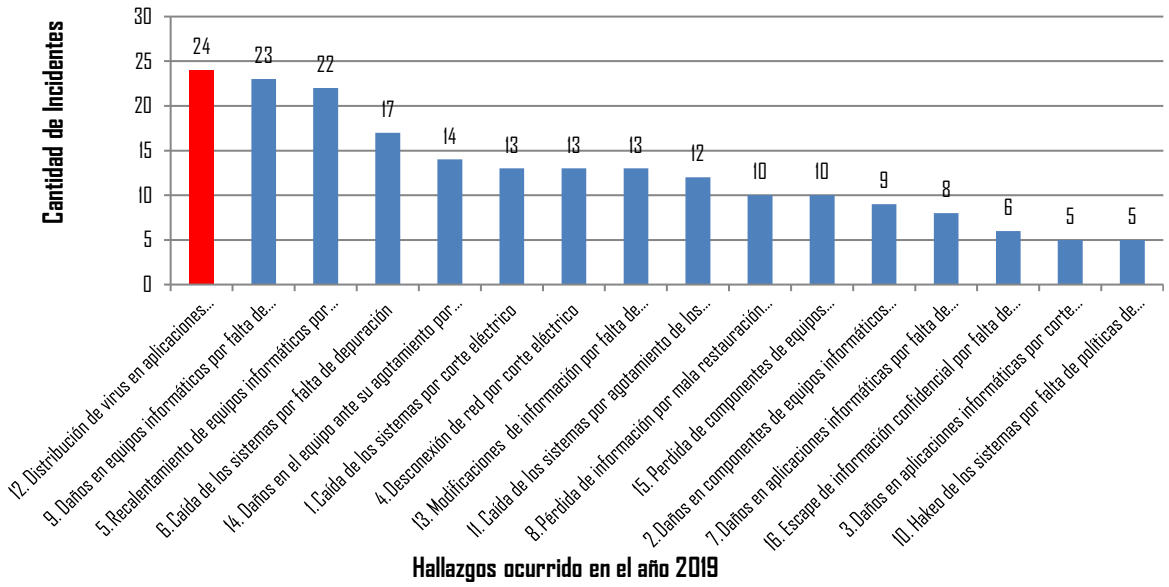
informáticas por desactualización de software de protección														
13. Modificaciones de información por falta de políticas de control de cambios	2	1	1		2		1	1	2	1	1	1	**13**
14. Daños en el equipo ante su agotamiento por obsolescencia	2	1	1	1	3		2	1	1		2		**14**
15. Perdida de componentes de equipos informáticos por falta de estrategias de control de entrada y salida de los recursos	2		4				1		1	1		1	**10**
16. Escape de información confidencial por falta de políticas de control de almacenamiento	1	1			1					1		2	**6**
Total	**37**	**24**	**22**	**13**	**15**	**0**	**27**	**5**	**19**	**13**	**14**	**13**	**204**

Nota: Tomado de la Unidad de Tecnologías de la Información de la Municipalidad Distrital de Papayal [14].

De acuerdo con la tabla 3, en el año 2019 se presentaron 204 situaciones de riesgos (bajo tipología estipulada en normas ISO 27001) que revelan un nivel alto de acontecimientos que perjudican la seguridad de la información en la Municipalidad, cuyo principal motivo radica en que el organismo gubernamental no posee métodos apropiados para el control de la seguridad de la información, ya que hasta ahora, no se ha abocado a gestionar evaluación alguna para determinar sus amenazas y vulnerabilidades, incumpliendo ante ello, su deber de resguardo de sus bienes públicos. Igualmente se pudo percibir que en el mes de junio y agosto los índices fueron nulos y bajos, debido a que en esos meses se hizo una supervisión general de riesgos en la institución que influyó en el sentido de cautela de los empleados.

Figura 2

Incidentes registrados en la gestión de seguridad informática ocurridos en el año 2019



Nota: Tomado de la Unidad de Tecnologías de la Información de la Municipalidad Distrital de

De acuerdo con la figura 2, que se desprende de los datos recaudados de la gestión anual de la Unidad de Tecnologías de la Información, los hallazgos suscitados en el tiempo de estudio, percibiéndose que el principal incidente detectado se debió al repartimiento de malware (virus) en los programas informáticos (aplicaciones) por la falta de actualización del software de seguridad, lo que ocurrió con una frecuencia de 24 en el año.

Le siguen las situaciones de riesgos por averías presentadas en los equipos informáticos dado a la falta de mantenimiento y actualización de software, que se presentaron en 23 ocasiones y el recalentamiento de equipos informáticos por exceso de temperatura experimentado 22 veces, caída de los sistemas por falta de depuración en 17 oportunidades, daños en el equipo ante su agotamiento por obsolescencia en 14 circunstancias, caída de los sistemas y desconexión de red por corte eléctrico, por 13 ocasiones. Esta situación la Institución tuvo que invertir en reposición de equipos informáticos que sufrieron daños por un costo promedio mensual de 17500 soles, según información aportada en el informe de gestión de la UTI.

Ante ese escenario, se vislumbra que el primer evento (en rojo) se considera crítico porque ocasionó lesiones graves, ya que se extendió a través de la red y ocasiono la falla total de los sistemas establecidos en la institución, por esta razón se perjudicaron los procedimientos administrativos y operativos por un de tiempo de 7 días, hasta que se logró su imperfecto restablecimiento y reciente restauración de estos.

Lo que sí es cierto, de que el hecho de no seguir las normas de protección para el manejo, control y seguimiento de la seguridad informática, que constituyan tácticas de prevención para salvaguardar los softwares y los equipos informáticos frente a los circunstanciales cortes de luz, amenazas de virus, manutención, innovación y mejoramiento las unidades, climatización de instalaciones, seguirá persistiendo hasta que los entes

competentes no tomen carta en el asunto.

Luego de haber determinado la situación, se procedió a desarrollar el segundo objetivo orientado a caracterizar la metodología MAGERIT, y así adaptar su método al análisis y tratamiento de los riesgos presentes en los activos de la institución, para su respectivo análisis de amenaza y vulnerabilidad.

Dicha metodología fue escogida para el desarrollo de modelo de gestión de riesgos dado a su buena adhesión a los criterios de selección sugeridos por López [7], y para demostrar su relevancia se procedió a estudiar sus bondades tomando en cuenta las experiencias de diversos autores que instan y recomiendan utilizarla, luego de compararla con otras metodologías como OCTAVE, MEHARI, CRAMM y EBIOS también utilizadas en el ámbito de gobiernos de estados latinoamericanos, tal como se percibe en la tabla 4.

Tabla 4

Comparación de MAGERIT con respecto a otras metodologías comúnmente utilizadas

Criterio de Comparación	**OCTAVE**	**MEHARI**	**CRAMM**	**EBIOS**	**MAGERIT**	**Autor (es)**
Funcionalidad	Apunta a la perspectiva en tres (03) fases para evaluar: (a) la organización y (b) ámbito	Se enfoca en sus tres (03) fases para: (a) diagnosticar la seguridad, (b) analizar las	Se complementa en tres (03) fases: (a) definición de la seguridad; (b) análisis de riesgos y (c) medidas y	Se lleva a cabo mediante el desempeño de cinco (05) fases: (a) análisis del contexto; (b) estudio de situaciones peligros. (c)	Aborda dos (02) fases que abarcan eventos como: (a) analizar riesgos y (b) aplicar	Alvarado, Pacheco y Martillo [14] López [7]

	tecnológico ; y (c) formula la planificació n para desarrollar la estrategia de seguridad.	implicacion es de la seguridad y (c) analizar los riesgos.	control de riesgos.	análisis de contexto ante amenazas. (d) estudio de los riesgos. (e) análisis de las medidas prácticas de seguridad: ejecución del modelo.	la gestión del riesgo.	Novoa & Rodrígu ez [15]
Ejecución	En su primera fase construye perfiles de amenazas, en la segunda por cada uno de los tipos activos. En la segunda identifica la plataforma tecnológica	En su primera fase detectan las salvaguard as con los que cuenta la organizaci ón. En su segunda fase estudia la importanci a que le	En su primera etapa fija en un plan estratégico sus objetivos de seguridad. En la segunda fase analiza los riesgos por tipo de activos en conjunto, en cuanto a amenazas y vulnerabilidad. Y en la tercera etapa identifica	En su primera fase se diagnostica la situación problemática. En la segunda fase los incidentes suscitados. En la tercera fase las amenazas que rodean la situación en estudio. En la cuarta fase se analizan los riesgos, es decir, se identifican y se evalúan por tipo	En su primera fase diagnostic a el contexto y sus riesgos, identifica elementos claves (activos, amenazas, vulnerabili dades y salvaguard	Alvarad o, Pachec o y Martillo [16] López [7]

	y su vulnerabilidad, y en su última fase, es que realiza la identificación de activos, evalúa riesgos y propone tratamiento.	dan a la seguridad y sus consecuencias. En su última fase propone las medidas de mitigación de estos.	y determina el tratamiento a corto y a largo plazo. Es una metodología que engloba y generaliza los elementos de análisis, independientemente de su criticidad.	de activos que intervienen en los procesos del negocio. En la quinta fase se perfilan y aplican las medidas de control a manera de aminorar su impacto en los procesos operativos y en la utilidad de la organización.	as). En la segunda aplica tratamiento y medidas para controlar el riesgo.	
Grupo de desarrollo	5 a 10 colaboradores	gestores y auditores externos	5 a 20 colaboradores	5 a 20 colaboradores o gestores y auditores externos.	1 a 5 colaboradores	López [7]
Capacidad y razón operativa	Para organizaciones de más de 300 personas centradas	Para organismos gubernamentales grandes;	Para organismos gubernamentales grandes y organizaciones grandes de	Para organismos gubernamentales grandes; para grandes y pequeñas organizaciones.	Para organizaciones gubernamentales, de comercio,	Novoa & Rodríguez [15] López [7]

	en el negocio por procesos.	para grandes y medianas organizaciones.	más de 300 personas.		de servicios públicos o privados, grandes, medianas y pequeñas.	
Nivel de dificultad	Medio	Complicado	Fácil	Complicado	Fácil	Novoa & Rodríguez [15]
Índice Usabilidad (AP Latinoamérica)	33,7%	5, 4%	5,1%	1,8	54%	López [7]
Índice Implementación (AP Latinoamérica)	44%	12%	8%	5%	96%	López [7]

A nivel de Funcionalidad, MAGERIT se centra en la importancia de los activos, lo que la pone en ventaja ante OCTAVE que le resta importancia a este procedimiento y EBIOS que sólo los usa como información de soporte.

A nivel de Ejecución, MAGERIT solo utiliza plantillas para levantar la información de

activos, amenazas, vulnerabilidades y salvaguardas, mientras que OCTAVE utiliza muchos documentos al construir los perfiles de amenazas y vulnerabilidades en el proceso de análisis de riesgos. Asimismo, OCTAVE requiere licencia no muy fácil de conseguir para su puesta en marcha, mientras que MAGERIT y las otras metodologías no. En el caso de MEHARI, la exposición de las medidas de control solo se define en la etapa de gestión de los riesgos, mientras que MAGERIT las toma en cuenta desde la etapa de análisis, y las ratifica en su segunda fase. Sucede el mismo caso con el estudio del impacto.

A nivel de Grupo de desarrollo, MAGERIT puede ser desarrollado por una o varias personas, mientras que las otras metodologías requieren de equipos integrados por un volumen medio/grande de personas, inclusive, con el apoyo de gestores y auditores externos.

A nivel de Capacidad y razón operativa, MAGERIT fue diseñado para instituciones pequeñas, pero no es una limitante para ser adaptada a medianas y grandes organizaciones, tanto públicas como privadas. A Diferencia de las otras metodologías que fueron modeladas para grandes organizaciones, y por lo tanto requieren de más esfuerzos procedimentales y más recursos humanos y materiales, por supuesto, económicos.

A Nivel de dificultad, MAGERIT al igual que CRAMM resultan ser las más fáciles, con respecto a MEHARI por su enfoque modular y EBIOS por su enfoque a procesos y aspectos económicos financieros, mientras que OCTAVE tiene un nivel medio, pero igual requiere como MEHARI y EBIOS de numerosas conocimiento especializado, y, por lo tanto, se requiere de un equipo de trabajo multidisciplinario y con conocimiento del área de SI.

A nivel de Usabilidad (AP Latinoamérica), MAGERIT tiene mayor preferencia de uso en las administraciones públicas (AP), dado a los atributos antes expuestos que la caracterizan y su poco nivel de dificultad en su aplicación lo que la coloca en el mayor puesto de usabilidad en Latinoamérica, a lo cual le sigue OCTAVE, MEHARI, CRAMM y EBIOS, este último es el que tiene mayor grado de dificultad, pero es el más completo según expertos.

A nivel de Eficacia en Implementación (AP Latinoamérica), MAGERIT también

encabeza el óptimo desempeño al momento de ejecutarlo, ya que en un 96% de los casos aplicados ha sido exitoso el desarrollo de la metodología en las AP. Le sigue OCTAVE, con un desempeño aceptable, mientras que de forma contraria ha sucedido con MEHARI, CRAMM y EBIOS, donde no llega ni a una cuarta parte el desarrollo de la metodología cuando ya esta tiene que ser desechada como alternativa para la gestión de riesgos, y por ende, debe comenzarse u optarse por otra.

Por otro lado, como parte de la investigación se desarrolló el tercer objetivo que conllevó a diseñar el modelo de gestión de riesgos para la Municipalidad Distrital de Papayal, y así garantizar la implantación y uso de TI. En base a esto se requirió demostrar su pertinencia en cuanto a eficiencia y eficacia, cuyas normas empezaron a propagarse de forma no oficial basado en las técnicas organizacionales y la aplicación de un modelo de gestión de riesgo manifestado ante la gerencia (Ver anexo 9), mediante el cual se empezó a difundir la explicación de su funcionamiento a través de diversas charlas en el mes de septiembre del presente año 2021, en todas las oficinas y unidades de la Institución, utilizándose para su revisión y verificación de eficiencia en la práctica el siguiente indicador:

$$\textbf{\textit{\% EFMO}} = \frac{IAAP - IDAP}{IAAP} \times 100$$

Donde:

%EFMO: Porcentaje de eficiencia del modelo de gestión de riesgos

IAAP: Incidentes antes de aplicación de políticas SI

IDAP: Incidentes después de aplicación de políticas SI

Incidentes (reportados): Número de incidentes reportados en 3 meses (marzo, abril y

mayo) en periodos iguales del año 2020 y 2021 (ver tabla 3), después de la distribución de normas de protección en enero y febrero de 2021. Se tuvo en cuenta los

Las denuncias de acontecimientos realizadas por los beneficiarios y por el subsidiario de la UTI, el cual efectuó diversas funciones de investigación, análisis, reconocimiento, verificación, muestreo y consultas al sistema.

Tabla 5

Evaluación de eficiencia del modelo propuesto para la gestión del riesgo

Año 2020		**Año 2021**		**Diferencia entre incidentes**	**Porcentaje de Eficiencia del Modelo**
Mes	**Cantidad**	**Mes**	**Cantidad**		
Marzo	22	Marzo	3	19	86%
Abril	13	Abril	3	10	77%
Mayo	15	Mayo	2	13	87%
Total Incidencias por año	**50**		**8**	**42**	**84%**

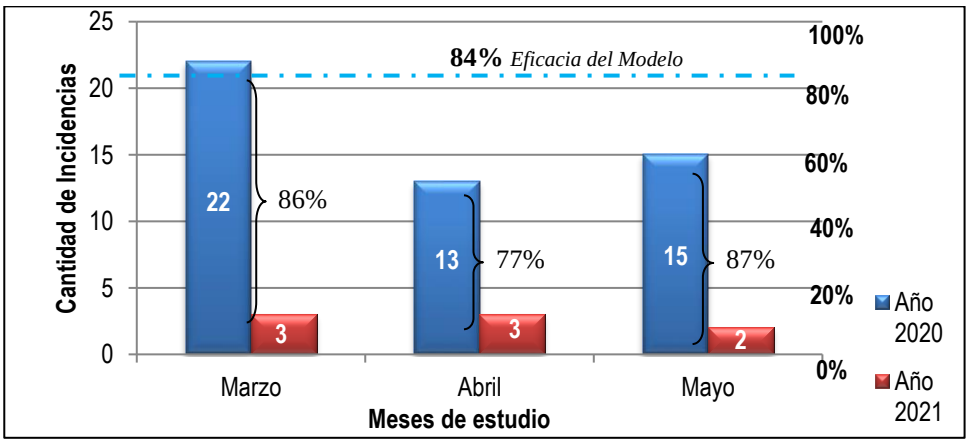
Basado en los resultados obtenidos de la comprobación hubieron 50 accidentes denunciados previamente al inicio de la investigación; y solo 8 accidentes posteriormente a la investigación con la aplicación del plan de implementación de medidas para la gestión de riesgos de la seguridad informática en la Municipalidad Distrital de Papayal que se expone en la tabla 22, más adelante, orientado a la difusión de las políticas de seguridad informática a partir de las conferencias que dieron origen a la actual investigación, envío de las políticas por correo electrónico a cada miembro de la organización, y publicación de las mismas a

través de la intranet.

Ante esto se evidenció un excelente nivel de mejora en cuanto a la reducción de incidentes, que llegó a un grado de significancia de 84%, que sobrepasa los pronósticos en estándares de calidad ISO 9000, la cual establece como óptimos niveles de eficacia a la proporción de 80% para una buena gestión en un primer año. Ante esto, la eficacia del modelo se apuntó un buen puntaje según coeficiente de Pearson donde se alcanzó 0,941 (ver anexo 11).

Figura 3

Evaluación de eficiencia del modelo propuesto para la gestión el riesgo



El resultado anterior en la figura 3, muestra la notable caída de los índices de incidentes entre un año y otro, siendo más perceptible en el mes de marzo del 2021 donde ocurrieron solo 3 incidentes de 22 que se presentaron en el año 2019, antes de que se comenzará a concientizar a los usuarios de los activos informáticos sobre los riesgos relatico a la SI, percibiéndose una brecha de mejora del 86% de eficacia. Esto indica, que, aplicándose los controles propuestos, se redujeron en el lapso de tres meses un 84% los riesgos que afectan la seguridad informática. Por consiguiente, es denegada la hipótesis nula y aprobada la hipótesis alterna. Lo anteriormente mencionado expone que el tratamiento de

un modelo de gestión de riesgo si minimiza los riesgos de la implantación y uso de TI en una Municipalidad del Perú.

Se hace salvedad de que el impacto mayor sobre la disminución de los riesgos es posible visualizarse en mediciones a mediano o largo plazo.

Asimismo, otro indicador que es importante revelar, es el de costos de perdidas ante incidentes:

$$PEM = \frac{(CREA - CRED)}{CREAÑO} \times 100$$

Donde:

PEM = Porcentaje de eficiencia del modelo de GR en costos asociados a daños

CREA = Costos reparación de equipos antes de aplicación de políticas SI

CRED = Costos reparación de equipos después de aplicación de políticas SI

CREAÑO = Costos de reparación de equipos año anterior

Del cual se pudo conocer que el año anterior, 2019, los costos promedios mensuales para reparar equipos dañados fueron de 17.578 soles, y en el promedio en el periodo entre septiembre y noviembre es 7.650 soles. Allí que la diferencia sea de 9.928 soles, marcando una eficiencia de aplicación de controles en un periodo inicial de 56%, lo que hace bastante considerable la reducción de las pérdidas.

Como parte importante se presentan los resultados, para dar repuesta al cuarto objetivo de la investigación que se basa en la aplicación el modelo de gestión de riesgos presentado en la Municipalidad, basado en el esquema estructurado expuesto en el anexo 9, del cual de logro una aplicación sin problemas por causas de restricciones ocurridas durante la pandemia, puesto que el investigador es integrante del personal activo perteneciente a la

institución en estudio, por esta razón tiene total libertad al acceso, y de esta manera se alcanzó el cumplimento de un 100% de la puesta en marcha del plan general, así como el 100% de la difusión de políticas y medidas, lo cual conllevó al resultados anterior, en donde con el cumplimento de todas las normas del esquema se lograron reconocer y estimar los activos presentes en la empresa, esto es muy significativo ya que es necesario tener en cuenta cuales equipos son los más críticos y de mayor relevancia dentro de la seguridad informática en dicha empresa.

Con la valoración de los activos con base a las dimensiones de Disponibilidad, Integridad y Confidencialidad, se obtuvieron en términos globales los siguientes resultados:

Tabla 6

Cantidad de activos críticos y alto valor en la seguridad informática en la Municipalidad Distrital de Papayal

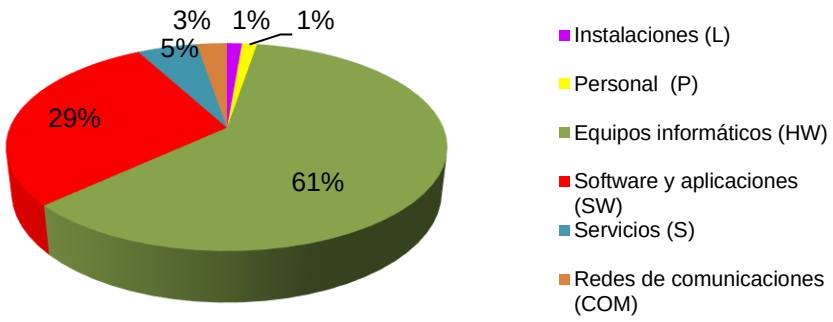
Tipo de activo	Nivel	Cantidad	Porcentaje
Instalaciones (L)	Alto	1	1%
Personal (P)	Alto	1	1%
Equipos informáticos (HW)	Alto	46	61%
Software y aplicaciones (SW)	Alto	22	29%
Servicios (S)	Alto	4	5%
Redes de comunicaciones (COM)	Alto	2	3%
Total		**76**	**100%**

Basado en la tabla 6, se puede detallar que son 76 los activos que poseen un rango elevado de tasación, vinculado al total de 204 activos que forman parte de la Municipalidad Distrital de Papayal. Los cuales se distribuyen proporcionalmente como se presenta en la

figura 7.

Figura 4

Distribución porcentual de los tipos de activos con nivel alto de valoración



La figura 4 refleja que el 61 por ciento de los activos con un rango elevado de estimación constituyen los equipos informáticos seguidos de las aplicaciones y software, servicios y personal, correspondientemente.

Significa esto, que ellos representan a los activos con mayor relevancia dentro de los procedimientos aplicables a la tecnología de la información, siendo estos los fundamentales para desarrollar los procedimientos en las estaciones de computación, tales como las desktops y laptops, los software que contribuyen en los procedimientos de administración y operantes de la empresa, al igual que todo lo relacionado a las redes e internet, sistemas operativos, cableados, el establecimiento donde están ubicados los servidores que en esta oportunidad seria la UTI, etc.

Fundamentado en los resultados de la estimación de los activos cuya sinopsis está representada en la tabla 6, se muestra la proyección de tasación generalizada de los riesgos en la tabla 7, en donde el informe efectuado con apoyo del instrumento de diagnóstico y

gestión de riesgo centrada en MAGERIT denominada R-Box, la cual especifica el reconocimiento del peligro de cada activo, la debilidad, la valoración de cada variable, la evaluación de la probabilidad del cumplimiento de las amenazas y la valoración del riesgo.

Tabla 7

Valoración del riesgo de los activos

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
P2	**Responsable de la UTI**	Perdida de personal clave	Carencia de lineamientos adecuados para retener a los trabajadores	3	3	3	3	9	**Mayor**	Evitar
		Accidentes Laborales	Carencia de lineamientos y políticas de seguridad industrial	3	2					Evitar

		Fuego	Pocos dispositivos para la protección contra incendios	2	3					Evitar
L27	**Unidad de Tecnologías de la Información (UTI)**	Exceso de temperatura y humedad	Ineficiente marcha o falta de equipos de climatización	3	3	3	3	9	**Mayor**	Reducir
		Robo de información	Insuficiencia de métodos para controlar en cuanto a recursos el acceso y salida	3	3					Reducir

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
HW1 - HW8	**Laptop**	Exceso de temperatura y humedad	Ineficiente marcha o falta de equipos de climatización	1	2	2	2	4	Significativo	Reducir
			Falta de dispositivos de enfriamiento	3	1					Reducir

		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2					Reducir
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2					Reducir
HW9-HW33	**Desktop**	Exceso de temperatura y humedad	Ineficiente marcha o falta de equipos de climatización	1	2	2	2	4	Significativo	Reducir

			Falta de dispositivos de enfriamiento	3	1					Reducir
		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2					Reducir

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción

					de la amenaza					
HW34-HW42	**Switch**	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2					Reducir
		Robo	Insuficiencia de métodos para controlar en cuanto a recursos el acceso y salida	2	2	2	2	4	Significativo	Evitar
		Caída del sistema por	Equipos en obsolescencia	2	2					Aceptar

		agotamiento de los recursos	con baja probabilidad de procesar datos							
		Exceso de temperatura y humedad	Ineficiente marcha o falta de equipos de climatización	3	2					Evitar
HW77-HW78	**Server**		Falta de dispositivos de enfriamiento	3	3	3	3	9	**Mayor**	Reducir
		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	3	2					Reducir

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	3	3					Reducir
		Manipulación de equipos informáticos	Mecanismos ineficaces para controlar	3	3					Evitar

	sustituciones de hardware				
Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3		Reducir
Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
HW79	**Router**	Robo	Insuficiencia de métodos para controlar en cuanto a recursos el acceso y salida	2	2	2	2	4	Significativo	Evitar

		Caída del sistema por agotamiento de los recursos	Equipos en obsolescencia con baja probabilidad de procesar datos	2	2						Aceptar
		Robo	Insuficiencia de métodos para controlar en cuanto a recursos el acceso y salida	2	2					Significativo	Evitar
HW80	**Antena**					2	2	4			
		Caída del sistema por agotamiento de los recursos	Equipos en obsolescencia con baja probabilidad de procesar datos	2	2						Aceptar

SW5	**Navegador web: Google Chrome**	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	3	3	3	3	9	**Mayor**	Reducir

Tabla 7

(Cont.)

Código	**Activo**	**Amenaza**	**Vulnerabilidad**	**Valor Amenaza**	**Valor Vulnerabilidad**	**Posibilidad de ocurrencia de la amenaza**	**Valor del activo en riesgo ante vulnerabilidad**	**Total riesgo**	**Nivel del riesgo**	**Acción**
SW7	**Antivirus: ESET End**	Hackers	Mecanismos ineficaces para	3	3	3	3	9	**Mayor**	Reducir

	Point Protection Standard		controlar la data cambiante							
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	3	3					Reducir
SW10		Hackers	Mecanismos ineficaces para	3	3	3	3	9	**Mayor**	Reducir

Asistencia Remota: AnyDesk	Expansión de software dañino	controlar la data cambiante Softwares ineficaces para proteger equipos contra virus	3	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia	Valor del activo en	Total riesgo	Nivel del riesgo	Acción

						de la amenaza	**riesgo ante vulnerabilidad**			
SW13	**Sistema Integrado de Administración Financiera del Sector Público - Gobiernos Locales (SIAF) (Usado en GP, OAR, OPP, UAL, UC, UT)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de	3	3					Evitar

	aplicaciones, equipos y sistemas				
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW14	**Web: SUNAT - Operaciones en Línea (Usado en UC, UT)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar

Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW15	**Sistema Integrado de Gestión Administrativa - Control Patrimonial**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de	Softwares ineficaces para	3	3					Evitar

(SIGA) (Usado en UAL, AL)	software dañino	proteger equipos contra virus				
	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
	Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir

		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW16	**Software de Abastecimiento**	Hackers	Mecanismos ineficaces para	3	3	3	3	9	**Mayor**	Reducir

(Usado en UAL, AL)		controlar la data cambiante				
	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3		Evitar
	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar

Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW17	**Web: Sistema Electrónico de Contrataciones del Estado (Usado en UAL, EC)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar

Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW18	**Web: Perú Compras (Usado en UAL)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir

Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3		Evitar
Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir

		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción

		Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3					Reducir
SW19	**Web: Registro Nacional de Proveedores (Usado en UAL)**	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3	3	3	9	**Mayor**	Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3					Evitar

Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW20	**Software de Control de Predios (Usado en UR)**	Hackers Expansión de software dañino	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Errores humanos	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar
		Corte de servicio eléctrico Usurpación	Poco adiestramiento	3	3					Evitar

de identidad	inducción ante el uso de aplicaciones, equipos y sistemas				
	Escasa dotación de generadores de electricidad	3	3		Reducir
	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW21	**Web: Sistema de Focalización de Hogares (Usado en UUS)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger	3	3					Evitar

	equipos contra virus				
Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir

		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción

		Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3						Reducir
SW22	**Software de Control de Beneficiarios (Usado en PVL)**	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3	3	3	9	**Mayor**		Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3						Evitar

Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW23	**Web: Sistema de Registro Nacional de Identificación y Estado Civil (Usado en ORC)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar

Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW24	**Web: Módulo de Programación Multianual de Inversiones**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de	Softwares ineficaces para	3	3					Evitar

(Usado en OPMI)	software dañino	proteger equipos contra virus				
	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
	Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir

		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción

		Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3					Reducir
SW25	**Web: Banco de Proyectos de Inversión Pública (Usado en UF, ODU, OPMI)**	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3	3	3	9	**Mayor**	Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3					Evitar

Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW26	**Web: Sistema Nacional de Información de Obras Públicas (Usado en EI)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar

Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW27	**Web: Módulo de Registro de**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir

Ejecución de Metas de Obras Públicas (Usado en EI)	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3			Evitar
	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3			Evitar
	Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3			Reducir

		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW31	**SUNAT - Programa**	Hackers	Mecanismos ineficaces para	3	3	3	3	9	**Mayor**	Reducir

de Declaración Telemática (Usado en URH)		controlar la data cambiante					
	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3			Evitar
	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3			Evitar

Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW33	**Windows Server 2012 R2 Standard (Usado en UTI)**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir
		Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3					Evitar

Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir
Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
SW34	**SQL Server 2008 Express**	Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3	3	3	9	**Mayor**	Reducir

(Usado en UTI)	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3		Evitar
	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3		Evitar
	Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3		Reducir

		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción

		Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3					Reducir
SW35	**Web: Panel de Control de Hosting y Dominio Institucional (Usado en UTI)**	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3	3	3	9	**Mayor**	Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3					Evitar

		Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3					Reducir
		Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia	Valor del activo en	Total riesgo	Nivel del riesgo	Acción

						de la amenaza	**riesgo ante vulnerabilidad**		
		Hackers	Mecanismos ineficaces para controlar la data cambiante	3	3				Reducir
S1	**Correo Electrónico**	Expansión de software dañino	Softwares ineficaces para proteger equipos contra virus	3	3	3	3	6	**Mayor** Evitar
		Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3				Evitar

Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	2	3		Reducir

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
S3	**Internet**	Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3	3	3	9	**Mayor**	Evitar
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	3					Reducir
		Caída del sistema por	Equipos en obsolescencia con baja	3						Aceptar

		agotamiento de los recursos	probabilidad de procesar datos y de almacenamiento							
S4	**Soporte Técnico**	Corte de servicio eléctrico	Escasa dotación de generadores de electricidad	3	3	2	3	6	Significativo	Evitar
		Indisponibilidad de personal	Poco o nulo control de las políticas de control del personal	1	2					Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
S5	**Creación de usuarios**	Usurpación de identidad	Mecanismos ineficaces para controlar la accesibilidad de usuario	3	3	3	3	9	**Mayor**	Evitar
		Cambio intencional de contenido informativo	Mecanismos ineficaces para controlar la data cambiante	2	2					Evitar

Manipulación de equipos informáticos	Mecanismos ineficaces para controlar sustituciones de hardware	3	3		Evitar

Tabla 7

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
COM1	**Cableado Estructurado, Integrado por: Cables UTP, Categoría 6. Puntos de Red**	Robo	Insuficiencia de métodos para controlar en cuanto a recursos el acceso y salida	2	2	2	2	4	Significativo	Evitar
		Caída del sistema por agotamiento de los recursos	Equipos en obsolescencia con baja probabilidad de procesar datos	2	2					Aceptar

Robo	Insuficiencia de métodos para controlar en cuanto a recursos el acceso y salida	2	2		Evitar
Caída del sistema por agotamiento de los recursos	Equipos en obsolescencia con baja probabilidad de procesar datos	2	2		Aceptar

Fuente: Elaboración Propia

Tal como se visualiza en la tabla 7, los activos que se encuentran ubicados en el nivel mayor de exhibición son de factor humano, que forman parte del personal de la UTI, los cuales son un recurso humano indispensable en los métodos de seguridad informática, debido a que son el único, si este llegara a alterarse o estar indisponible la municipalidad y sus activos estarían desamparados en lo referente a asistencia técnica en ese instante, por lo cual estas circunstancias se deben evitar.

De igual modo, la UTI, lugar donde se encuentran resguardadas las unidades de difusión de datos de la institución, mostro un nivel mayor de riesgo relacionado a la inexistencia de normas de tecnología de información, se encuentran muy expuestos frente a los peligros del ambiente, puesto que son un punto muy vulnerable ante amenazas para la información de esta organización gubernamental, por esta razón los riesgos se deben evitar y reducir.

En relación con los activos que conforman los equipos informáticos, a pesar de que todos son muy relevantes ya que presentaron un nivel significativo, los que presentan una mayor exposición en los procedimientos administrativos y operacionales de la Municipalidad son los servers, puesto que si estos se ven perjudicados se daña la secuencia de los procedimientos frecuentes de la institución. Dichos activos son los encargados de procesar y almacenar toda la información vital de las funciones que se realizan en la Municipalidad. Por esta razón, es fundamental disminuir e impedir los peligros frente a los cuales se encuentran expuestos, así como ocurre con los activos de tipo software y aplicaciones, de carácter administrativo, ya sean situados en la red o los que están adecuados en el internet, que de igual manera poseen un nivel mayor de riesgo.

Por otro lado, los activos adjuntos a los servicios, de asistencia técnica y red reflejaron ser los de mayor efecto y riesgo a lo largo de la investigación, ya que son dos medios obligatorios para la secuencia de todos los procedimientos y acciones que se efectúan en la institución.

De igual manera, es primordial prestarle interés a los activos totales de tipo informáticos que conforman la institución, en vista de que están en un nivel significativo, el que se puede calificar como admisible por su parte, puesto que si se llegara a materializar un peligro también producirá un efecto negativo en sus operaciones; en tanto que los de nivel mayor presentarían un efecto contraproducente de gran magnitud, por lo cual se pretende ser disminuido en todos los acontecimientos.

Luego de implementado el modelo de gestión de riesgos diseñado, se ejecutó el quinto y último objetivo de la investigación que tuvo el propósito de validar por juicio de expertos el modelo de gestión de riesgos propuesto para la Municipalidad, en el cual participaron tres (03) profesionales del área de TI, donde se indagó acerca de su correspondencia con la metodología MAGERIT, con la intención de fortalecer la credibilidad. Frente a esto se desarrollaron en la checklist (ver anexo 6) los próximos aspectos a validar:

P1. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta.

P2. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la caracterización expuesta.

P3. El modelo gestión de riesgos basado en MAGERIT cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.

P4. El modelo gestión de riesgos propuesto cumple con las fases de la metodología MAGERIT.

P5. El modelo propuesto para la gestión de riesgos basado en MAGERIT sigue una secuencia lógica de los procesos que lo integran.

P6. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente graficado.

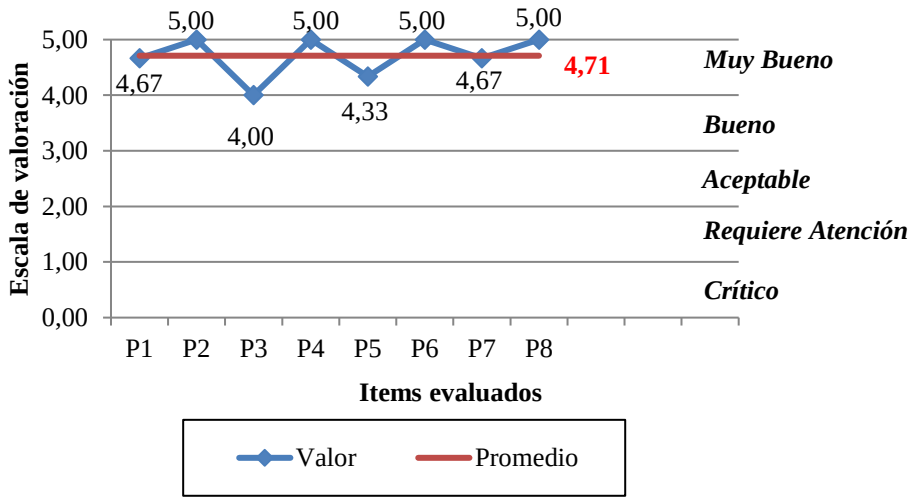
P7. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente explicado de manera que pueda guiar su implementación.

P8. El modelo integra el proceso de tratamiento de los riesgos analizados y evaluados.

En la figura 5 se presenta el rango de adaptación e inclinación del modelo presentado basado en el punto de vista de los especialistas.

Figura 5.

Valoración de adherencia del modelo diseñado bajo el enfoque MAGERIT



De la figura 5 se puede determinar, que el punto de vista de los especialistas sobre la adherencia del modelo de gestión de riesgo diseñado que se presenta bajo el enfoque MAGERIT, consiguió un nivel Muy bueno al atribuirse 4,71 como calificación, favoreciendo este resultado logrado, todos los índices que lo constituyen desde P1 a P8, lo cual puede certificar que el modelo obedece a las medidas expuestas en base a las líneas de MAGERIT en los tres (03) libros que editados para su sustentación, en lo concerniente a su

caracterización, los aspectos generales y específicos detallados, puesto que el modelo trazado está orientado a sus procesos expuestos, incluyendo técnicas de regulación frente a cada riesgo, detallados en sus dos (02) fases claves, las cuales se demuestran en procedimientos consecutivos perfectamente organizados y representados en un mapa de procesos, que los procedimientos introducidos son idóneos, y como parte del compromiso, más adelante son definidos minuciosamente.

3.2. Discusión

En este trabajo de investigación, el principal incidente que afecta la seguridad informática es causado por la distribución de programas maliciosos o virus, que son los encargados de dañar el sistema operativo del equipo, y por ende deja de funcionar tanto el terminal de trabajo, como el proceso donde interviene. Esto coincide con los resultados obtenidos por [1], quienes encontraron que los principales riesgos que se presentaron en la institución gubernamental que estudiaron se debía a que los equipos estaban desprotegidos al tener el antivirus desactualizado, lo que provocó serios daños en las operaciones y pérdida de valiosa información en la entidad, tal como sucedió en la Municipalidad Distrital de Papayal.

Asimismo, al identificarse los activos informáticos en el presente trabajo se distinguieron seis rubros que se calificaron como cruciales y viables de investigación, entre los cuales se encuentran equipos informáticos, software y aplicaciones, servicios y redes de comunicación. Mientras que en el estudio de [2] solo priorizaron equipos informáticos y software, en otras palabras, lo que para ellos se distingue debidamente como unidades de las TICs. Acá MAGERIT, claramente integra a esos elementos los servicios de soporte y las redes de comunicación ya que son esenciales para un excelente trabajo generalizado de los sistemas informáticos que ponen en funcionamiento los procedimientos primordiales de los entes gubernamentales.

Por su parte, Cabrejos (2020) determinó que los principales daños percibidos en los activos informáticos se debieron a los cortes eléctricos, situación que coincide con uno de los aspectos relevantes de este estudio, donde también hubo un elevado índice de incidentes por esa misma razón, siendo este motivado a la precariedad de los servicios básicos donde se adhiere el servicio eléctrico, y ante el cual la Municipalidad no ha tomado las previsiones óptimas, tales como implementar un generador auxiliar de electricidad, o planta eléctrica, que al momento de un corte eléctrico este sirva de complemento y lo restituya temporalmente.

De igual manera se puede señalar, que un inconveniente semejante ocasiono un efecto domino, causando efectos nocivos tanto en las aplicaciones y sistemas, como en los equipos informáticos, generando serios desperfectos en ellos, a tal magnitud de reemplazar los equipos iníciales o restáuralos, lo que represento una gran pérdida de dinero para la empresa; y los nuevos equipos se debieron reinstalar, a pesar de que numerosos datos primordiales fueron extraviados, desistiendo de mucha información relevante para algunas divisiones. Frente a esto [16] comentan sobre la importancia de los equipos de protección como UPS para sostenibilidad de los servicios, y la implementación de plantas eléctricas en los centros de datos de las instituciones gubernamentales como medida indispensable de seguridad informática.

Por otra parte, en este trabajo se detallaron los aspectos básicos para poner en marcha la metodología MAGERIT, desde la perspectiva de su caracterización, y en concurrencia con las teorías expuestas de trabajos como el de [17], [18] [19] y [20], se pudo inferir que si es una metodología sencilla y flexible, y con ventajas favorables para delimitar el grupo de activos que se quiere estudiar en una institución de administración pública donde es crítico levantar la información dado a sus políticas de confidencialidad. La misma se divide en todo caso en etapas que generalizan el análisis y evaluación del riesgo, y el tratamiento del riesgo, tal como también lo afirman los citados autores. Sin embargo, MAGERIT incorpora en su primera etapa a estudiar la apreciación del riesgo, como parte del diagnóstico de contexto, lo cual fue consideró en el presente trabajo de investigación, mientras que los otros

estudios esa alternativa no la aplicaron. Yéndose directamente a la identificación de activos, como parte del análisis de riesgos.

Considerando estas apreciaciones fueron subdividas las fases para diseñar el modelo de gestión de riesgos en el cual se fusiona con los modelos presentados por [21], [22], ya que se basan también en varios aspecto que se establecen las normas ISO 27001: 2013 e ISO 31000; invocando fases para conocer a la institución y realidad social, análisis de riesgos, evaluación y tratamiento mediante los métodos de gestión de riesgos que estén en relación con las particularidades de la empresa.

La aplicación del modelo de gestión de riesgo de seguridad informática estuvo centrada en una técnica planificada, cuya práctica implico emplear el esquema propuesto, donde en su primera etapa de evaluación de riesgo se reveló que el más grande activo informático de riesgo está representado por los servers, lo cual se manifestó de forma semejante en la investigación de [23] y [24], donde manifestaron que sus activos con mayor nivel de riesgo se localizaban en los centro de procesamiento de datos, donde se encontraban en primer lugar los server. Semejantes eventualidades ratifican la necesidad de darle prioridad a los métodos de seguridad para estos componentes, cabe destacar que esto no se tomó en cuenta en las citadas investigaciones, las cuales se delimitaron a la evaluación de riesgos, en cambio en esta investigación si se consideró.

Una vez difundidas las medidas, se determinó aquí mediante la implementación, que el modelo propuesto para la gestión de riesgos tuvo un efecto concreto frente a la seguridad informática puesto que se disminuyó de forma efectiva las eventualidades semejantes ocurridas previamente, así como lo estableció [25] y [26], cuyas investigaciones reafirmaron su teoría sobre la efectividad de la puesta en marcha de técnicas para mitigar los riesgos en las instituciones gubernamentales donde se emplearon, ya que todas las normas de gestión de riesgos conceden una amplia percepción sobre cómo proceder frente a la protección de los dispositivos que conforman las tecnología de información, optimizando las fases delicadas

para las entidades de administración pública.

Asimismo, se validó mediante juicio de experto el modelo propuesto, comprobándose según sus perspectivas un nivel Muy Bueno de coherencia con respecto a la metodología MAGERIT, al coincidir los ítems evaluados en estudios como el de [23] y [24], para evaluar la estructura de diseño y soporte del modelo. De igual forma, en los citados estudios se desarrolló el método de Delphi para su certificación, donde solo se cometió un error en un solo debate de análisis de los resultados en el de Linares et al, 2022 y cinco (05) rondas en el de Cabrejos (2020), para poder aprobarlos luego de su rediseño, ya que se consideró que contenía detalles que ameritaban mejora y que no estaban claro. En el presente estudio, se llevaron cabo tres (03) rondas, con el fin de aclarar puntos de semejanza del modelo presentado en relación con las normas que considera MAGERIT, y finalmente se dejó el diseño inicial del cual se corroboró que cumplía con todas las expectativas.

3.3. Aporte de la investigación

La Municipalidad Distrital de Papayal, como institución perteneciente a la administración pública, se alinea a lo establecido primeramente en la Constitución Política de Perú, seguido a la Ley Orgánica de Municipalidades en que fundamenta la entidad bajo una función autónoma a nivel administrativo, operativo y económico; contando con su Alcaldía y Consejo Municipal, para hacer cumplir las necesidades públicas individuales y colectivas de los ciudadanos que se circunscriben en su ámbito de acción y zonas adyacentes, abarcando entre ellos el mantenimiento general de la atención en lo que respecta al ordenamiento urbanístico y de infraestructuras, recolección de basura, atención en el área civil, recaudación de tributos municipales, entre otras.

Cabe destacar, que para ejecutar sus procedimientos operacionales y de administración, esta institución posee el departamento de tecnología que destaca mucha importancia a nivel tecnológico en la organización, y vinculado a su personal y sus amplios

sistemas y equipamientos para su gestión integral de TI, dan sustento a sus deberes y atribuciones para lo cual fue estipulado como ente público.

Ante este contexto, es conveniente resaltar los principales activos que se alojan en el área de la seguridad informática a lo largo y extenso de los 800 mts2 que ocupa el edificio de dos (02) pisos de la municipalidad, donde se pueden distinguir los aspectos a saber:

a. *Instalaciones*: que corresponde a las áreas y departamentos que integran la institución, y también pueden encontrarse diversos activos.

b. *Personal*: vinculado con los trabajadores los cuales operan los activos de la institución.

c. *Equipos Informáticos*: corresponden a todos los componentes de físicos empleados en la administración de los datos de información.

d. *Software y aplicaciones*: abarca todos los componentes internos, aplicaciones o redes empleados en la base de los procedimientos

e. *Servicios*: se refiere a la colaboración que ofrece un método interiormente en las aéreas de la misma entidad.

f. *Redes de comunicación*: son las vías de interconexión y sistemas entre las diferentes áreas de la institución.

Detallado lo anterior, se presenta en la tabla 8, los activos que caracterizan el ámbito funcional de la municipalidad en estudio según formato normativo de la ISO 27001 y MAGERIT, que indican desglosar los ítems del literal “a” hasta “f” antes mencionados.

Tabla 8

Activos que caracterizan la seguridad informática en la Municipalidad Distrital de Papayal. Año 2020

Instalaciones	Personal	Equipos Informáticos	Software y Aplicaciones	Servicios	Redes de Comunicaciones
1. Alcaldía (A) **2. Consejo Municipal (CM)** **3. Gerencia Municipal (GM)**	**1.** Alcalde **2.** Regidor 1 **3.** Regidor 2 **4.** Regidor 3 **5.** Regidor 4 **6.** Regidor 5 **7.** Gerente **8.** Secretaria de Gerencia	**1.** **U**na (01) laptop Dell **2.** Un (01) estación de trabajo de escritorio genérico. **3.** Una (01) impresora Epson. **4.** Una (01) laptop Dell **5.** Un (01) estación de trabajo de escritorio genérico. **6.** Una (01) impresora Epson **7.** Un (01) switch Tp-Link.	***Usados en todos los departamentos***: **1.** Sistema Operativo: Microsoft Windows 10 Professiona1 **2.** Sistema Operativo: Microsoft Windows 8.1 Professional	**1.** Correo Electrónico **2.** Telefonía Fija **3.** Internet **4.** Soporte Técnico **5.** Creación de usuarios **6.** Redirección de Archivos	**1.** Cableado Estructurado, Integrado por: Cables UTP, Categoría 6. Puntos de Red **2.** Conexión inalámbrica, Señal Wi-Fi de 150

4. Oficina de Asesoría Legal (OAL)	**9.** Jefe **10.** Asistente Técnico Legal	**8.** Una (01) laptop Dell **9.** Un (01) estación de trabajo de escritorio genérico **10.** Una (01) impresora Epson **11.** Un (01) switch TP-LINK .	**3.** Sistema Operativo: Microsoft Windows 7 Professional **4.** Navegador web: Microsoft Edge **5.** Navegador web: Google Chrome **6.** Navegador web: Mozilla Firefox **7.** Antivirus: ESET End Point Protection Standard **8.** Ofimática: Microsoft Office 2013 Standard **9.** Compresor de Carpetas y Archivos: WinRAR
5. Oficina de Planificación y Presupuesto (OPP)	**11.** Jefe **12.** Asistente Técnico Contable **13.** Asistente Técnico en Inversiones	**12.** Un (01) estación de trabajo de escritorio genérico **13.** Una (01) laptop Dell **14.** Una (01) laptop Dell **15.** Una (01) impresora Epson **16.** Una (01) impresora Epson **17.** Un (01) switch TP-LINK.	

			10. Asistencia Remota: AnyDesk **11.** Lector de PDF: Adobe Reader DC **12.** Web: Aplicativos de Contraloría General de la República		

Tabla 8

(Cont.)

Instalaciones	Personal	Equipos Informáticos	Software y Aplicaciones	Servicios	Redes de Comunicaciones
6. Oficina de Programación Multianual de Inversiones (OPMI)	**14.** Jefe	**18.** Una (01) laptop Dell	***Usados en departamentos específicos***: **13.** Sistema Integrado de Administración Financiera		

7. Unidad Formuladora (UF)	**15.** Jefe	**19.** Una (01) laptop Dell **20.** Una (01) impresora Epson **21.** Un (01) estación de trabajo de escritorio genérico **22.** Un (01) switch TP-LINK. **23.** Un (01) estación de trabajo de escritorio genérico **24.** Una (01) impresora Epson. **25.** Un (01) escáner Hp.	del Sector Público - Gobiernos Locales (SIAF) (Usado en GP, OAR, OPP, UAL, UC, UT) **14.** Web: SUNAT - Operaciones en Línea (Usado en UC, UT) **15.** Sistema Integrado de Gestión Administrativa - Control Patrimonial (SIGA) (Usado en UAL, AL) **16.** Software de Abastecimiento (Usado en UAL, AL) **17.** Web: Sistema Electrónico de
8. Especialista en Inversiones (EI)	**16.** Jefe		
9. Oficina de Secretaría General (OSG)	**17.** Jefe **18.** Asistente Administrativo 1 **19.** Asistente Administrativo 2		

10. Unidad de Relaciones Públicas e Imagen Institucional (URP)	**20.** Responsable	**26.** Un (01) estación de trabajo de escritorio genérico **27.** Una (01) impresora Epson **28.** Un (01) proyector multimedia Hp.	Contrataciones del Estado (Usado en UAL, EC) **18.** Web: Perú Compras (Usado en UAL) **19.** Web: Registro Nacional de Proveedores (Usado en UAL) **20.** Software de Control de Predios (Usado en UR) **21.** Web: Sistema de Focalización de Hogares (Usado en UUS) **22.** Software de Control de Beneficiarios (Usado en PVL) **23.** Web: Sistema de Registro Nacional de
11. Unidad de Abastecimiento Logística y Control Patrimonial (UAl)	**21.** Jefe **22.** Asistente Administrativo 3 **23.** Especialista en Contrataciones **24.** Asistentes Administrativo 4	**29.** Un (01) estación de trabajo de escritorio genérico **30.** Un (01) estación de trabajo de escritorio genérico **31.** Una (01) impresora Epson	

		32. Una (01) impresora Epson **33.** Un (01) switch TP-LINK.	Identificación y Estado Civil (Usado en ORC) **24.** Web: Módulo de Programación Multianual de Inversiones (Usado en OPMI)		

Tabla 8

(Cont.)

Instalaciones	**Personal**	**Equipos Informáticos**	**Software y Aplicaciones**	**Servicios**	**Redes de Comunicaciones**
12. Almacén - Unidad de Abastecimiento	**25.** Jefe **Logística y Control**	**34.** Un (01) estación de trabajo de escritorio genérico **35.** Una (01) impresora Epson	**25.** Web: Banco de Proyectos de Inversión Pública (Usado en UF, ODU, OPMI)		

Patrimonial (AL)			
13. Unidad de Tesorería (UT)	**26.** Jefe **27.** Asistente Técnico y Administrativo	**36.** Un (01) estación de trabajo de escritorio genérico **37.** Una (01) impresora Epson **38.** Un (01) switch TP-LINK.	**26.** Web: Sistema Nacional de Información de Obras Públicas (Usado en EI) **27.** Web: Módulo de Registro de Ejecución de Metas de Obras Públicas (Usado en EI) **28.** Adobe PhotoShop (Usado en URP) **29.** Corel Draw (Usado en URP) **30.** Sony Vegas (Usado en URP)
14. Unidad de Rentas (UR)	**28.** Jefe **29.** Asistente Administrativo 5	**39.** Un (01) estación de trabajo de escritorio genérico **40.** Una (01) impresora Epson	

15. Unidad de Recursos Humanos y Bienestar Social (URH)	**30.** Jefe	**41.** Un (01) estación de trabajo de escritorio genérico **42.** Una (01) impresora Epson	**31.** SUNAT - Programa de Declaración Telemática (Usado en URH) **32.** AutoCAD 2019 (Usado en ODU) **33.** Windows Server 2012 R2 Standard (Usado en UTI) **34.** SQL Server 2008 Express (Usado en UTI) **35.** Web: Panel de Control de Hosting y Dominio Institucional (Usado en UTI)
16. Oficina de Desarrollo Urbano e Infraestructura (UDU)	**31.** Jefe **32.** Asistente Técnico Ingeniería Civil **33.** Secretaria de ODUeI **34.** Asistente Técnico Administrativo	**43.** Una (01) laptop Dell **44.** Una (01) impresora Epson **45.** Un (01) estación de trabajo de escritorio genérico **46.** Un (01) Plotter Canon **47.** Un (01) switch TP-LINK. **48.** Un (01) estación de trabajo de escritorio genérico	

		49. Una (01) impresora Epson			

Tabla 8

(Cont.)

Instalaciones	Personal	Equipos Informáticos	Software y Aplicaciones	Servicios	Redes de Comunicaciones
17. Unidad de Maquinaria y Maestranza (UMM)	**35.** Responsable	**50.** Un (01) estación de trabajo de escritorio genérico **51.** Una (01) impresora Epson			
18. Oficina de Desarrollo Social	**36.** Jefe	**52.** Un (01) estación de trabajo de escritorio genérico			

y Servicios Públicos (UDS)		**53.** Una (01) impresora Epson
19. Unidad de Salud, Limpieza, Ornato, Medio Ambiente-Ecología, Parques-Jardines, Control de Cementerio y Estadio, y ATMSR - Área Técnica Municipal de Saneamiento Rural. (USL)	**37.** Jefe **38.** Asistente Técnico Ambiental	**54.** Una (01) laptop Dell **55.** Una (01) impresora Epson

20. Unidad de SISFOH, Complementación Alimentaria, PVL y Comercialización (USI)	**39.**Jefe	**56.** Un (01) estación de trabajo de escritorio genérico **57.** Una (01) impresora Epson **58.** Un (01) switch TP-LINK			

Tabla 8

(Cont.)

Instalaciones	Personal	Equipos Informáticos	Software y Aplicaciones	Servicios	Redes de Comunicaciones
21. Programa de Vaso de Leche y	**40.**Jefe	**59.** Una (01) laptop Dell **60.** Una (01) impresora Epson			

Complementación Alimentaria (PVL)		
22. DEMUNA - Defensoría de la Municipal del Niño y del Adolescente (DEM)	**41.**Jefe **42.**Psicóloga	**61.** Un (01) estación de trabajo de escritorio genérico **62.** Una (01) impresora Epson
23. OMAPED - Oficina Municipal de Atención a la Persona con Discapacidad (OMA)	**43.**Jefe **44.**Asistente Administrativo 6	**63.** Un (01) estación de trabajo de escritorio genérico **64.** Una (01) impresora Epson

24. Seguridad Ciudadana (SC)	**45.**Jefe **46.**Asistente Administrativo 7 **47.**Chofer	**65.** Un (01) estación de trabajo de escritorio genérico **66.** Una (01) impresora Epson **67.** Un (01) DVR - Digital Video Recorder LG **68.** Una (01) Cámara de Video Vigilancia Tp-Link **69.** Una (01) Cámara de Video Vigilancia Tp-Link **70.** Una (01) Cámara de Video Vigilancia Tp-Link

Tabla 8

(Cont.)

Instalaciones	Personal	Equipos Informáticos	Software y Aplicaciones	Servicios	Redes de Comunicaciones
25. Defensa Civil (DC)	**48.** Jefe	**71.** Un (01) estación de trabajo de escritorio genérico **72.** Una (01) impresora Epson			
26. Oficina de Registro Civil (ORC)	**49.** Jefa **50.** Asistente Administrativo 8	**73.** Un (01) estación de trabajo de escritorio genérico **74.** Una (01) impresora Epson **75.** Una (01) Fotocopiadora Cannon			
27. Unidad de Tecnologías	**51.** Responsable	**76.** Un (01) Server Hp **77.** Un (01) Server Hp			

de la Información (UTI)		**78.** Un (01) switch TP-LINK. **79.** Un (01) Router Cisco **80.** Una (01) Antena Cisco			
27 Departamentos	**51 Personas**	**80 Equipos informáticos**	**35 Software y aplicaciones**	**6 Servicio de informática**	**2 Redes de Comunicaciones**

Nota: Unidad de Tecnologías de la Información de la Municipalidad Distrital de Papayal. (2020).

Se pudo determinar de la tabla 8, que actualmente la Municipalidad Distrital de Papayal cuenta con 201 activos informáticos, entre ellos 80 estaciones de trabajo, 35 software, 6 servicios de informática y 2 redes de comunicaciones, distribuidos entre 27 instalaciones a lo largo de la institución para el uso de 51 trabajadores. Sin embargo, de acuerdo al responsable de la Unidad de Tecnologías de la Información (UTI), dichos activos se hallan indefensos, ya que no cuentan con los recursos necesarios, al igual que los de verificación, para lograr su perfecta seguridad, lo que se afirmó a través de la notificación de gestión operacional y administrativa de institución, de la cual resulto que entre todas las circunstancias de riesgo que afectaron a los activos estaban presentes, los riesgos de tipo institucional, como lo son las caídas de los sistemas y desconexión de red por cortes de luz, averías de los equipos informáticos tales como las aplicaciones, por la razón expuesta y continuos recalentamientos de los equipos informáticos por altas temperaturas.

Igualmente, se logró determinar que entre otros riesgos que sucedieron fueron de tipo personas (causas accidentales), entre las cuales se encontraron declives en los sistemas por falta de mantenimiento, fallas en las aplicaciones informáticas por carencias en las actualizaciones, extravió de información por un defectuoso restablecimiento de respaldos, averías de los equipos informáticos por escasez en los mantenimientos y actualizaciones de software.

Finalmente, se evidenció que frente al tipo de riesgo antes mencionado, se encontraron rastros de hackeo en los sistemas por la carencia de normas de control, caídas de los sistemas por colapso de los elementos debido al uso de unidades obsoletas, distribución de virus en aplicaciones informáticas por la falta de actualización del software de seguridad, alteraciones en la información por la inexistencia de técnicas de control de cambio, el tiempo de los equipos frente a su colapso por antigüedad, descuido de los equipos informáticos por la carencia de métodos de control para la entrada y la salida de elementos, y fuga de información por la inexistencias de técnicas de control de almacenamiento. Frente a lo anteriormente presentado, se logra visualizar el índice global de acontecimiento ocurridos

por factores de riegos, el cual reflejo en términos a nivel general:

Tabla 9

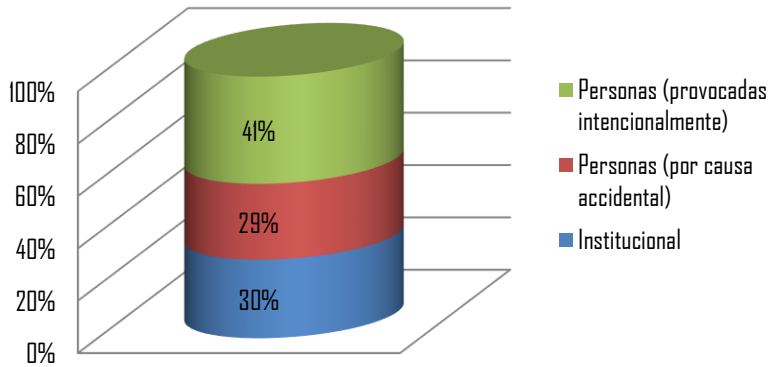
Volumen de riesgos suscitados por tipología en el año 2020

Alternativa	Frecuencia	Porcentaje (%)
Institucional	62	30%
Personas (por causa accidental)	58	29%
Personas (provocadas intencionalmente)	84	41%
Total	**204**	**100%**

Nota: Informe de Gestión de seguridad informática en Municipalidad, enero 2020 presentado por la UTI de la Municipalidad Distrital de Papayal. (2020).

Figura 6

Distribución Porcentual de riesgos suscitados por tipología en el año 2020



En la figura 6, se logra percibir los hallazgos tipificados por riesgos de tipo “personas” (provocados intencionalmente) (41%) y “personas (por causa accidental)” (29%), con una valoración porcentual de 70 por ciento de efectos ocasionados principalmente en los software y equipos informático que se encuentran en el área laboral, proseguido por los riesgos de tipo “Institucional” (30%) los cuales son particulares del dinamismo cotidiano del personal que trabaja en la municipalidad.

Basado en esto, es necesario tener presente el desarrollo de técnicas de control de la seguridad informática, debido a este primordial motivo se eliminan los intentos para ser eficaces frente a los riesgos y peligros a los que están expuestos los activos. De igual manera, es primordial la aplicación de un mejoramiento de la capacidad de los equipos y software, de igual modo en la instalación donde se encuentran ubicados, debido a la relevancia que figuran estos activos en la protección y procesos de la información que operan la institución, que a su vez es de importancia para toda la comunidad por lo que cualquier amenaza podría tener un enorme impacto en cuanto a la realización de las actividades con total normalidad de la gestión ciudadana llevada a cabo en la Municipalidad.

Siendo reconocido el contexto preliminar, se persigue en esta tesis, regularizar una perspectiva operacional para cubrir el problema presentado frente a los riegos reconocidos con anterioridad, siendo esencial caracterizar la metodología a utilizar, siendo MAGERIT la escogida por el presente investigador, y a así adaptar su método al análisis y tratamiento de los riesgos presentes en los activos de la institución, en lo inherente al análisis de amenaza y vulnerabilidad.

Cabe destacar, que a priori se selecciona esta metodología, por ser única que ha sido certificada de manera exclusiva por un gobierno en idioma español, que en este caso es el de España a través de su Consejo Superior de Informática para poner en marcha en las administraciones públicas de ese país, ya sea a nivel gubernamental, organismos de salud, educación, recaudación fiscal, seguridad ciudadana, ministerios, entre otros, además de otros

atributos ya evaluados en la tabla 4, lo que la convierte en la excelente elección para ejecutarla en esta tesis.

Siendo así, a manera de dar relevancia al enfoque metodológico escogido y fundamentar el motivo de implementarla en la investigación, se citan en la tabla 10, diversos autores que han tenido experiencias exitosas en la aplicación de MAGERIT como metodología de análisis de riesgos en la gestión informática en instituciones de la administración pública, para lo cual se indica: la identificación de los investigadores y año de publicación de su obra, el caso con el que trabajaron, buscador con el que se detectó el trabajo, y los aspectos que los investigadores dan a conocer en su trabajo para caracterizar la mencionada metodología.

Tabla 10

Caracterización de la metodología MAGERIT según experiencias de algunos investigadores

N°	Autor (es)	Caso de aplicación de MAGERIT	Buscador de obtención	Aspectos que resaltan en su caracterización
1	Ferruzola, Duchimaza, Ramos & Alejandro (2019)	Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT	Researchgate.net	- Es un método de trabajo efectivo ya que responde a la perspectiva de las instituciones del estado, así como a toda organización social que experimente con cuantioso volumen de activos informáticos para cumplir con su función social. - Puede trabajar o no, con sistemas informáticos para tratarla. Esto, ante las limitantes de diligencia de las licencias de uso de las herramientas. Es por ello hay al alcance diversas plantillas en Excel, que también pueden ser programadas por investigadores. - Fácil manejo del método en cuanto a levantamiento de información, calificación, manejo de herramientas, y estimación en las evaluaciones. - Pone a mano un método estructurado en las siguientes etapas: a. Análisis de Riesgos (identifica y realiza tasación de activos, determina sus amenazas y vulnerabilidades, y evalúa la posibilidad de que estas ocurran). (b) Gestión del riesgo, determinan las

				acciones para mitigar los riesgos. (c) Diseño de Control de Riesgos (Planes de seguridad, contingencia, políticas de control, entre otras).
2	Alvarado, Pacheco y Martillo (2018).	El análisis y gestión de riesgos en gobiernos de TI desde el enfoque de la metodología MAGERIT	Eumed.net	- Es una metodología con mucha receptividad al momento de implementarse para su gestión de SI en las organizaciones de tipo gubernamental, dado su propiedad versátil, flexible y sencilla, lo cual es muy valorado en instituciones donde las exigencias de entrada y acceso a la información no son fáciles de levantar. - Se basa en proponer un esquema para: (1) Organizar los activos por clase, y así identificar los riesgos que los acechan. (2) Evaluar su impacto y ocurrencia. (3) Encausar las medidas pertinentes a cada caso para tratarlos, aceptarlos y corregirlos. - Se alinea a emitir políticas para hacer cumplir los principios y requisitos básicos que garanticen la eficacia en el plan para proteger la información. - Toma como referencia sólo los activos con valoración *alta* para o críticos para el estudio de vulnerabilidades y amenazas.
3	Villón (2021)	Modelo de gestión de riesgos para seguridad informática bajo	Google Scholar (Google Académico)	- Metodología documentada en idioma español especialmente para instituciones gubernamentales y pertenecientes al estado. - Las etapas que lo conforman cumplen con las políticas que estipulan las normas ISO 31000 y MAGERIT.

	ISO/IEC 27001:2013 en empresa de entretenimiento y juegos de azar, Lima-2021		- Se hace cobertura sobre las fases para analizar, evaluar y tratar el riesgo. - Eficiencia al aplicarse en ámbitos críticos. - Flexibilidad en la adecuación de códigos en el inventario de activos. - Flexibilidad en la escala de valoración de activos, tanto a nivel cualitativo como cuantitativo, donde se establece a juicio del investigador.

Tabla 10

(Cont.)

N°	Autor (es)	Caso de aplicación de MAGERIT	Buscador de obtención	Aspectos que resaltan en su caracterización
4	Linares et al. (2022)	Políticas de seguridad de la información y metodología Magerit en la	Redalyc.org	- Se enfoca al desarrollo de 2 fases básicas: (I) análisis y evaluación de riesgos y (II) Tratamiento de la gestión de Riesgos. - Detalla la tasación de los riesgos por criterios. - Valora el activo, la amenaza y vulnerabilidad y luego define un sistema de control de seguridad que esté en consonancia con los hallazgos encontrados.

		empresa Induamerica Chiclayo S.A.C		- Aunque presenta un estándar para clasificar y codificar activos, amenazas y vulnerabilidades, estas pueden adecuarse a decisión del investigador, así como las escalas de valoración.
5	Cabrejos (2020)	Influencia de la metodología MAGERIT V3 en la seguridad de información de la empresa Deco Interiors SAC	Universia	- Recurre a identificar riesgos en activos, y según su valoración resaltar su estado de criticidad e importancia. - Su primera fase se aboca a Identificar el riesgo, para lo que se crea un inventario y luego se identifica y valoran las amenazas y las vulnerabilidades. - Su segunda fase, se enfila a evaluar el riesgo, donde se determina el impacto y el índice de riesgo, así como las salvaguardas - La tercera fase corresponde a la gestión del riesgo, donde se refieren las medidas respectivas para tratarlo. - Contiene un catálogo de elementos que permite guiar la codificación de los activos, las amenazas y las vulnerabilidades. Sin embargo, estas dos últimas variantes pueden manejarse según criterio del investigador, ya que en todos los casos no aplican los mismos criterios característicos. - Aunque existen muchos tipos de dimensiones para valorar activos, MAGERIT

prioriza la de Disponibilidad, Integridad, Confidencialidad.

Una vez conocida las perspectivas de los citados autores acerca de característica de MAGERIT, se presentan aquí un esbozo de los estándares de la metodología presente en los tres (03) libros que la representan:

La Metodología MAGERIT se ejecuta en dos fases básicas que permiten: (a) analizar y evaluar el riesgo y. (b) gestión para tratar el riesgo.

En la *fase I: del análisis de riesgo*, se identifican y codifican los activos de acuerdo con el estándar que se presentan en la tabla 11, Sus siglas pueden estar proseguida de un digito o 3 caracteres que esté relacionado con el calificativo de este.

Tabla 11

Codificación para identificar los activos de la organización

Tipo de activo	Sigla asignada
Instalaciones	(L)
Personal	(P)
Equipos informáticos	(HW)
Software y aplicaciones	(SW)
Servicios	(S)
Redes de comunicaciones	(COM)

Fuente: libro II-MAGERIT- catálogo de elementos

Posteriormente, la tasación del activo se hace considerando las dimensiones de: disponibilidad (D), Integridad de datos (I) y confidencialidad (C)

Criterios de valorización

En base a los resultados presentados, con la ayuda de los trabajadores encargados de los activos de la institución, se efectuó la estimación tanto de calidad como en cantidad reflejado en las tablas 12, 13 y 14, basado en la calificación estime favorable.

Disponibilidad: esta evaluación solicita acreditar las circunstancias si no son apropiadas para el acceso del personal autorizado a los activos en el instante que son solicitados.

Tabla 12

Criterio de Valorización de la Disponibilidad

Disponibilidad		**Descripción**
Valor Cuantitativo	**Valor Cualitativo**	
1	**B (Bajo)**	Cuando no estuviera a disposición la información y no hubiese impactos negativos a nivel operativo.
2	**M (Moderado)**	Cuando no estuviera a disposición la información y hubiese impactos negativos, pero no a nivel operativo.
3	**A (Alto)**	Si la información no llegara a estar disponible cuando sea necesitada, habría un efecto fatal en las operaciones. Cuando no estuviera a disposición la información y hubiese impactos negativos y fatales a nivel operativo.

Nota: Tomado de libro II-MAGERIT- catálogo de elementos

Integridad: esta evaluación solicita acreditar las circunstancias si no precisa y total la información empleada por el activo.

Tabla 13

Criterio de Valorización de la Integridad

Confidencialidad		Clase	Descripción
Valor Cuantitativo	**Valor Cualitativo**		
1	**B (Bajo)**	No necesaria	Utilizado únicamente para consultar.
2	**M (Moderado)**	Necesaria	En caso de que el contenido se falsifique y hubiese dificultades, que no afecten a gran escala la operatividad.
3	**A (Alto)**	Importante	Si la integridad se perdiera, habría un efecto fatal en las operaciones. En caso de que se pierda la integridad y hubiese dificultades fatales, que afecten a gran escala la operatividad.

Nota: Tomado de libro II-MAGERIT- catálogo de elementos

Confidencialidad: esta evaluación solicita acreditar las circunstancias si la información asequible es únicamente para el personal autorizado para su acceso.

Tabla 14

Criterio de Valorización de la Confidencialidad

Confidencialidad		Clase	Descripción
Valor Cuantitativo	**Valor Cualitativo**		
1	**B (Bajo)**	Pública	Se pudiese revelar y proporcionar a terceras personas.
2	**M (Moderado)**	Uso interno	Se pudiese revelar y proporcionar. Si lo establecido fuese informado y no surgiera gran efecto en la operatividad.
3	**A (Alto)**	Secreto	Se pudiese revelar y proporcionar a gente de confianza.

Nota: Tomado de libro II-MAGERIT- catálogo de elementos

Una vez valorado los activos se procede a la valoración de acontecimientos de los peligros, al igual que su debilidad, y por último lograr la obtención de la valoración del riesgo eventual, utilizando criterios expuestos en la tabla 15, 16 y 17 respectivamente:

Tabla 15

Criterio de Valorización de la Ocurrencia de la Amenaza

NIVEL		Descripción
Valor Cuantitativo	**Valor Cualitativo**	
1	**B (Bajo)**	Rara vez se da en el año.
2	**M (Moderado)**	Es probable que se presente.
3	**A (Alto)**	Es muy probable que se presente, alguna vez.

Nota: Tomado de libro II-MAGERIT- catálogo de elementos

Tabla 16

Criterio de Valorización de la Vulnerabilidad

NIVEL		Descripción
Valor Cuantitativo	**Valor Cualitativo**	
1	**B (Baja)**	Existen suficientes controles.
2	**M (Moderada)**	Existen pocos controles.
3	**A (Alta)**	No existen controles o son escasos.

Nota: Tomado de libro II-MAGERIT- catálogo de elementos

Tabla 17

Criterio de Valorización del Riesgo

NIVEL		Descripción
Valor Cuantitativo	**Valor Cualitativo**	
1	**Insignificante: B (Bajo)**	Impacto muy bajo - No requiere acción.
2	**Menor: B (Bajo)**	Impactos menores en el negocio - No se necesita tomar acción.
3	**Poco Significativo: M (Moderado)**	Tiene algún impacto negativo - No se necesita tomar acción.

4 - 6	**Significativo: M (Moderado)**	Impacto negativo en la organización. Los riesgos son se consideran aceptables.
7 - 8	**Importante: A (Alto)**	Se develan un gran impacto negativo en la organización.
9	**Mayor: A (Alto)**	Se perciben un gran impacto negativo en la organización, y debiéndose reducir a toda escala.

Nota: Tomado de libro II-MAGERIT- catálogo de elementos

Una vez elaborada la valoración del riesgo, se pasa la segunda fase de gestión del riesgo, donde es considerado su tratamiento considerado políticas de seguridad y control, a los fines de:

Evitar, empleando técnicas de resguardo.

Reducir, previniendo que ocurran las circunstancias que originan el riesgo.

Transferir, desplazar a otro ambiente la obligación del riesgo, ejemplo un intermediario.

Aceptar, no tomar acción con relación al riesgo y aceptarlo.

Así pues, siguiendo los lineamientos de la metodología MAGERIT, se presenta a continuación un modelo de gestión de riesgos para la Municipalidad Distrital de Papayal, de manera que sirva como soporte garantizar la implantación y uso de TI, lo cual permitirá a su vez guiar el desarrollo de su ejecución en este trabajo de investigación.

El modelo está estructurado, como se presenta en la figura 7, contentivo de cuatro

fases señaladas a continuación:

Fase I: Apreciación del riesgo.

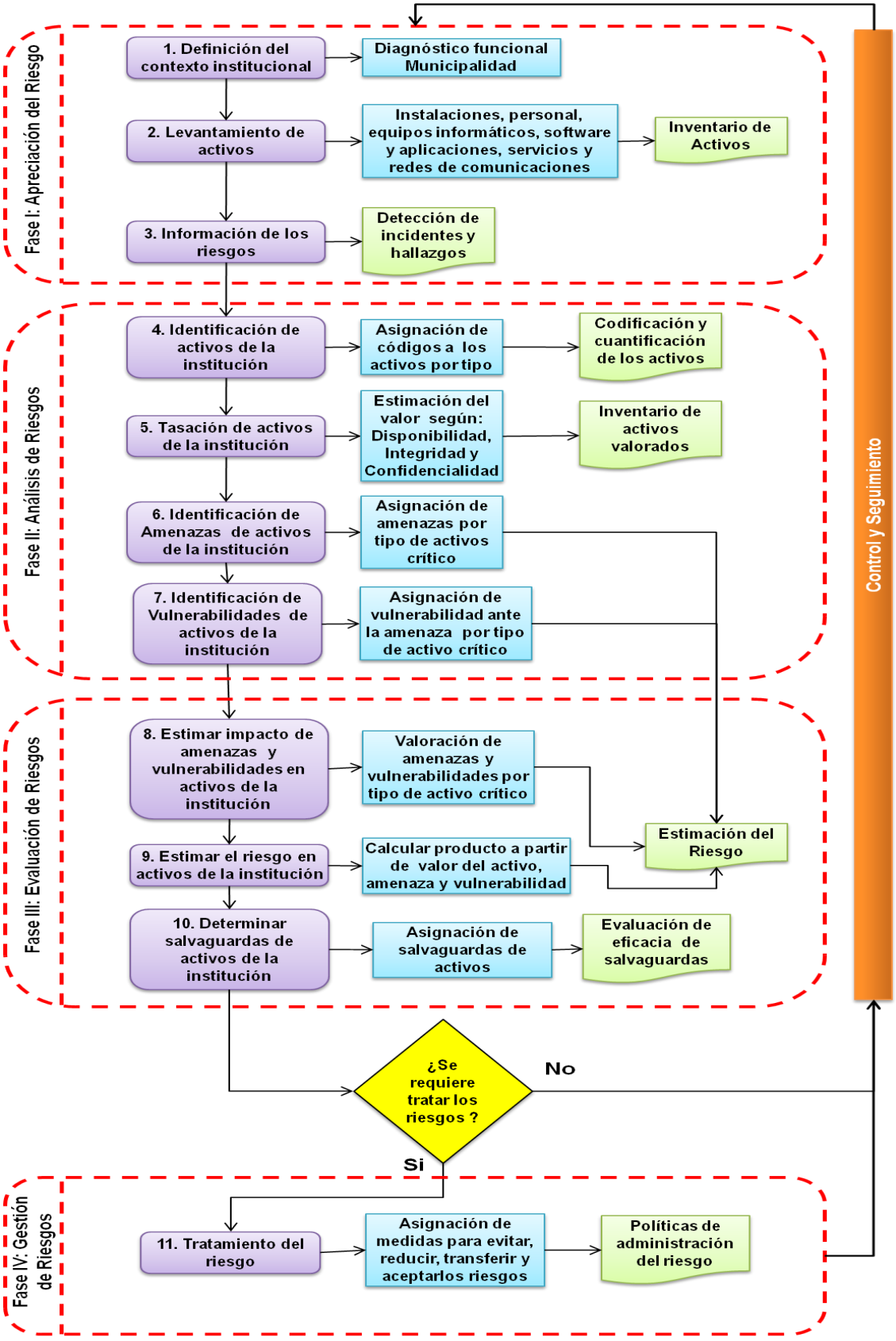
Fase II: Análisis de riesgos.

Fase III: Evaluación de riesgos.

Fase IV: Gestión de riesgos.

Figura 7

Modelo diseñado para la gestión de riesgos en la Municipalidad Distrital de Papayal basado en la metodología MAGERIT



Nota: Elaboración Propia

Descripción del Modelo Propuesto

Fase I. Apreciación del riesgo: en esta fase se desarrolla el análisis inicial del ambiente laboral, ya previamente dado a conocer en las primeras secciones de esta investigación. El cual contempló:

1. *Definición del contexto institucional*: este aspecto, proviene del diagnóstico de la situación actual de la Municipalidad Distrital de Papayal, donde se dio a conocer su razón social y las funciones esenciales de las gestiones operacionales y administrativas, con el objetivo de identificar el vínculo con los activos que tiene como sustento a sus acciones.

2. *Levantamiento de activos*: en este paso, mediante la técnica de observación directa se llevó a cabo mediante una matriz de doble entrada, cuáles son los activos con los que cuenta la Municipalidad Distrital de Papayal, organizándose ante esto un inventario contentivo de los activos que posee la institución, ya expuestos en la tabla 3.

3. *Información de los riesgos*: durante este proceso, se obtuvo información documental de los registros históricos de la UTI de la Municipalidad Distrital de Papayal resultante de su gestión operativa, acerca de los incidentes y hallazgos que ocurrieron en el año anterior con respecto la seguridad informática, diagnosticándose el riesgo potencial que distinguen los procedimientos operacionales y administrativos de la empresa.

Fase II. Análisis de riesgos: por medio de esta etapa se busca identificar los riesgos y motivos lograrían ocasionar un suceso grave para los activos, frente a los peligros y debilidades.

4. *Identificación de activos de la institución*: mediante este proceso se ejecutó la técnica de calificación basado en las siglas estándar de MAGERIT en la tabla 6, los activos pertenecientes la Municipalidad Distrital de Papayal, lo cual permitió su denominación por códigos y por tipo.

5. *Tasación de activos de la institución*: Durante esta etapa el personal de gerencia y jefaturas de la Municipalidad especifico en términos de *Disponibilidad* (D), *Integridad* (I) y *Confidencialidad* (C), cuáles son los activos de alto riesgo tanto para la institución como para ellos, quienes se podría ver perjudicados si llegara a suceder un efecto dañino en su secuencia de procedimientos productivos donde participan. Cabe destacar, que por anticipado los trabajadores entrevistados decidieron denominar como activos de alto riesgo solo aquello que constituyen a equipos informáticos software y aplicaciones, servicios técnico y redes de comunicación, así como se señala que se puede realizar el método MAGERIT. A continuación, se presentan los aspectos que se consideraron para la estimación de relevancia de parte del personal:

(HW) Hardware: está compuesto por todos los elementos físicos del sistema informático, quienes se encargan de dar soporte a los trabajos que ofrece la institución, sin estos equipos es imposible que ocurra el proceso de datos.

(SW) Software y aplicaciones: administran de manera automática las operaciones por medio de un equipo informático, que juntos intervienen en el proceso de la información para

arrojar deducciones en la asistencia de sus prestaciones.

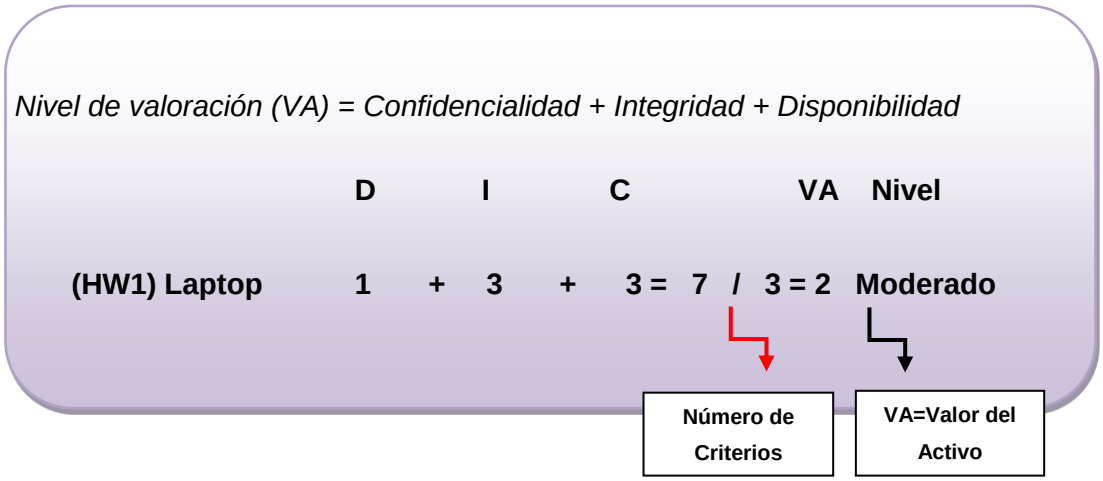
(S) Servicios: el refuerzo frente a la gestión de información y proceso de datos son la base para el progreso de la empresa para facilitar de forma constante sus asistencias.

(COM) Redes de comunicaciones: se reconocen como los componentes físicos que habilitan la difusión de la información vital internamente en toda la dimensión de la empresa.

La valoración del activo se realiza como sigue en la figura 8, con un ejemplo:

Figura 8

Ejemplo de valoración del activo



Nota: Adaptado de libro II-MAGERIT

6. *Identificación de amenazas de activos de la institución*: en esta etapa, se originó un número de riesgos particulares que figuran un peligro para los procedimientos de regulación de la Municipalidad Distrital de Papayal, los cuales concuerdan con los anteriormente suscitados durante el año 2019, debido a que han estado presentes a

lo largo de los años posteriores. Se destinaron aquí los riesgos característicos de cada activo de alto riesgo.

7. *Identificación de vulnerabilidades de activos de la institución*: en este proceso, dado un crítico, se determinan las diversas debilidades frente algún suceso que pueda generar un inconveniente de seguridad. Este va relacionado con el peligro de cada tipo de activo de alto riesgo.

Fase III. Evaluación de riesgos. En esta fase se desarrolló la valoración cuantitativa del riesgo, señalando las técnicas para su consecuente método.

8. *Estimación del impacto de amenazas y vulnerabilidades en activos de la institución*: Durante esta etapa se evaluó el impacto prejudicial relacionado a los activos en la situación de materializarse un peligro. Se realizo la suma total de las debilidades y se obtuvo el promedio para reconocer el grado del efecto.

9. *Estimación del riesgo en activos de la institución*: En esta etapa se obtuvo el índice de riesgo de los activos en relación con una amenaza. Este valor es obtenido mediante la multiplicación del valor del activo por el valor de amenaza y vulnerabilidad.

Ante esto, se coloca un ejemplo para calcular el nivel de riesgo del activo en la figura 9:

Figura 9

Ejemplo de valoración del riesgo del activo

1 + 3 + 2 + 2 = 8/2 = 2

Código de riesgo	Código de Activo	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor de Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo
R1	(SW1)	Laptop	Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	1	2	2	2	4	Significativo
R2			Exceso de temperatura y humedad	Falta de dispositivos de enfriamiento	3	1		2 x 2 = 4		
R3			Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2				
R4			Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2				

2 + 1 + 2 + 2 = 7/2 = 1,7 ≈ 2

Nota: Adaptado de libro II-MAGERIT

10. *Determinación de salvaguardas de activos de la institución*: en este proceso se persigue el reconocimiento de las salvaguardas empleadas en los activos de la Municipalidad, catalogándolas en base a su eficiencia ante las amenazas que desean reprimir.

En caso de que no se requiera tratar los riesgos: se hace un seguimiento de continuo de los mismos.

En caso de que si se requiera tratar los riesgos:

Fase IV: Gestión de riesgos: Esta fase se delimitan las pautas para gestionar los riesgos según su relevancia y estimación, en base a prevenciones apropiadas para garantizar su control y facilidad en los procedimientos de la organización.

11. *Tratamiento del riesgo*: mediante esta etapa se concretan las funciones para el tratamiento de los riesgos con el fin de impedir, disminuir, trasladar y aceptarlos riesgos. Asimismo, posteriormente se emiten las políticas de administración del riesgo.

12. *Control y seguimiento*: generar indicadores de gestión que permitan medir la eficiencia del desempeño de las normas de protección.

Luego de haber reconocido los lineamientos a ejercer para implementar el modelo presentado para la gestión de riesgo en la Municipalidad, se aplica aquí su implementación en base al esquema presentado en el anexo 9, se lleva a cabo la implementación de este, ejerciendo sistemáticamente lo estipulado en la figura 7, y eludiendo la etapa 1, vinculada a la apreciación del riesgo, de lo cual los resultados se encuentran representados en el primer objetivo enfocado al diagnóstico de la situación actual de este estudio.

Es por ello, que se da paso a la segunda fase del modelo, correspondiente análisis de riesgos, comenzando por identificar los activos de la institución, catalogarlos, y evaluarlos, mediante su nivel de Disponibilidad (D), Integridad (I) y Confiabilidad (C) y las pautas presentadas tablas 12, 13 y 14, en donde B representa un nivel “Bajo”, M representa un nivel “Moderado” y A representa un nivel “Alto”. Los resultados se pueden observar tal y como se muestra en la tabla 18.

Tabla 18

Valoración de los activos de la Municipalidad Distrital de Papayal. Año 2020

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA

Personas (P)	P1	Usuarios de la Institución	50	2	**2**	M
Personas (P)	P2	Responsable UTI	1	3	**3**	**A**
Instalaciones (L)	L1	Alcaldía (A)	1	2	**2**	M
Instalaciones (L)	L2	Consejo Municipal (CM)	1	2	**2**	M
Instalaciones (L)	L3	Gerencia Municipal (GM)	1	2	**2**	M
Instalaciones (L)	L4	Oficina de Asesoría Legal (OAL)	1	2	**2**	M
Instalaciones (L)	L5	Oficina de Planificación y Presupuesto (OPP)	1	2	**2**	M
Instalaciones (L)	L6	Oficina de Programación Multianual de Inversiones (OPMI)	1	2	**2**	M
Instalaciones (L)	L7	Unidad Formuladora (UF)	1	2	**2**	M
Instalaciones (L)	L8	Especialista en Inversiones (EI)	1	2	**2**	M
Instalaciones (L)	L9	Oficina de Secretaría General (OSG)	1	2	**2**	M

Instalaciones (L)	L10	Unidad de Relaciones Públicas e Imagen Institucional (URP)	1	2	**2**	M
Instalaciones (L)	L11	Unidad de Abastecimiento Logística y Control Patrimonial (UAl)	1	2	**2**	M
Instalaciones (L)	L12	Almacén - Unidad de Abastecimiento Logística y Control Patrimonial (AL)	1	2	**2**	M
Instalaciones (L)	L13	Unidad de Tesorería (UT)	1	2	**2**	M
Instalaciones (L)	L14	Unidad de Rentas (UR)	1	2	**2**	M
Instalaciones (L)	L15	Unidad de Recursos Humanos y Bienestar Social (URH)	1	2	**2**	M
Instalaciones (L)	L16	Oficina de Desarrollo Urbano e Infraestructura (UDU)	1	2	**2**	M
Instalaciones (L)	L17	Unidad de Maquinaria y Maestranza (UMM)	1	2	**2**	M

Tabla 18

(*Cont.)*

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Instalaciones (L)	L18	Oficina de Desarrollo Social y Servicios Públicos (UDS)	1	2			**2**	M
Instalaciones (L)	L19	Unidad de Salud, Limpieza, Ornato, Medio Ambiente-Ecología, Parques-Jardines, Control de Cementerio y Estadio, y ATMSR - Área Técnica Municipal de Saneamiento Rural. (USL)	1	2			**2**	M
Instalaciones (L)	L20	Unidad de SISFOH, Complementación Alimentaria, PVL y Comercialización (USI	1	2			**2**	M
Instalaciones (L)	L21	Programa de Vaso de Leche y Complementación Alimentaria (PVL)	1	2			**2**	M
Instalaciones (L)	L22	DEMUNA - Defensoría de la Municipal del Niño	1	2			**2**	M

		y del Adolescente (DEM)						
Instalaciones (L)	L23	OMAPED - Oficina Municipal de Atención a la Persona con Discapacidad (OMA)	1	2			**2**	M
Instalaciones (L)	L24	Seguridad Ciudadana (SC)	1	2			**2**	M
Instalaciones (L)	L25	Defensa Civil (DC)	1	2			**2**	M
Instalaciones (L)	L26	Oficina de Registro Civil (ORC)	1	2			**2**	M
Instalaciones (L)	L27	Unidad de Tecnologías de la Información (UTI)	1	3	3	3	**3**	**A**
Equipos Informáticos (HW)	HW1 - HW8	Laptop	8	3	2	3	**3**	**A**
Equipos Informáticos (HW)	HW9- HW33	Desktop	25	3	2	3	**3**	**A**
Equipos Informáticos (HW)	HW34- HW42	Switch	9	3	2	3	**3**	**A**

Equipos Informáticos (HW)	HW43-HW68	Impresora	26	2		**2**	M
Equipos Informáticos (HW)	HW69	Escáner	1	2		**2**	M
Equipos Informáticos (HW)	HW70	Proyector Multimedia	1	2		**2**	M
Equipos Informáticos (HW)	HW71	Plotter	1	2		**2**	M

Tabla 18

(*Cont.)*

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Equipos Informáticos (HW)	HW72	DVR - Digital Video Recorder	1	2			**2**	M
Equipos Informáticos (HW)	HW73-HW75	Cámara de Video Vigilancia	3	2			**2**	M

Equipos Informáticos (HW)	HW76	Fotocopiadora	1	2			**2**	M
Equipos Informáticos (HW)	HW77-HW78	Server	2	3		3	**3**	**A**
Equipos Informáticos (HW)	HW79	Router	1	3		3	**3**	**A**
Equipos Informáticos (HW)	HW80	Antena	1	3		3	**3**	**A**
Software y aplicaciones	SW1	Sistema Operativo: Microsoft Windows 10 Professiona1	1	2	2	2	**2**	M
Software y aplicaciones	SW2	Sistema Operativo: Microsoft Windows 8.1 Professional	1	2	2	2	**2**	M
Software y aplicaciones	SW3	Sistema Operativo: Microsoft Windows 7 Professional	1	2	2	2	**2**	M
Software y aplicaciones	SW4	Navegador web: Microsoft Edge	1	2	2	2	**2**	M

Software y aplicaciones	SW5	Navegador web: Google Chrome	1	3	2	3	**3**	**A**
Software y aplicaciones	SW6	Navegador web: Mozilla Firefox	1	2	2	2	**2**	M
Software y aplicaciones	SW7	Antivirus: ESET End Point Protection Standard	1	3			**3**	**A**
Software y aplicaciones	SW8	Ofimática: Microsoft Office 2013 Standard	1	2	2	2	**2**	M
Software y aplicaciones	SW9	Compresor de Carpetas y Archivos: WinRAR	1	2	2	2	**2**	M
Software y aplicaciones	SW10	Asistencia Remota: AnyDesk	1	3	2	3	**3**	**A**
Software y aplicaciones	SW11	Lector de PDF: Adobe Reader DC	1	2	2	2	**2**	M
Software y aplicaciones	SW12	Web: Aplicativos de Contraloría General de la República	1	2	2	2	**2**	M

Tabla 18

(*Cont.)*

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Software y aplicaciones	SW13	Sistema Integrado de Administración Financiera del Sector Público - Gobiernos Locales (SIAF) (Usado en GP, OAR, OPP, UAL, UC, UT)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW14	Web: SUNAT - Operaciones en Línea (Usado en UC, UT)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW15	Sistema Integrado de Gestión Administrativa - Control Patrimonial (SIGA) (Usado en UAL, AL)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW16	Software de Abastecimiento (Usado en UAL, AL)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW17	Web: Sistema Electrónico de Contrataciones del Estado (Usado en UAL, EC)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW18	Web: Perú Compras (Usado en UAL)	1	3	3	3	**3**	**A**

Software y aplicaciones	SW19	Web: Registro Nacional de Proveedores (Usado en UAL)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW20	Software de Control de Predios (Usado en UR)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW21	Web: Sistema de Focalización de Hogares (Usado en UUS)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW22	Software de Control de Beneficiarios (Usado en PVL)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW23	Web: Sistema de Registro Nacional de Identificación y Estado Civil (Usado en ORC)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW24	Web: Módulo de Programación Multianual de Inversiones (Usado en OPMI)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW25	Web: Banco de Proyectos de Inversión Pública (Usado en UF, ODU, OPMI)	1	3	3	3	**3**	**A**

Software y aplicaciones	SW26	Web: Sistema Nacional de Información de Obras Públicas (Usado en EI)	1	3	3	3	**3**	**A**

Tabla 18

(*Cont.)*

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Software y aplicaciones	SW27	Web: Módulo de Registro de Ejecución de Metas de Obras Públicas (Usado en EI)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW28	Adobe PhotoShop (Usado en URP)	1	2			**2**	M
Software y aplicaciones	SW29	Corel Draw (Usado en URP)	1	2			**2**	M
Software y aplicaciones	SW30	Sony Vegas (Usado en URP)	1	2			**2**	M
Software y aplicaciones	SW31	SUNAT - Programa de Declaración Telemática (Usado en URH)	1	3	3	3	**3**	**A**

Software y aplicaciones	SW32	AutoCAD 2019 (Usado en ODU)	1	2			**2**	M
Software y aplicaciones	SW33	Windows Server 2012 R2 Standard (Usado en UTI)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW34	SQL Server 2008 Express (Usado en UTI)	1	3	3	3	**3**	**A**
Software y aplicaciones	SW35	Web: Panel de Control de Hosting y Dominio Institucional (Usado en UTI)	1	3	3	3	**3**	**A**
Servicios (S)	S1	Correo Electrónico	1	3	3	3	**3**	**A**
Servicios (S)	S2	Telefonía Fija	1	2			**2**	M
Servicios (S)	S3	Internet	1	3	3	3	**3**	**A**
Servicios (S)	S4	Soporte Técnico	1	3	3	3	**3**	**A**
Servicios (S)	S5	Creación de usuarios	1	3	3	3	**3**	**A**
Servicios (S)	S6	Redirección de Archivos	1	2			**2**	M
Redes de comunicaciones (COM)	COM1	Cableado Estructurado, Integrado por: Cables UTP, Categoría 6. Puntos de Red	1	3	3	3	**3**	**A**

Redes de comunicaciones (COM)	COM2	Conexión inalámbrica, Señal Wi-Fi de 150	1	3	3	3	**3**	**A**

Con base a los apuntes señalados en la tabla 8, hay 76 equipos con un nivel elevado de estimación frente a la seguridad informática de la institución.

Fueron tomados en distinción estos equipos en lo consecutivo para identificar la amenazas y vulnerabilidades, y luego la valoración de riesgos, por ser considerados equipos de alto rango de gravedad.

Es por esto, que en el proceso de identificación de amenazas y vulnerabilidades presentadas en el modelo propuesto, se persigue le reconocimiento de estos dos elementos característicos de la situación actual de la Municipalidad Distrital de Papayal, para posteriormente ser evaluados, los cuales se lograron relacionar con los ya establecidos en el índice de elementos que expone MAGERIT, son los siguientes que se registran por tipo de origen (de donde proviene) y tipo de activo que se ve afectado, en la tabla 19:

Tabla 19

Amenazas y vulnerabilidades que afectan los activos en la Municipalidad Distrital de Papayal

Tipo de Amenaza por su origen	Amenaza (denominación)	Vulnerabilidad	Tipos de activos afectados
Natural	Fuego	Carencia de sistemas de protección contra incendios	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
	Daños por agua	Falta de mecanismos de protección contra el agua	Equipos Informáticos, Instalaciones, Redes de Comunicación
	Desastres naturales (sismos)	Problemas estructurales de mobiliarios e infraestructuras donde se ubica el activo	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
Industrial	Desastres industriales (fuga de gases, explosión)	Falta de controles previos del tipo de desastre	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
	Corte de servicio eléctrico	Mal funcionamiento de la unidades protección auxiliar, falta de generadores eléctricos	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización, falta de dispositivos de enfriamiento	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
Personas (por causa accidental)	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas

Tabla 19

(*Cont.)*

Tipo de Amenaza por su origen	Amenaza (denominación)	Vulnerabilidad	Tipos de activos afectados
	Expansión de software dañino	Falla o carencia de software de protección o antivirus	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Debilidad de uso del software	Desactualización del software, inadecuada depuración del mismo	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento y de almacenamiento	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Mala restauración de respaldos	Inexistencia de mecanismos para garantizar el respaldo o recuperar los mismos	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Fallas gestión de mantenimiento y actualización de equipos	Poco o nulo control de actualización de los equipos	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Indisponibilidad de personal	Poco o nulo control de de las políticas de control del personal	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
Personas (provocadas intencionalmentel)	Uso no previsto de los recursos	Poco o nulo control de de las políticas de control del personal	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	Equipos Informáticos, Personas, Redes de Comunicación, Software
	Cambio intencional de contenido informativo	Falta de mecanismos eficaces de control de cambios de información	Equipos Informáticos, Personas, Redes de Comunicación, Software
	Difusión de información	Falta de mecanismos eficaces de control de cambios de almacenamiento de la información	Equipos Informáticos, Redes de Comunicación, Software

Tabla 19

(*Cont.)*

Tipo de Amenaza por su origen	Amenaza (denominación)	Vulnerabilidad	Tipos de activos afectados
	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	Equipos Informáticos, Redes de Comunicación, Software
	Cambios de contenidos de software	Falta de mecanismos eficaces de control de cambios y manipulación de programas	Software
	Manipulación de equipos informáticos	Falta de mecanismos eficaces de control de cambios y manipulación de equipos informáticos	Equipos Informáticos, Redes de Comunicación

Nota: Adaptado de Libro II de MAGERIT

Al igual que se visualiza los tipos de amenazas que originan los inconvenientes que perjudican a los procedimientos de la Municipalidad son caracterizados por ser de orientación natural, industrial o institucional, originados por personas ya sean por causas accidentales o provocadas intencionalmente.

Estos hallazgos, colocaron según tabla 7 inherente al mapa de evaluación de riesgos ya realizado, a 29 activos de la institución en un nivel mayor de riesgo, los cuales serán relevantes para tomar en cuenta en las políticas de control en la etapa de tratamiento:

Tabla 20

Activos destacados en la valoración de amenazas, vulnerabilidades, impacto y nivel de riesgos

Código	Activo	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Nivel de riesgos	Medidas de acción ante el riesgo
P2	**Responsable de la UTI**	Alta	Alto	Mayor	Implementar políticas de motivación al RRHH. Incrementar el grupo de trabajo en la UTI. Reforzar políticas de seguridad industrial

Tabla 20

(*Cont.)*

Código	Activo	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Nivel de riesgos	Medidas de acción ante el riesgo
L27	**Unidad de Tecnologías de la Información (UTI)**	Alta	Alto	Mayor	Dotar de sistemas contra incendios todas las áreas d la institución. Dotar de aires acondicionados más eficiente el área.

					Adoptar políticas de seguridad y control para la entrada y salida de recursos
		Alta	Alto	Mayor	Dotar de aires acondicionados más eficiente el área. Repotenciar los recursos de los servers. Mejorar y hacer cumplir las políticas de control de mantenimiento de los equipos a nivel hardware y software. Actualizar los programas periódicamente. Referir políticas de control de cambios y manipulación de equipos informáticos. Referir políticas de control de cambios de información.
HW77-HW78	**Server**				

					Mantener licencia de software de protección o antivirus actualizada.
SW5	**Navegador web: Google Chrome**	Alta	Alto	Mayor	Actualizar los programas periódicamente.
		Alta	Alto	Mayor	Referir políticas de control de cambios de información.
SW7	**Antivirus: ESET End Point Protection Standard**				Mantener licencia de software de protección o antivirus actualizada. Actualizar los programas periódicamente.
		Alta	Alto	Mayor	Referir políticas de control de cambios de información.
SW10	**Asistencia Remota: AnyDesk**				Mantener licencia de software de protección o antivirus actualizada. Actualizar los programas periódicamente.

Tabla 20

(*cont.)*

Código	Activo	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Nivel de riesgos	Medidas de acción ante el riesgo
SW13 – SW35	**Sistemas administrativos de la Municipalidad, instalados en la red y disponibles en la web.**	Alta	Alto	Mayor	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Crear programas de capacitación para que el personal adquiera habilidades en el manejo de aplicaciones, equipos y sistemas Dotar de generadores eléctricos y equipos auxiliares UPS. Mejorar las políticas de control de acceso de usuario.

		Alta	Alto	Mayor	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Dotar de generadores eléctricos y equipos auxiliares UPS. Mejorar las políticas de control de acceso de usuario.
S1	**Correo Electrónico**				
		Alta	Alto	Mayor	Mecanismos ineficaces para controlar sustituciones de hardware. Mejorar las políticas de control de acceso de usuario. Referir políticas de control de cambios de información.
S5	**Creación de usuarios**				

En la tabla anterior, se exponen las medidas que serán consideradas para minimizar los riesgos a los que se encuentran exhibidos, ya que abordan los activos de mayor relevancia

en la seguridad informática dentro de la Municipalidad Distrital de Papayal, para lo cual también fue conveniente como apertura a la fase de gestión de riesgos, en cuanto a su tratamiento, realizar un diagnóstico de los salvaguardas con los que esta institución actualmente cuenta, y posteriormente sirvan de marco de desarrollo de la estrategia de gestión de riesgo a formular en este trabajo de investigación.

De allí, luego de la valoración del inventario, se busca evaluar porcentualmente la eficacia de las salvaguardas, mediante una lista de chequeo o checklist.

Para este punto se registraron las observaciones de la evaluación de salvaguardas en la gestión de seguridad informática, a partir de la aplicación de formato de observación directa checklist (anexo 5), estandarizado por MAGERIT y adaptado a la institución en estudio por el presente investigador ante las evidencias encontradas en la UTI y a lo largo de la infraestructura de la Municipalidad, por lo cual se presenta el correspondiente análisis de los resultados arrojados.

Tabla 21

Evaluación de salvaguardas en la seguridad informática de la Municipalidad

N°	ÍTEMS PARA EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
1.	**Seguridad Física**						**20%**
1.1.	Instalaciones de la UTI protegidas de acceso no autorizado.						
1.2.	Tipos de controles físicos aplican para la UTI:						
	a) Contorno de seguridad bien delimitado						
	b) Mecanismos para detectar intrusos						
	c) Puertas con mecanismos seguros de						

N°	ÍTEMS PARA EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
	entrada						
	d) Carné de Identificación						
	e) Registro de visitantes						
1.3.	La UTI cuenta con condiciones físicas adecuadas de acuerdo con normas definidas de por EIA/TIA, de a acuerdo a:						
	a) Paredes						
	b) Piso						
	c) Techo						
	c) Climatización						
	d) Iluminación						
1.4.	Mecanismos contra incendios utilizados:						
	a) Avisos alarmantes						

Tabla 21

(*Cont.)*

N°	ÍTEMS PARA EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
	b) Extinguidores						
	c) Sistema contra incendios						
1.5.	El cableado de la red de comunicación está esquematizado de acuerdo con los estándares internacionales vigentes.						
1.7.	Está sustentado el diseño de la red institucional.						

1.8.	Existen medidas de control que estructuren los pasos para el mantenimiento preventivo y correctivo de los equipos de la UTI.	
1.9.	Cuentan con suficiente personal para la gestión de mantenimiento a equipos informáticos.	
1.10.	Tienen controles para llevar a cabo el mantenimiento de equipos informáticos en todas las instalaciones de la Municipalidad.	
1.11.	Cuentan con equipos de auxiliares para proveer energía eléctrica.	
2.	**Red**	**40%**
2.1.	Se tiene definido quienes pueden compartir información mediante la red y la manera de hacerlo.	
2.2.	Documentan y actualizan a nivel de red sus inventarios tanto lógicos como físicos.	
2.3.	Se registran las incidencias de fallas que se suscitan en la red.	
2.4.	Cuentan con mecanismos de entrada a la intranet institucional.	
2.5.	Cuentan con mecanismos firewall para el aseguramiento y protección de redes.	
3.	**Software**	**40%**
3.1.	Los equipos laptops y desktops, así como server tienen Antivirus en constante	

	estado de actualización.						
3.2.	Los softwares dispuestos en el servidor de BD están en constante estado de actualización.						
3.3.	Se implementa la monitorización continua del rendimiento de servidores, y la entrada a los mismos.						
3.4.	Se garantiza la seguridad de la información clave manejada en los equipos mediante su respaldo antes de formateo de estos						
3.5.	La información que transita por la red interna se encuentra en estatus de encriptación.						
4.	**Organización**						**16%**
4.1	Tienen política general de seguridad informática						
4.2.	Tienen un departamento o dependencia que se dedique a la administración de la red y los servicios de TI						

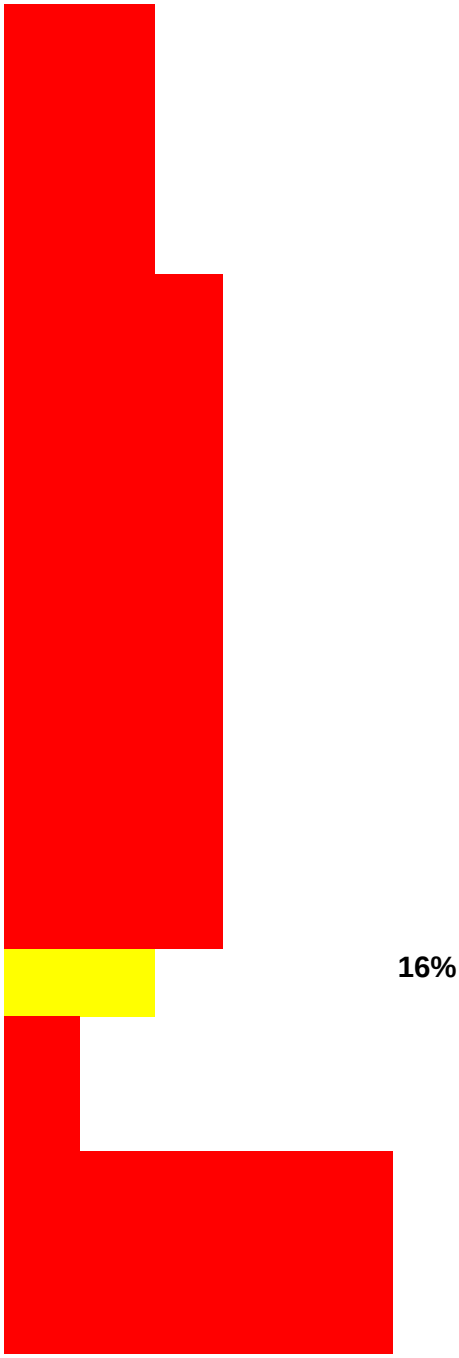


Tabla 21

(*Cont.)*

N°	ÍTEMS PARA EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
4.3.	El número de personas que constituyen actualmente la UTI son suficientes para						

	controlar los diferentes procesos de TI	
4.4.	Tienen plan de formación y desarrollo para empleados de la UTI en aspectos relacionados con las TIC, gestión de riesgos y procesos de certificación	
4.5.	Aplican análisis y evaluación de riesgos informáticos	
4.6.	Conocen los riesgos de seguridad informática que amenazan los activos de la Institución, así como la vulnerabilidad ante estas.	
4.7.	Poseen lineamientos para la gestión de riesgos de seguridad informática	
4.8.	Existen políticas de seguridad actualizadas.	
4.9.	Las políticas de seguridad están debidamente socializadas con el personal de la Municipalidad.	
	Total Eficacia Salvaguarda	**29 %**

Fuente: Elaboración Propia. Adaptado de libro II-MAGERIT

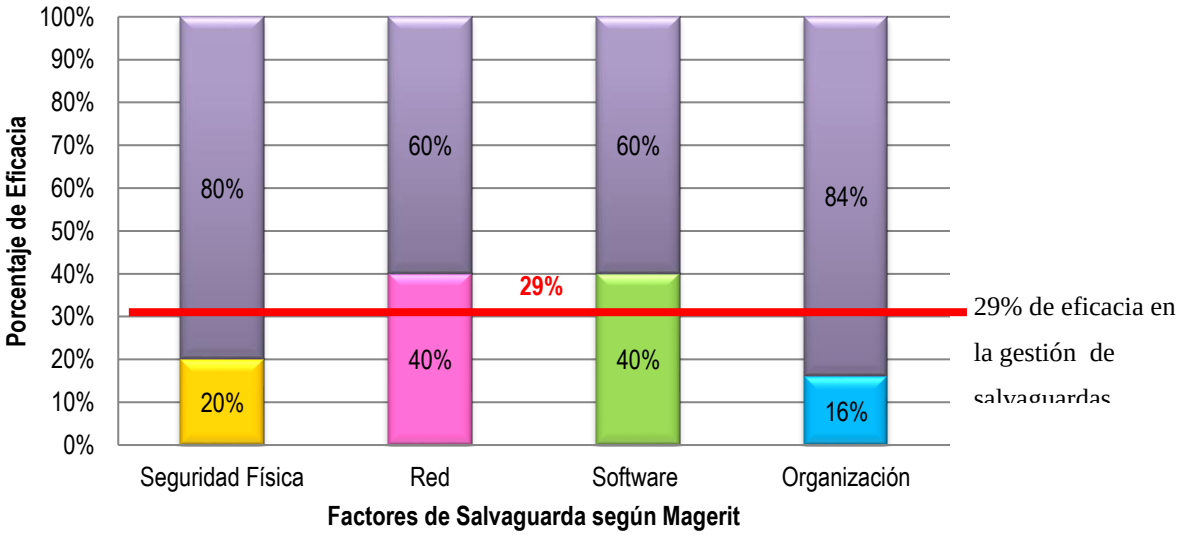
En la tabla 21, se detallan los aspectos a evaluar en la gestión de seguridad en cuanto a las medidas que pone en práctica la institución para garantizar el aseguramiento de sus activos, en función de una escala de 0% al 100%, ante los factores estudiados que abordan la seguridad física, la red, el software y la organización.

De acuerdo con lo registrado en el diagnóstico realizado, la eficacia total de la gestión

de salvaguardas con la que cuenta la Municipalidad es de 29 por ciento, los cual se puede visualizar en la figura 10, donde se detalla el nivel de cumplimiento de medidas que acercan a la gestión de seguridad informática y las brechas existentes.

Figura 10

Eficacia de las salvaguardas



La figura 10, devela que conjunto de alternativas que evalúa la eficacia de la seguridad física reveló que esta se cumple en un 20 por ciento, lo que la coloca en un nivel de eficacia deficiente. Ante esto, la brecha que la aleja de un buen desempeño es de 80 por ciento, y se debe a que la UTI no cuenta con protección de acceso no autorizado, ni controles de perímetro, ni puertas de seguridad para entrar al recinto; tampoco con las condiciones físicas de climatización, ni con generadores de energía eléctrica que los resguarde ante una eventualidad de un corte eléctrico. Del mismo modo, no se alinean a la seguridad general ante un desastre por fuego, ya que carecen de sistemas contraincendios, cuyas medidas solo cumplen ante la existencia de 12 extintores existentes en toda la extensión de la infraestructura.

Asimismo, se determinó que controles para llevar a cabo el mantenimiento preventivo

y correctivo de los equipos de la UTI, así como en toda la organización, pero no lo aplican con eficiencia, ya que existen debilidades inherentes a la insuficiencia de personal para cubrir ciertos trabajos orientados a este contexto.

En cuanto al factor Red, se obtuvo una eficacia de 40 por ciento, posicionándose en un nivel que requiere atención, que cuya brecha de incumplimiento de 60 por ciento se debe a que no tiene una buena gestión de control de las fallas que se suscitan en la infraestructura de red, ni de sus sistemas y activos que están involucrados en la plataforma tecnológica, y aun cuando cuentan con medidas de control, poco se abocan hacia su cumplimiento; tampoco cuentan con medios de aseguramiento y protección de la red, tal como los firewall.

En relación con al factor Software, se manejó una eficacia de 40 por ciento ya que indica que requiere atención, donde su brecha igual a 60 por ciento dista a un buen desempeño en la seguridad y salvaguarda debido a que no se gestiona con vehemencia que los equipos de computación, ya sea portátiles o de escritorio, así como los servers mantengan sus programas de antivirus actualizados, tampoco aplicaciones de BD, ni poseen medios ante ataques de intrusos o hackers.

En cuanto al factor de Organización, se registró una eficacia de 16 por ciento, siendo la más débil de todo el estudio, ubicándose así en una gestión crítica. Su brecha ante el buen desempeño es de 84 por ciento ya que no poseen política alguna relacionada con seguridad informática, y ante esto nunca ha llevado a cabo el análisis y evaluación de riesgos informáticos, y por ello, muy poco conocen los riesgos de seguridad informática que amenazan los activos de la institución, así como la vulnerabilidad ante estos. Esta situación, los pone en un estado de carencia de lineamientos y políticas para la gestión de riesgos de seguridad informática.

Así pues, ante estos detalles que se deslindan del análisis y evaluación riesgo que permitió valorizar el riesgo y conocer cuáles son los activos de información que tienen mayor exposición, y por lo tanto conocer donde enfocar los recursos de la organización, se plantea

a continuación un plan de implementación de medidas para la gestión de riesgos vinculados a las necesidades de los activos de mayor riesgo de la institución. En este plan (tabla 22) se especifica las políticas de control, el porcentaje avance de implementación de la medida en cada activo, el avance acumulado de la estrategia integral, el tipo de recurso generado, el responsable de ejecutarlo, y la fecha de comienzo de su ejecución de prueba, durante su formal aprobación en la Municipalidad, y su total difusión y puesta en marcha de las acotaciones dispuestas en la misma.

Tabla 22

Plan de implementación de medidas para la gestión de riesgos de la seguridad informática en la Municipalidad Distrital de Papayal

Código	Activo	Medidas de acción ante el riesgo	Políticas de Control	Avance de las medidas	Avance Acumulado	Recurso	Responsable	Fecha
P2	**Responsable Unidad de Tecnologías de la Información**	Implementar políticas de motivación al RRHH. Incrementar el grupo de trabajo en la UTI. Reforzar políticas de seguridad industrial.	- Políticas de seguridad - Políticas generales - Políticas de Seguridad a nivel del Personal	100%	11,1%			
L27	**Unidad de Tecnologías de la Información (UTI)**	Dotar de sistemas contra incendios todas las áreas d la institución. Dotar de aires acondicionados más eficiente el área. Adoptar políticas de seguridad y control para la entrada y salida de recursos.	- Políticas de seguridad - Políticas generales - Políticas de seguridad a nivel físico - Políticas de seguridades a nivel lógico - Políticas de seguridades a nivel de sistemas - Políticas de respaldos y recuperación de información - Políticas relacionadas a los equipos de computación - Políticas de mantenimiento de equipos - Políticas de actualización de los equipos - Políticas de accesos remotos - Políticas del WWW - Política de control de virus, uso de software	100%	22,2%	Manual de Políticas de Gestión de Riesgos para la Seguridad Informática en la Municipalidad Distrital de Papayal	Responsable de la UTI, Investigador	Enero – Febrero 2021

Código	Activo	Medidas de acción ante el riesgo	Políticas de Control	Avance de las medidas	Avance Acumulado	Recurso	Responsable	Fecha
HW77-HW78	**Server**	Dotar de aires acondicionados más eficiente el área. Repotenciar los recursos de los servers. Mejorar y hacer cumplir las políticas de control de mantenimiento de los equipos a nivel hardware y software. Actualizar los programas periódicamente. Referir políticas de control de cambios y manipulación de equipos informáticos. Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada.	- Políticas de seguridad - Políticas generales - Políticas de seguridad a nivel físico - Políticas de seguridades a nivel de sistemas - Políticas de respaldos y recuperación de información - Políticas relacionadas a los equipos de computación - Políticas de mantenimiento de equipos - Políticas de actualización de los equipos - Políticas de accesos remotos - Política de control de virus, uso de software	100%	33,3%	Manual de Políticas de Gestión de Riesgos para la Seguridad Informática en La Municipalidad Distrital de Papayal	Responsable de la UTI, Investigador	Enero - Febrero 2021

Código	Activo	Medidas de acción ante el riesgo	Políticas de Control	Avance de las medidas	Avance Acumulado	Recurso	Responsable	Fecha
SW5	**Navegador web: Google Chrome**	Actualizar los programas periódicamente.	- Políticas de seguridad - Políticas generales	100%	44,4%			
SW7	**Antivirus: ESET End Point Protection Standard**	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Actualizar los programas periódicamente.	- Políticas de seguridad a nivel físico - Políticas de seguridades a nivel de sistemas	100%	55,5%			
SW10	**Asistencia Remota: AnyDesk**	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Actualizar los programas periódicamente.	- Políticas de respaldos y recuperación de información - Políticas relacionadas a los equipos de computación	100%	66,6%	Manual de Políticas de Gestión de Riesgos para la Seguridad Informática en La Municipalidad Distrital de Papayal.	Responsable de la UTI, Investigador	Enero – Febrero 2021
SW13 – SW35	Sistemas administrativos de la Municipalidad, instalados en la red y disponibles en la web.	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Crear programas de capacitación para que el personal adquiera habilidades en el manejo de aplicaciones, equipos y sistemas Dotar de generadores eléctricos y equipos auxiliares UPS. Mejorar las políticas de control de acceso de usuario.	- Políticas de mantenimiento de equipos - Políticas de actualización de los equipos - Políticas de accesos remotos - Política de control de virus, uso de software	100%	77,7%			

Código	Activo	Medidas de acción ante el riesgo	Políticas de Control	Avance de las medidas	Avance Acumulado	Recurso	Responsable	Fecha
S1	**Correo Electrónico**	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Dotar de generadores eléctricos y equipos auxiliares UPS. Mejorar las políticas de control de acceso de usuario.	- Políticas de seguridad - Políticas generales - Políticas de seguridades a nivel de sistemas - Políticas relacionadas a los equipos - Políticas de accesos remotos - Políticas del WWW - Política de control de virus, uso de software	100%	88,8%	Manual de Políticas de Gestión de Riesgos para la Seguridad Informática en la Municipalidad Distrital de Papayal.	Responsable de la UTI, Investigador	Enero - Febrero 2021
S5	**Creación de usuarios**	Falta de mecanismos eficaces de control de cambios y manipulación de equipos informáticos. Mejorar las políticas de control de acceso de usuario. Referir políticas de control de cambios de información.	- Políticas de seguridad - Políticas generales - Políticas de seguridades a nivel de sistemas - Políticas relacionadas a los equipos - Políticas de accesos remotos - Políticas del WWW - Política de control de virus, uso de software	100%	100%			

En función de dar cumplimiento a las acciones planificadas para disminuir y prevenir los riesgos en la seguridad informática la Municipalidad Distrital de Papayal, se definieron políticas que dejaran tener un enfoque claro de la conducta y desempeño generalizado de los integrantes de esta institución para lograr su principal objetivo (ver anexo 10), del cual como se pudo observar fueron ya difundidas entre las diversas unidades departamentales de la organización en un 100% entre los meses de enero y febrero del presente año 2021, marcando como se expuso en la tabla 5 una efectividad de 84% de efectividad del modelo propuesto, vinculado al manual de políticas que incorpora lo siguiente.

- Objetivo.
- Alcance.
- Política de seguridad.
- Políticas generales.
- Políticas a nivel del personal.
- Políticas de seguridad a nivel físico.
- Políticas de seguridades a nivel lógico.
- Políticas de seguridades a nivel de sistemas.
- Políticas de respaldos y recuperación de información.
- Políticas relacionadas a los equipos de computación.
- Políticas de mantenimiento de equipos.
- Políticas de actualización de los equipos.
- Políticas de accesos remotos.
- Políticas del WWW.
- Política de control de virus, uso de software.
- Políticas de gestión: indicadores y monitoreo de gestión, comunicación y difusión.

Asimismo, el instrumento está estructurado en base a las normas que son utilizadas

en el organismo para sus documentos oficiales para su pertinente verificación y aprobación.

Finalmente, una vez aplicado e implementado el modelo, y comprobada su eficiencia, se procedió a validar el mismo con el apoyo de estos tres (03) expertos en seguridad informática (ver tabla 23), quienes expresaron su posición con el enfoque que caracteriza la metodología MAGERIT, y en este sentido verificar su grado de alineamiento al mismo.

Tabla 23

Expertos en seguridad informática

Nombre y Apellido	**Profesión**	**Especialización/ Conocimiento en SI**	**Cargo**	**Telf. y Ubicación**
Joisy Del Valle Rojas Rojas	Ingeniero de Sistemas	Máster en Seguridad de la Información	Auditor de Sistemas y Docente	+584122186547 Venezuela
Nelson Ángeles Quiñones	Ingeniero de Sistemas	Normas ISO 27001 y 31000, ITIL	Consultor y Auditor	+51 949 929 179 Perú
Luis Vicente Castillo Boggio	Ingeniero de Sistemas	COBIT y MAGERIT	Administrador de TI y Docente	+51 972 609 117 Perú

Frente a esto, fue preciso estar en comunicación con los expertos vía telefónica y exponerle una introducción del modelo de gestión de riesgos y su manera de operar, para después enviar por correo electrónico una sinopsis del trabajo donde se expone el planteamiento del problema, la hipótesis sustentada por la metodología MAGERIT, el esquema del modelo de gestión de riesgo propuesto (gráfico y descripción de los procesos), y la checklist preliminar (ver anexo 6.3.), con los ocho (08) elementos valorados con base a

los promedios aritméticos en la incidencia con cada ítems de análisis, para luego establecer la relación con los resultados de la escala de Lickert presentada en la tabla 24.

Tabla 24

Escala utilizada para el análisis de la lista de chequeo

Alternativas	Criterio de Evaluación
Totalmente de acuerdo (TA)	Muy Bueno (de 4,1 puntos a 5 puntos)
De acuerdo (DA)	Bueno (de 3,1 puntos a 4 puntos)
Neutral (N)	Aceptable (de 2,1 puntos a 3 puntos)
En desacuerdo (ED)	Requiere Atención (de 1,1 puntos a 2 puntos)
Totalmente en desacuerdo (TD)	Crítico (de 0,1 puntos a 1 puntos)

Estos resultados, se registraron y tabularon para su correspondiente evaluación, mostrando su registro en la tabla 25:

Tabla 25

Medición del nivel de coherencia y correspondencia del modelo de gestión de riesgo con respecto a la metodología MAGERIT

ítems	TDA 5	DA 4	N 3	D 2	TD 1	Total	Promedio
P1. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta	2	1	0	0	0	**3**	4,67
P2. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la caracterización expuesta	3	0	0	0	0	**3**	**5,00**
P3. El modelo gestión de riesgos basado en MAGERIT cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica	0	3	0	0	0	**3**	4,00
P4. El modelo gestión de riesgos propuesto cumple con las fases de la metodología MAGERIT	3	0	0	0	0	**3**	**5,00**
P5. El modelo propuesto para la gestión de riesgos basado en MAGERIT sigue una secuencia lógica de los procesos que lo integran	1	2	0	0	0	**3**	4,33
P6. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente graficado	3	0	0	0	0	**3**	**5,00**
P7. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente explicado de manera que pueda guiar su implementación	2	1	0	0	0	**3**	4,67
P8. El modelo integra el proceso de tratamiento de los riesgos analizados y evaluados	3	0	0	0	0	**3**	**5,00**
Total Promedio de Coherencia y Correspondencia							**4,71**

Con referencia a los resultados obtenidos mediante la checklist, la correspondencia del modelo de gestión de riesgos enfocado en MAGERIT de acuerdo con su caracterización (P2) y teoría (P1) refleja una valoración de calidad como Muy Buena.

Igualmente, se visualiza una concordancia Muy Buena, entre el modelo gestión de riesgos propuesto en función de las fases de la metodología MAGERIT (P4), su diseño gráfico (P6) y su explicación a detalle (P7), y su función final de adaptación de medidas de control y tratamiento ante cada uno de los riegos estudiados (P8).

Sin embargo, a pesar de tener el modelo gestión de riesgos basado en MAGERIT una Buena coherencia ante el cumplimiento de todas las pautas establecidas en los textos que sustentan su esquema por el Consejo Superior de Administración Electrónica (P3) y una secuencia lógica de los procesos plasmados en el diseño presentado (P5), estos ítems fueron los de menor valor, colocándose por debajo del promedio de 4,71 (Muy Bueno); lo cual motivó

a los expertos a sugerir en una segunda ronda de feedback y consultar la revisión y cotejo de los procesos que contemplan las fases tanto en los libros como en otras literaturas sobre el tema, coincidiendo finalmente en una tercera ronda de discusión entre ellos y el presente investigador, que además de existir una total correspondencia del modelo propuesto con el método MAGERIT, el nuevo diseño fue enriquecido con otros aportes de la metodologías análogas con las que fue comparada MAGERIT, y que profundizan en entorno general de análisis y la gestión de riesgos.

Por lo tanto, es pertinente dejar el diseño como inicialmente se encuentra, de manera que sirva de antecedente para otras investigaciones y estudios de análisis de riesgos en la Municipalidad.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Del proceso diagnóstico llevado a cabo, se pudo determinar que actualmente la Municipalidad Distrital de Papayal no posee normas de control para certificar las de seguridad informática, inclusive cuando tiene 204 activos que debe salvaguardar, y en base a esto, no se ha condicionado un esquema de regularización referente a ello, tampoco cuenta con procedimientos acreditados para el resguardo de la información.

La metodología MAGERIT, se caracteriza por ser un método sistemático para determinar y examinar los riesgos que afectan de manera adversa algún tipo de daño que interfiere en la seguridad informática de los SI dentro de las instituciones de la administración pública, para la cual fue dirigida básicamente por sus impulsadores del Consejo Superior de Administración Electrónica de España, ya que MAGERIT implementa medidas de control que permitan tener lo riesgos controlados.

El modelo propuesto para la gestión de riesgos en la implementación y uso de las TI demostró su efectividad en 57 por ciento ante la mitigación de los incidentes que caracterizan el entorno tecnológico de la Municipalidad Distrital de Papayal.

Con la ejecución e implementación del modelo de gestión de riesgos propuesto se determinaron las principales amenazas y vulnerabilidades involucradas con los activos de la Municipalidad, donde los de mayor nivel sirvieron de base para formular las medidas de seguridad informática que ya han sido difundidas en el entorno de trabajo e instalaciones de la Institución, para tratar de manera directa las causas de los riesgos detectados con el diagnóstico, del análisis anterior.

La validación de la coherencia y correspondencia del modelo de gestión de riesgos presentado con enfoque a la metodología MAGERIT, resultó tener un contundente apego al cumplimiento de esta, evidenciándose un comportamiento Muy Bueno ante la apreciación de los expertos.

4.2. Recomendaciones

Fundamentados en la situación actual encontrada al momento de diagnosticar la institución, se exhorta a incluir internamente de los procedimientos operacionales y administrativos de la Municipalidad la evaluación y gestión de riesgos informáticos para incrementar la protección de la información, y disminuir el nivel de accidentes que perjudican la gestión mensual de distintos ámbitos de la organización, al igual que los activos a los activos informáticos más críticos.

Dado que la metodología MAGERIT se caracteriza por su flexibilidad, es importante día a día adecuar lo que se considere conveniente en pro de mejorar las buenas prácticas de uso de los activos, y en ese sentido, se exhorta realizar revisión periódica de los controles de seguridad establecidos para verificar su efectividad y su continua actualización.

Aun cuando el modelo de gestión trazado posee una técnica de evaluación de riesgos basados en un listado de registro de los tipos de riesgo que existen, es importante en la fase de apreciación del riesgo crear un sistema de incidencias que recoja las notificaciones continuas por parte de los usuarios y que permitan identificar las nuevas amenazas.

Tomando en cuenta la estrategia de aplicación del modelo de gestión de riesgo para la seguridad de información que se encuentra marcha, se recomienda la vigilancia constante de los peligros y riesgos encontrados, teniendo presente los diversos elementos que impactan en su incidencia, como lo son las modificaciones tecnológicas, ejecución de nuevas planeaciones, entre otras.

Aprovechando el alto nivel de validez del modelo de gestión de riesgos propuesto en esta investigación, se sugiere su total implementación para comprobar de forma práctica la total efectividad de las políticas de seguridad definidas.

REFERENCIAS

[1] J. Alvarado, J. Pacheco y I. Martillo, «El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT,» 2018. [En línea]. Available: https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html.

[2] V. Zeña, «Estándar Internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG,» 2015. [En línea]. Available: http://190.108.84.117/bitstream/handle/UNPRG/166/BC-TES-3899.pdf?sequence=1&isAllowed=y.

[3] A. Oliván, «Guía de Controles de Ciberseguridad para la Proteccion Integral de la Pyme,» 2017. [En línea]. Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73066/6/aolivan1TFM0118memoria.pdf.

[4] V. Granadino, «Conexion ESAN,» 2019. [En línea]. Available: https://www.esan.edu.pe/apuntes-empresariales/2019/02/el-plan-de-respuestas-a-los-riesgos-las-estrategias-y-acciones-clave/.

[5] Magerit, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» 2012. [En línea]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

[6] Agencia Española de Protección de Datos, «Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD,» 2018. [En línea]. Available: https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf.

[7] M. López, «Revista Especializada en Ingeniería (UNAD),» 2018. [En línea]. Available: http://polux.unipiloto.edu.co:8080/00004422.pdf.

[8] J. P. J. y. M. I. Alvarado, «El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT,» 2018. [En línea]. Available: https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html.

[9] S. Cuervo Alvarez, «Implementación ISO 27001,» 2017. [En línea]. Available: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/8/scuervoTFM0617memoria.pdf.

[10] Congreso de la República del Perú, *Ley de Protección de Datos Personales,* Lima: http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf, 2011.

[11] INDECOPI, «Norma Técnica Peruana “NTP-ISO/ IEC 27001:2014. Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requisitos. Segunda edición. Lima,Perú,» 2014. [En línea].

[12] ISO 27001, *Norma Técnica Peruana,* 2022.

[13] F. Arias, El Proyecto de la Investigación: Introducción a la Investigación Científica, Caracas - Venezuela: Epísteme, 2012.

[14] R. Hernandez Sampieri, C. Fernandez Collado y P. Baptista Lucio, «Metodología de la Investigación,» 24 05 2010. [En línea]. Available: https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf.

[15] H. Novoa y C. Rodríguez, «Methodologies for AnAlysis of risks in the isMs,» 2014. [En línea]. Available: DOI: 10.22490/25394088.1435. https://www.researchgate.net/publication/317149870_Metodologias_para_el_analisis_de_riesgos_en_los_sgsi.

[16] E. F. Alvarado Meza, «Propuesta para la implementación de un sistema de gestión de

6] seguridad de la información aplicando la normal ISO 27001 para industrial ALES (Tesis de Grado),» 07 06 2016. [En línea]. Available: http://repositorio.ug.edu.ec/bitstream/redug/19804/1/INFORME%20ERICK%20ALVARADO%20TESI.pdf.

[1 MAGERIT, «Metodología de Análisis y Gestión de Riesgos de los Sistemas de
7] Información,» 18 09 2012. [En línea]. Available: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html.

[1 Cisco, «Cómo fortifica el mercado de empresas medianas y pequeñas sus defensas
8] contra las amenazas actuales. Obtenido de Informe Especial de Ciberseguridad,» 2018. [En línea]. Available: https://www.cisco.com/c/dam/global/es_mx/products/pdfs/cisco-2018-smb-report-spa.pdf. [Último acceso: 18 Abril 2020].

[1 A. G. Alexander, Diseño de un sistema de seguridad de información, Colombia: Alfa
9] omega Colombiana S.A., 2007.

[2 H. Cabrera, «Diseño de un modelo de políticas basado en la norma ISO 27001, para
0] mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida,» 2018. [En línea]. Available: https://repositorio.upeu.edu.pe/handle/UPEU/1542.

[2 E. Ferruzola, J. Duchimaza y J. &. A. M. Ramos, «Plan de contingencia para los equipos
1] y sistemas informáticos utilizando la metodología MAGERIT,» *Revista Científica Y Tecnológica UPSE,* pp. 34-41, 2019.

[2 E. y. L. M. Morales, «Sistemas de gestión de seguridad de la información para empresas
2] KPO: una aproximación,» 2018. [En línea]. Available: DOI: 10.30554/ventanainform.37.2723.2017. https://www.researchgate.net/publication/333012746_Sistemas_de_gestion_de_seguridad_de_la_informacion_para_empresas_KPO_una_aproximacion.

[23] D. Gonzales, «Design of a strategic plan for information security, through the application of risk analysis with ISO / IEC 27005. Case study INAMHI,» 2018. [En línea]. Available: DOI: https://doi.org/10.33890/innova.v3.n2.1.2018.672. Disponible en: https://revistas.uide.edu.ec/index.php/innova/article/view/672.

[24] M. Corda, M. Viñas y M. Coria, «Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje,» 2017. [En línea]. Available: https://doi.org/10.24215/18539912e032.

[25] F. Arévalo, I. Cedillo y S. Moscoso, «Agile Methodology for Computer Risk Management,» 2017. [En línea]. Available: DOI: 10.26871/killkana_tecnica.v1i2.81. https://www.researchgate.net/publication/321176840_Metodologia_Agil_para_la_Gestion_de_Riesgos_Informaticos.

[26] M. Miranda, O. Valdés, I. Pérez, R. Portelles y R. Sánchez, «Methodology for the Implementation of Automated Management of Computer Security Controls,» 2016. [En línea]. Available: https://www.researchgate.net/publication/317514696_Metodologia_para_la_Implementacion_de_la_Gestion_Automatizada_de_Controles_de_Seguridad_Informatica.

[27] F. Solarte, E. Enriquez y M. Benavides, «Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001,» 2015. [En línea]. Available: https://doi.org/10.37815/rte. Disponible en: http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456.

[28] J. Monsalve, F. Aponte-Novoa y D. Chaves, «Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department,» 2014. [En línea]. Available: https://doi.org/10.19053/01211129.2791. En línea: https://revistas.uptc.edu.co/index.php/ingenieria/article/view/2791/4356.

[29] J. Figueroa, R. Rodríguez, C. Bone y J. Saltos, «La seguridad informática y la seguridad de la información,» 2017. [En línea]. Available: DOI: 10.23857/pc.v2i12.420. Disponible en: https://polodelconocimiento.com/ojs/index.php/es/article/view/420.

[30] Y. Bocanegra, «Análisis y gestión de riesgos de los sistemas de información de la Alcaldía Municipal De Tuluá aplicando la metodología MAGERIT,» 2015. [En línea]. Available: https://repository.unad.edu.co/handle/10596/3632.

ANEXO

Resolución de Ampliación de Plazo de Vigencia de Tema de Tesis

Universidad Señor de Sipán

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N° 0054-2023/FIAU-USS

Pimentel, 28 de enero de 2023
ANEXO

AMPLIACION DE VIGENCIA DE TEMA DE TESIS

	APELLIDOS	TESIS	OBSERVACION	RESOLUCION ANTERIOR	ESTADO
1	GONZALES GONZALES CHRISTIAN ERICK	ANÁLISIS COMPARATIVO DE PATRONES DE DISEÑO MVC Y MVP PARA EL RENDIMIENTO DE APLICACIONES WEB	**AMPLIAR HASTA EL 31 DE JULIO DEL 2023**	Resolución de ampliación anterior **0956-2021/FIAU-USS**	**APROBADO**
2	MOGOLLON GARCIA MANUEL ESTBAN	DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ	**AMPLIAR HASTA EL 31 DE JULIO DEL 2023**	Resolución de cambio de titulo 2322-2020/FIAU-USS	**APROBADO**

DR. VICTOR ALEXCI TUESTA MONTEZA
DECANO (E) FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
UNIVERSIDAD SEÑOR DE SIPÁN SAC.
CHICLAYO

DR. HALYN ALVAREZ VÁSQUEZ
SECRETARIO ACADÉMICO | FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
UNIVERSIDAD SEÑOR DE SIPÁN SAC.
CHICLAYO

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE

Cc: Interesado, Archivo

Anexo 1. Instrumentos de recolección de datos:

Formato de registros históricos de frecuencia de incidentes de SI

(a) Antes de la Puesta en marcha del modelo

Hallazgo	Ene	Feb	Mar	Abr	Ma	Jun	Jul	Ag	Sep	Oct	No	Dic

					y			**o**			**v**	

(b) Después de la puesta en marcha del modelo

Hallazgo	**Mar**	**Abr**	**May**

Anexo 2. Formato de ficha documentaria para el registro de características *de la metodología MAGERIT*

N°	Autor (es)	Caso de aplicación de MAGERIT	Buscador de obtención	Aspectos que resaltan en su caracterización

Anexo 3. Matriz de registro y observación

Anexo 3.1. Inventario de personal y equipos

MUNICIPALIDAD DISTRITAL DE PAPAYAL

CREADA POR LEY N° 9667 | 25.NOVIEMBRE.1942

GERENCIA MUNICIPAL / OFICINA DE ADMINISTRACIÓN Y RENTAS

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Nro. EI	Equipo Informático	Oficina / Unidad	Nro. Personal	Cargo	Apellidos	Nombres
1	LapTop	**Alcaldía**: una (01) laptop Dell, para uso del Alcalde.	1	Alcalde	COLLANTES MOGOLLÓN	WILSON ALFREDO
2	DeskTop	**Consejo Municipal**: un (01)	2	Regidora	CARRASCO MEDINA	MABERLY ERILSA

		equipo de computación desktop tipo genérico compatible. Una (01) impresora Epson, para 5 regidores.				
3	Impresora		3	Regidora	PÉREZ OYOLA	ZARELA JOSSELYN
			4	Regidor	SERNA ALVAREZ	JOSÉ
			5	Regidor	CISNEROS ZAPATA	DIKSON PAUL
			6	Regidor	OYOLA ROMERO	TONNY
4	LapTop	**Gerencia Municipal**: una (01) laptop Dell, para uso del Gerente. Un (01) equipo de computación desktop tipo	7	Gerente	PARDO NEUMANN	CÉSAR RICARDO HILARION

		genérico compatible, para la secretaria de gerencia. Una (01) impresora Epson y un (01) switch ZTE.				
5	DeskTop		8	Secretaria de Gerencia		
6	Impresora					
7	Switch					
8	LapTop	**Oficina de Asesoría Legal**: una (01) laptop Dell, para uso del jefe. Un (01) equipo de computación desktop tipo genérico compatible , para los 10 asistentes tecnico legal. Una (01) impresora Epson y un (01) switch ZTE.	9	Jefe	VALLADARES MEDINA	JOSÉ AUGUSTO

9	DeskTop		10	Asistente Técnico Legal		
10	Impresora					
11	Switch					
12	DeskTop	**Oficina de Planificación y Presupuesto**: Un (01) equipo de computación desktop tipo genérico compatible para el jefe. Dos (02) laptop Dell, para usodel Asistente Técnico Contable y el Asistente Técnico en Inversiones. Dos (02) impresoras Epson y un (01) switch ZTE.	11	Jefe	BELLO PURIZACA	CARLOS JACKDIEL
13	LapTop		12	Asistente Técnico Contable		
14	LapTop		13	Asistente Técnico en Inversiones		

15	Impresora					
16	Impresora					
17	Switch					
18	LapTop	**Oficina de Programación Multianual de Inversiones**: una (01) laptop Dell, para uso del jefe.	14	Jefe	DEL ROSARIO FACHIN	YANET
19	LapTop	**Unidad Formuladora**: una (01) laptop Dell, para uso del jefe. **Una impresora Epson.**	15	Jefe	MIÑANO GUERRERO	INDIRA LEONOR
20	Impresora					
21	DeskTop	**Especialista en Inversiones**: Un (01) equipo de computación desktop tipo genérico compatible, para el jefe. Un (01) switch ZTE.	16	Jefe	RIVERA ESPINOZA	ALEJANDRO

22	Switch					
23	DeskTop	**Oficina de Secretaría General**: Un (01) equipo de computación desktop tipo genérico compatible, para el jefe, y dos (02) asistentes administrativos. Una (01) impresora Epson. Un (01) escaner Hp.	17	Jefe	GARCÍA OYOLA	CELINDA YUDITH
24	Impresora		18	Asistente Administrativo		
25	Escaner		19	Asistente Administrativo		
26	DeskTop	**Unidad de Relaciones Públicas e Imagen Institucional**: Un (01) equipo de computación	20	Responsable	INFANTE ALAMA	JUAN ALBERTO

		desktop tipo genérico compatible, para el responsable. Una (01) impresora Epson. Un (01) proyector multimedia Hp.				
27	Impresora					
28	Proyector Multimedia					
29	DeskTop	**Unidad de Abastecimiento Logística y Control Patrimonial**: Un (01) equipo de computación desktop tipo genérico compatible, para el jefe y el asistente administrativo. Un (01) equipo de	21	Jefe	CARRASCO CHICA	MAGNO PASCUAL

		computación desktop tipo genérico compatible, para el especialista en contrataciones y el astentes administrativo. Una (01) impresora Epson. Un (01) swith ZTE.				
30	Impresora		22	Asistente Administrativo		
31	Switch		23	Asistente Administrativo		
32	DeskTop		24	Especialista en Contrataciones		
33	Impresora					
34	DeskTop	Almacén - Unidad de Abastecimiento Logística y Control Patrimonial	25	Jefe	LOAYZA CRUZ	ROBERTO CARLOS
35	Impresora					

36	DeskTop	Unidad de Tesorería	26	Jefe	ROMERO ESPINOZA	LEWIS EDIL
37	Impresora		27	Asistente Técnico y Administrativo		
38	Switch					
39	DeskTop	Unidad de Rentas	28	Jefe	CHICA ARICA	MARITZA
40	Impresora		29	Asistente Técnico Administrativo		
41	DeskTop	Unidad de Recursos Humanos y Bienestar Social	30	Jefe	MARCHÁN ROSILLO	JOSEFINA
42	Impresora					
43	LapTop	Oficina de Desarrollo Urbano e Infraestructura	31	Jefe	FLORES NÚÑEZ	MARTÍN ANSELMO
44	Impresora		32	Asistente Técnico Ingeniería Civil		
45	DeskTop		33	Secretaria de ODUeI		

46	Plotter		34	Asistente Ténico Administrativo		
47	Switch					
48	DeskTop					
49	Impresora					
50	DeskTop	Unidad de Maquinaria y Maestranza	35	Responsable	QUIÑONES ZAPATA	LUIS ABEL
51	Impresora					
52	DeskTop	Oficina de Desarrollo Social y Servicios Públicos	36	Jefe	DEL ROSARIO CARRASCO	ROSA ANNEL
53	Impresora					
54	LapTop	Unidad de Salud, Limpieza, Ornato, Medio Ambiente-Ecología, Parques-Jardines, Control de	37	Jefe	GARCÍA NÚÑEZ	GERCY PAUL

		Cementerio y Estadio, y ATMSR - Área Técnica Municipal de Saneamiento Rural.				
55	Impresora		38	Asistente Técnico Ambiental		
56	DeskTop	Unidad de SISFOH, Complementación Alimentaria, PVL y Comercialización	39	Jefe	ELIZALDE ATOCHE	CARLOS ULISES
57	Impresora					
58	Switch					
59	DeskTop	Programa de Vaso de Leche y Complementación Alimentaria	40	Jefe	CHÁVEZ OLAYA	MÓNICA MARISOL
60	Impresora					

61	DeskTop	DEMUNA - Defensoría de la Municipal del Niño y del Adolescente	41	Jefe	DIOSES RUJEL	DELMIS DALY
62	Impresora		42	Psicologa		
63	DeskTop	OMAPED - Oficina Municipal de Atención a la Persona con Discapacidad	43	Jefe	LÓPEZ GARCÍA	LORENZO
64	Impresora		44	Asistente Administrativo		
65	DeskTop	Seguridad Ciudadana	45	Jefe	ARICA LAVALLE	JUAN
66	Impresora		46	Asistente Administrativo		
67	DVR - Digital Video Recorder		47	Chofer		
68	Cámara de Video Vigilancia					
69	Cámara de Video Vigilancia					
70	Cámara de Video Vigilancia					
71	DeskTop	Defensa Civil	48	Jefe	MEDINA LOAYZA	CELINA YSABEL
72	Impresora					

73	DeskTop	Oficina de Registro Civil	49	Jefa	GARCÍA PURIZAGA	GLORIA
74	Fotocopiadora		50	Asistente Administrativo	CRUZ ZAPATA	JUAN
75	Impresora					
76	Server	Unidad de Tecnologías de la Información	51	Responsable	MOGOLLÓN GARCÍA	MANUEL ESTEBAN
77	Server					
78	Switch					
79	Router					
80	Antena					

Anexo 3.2. Inventario de Software

MUNICIPALIDAD DISTRITAL DE PAPAYAL

CREADA POR LEY N° 9667 | 25.NOVIEMBRE.1942

GERENCIA MUNICIPAL / OFICINA DE ADMINISTRACIÓN Y RENTAS

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Nro. Software	Software	Oficina / Unidad
1	Sistema Operativo: Microsoft Windows 10 Professiona1	Todas
2	Sistema Operativo: Microsoft Windows 8.1 Professional	

3	Sistema Operativo: Microsoft Windows 7 Professional	
4	Navegador web: Microsoft Edge	
5	Navegador web: Google Chrome	
6	Navegador web: Mozila FireFox	
7	Antivirus: ESET EndPoint Protection Standard	
8	Ofimática: Microsoft Office 2013 Standard	
9	Compresor de Carpetas y Archivos: WinRAR	
10	Asistencia Remota: AnyDesk	
11	Lector de PDF: Adobe Reader DC	
12	Web: Aplicativos de Contraloría General de la República	
13	Sistema Integrado de Administración Financiera del Sector Público - Gobiernos Locales (SIAF) (Usado en GP, OAR, OPP, UAL, UC, UT)	Gerencia Municipal / Oficina de Administración de Rentas
		Oficina de Planificación y Presupuesto
		Unidad de Abastecimiento, Logística y Control Patrimonial
		Unidad de Contabilidad

		Unidad de Tesorería
14	Web: SUNAT - Operaciones en Línea (Usado en UC, UT)	Unidad de Contabilidad
		Unidad de Tesorería
15	Sistema Integrado de Gestión Administrativa - Control Patrimonial (SIGA) (Usado en UAL, AL)	Unidad de Abastecimiento, Logística y Control Patrimonial
		Almacén
16	Software de Abastecimiento (Usado en UAL, AL)	Unidad de Abastecimiento, Logística y Control Patrimonial
		Almacén
17	Web: Sistema Electrónico de Contrataciones del Estado (Usado en UAL, EC)	Unidad de Abastecimiento, Logística y Control Patrimonial
		Especialista de Contrataciones
18	Web: Perú Compras (Usado en UAL)	Unidad de Abastecimiento, Logística y Control Patrimonial

19	Web: Registro Nacional de Proveedores (Usado en UAL)	
20	Software de Control de Predios (Usado en UR)	Unidad de Rentas
21	Web: Sistema de Focalización de Hogares (Usado en UUS)	Unidad de ULE y SISFOH
22	Software de Control de Beneficiarios (Usado en PVL)	Programa de Vaso de Leche y Complementación Alimentaria
23	Web: Sistema de Registro Nacional de Identificación y Estado Civil (Usado en ORC)	Oficina de Registro Civil
24	Web: Módulo de Programación Multianual de Inversiones (Usado en OPMI)	Oficina de Programación Multianual de Inversiones
25	Web: Banco de Proyectos de Inversión Pública (Usado en UF, ODU, OPMI)	Unidad Formuladora
		Oficina de Desarrollo Urbano e Infraestructura
		Oficina de Programación Multianual de Inversiones
26	Web: Sistema Nacional de Información de	Especialista en

	Obras Públicas (Usado en EI)	Inversiones
27	Web: Módulo de Registro de Ejecución de Metas de Obras Públicas (Usado en EI)	
28	Adobe PhotoShop (Usado en URP)	Unidad de Relaciones Públicas e Imagen Institucional
29	Corel Draw (Usado en URP)	
30	Sony Vegas (Usado en URP)	
31	SUNAT - Programa de Declaración Telemática (Usado en URH)	Unidad de Recursos Humanos y Bienestar Social
32	AutoCAD 2019 (Usado en ODU)	Oficina de Desarrollo Urbano e Infraestructura
33	Windows Server 2012 R2 Standard (Usado en UTI)	Unidad de Tecnologías de la Información
34	SQL Server 2008 Express (Usado en UTI)	
35	Web: Panel de Control de Hosting y Dominio Institucional (Usado en UTI)	

Anexo 3.3. Inventario de infraestructura

MUNICIPALIDAD DISTRITAL DE PAPAYAL
CREADA POR LEY N° 9667 | 25.NOVIEMBRE.1942
GERENCIA MUNICIPAL / OFICINA DE ADMINISTRACIÓN Y RENTAS
UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Nro. Infraestructura	Infraestructura
1	Edificio de 02 Pisos
2	Cableado Estructurado de Par Trenzado Categoría 5e
3	Cableado Estructurado de Par Trenzado Categoría 6
4	Oficina de Tecnologías de la Información

Anexo 4. Formato de plantillas de análisis y evaluación

Anexo 4.1. Formato de valoración de activos de acuerdo a la herramienta R-Box

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Personas (P)								
Personas (P)								
Instalaciones (L)								
Instalaciones (L)								
Instalaciones (L)								
Equipos Informáticos (HW)								
Equipos Informáticos (HW)								
Equipos Informáticos (HW)								

Equipos Informáticos (HW)								
Software y aplicaciones								
Software y aplicaciones								
Software y aplicaciones								
Software y aplicaciones								
Software y aplicaciones								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Redes de comunicaciones (COM)								

Redes de comunicaciones (COM)								

Anexo 4.2. Formato de valoración de amenazas y vulnerabilidades en activos de acuerdo a la herramienta R-Box

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
P1										
P2										
P3										
P4										
L1										
L2										
L3										
L4										

HW1										
HW2										
HW3										
HW4										
SW1										
SW2										
SW3										
S1										
S3										
S4										
COM1										
COM2										
COM3										

COM4										

Anexo 5. Formato Checklist para el diagnóstico de salvaguardas presentes en la seguridad informática de la Municipalidad

N°	ÍTEMS QUE EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
1.	Seguridad Física						
1.1.	Instalaciones de la UTI protegidas de acceso no autorizado.						
1.2.	Tipos de controles físicos aplican para la UTI:						
	a) Contorno de seguridad bien delimitado						
	b) Mecanismos para detectar intrusos						
	c) Puertas con mecanismos seguros de entrada						
	d) Carnet de Identificación						
	e) Registro de visitantes						
1.3.	La UTI cuenta con condiciones físicas adecuadas de acuerdo con normas definidas de por EIA/TIA, de a acuerdo a:						
	a) Paredes						
	b) Piso						
	c) Techo						
	c) Climatización						
	d) Iluminación						
1.4.	Mecanismos contra incendios utilizados:						
	a) Avisos alarmantes						

N°	ÍTEMS QUE EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
	b) Extinguidores						
	c) Sistema contra incendios						
1.5.	El cableado de la red de comunicación está esquematizado de acuerdo a los estándares internacionales vigentes.						
1.7.	Está sustentado el diseño de la red institucional.						
1.8.	Existen medidas de control que estructuren los pasos para el mantenimiento preventivo y correctivo de los equipos de la UTI.						
1.9.	Cuentan con suficiente personal para la gestión de mantenimiento a equipos informáticos.						
1.10.	Tienen controles para llevar a cabo el mantenimiento de equipos informáticos en todas las instalaciones de la Municipalidad.						
1.11.	Cuentan con equipos de auxiliares para proveer energía eléctrica.						
2.	**Red**						
2.1.	Se tiene definido quienes pueden compartir información mediante la red y la manera de hacerlo.						
2.2.	Documentan y actualizan a nivel de red						

N°	ÍTEMS QUE EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
	sus inventarios tanto lógicos como físicos.						
2.3.	Se registran las incidencias de fallas que se suscitan en la red.						
2.4.	Cuentan con mecanismos de entrada a la intranet institucional.						
2.5.	Cuentan con mecanismos firewall para el aseguramiento y protección de redes.						
3.	**Software**						
3.1.	Los equipos laptops y desktops, así como server tienen Antivirus en constante estado de actualización.						
3.2.	Los softwares dispuestos en el servidor de BD están en constante estado de actualización.						
3.3.	Se implementa la monitorización continua del rendimiento de servidores, y la entrada a los mismos.						
3.4.	Se garantiza la seguridad de la información clave manejada en los equipos mediante su respaldo antes de formateo de estos.						
3.5.	La información que transita por la red interna se encuentra en estatus de encriptación.						

N°	ÍTEMS QUE EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
4.	**Organización**						
4.1	Tienen política general de seguridad informática						
4.2.	Tienen un departamento o dependencia que se dedique a la administración de la red y los servicios de TI						
4.3.	El número de personas que constituyen actualmente la UTI son suficientes para controlar los diferentes procesos de TI						
4.4.	Tienen plan de formación y desarrollo para empleados de la UTI en aspectos relacionados con las TIC, gestión de riesgos y procesos de certificación						
4.5.	Aplican análisis y evaluación de riesgos informáticos						
4.6.	Conocen los riesgos de seguridad informática que amenazan los activos de la Institución, así como la vulnerabilidad ante estas.						
4.7.	Poseen lineamientos para la gestión de riesgos de seguridad informática						
4.8.	Existen políticas de seguridad actualizadas.						
4.9.	Las políticas de seguridad están						

N°	ÍTEMS QUE EVALUAR	NIVEL DE EFICACIA					
		0%	25%	50%	75%	100%	Total
	debidamente socializadas con el personal de la Municipalidad.						

Anexo 6. Documentación Formal utilizada para el juicio de Expertos

5.1. Cartas de solicitud a Expertos para la validación del modelo propuesto para la gestión de riegos de SI

EXPERTO 1

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Solicitud de apoyo para revisión, análisis y validación de un modelo propuesto para la gestión de riegos de SI en la Municipalidad Distrital de Papayal

Señora: Joisy Del Valle Rojas Rojas

Experto en: Auditoría y Seguridad de Sistemas de información

Distinguido Profesional: Ingeniero en Sistemas

Yo, **Manuel Esteban Mogollon Garcia** identificado con **DNI Nº 00252937**, estudiante del **X ciclo de Ingeniería de Sistemas** de la Universidad "Señor de Sipán" en Chiclayo, ante Ud. Con el debido respeto me presento y expongo:

Que estando realizando el trabajo de investigación titulado: "**DESARROLLO DE UN**

MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ", siendo una de las herramientas de evaluación del mismo un test para: **la validación del modelo propuesto para la gestión de riegos de SI**, destacando su experiencia profesional en este campo, es que recurro a su honorable persona para solicitarle su valiosa colaboración consistente en la revisión, análisis y validación de los ítems propuestos en el test anexo cuyo objetivo es: **analizar la coherencia y correspondencia del modelo propuesto con los fundamentos de la metodología MAGERIT**.

Sus observaciones y recomendaciones como juez de validación serán de gran ayuda para la elaboración final del modelo de gestión de SI, agradeciéndole de antemano.

Esperando la debida atención a la presente, me despido de Ud.

Chiclayo, 20 días de Noviembre de 2020

_____

Manuel Esteban Mogollón García

DNI N°: 00252937

Estudiante de Ingeniería de Sistemas

EXPERTO 2

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Solicitud de apoyo para revisión, análisis y validación de un modelo propuesto para la gestión de riegos de SI en la Municipalidad Distrital de Papayal

Señor: Nelson Ángeles Quiñones

Experto en: Seguridad de la Información

Distinguido Profesional: Ingeniero en Sistemas

Yo, **Manuel Esteban Mogolloón Garcia** identificado con **DNI Nº 00252937**, estudiante del **X ciclo de Ingeniería de Sistemas** de la Universidad "Señor de Sipán" en Chiclayo, ante Ud. Con el debido respeto me presento y expongo:

Que estando realizando el trabajo de investigación titulado: "**DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ**", siendo una de las herramientas de evaluación del mismo un test para: **la validación del modelo propuesto para la gestión de riegos de SI**, destacando su experiencia profesional en este campo, es que recurro a su honorable persona para solicitarle su valiosa colaboración consistente en la revisión, análisis y validación de los ítems propuestos en el test anexo cuyo objetivo es: **analizar la coherencia y correspondencia del modelo propuesto con los fundamentos de la metodología MAGERIT**.

Sus observaciones y recomendaciones como juez de validación serán de gran ayuda para la elaboración final del modelo de gestión de SI, agradeciéndole de antemano.

Esperando la debida atención a la presente, me despido de Ud.

Chiclayo, 20 días de Noviembre de 2020

_____

Manuel Esteban Mogollón García

DNI N°: 00252937

Estudiante de Ingeniería de Sistemas

EXPERTO 3

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Solicitud de apoyo para revisión, análisis y validación de un modelo propuesto para la gestión de riegos de SI en la Municipalidad Distrital de Papayal

Señor (a): Luis Vicente Castillo Boggio

Experto en: Administración de Tecnologías de la Información

Distinguido Profesional: Ingeniero de Sistemas

Yo, **Manuel Esteban Mogollón García** identificado con **DNI Nº 00252937**, estudiante del **X ciclo de Ingeniería de Sistemas** de la Universidad "Señor de Sipán" en Chiclayo, ante Ud. Con el debido respeto me presento y expongo:

Que estando realizando el trabajo de investigación titulado: "**DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ**", siendo una de las herramientas de evaluación del mismo un test para: **la validación del modelo propuesto para la gestión de riegos de SI**, destacando su experiencia profesional en este campo, es que recurro a su honorable persona para solicitarle su valiosa colaboración consistente en la revisión, análisis y validación de los ítems propuestos en el test anexo cuyo objetivo es: **analizar la coherencia y correspondencia del modelo propuesto con los fundamentos de la metodología MAGERIT**.

Sus observaciones y recomendaciones como juez de validación serán de gran ayuda para la elaboración final del modelo de gestión de SI, agradeciéndole de antemano.

Esperando la debida atención a la presente, me despido de Ud.

Chiclayo, 20 días de Noviembre de 2020

_____

Manuel Esteban Mogollón García

DNI N°: 00252937

5.2. Resumen del Enfoque de la Metodología MAGERIT y Exposición del Modelo de Gestión de Riesgos de SI propuesto

Fundamento que Sustenta el Estudio

MAGERIT como metodología de seguridad informática

MAGERIT, por ahora en su versión 3, es una metodología propuesta por el Consejo Superior de Administración Electrónica para el análisis y gestión de riesgos de los Sistemas de Información a los fines de minimizarlos cuando se implantan en las Administraciones Públicas [1].

López [7], agrega que es una metodología sencilla de utilizar, y por lo tanto no necesita de especialización en conocimientos para aplicarla; en función de ello puede ser aplicada por una o dos personas, pertenecientes al ente gubernamental, ya sea grande o pequeño su factor humano.

Al estar alineada MAGERIT al mencionado contexto, es decir: (a) por ser diseñada explícitamente para ser aplicadas en instituciones del gobierno a disposición de un servicio público como lo es la Municipalidad Distrital de Papayal, (b) catalogada como una organización pequeña al contar solo con 51 funcionarios, y (c) con muy reducido personal en el área de TI (sólo una persona y un colaborador en ocasiones) para llevar a cabo el análisis

y gestión del riesgo, en este informe de investigación se pretende poner en práctica dicha metodología ya que los aspectos detallados se identifican con los criterios de selección para ser aplicada en dicha institución. Siendo así, se destacan a continuación los aspectos que más resaltan de la metodología MAGERIT, aplicada al proceso de gestión del riesgo en los sistemas de información, en cuanto a la identificación, evaluación y tratamiento.

Principales características de MAGERIT

Ante esto, Alvarado [8] dice que entre las bondades que ofrece la Metodología MAGERIT es que está en Español, aunque se coloca en primera instancia el conjunto de procedimientos metódicos y continuos para valorar y medir los riesgos a los que se ven expuestos las TIC, de manera de poder enfocar controles óptimos que sean eficientes en lo que a gestión de seguridad se refiere, identificando amenazas latentes en la organización ante las cuales se puedan adecuar las medidas preventivas y correctivas más eficaces.

Objetivos de MAGERIT

La Metodología MAGERIT tiene como objetivos sensibilizar a los miembros de la organización a que se adecuen a los riesgos y amenazas existentes, y que a su vez, estos sepan afrontarlos, así como poner a la orden un instrumento de trabajo que les permita analizar los riesgos que se desprenden de las TIC. Esto permitirá llevar a cabo planes y tratamiento en el momento requerido para controlar el índice de riesgos.

Elementos considerados en MAGERIT

Cuervo Álvarez [9], señala que la metodología MAGERIT toma los siguientes elementos para llevar a cabo la seguridad de la información:

Activos: es el componente central que resguardar, y están representados por los diferentes recursos que integran una entidad y forman parte de su sistema de información. Son el todo poblacional, en el contexto de estudio.

Amenazas al activo: son los peligros en los que se ven inmersos los activos de la organización, ante alguna eventualidad. Al materializarse se incurre en daños tangibles e intangibles de algún activo institucional.

Vulnerabilidad del activo: es la probabilidad de que se lleve a cabo o se concrete una amenaza sobre un activo.

Impacto de un activo: es la consecuencia de que se concrete una amenaza sobre un activo.

Fases de la gestión de riesgos bajo la metodología MAGERIT

De acuerdo con Cuervo Álvarez [9], la metodología se amolda al siguiente esquema en dos (02) subprocesos bases:

c. **Análisis de Riesgos**: se aproxima metódicamente a establecer el riesgo presente, tal como se señala a continuación:

- Identificación de activos a proteger.
- Valoración de los activos.
- Identificación de amenazas a las que se encuentran expuestos estos activos.
- Cálculo de Impacto bajo la cuantificación del daño que puede sufrir sobre un activo ante algún evento subestándar. Este se estima mediante la ecuación:

$$Impacto = Valor\ del\ activo\ x\ Porcentaje\ de\ Impacto$$

- Cálculo del riesgo ante el impacto potencial considerando la frecuencia en que se puede dar.

$$Riesgo = Frecuencia\ x\ Impacto$$

- Selección adecuada del tratamiento de los riesgos identificados a través de acciones pertinentes.

- Reducción del riesgo y riesgo residual ya que al reducirse cierta cantidad de riesgos, se disminuye su margen inicial, el cual se denomina riesgo residual.

- Estimar el riesgo, definido como el impacto por probabilidad.

Cabe destacar, que los criterios de valoración de los activos, amenazas, vulnerabilidades y los riesgos, son Bajo cuando es igual a 1, Medio cuando es igual a 2 y Alto cuando es igual a 3.

d. **Tratamiento de riesgos**: donde se planifica y programa los controles ante los incidentes de inseguridad, y así garantizar la continuidad de las operaciones.

La aplicación, ofrece las funciones:

a. R-Box: herramienta para analizar y evaluar riesgo bajo el marco de la metodología MAGERIT.

b. GxSGSI: herramienta para gestionar el desempeño del riesgo en función de la metodología MAGERIT.

Tal como se observa, MAGERIT se caracteriza por ser un instrumento para facilitar la implantación y aplicación del Esquema de Seguridad.

Modelo de gestión de riesgos basado en MAGERIT

Cuervo Alvarez [9], comenta que su Sistema de Gestión de Riesgos (SGR) se basa en vinculación con la norma ISO 27001, y contienen:

Tabla 1

Contenido del Sistema de Gestión Bajo Metodología MAGERIT

Dominio	Descripción
Definición de la política de seguridad	Abarca los objetivos, el marco general, los requerimientos legales, los criterios de evaluación de riesgos.
Definición del alcance del SGR	Delimita hasta dónde llega el plan de acción dentro de la organización considerando los activos, las TI, con sus respectivas descripciones.
Identificación de los riesgos	Describe las amenazas a las que están expuestos los activos de la organización, los responsables directos, a qué son vulnerables y el impacto en los activos en caso de que se vea afectada su confidencialidad, integridad y disponibilidad.
Análisis y evaluación de los riesgos	Corresponde a estimar el impacto de algunos de los riesgos si se llega a materializar. Se percibe allí la probabilidad de ocurrencia y cómo esto afectaría los controles implementados.
Tratamiento de riesgos	Se sugieren o aplican aquí los controles necesarios, de acuerdo con los riesgos identificados. También se clasifican los niveles de riesgo.
Políticas de Gestión para la seguridad en TI	Se define el tratamiento de los riesgos, vinculados a los controles, y ante esto se diseñan los indicadores para medir la eficiencia y eficacia de la gestión. Igualmente se

	plantea el plan de comunicación del SGR para promover la concientización y fomentar una cultura organizacional sobre el cumplimiento de este.
Monitoreo	Se lleva a cabo el diseño de estrategia de verificación y revisión periódica del SGR a través de la formulación de indicadores de gestión para determinar hasta qué nivel se está cumpliendo con la normativa.

Fuente: Cuervo Álvarez (2017)

Una vez concretado el análisis y evaluación de riesgos, será necesario desarrollar un sistema de gestión para garantizar la seguridad de la información, aplicando el esquema de elaboración del modelo de gestión planteado por MAGERIT, y con ello conllevar a la institución de administración pública a minimizar los riesgos a los cuales están expuestos todos sus activos.

Diseño del Modelo Propuesto

El modelo está estructurado, como se presenta en la figura 7, comprendido de cuatro fases señaladas a continuación:

Fase I: Apreciación del riesgo.

Fase II: Análisis de riesgos.

Fase III: Evaluación de riesgos.

Fase IV: Gestión de riesgos.

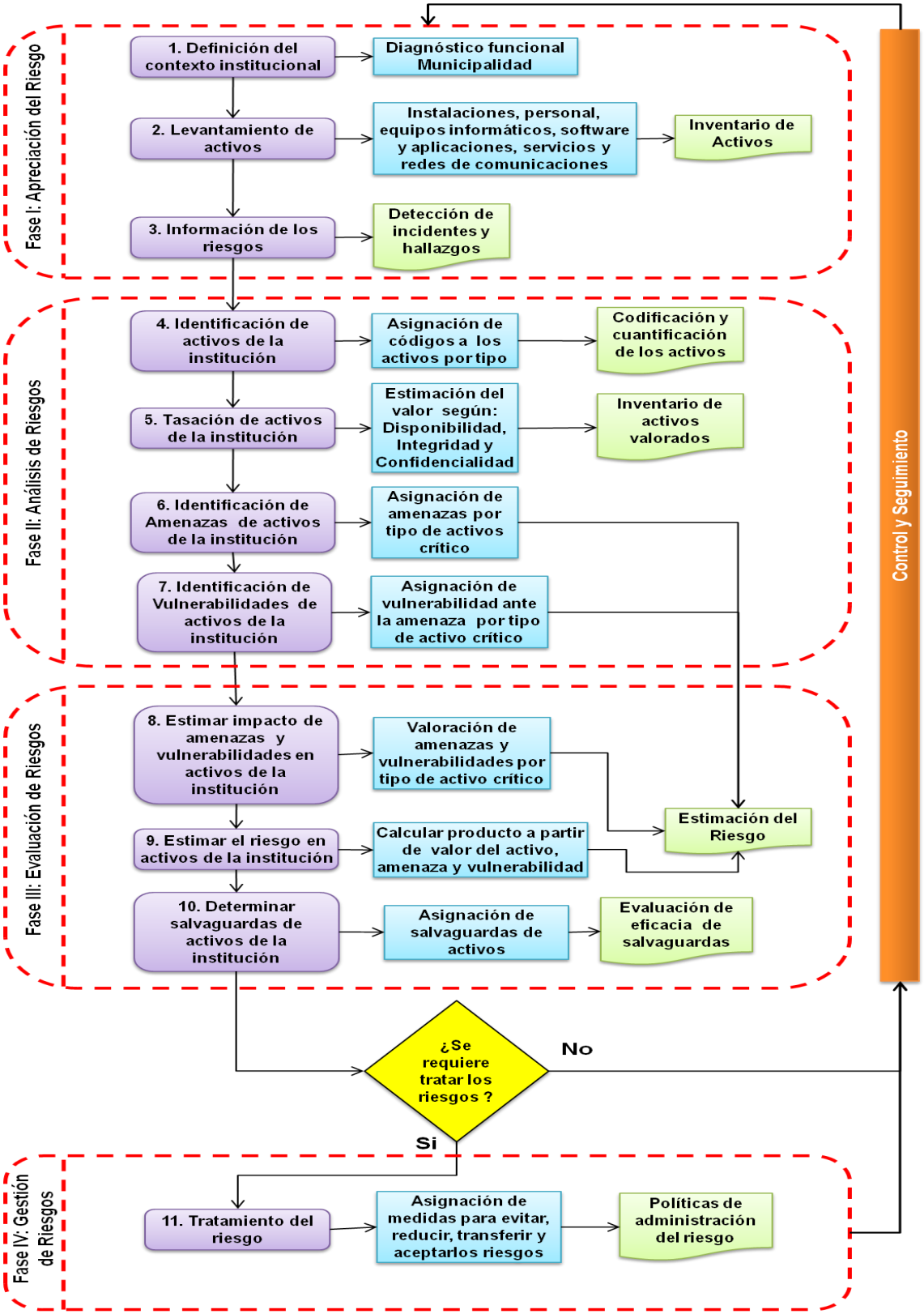


Figura 7. Modelo diseñado para la gestión de riesgos en la Municipalidad Distrital de Papayal basado en la metodología MAGERIT

Descripción del Modelo Propuesto

El modelo que se propone en este trabajo de investigación está basado en los parámetros estipulados en la metodología MAGERIT, así como en las normas 2701:2013 que insta a analizar, evaluar y tratar los riesgos para reducir su nivel de potencial. A continuación se describen las fases que lo conforman de acuerdo con lo expuesto en la figura 4.

Fase I. Apreciación del riesgo: se lleva a cabo en esta fase el estudio preliminar del escenario de trabajo, ya previamente dado a conocer en las primeras secciones de esta investigación. El cual contempló:

1. *Definición del contexto institucional*: este aspecto, proviene del diagnóstico de la situación actual de la Municipalidad Distrital de Papayal, donde se dio a conocer su razón social y su función básica de gestión operativa y administrativa, con el fin de conocer su relación con los activos que posee como base de apoyo a sus actividades.

2. *Levantamiento de activos*: en este paso, mediante la técnica de observación directa se llevó a cabo mediante una matriz de doble entrada, cuáles son los activos con los que cuenta la Municipalidad Distrital de Papayal, organizándose ante esto un inventario contentivo de los activos que posee la institución, ya expuestos en la tabla 3, contentivo de las instalaciones, personal y equipos informáticos adscritos a estas, software y aplicaciones que posee cada instalación, servicios y redes de comunicaciones que están a disposición para toda la organización.

3. *Información de los riesgos*: durante este proceso, se obtuvo información documental de los registros históricos de la UTI de la Municipalidad Distrital de Papayal resultante de su gestión operativa, acerca de los incidentes y hallazgos que ocurrieron en el año anterior con respecto la seguridad informática, detectándose los riesgos potenciales que caracterizan los procesos operativos y administrativos de la institución.

Fase II. Análisis de riesgos: mediante esta fase se persigue conocer los riesgos y las causas que podrían generar una situación crítica para los activos, ante las amenazas y vulnerabilidades.

4. *Identificación de activos de la institución*: durante esta actividad se llevó a cabo el proceso de denominar según las siglas estandarizadas por de MAGERIT en la tabla 6, los activos que posee la Municipalidad Distrital de Papayal, lo cual permitió clasificarlos por tipo y a codificarlos.

5. *Tasación de activos de la institución*: en esta actividad el personal de gerencia y jefaturas de la Municipalidad definió en términos de *Disponibilidad* (D), *Integridad* (I) y *Confidencialidad* (C), cuáles son los activos críticos (de alto riesgo) para ellos y la organización, y que pueden verse afectados en caso de que se produzca un impacto negativo en su continuidad del proceso productivo donde interviene. Cabe destacar, que de antemano el personal entrevistado decidió clasificar como activos críticos solo los pertenecientes a equipos informáticos, software y aplicaciones, servicios y redes de comunicaciones tal como lo indica que se puede hacer la metodología MAGERIT. Aspectos considerados para valorar su importancia de parte del personal:

   (HW) Hardware: o bienes materiales de tipo físicos destinados a dan soporte a los servicios que presta la organización, sin estos no ocurre el procesamiento de los datos.

   (SW) Software y aplicaciones: gestionan de forma automatizada las actividades funcionales mediante un equipo informático, que en conjunto actúan en el procesamiento de la información para emitir resultados en la prestación de los servicios.

   (S) Servicios: la asistencia ante la gestión de información y el procesamiento de datos son la clave de avance de la institución para prestar de manera continua sus servicios.

(COM) Redes de comunicaciones: Se consideran dispositivos físicos que permiten la transmisión de la información clave dentro de toda la extensión de la institución.

La valoración del activo se realiza como sigue en la figura 8, con un ejemplo:

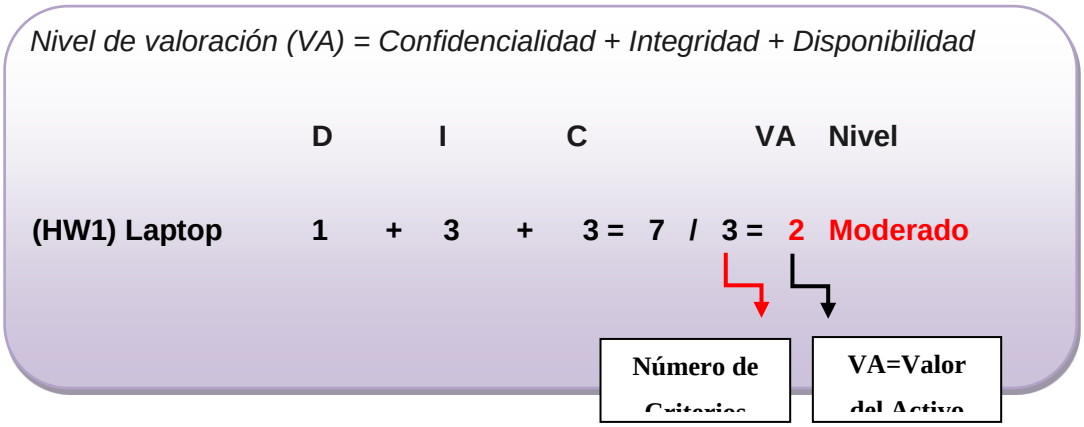


Figura 8. Ejemplo de valoración del activo

6. *Identificación de amenazas de activos de la institución*: en este paso, se generó una lista de riesgos característicos que representan una amenaza para los procesos organizacionales de la Municipalidad Distrital de Papayal, y que coinciden con las ya suscitados en el año 2019, ya que han sido concurrentes durante los últimos años. Se designaron aquí las amenazas que caracterizan cada tipo de activo crítico o de alto riego.

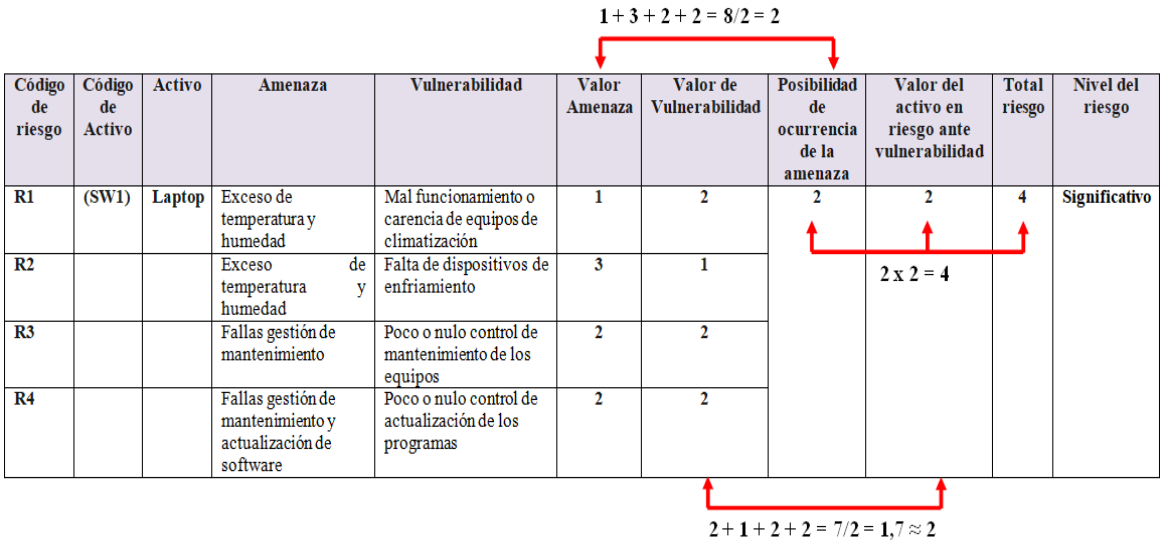
7. *Identificación de vulnerabilidades de activos de la institución*: ente paso, dado un crítico, se le asigna las diferentes vulnerabilidades ante cualquier situación que pueda desembocar en un problema de seguridad. Esta va en consonancia con la amenaza de cada tipo de activo crítico.

Fase III. Evaluación de riesgos. En esta fase se llevó a cabo la evaluación cuantitativa del riesgo, indicando las medidas para su posterior tratamiento.

8. *Estimación del impacto de amenazas y vulnerabilidades en activos de la institución*: mediante este paso se midió el efecto adverso vinculado a cada activo crítico en caso de que se concrete un riesgo. Se llevó aquí la sumatoria de las vulnerabilidades y se promediaron para conocer el impacto.

9. *Estimación del riesgo en activos de la institución*: En este paso se llevó a cabo la multiplicación de valor de activo por el valor de la amenaza y vulnerabilidad. De esta forma se obtiene el nivel de riesgo de cada activo con respecto a una amenaza.

Ante esto, se coloca un ejemplo para calcular el nivel de riesgo del activo en la figura 9:



Código de riesgo	Código de Activo	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor de Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo
R1	(SW1)	Laptop	Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	1	2	2	2	4	Significativo
R2			Exceso de temperatura y humedad	Falta de dispositivos de enfriamiento	3	1				
R3			Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2				
R4			Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2				

Figura 9. Ejemplo de valoración del riesgo del activo

10. *Determinación de salvaguardas de activos de la institución*: Esta actividad busca identificar las salvaguardas desplegadas en los activos de la Municipalidad, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

    En caso de que no se requiera tratar los riesgos: se hace un seguimiento de continuo de los mismos.

    En caso de que si se requiera tratar los riesgos:

Fase IV: Gestión de riesgos: Esta fase se delimitan los lineamientos para administrar los riesgos detectados de acuerdo con su importancia y valoración, a partir de medidas adecuadas que garanticen su control y fluidez en los procesos organizacionales.

11. *Tratamiento del riesgo*: en este paso se determina la acción para tratar el riesgo en función de evitar, reducir, transferir y aceptar los riesgos. Asimismo, posteriormente se emiten las políticas de administración del riesgo.

12. *Control y seguimiento*: generar indicadores de gestión que permitan medir la efectividad del cumplimiento de políticas de seguridad.

5.3. Lista de Chequeo para la validación de expertos del Modelo Propuesto

EXPERTO 1

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de la metodología MAGERIT

Dirigido a:

Expertos en SI

Esta checklist a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de la metodología MAGERIT, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de ocho (08) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, este análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

1. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:

- Totalmente de acuerdo (TA)
- De acuerdo (DA)
- Neutral (N)
- En desacuerdo (ED)
- Totalmente en desacuerdo (TD)

2. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
3. Se garantiza total confidencialidad de la información proporcionada individualmente.
4. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
5. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
1. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta.		X				***RONDA 1***: Me llama la atención que la metodología MAGERIT comienza de una vez en su primera fase con el análisis de riesgos, y no incluye el diagnóstico del contexto como aparece en el modelo diseñado. ***RONDA 2***: se acordó la conveniencia de la fase I,

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
						inherente a la “apreciación de los riesgos”, ya que es necesario conocer las unidades que conforman la organización y así poder levantar la información de los activos y diagnosticar e identificar la naturaleza de los riesgos que los caracterizan.
2. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la caracterización expuesta.	X					
3. El modelo gestión de riesgos basado en MAGERIT cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de		X				***RONDA 1***: No todas las codificaciones los activos, amenazas y vulnerabilidades están sujetas con los estándares de MAGERIT. ***RONDA 2***: se acordó acogerse a la flexibilidad de MAGERIT de adaptar su método, facilitando la

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
Administración Electrónica.						identificación numéricamente de los tipos de amenazas y vulnerabilidades.
4. El modelo gestión de riesgos propuesto cumple con las fases de la metodología MAGERIT.	X					
5. El modelo propuesto para la gestión de riesgos basado en MAGERIT sigue una secuencia lógica de los procesos que lo integran.	X					
6. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente graficado.	X					

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
7. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente explicado de manera que pueda guiar su implementación.		X				***RONDA 1***: veo buena explicación, solo me gustaría revisar las políticas y lineamientos de SI pertenecientes a los procesos de tratamiento, control y monitoreo del riesgo. ***RONDA 2***: se recibió un instrumento basado en una política de administración del riesgo, y los indicadores de gestión para el control y monitoreo. Todo conforme a lo esperado.
8. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta.	X					

EXPERTO 2

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de la metodología MAGERIT

Dirigido a:

Expertos en SI

Esta checklist a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de la metodología MAGERIT, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de ocho (08) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, éste análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

6. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:
    - Totalmente de acuerdo (TA)
    - De acuerdo (DA)
    - Neutral (N)
    - En desacuerdo (ED)
    - Totalmente en desacuerdo (TD)
7. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
8. Se garantiza total confidencialidad de la información proporcionada individualmente.
9. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
10. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones

1. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta.	X					
2. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la caracterización expuesta.	X					
3. El modelo gestión de riesgos basado en MAGERIT cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.		X				***RONDA 1***: No todas las codificaciones de los elementos están acordes con las políticas de MAGERIT. ***RONDA 2***: se acordó acogerse a la flexibilidad de MAGERIT de adaptar su método, facilitando la identificación numéricamente de los tipos de amenazas y vulnerabilidades.
4. El modelo gestión de riesgos propuesto cumple con las fases	X					

de la metodología MAGERIT.						
5. El modelo propuesto para la gestión de riesgos basado en MAGERIT sigue una secuencia lógica de los procesos que lo integran.		X				***RONDA 1***: No me queda claro que las fases del modelo se amolden fielmente a la metodología MAGERIT. Veo muchos más procesos en el nuevo modelo. ***RONDA 2***:se acordó la conveniencia de adoptar un proceso más inherente a la fase I, “apreciación de los riesgos”, ya que es necesario conocer las unidades que conforman la organización y así poder levantar la información de los activos y diagnosticar e identificar la naturaleza de los riesgos que los caracterizan.
6. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente graficado.	X					

7. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente explicado de manera que pueda guiar su implementación.	X					
8. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta.	X					

EXPERTO 3

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de la metodología MAGERIT

Dirigido a:

Expertos en SI

Esta lista de chequeo a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de la metodología MAGERIT, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de ocho (08) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, éste análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

11. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:
    - Totalmente de acuerdo (TA)
    - De acuerdo (DA)
    - Neutral (N)
    - En desacuerdo (ED)

- Totalmente en desacuerdo (TD)

12. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
13. Se garantiza total confidencialidad de la información proporcionada individualmente.
14. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
15. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
1. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la teoría expuesta.	X					
2. Se establece un modelo de gestión de riesgos basado en MAGERIT de acuerdo con la caracterización expuesta.	X					

3. El modelo gestión de riesgos basado en MAGERIT cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.		X				***RONDA 1***: La identificación de activos coincide con el estándar de MAGERIT, pero el de las amenazas y vulnerabilidades tengo mis dudas. ***RONDA 2***: se acordó acogerse a la flexibilidad de MAGERIT de adaptar su método, facilitando la identificación numéricamente de los tipos de amenazas y vulnerabilidades.
4. El modelo gestión de riesgos propuesto cumple con las fases de la metodología MAGERIT.	X					
5. El modelo propuesto para la gestión de riesgos basado en MAGERIT sigue una secuencia lógica de los procesos que lo integran		X				***RONDA 1***: Observo buena secuencia de procesos, pero hay uno demás, que no está en MAGERIT. ***RONDA 2***: se acordó la conveniencia de adoptar un proceso más inherente a la fase

						l, “apreciación de los riesgos”, ya que es necesario conocer las unidades que conforman la organización y así poder levantar la información de los activos y diagnosticar e identificar la naturaleza de los riesgos que los caracterizan.
6. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente graficado	X					
7. El modelo propuesto para la gestión de riesgos basado en MAGERIT está claramente explicado de manera que pueda guiar su implementación	X					
8. Se establece un modelo de gestión de riesgos basado en	X					

MAGERIT de acuerdo con la teoría expuesta						

5.4. Constancias de Juicio de Experto

EXPERTO 1

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: Joisy Del Valle Rojas Rojas

Especialidad: MSc. Ingeniero de Sistemas, con especialidad en Seguridad en Sistemas de Información

C.I.: V. 11.511.314 (Venezolana)

Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la Municipalidad Distrital de Papayal, elaborado por Manuel Esteban Mogollon Garcia – estudiante del X ciclo de Ingeniería de Sistemas de la Universidad "Señor de Sipán", quien está realizando un trabajo de investigación titulado: "**DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ".**

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Chiclayo, 28 días de Noviembre de 2020.

_____

MSc. Ing. Joisy Del Valle Rojas Rojas

C.I. N°: V. 11.511.314

EXPERTO 2

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: Nelson Ángeles Quiñones

Especialidad: Ingeniero de Sistemas, con especialidad en Seguridad de la Información

DNI N°:18140225

Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la Municipalidad Distrital de Papayal, elaborado por Manuel

Esteban Mogollon Garcia – estudiante del X ciclo de Ingeniería de Sistemas de la Universidad “Señor de Sipán”, quien está realizando un trabajo de investigación titulado: “**DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ”.**

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Chiclayo, 28 días de Noviembre de 2020.

_____

Ing. Nelson Ángeles Quiñones

DNI N°: 18140225

EXPERTO 3

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: Luis Vicente Castillo Boggio

Especialidad: Ingeniero de Sistemas, con especialidad en Administración de TI

DNI N°:18022120

Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la Municipalidad Distrital de Papayal, elaborado por Manuel Esteban Mogollon Garcia – estudiante del X ciclo de Ingeniería de Sistemas de la Universidad "Señor de Sipán", quien está realizando un trabajo de investigación titulado: "**DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ".**

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Chiclayo, 28 días de Noviembre de 2020.

_____

Mg. Ing. Luis Vicente Castillo Boggio

DNI N°: 18022120

Anexo 7. Carta de consentimiento informado

Informante 1

CONSENTIMIENTO INFORMADO

Institución: Universidad Señor de Sipán

Investigador: Manuel Esteban Mogollon Garcia

Título: DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ.

Yo, ……, identificado con DNI…….., DECLARO:

Haber sido informado de forma clara, precisa y suficiente sobre los fines y objetivos que busca la presente investigación, así como en qué consiste mi participación.

Estos datos que yo otorgué serán tratados y custodiados con respeto a mi intimidad, manteniendo el anonimato de la información y la protección de datos desde los principios éticos de la investigación científica. Sobre estos datos me asisten los derechos de acceso, rectificación o cancelación que podré ejercitar mediante solicitud ante el investigador responsable.

Al término de la investigación, seré informado de los resultados que se obtengan. Por lo expuesto otorgo MI CONSENTIMIENTO para que se realice la discusión de observaciones en la plantilla de evaluación de riesgos de seguridad informática que permita contribuir con los objetivos de la investigación destinados a obtener la gestión de riesgos.

Chiclayo, 13 de Octubre del 2020

_____

FIRMA

DNI:

Informante 2

CONSENTIMIENTO INFORMADO

Institución: Universidad Señor de Sipán

Investigador: Manuel Esteban Mogollon Garcia

Título: DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ.

Yo, ……, identificado con DNI…….., DECLARO:

Haber sido informado de forma clara, precisa y suficiente sobre los fines y objetivos que busca la presente investigación, así como en qué consiste mi participación.

Estos datos que yo otorgué serán tratados y custodiados con respeto a mi intimidad, manteniendo el anonimato de la información y la protección de datos desde los principios éticos de la investigación científica. Sobre estos datos me asisten los derechos de acceso, rectificación o cancelación que podré ejercitar mediante solicitud ante el investigador responsable.

Al término de la investigación, seré informado de los resultados que se obtengan. Por lo expuesto otorgo MI CONSENTIMIENTO para que se realice la discusión de observaciones en la plantilla de evaluación de riesgos de seguridad informática que permita contribuir con los objetivos de la investigación destinados a obtener la gestión de riesgos.

Chiclayo, 13 de Octubre del 2020

_____

FIRMA

DNI:

Anexo 8. Carta de autorización para la recolección de la información

UNIVERSIDAD SEÑOR DE SIPÁN

"Año de la Universalización de la Salud"

Pimentel, miércoles 07 de diciembre de 2020

Señor(a):
MG. CÉSAR RICARDO HILARION PARDO NEUMANN
GERENTE MUNICIPAL
MUNICIPALIDAD DISTRITAL DE PAPAYAL
Ciudad.-

ASUNTO:
Presentación de estudiante para realizar caso de estudio.

Es grato dirigirme a usted para expresarle el saludo institucional a nombre de la Escuela Profesional de Ingeniería de Sistemas, perteneciente a la Facultad de Ingeniería, Arquitectura y Urbanismo, de la Universidad Señor de Sipán, a la vez presentar al estudiante del X ciclo, MANUEL ESTEBAN MOGOLLÓN GARCÍA con código universitario 2150815083, e identificado con DNI 00252937, quien recogerá información relevante en la institución que usted representa, como parte de su trabajo de INVESTIGACIÓN, aprobado con resolución N° 2322-2020/FIAU-USS, del proyecto titulado "DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ".

Para ello, solicitamos su autorización, esperando que el estudiante cumpla con todos los requerimientos necesarios.

En espera de su atención a la presente, aprovecho la oportunidad para expresarle mi consideración y estima personal.

Cordialmente,

Mag. Ing. Heber Ivan Mejia Cabrera
Director (e) de la Escuela Profesional de Ingeniería de Sistemas
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Municipalidad Distrital de Papayal
Ley N° 9017 del 25-11-1942
Gerencia Municipal
Reg.: 3988 Folio N°:
Fecha de Ingreso: 16/12/2020 Hora: 11:30
Recibido por:

MUNICIPALIDAD DISTRITAL DE PAPAYAL

CREADA POR LEY N° 9667 | 25.NOVIEMBRE.1942

"AÑO DE LA UNIVERSALIZACIÓN DE LA SALUD"

Papayal, 16 de diciembre del 2020

CARTA N° 012-2020/MDP-GM-CRHPN

MAG. ING. HEBER IVAN MEJÍA CABRERA
DIRECTOR (E) DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
UNIVERSIDAD "SEÑOR DE SIPÁN"

ASUNTO : AUTORIZACIÓN PARA REALIZACIÓN DE CASO DE ESTUDIO DE PROYECTO DE INVESTIGACIÓN

Es grato dirigirme a usted para expresarle el saludo institucional a nombre de la Municipalidad Distrital de Papayal, y comunicarle que se AUTORIZA la realización del caso de estudio para el proyecto de investigación titulado: "DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ", a cargo del estudiante de X ciclo, MANUEL ESTEBAN MOGOLLÓN GARCÍA, con código universitario 2150815083, e identificado con DNI 00252937.

Teniendo en cuenta que el estudiante es el responsable de la Unidad de Tecnologías de la Información de esta Municipalidad, desarrollará el caso de estudio en el horario que previamente coordine con el personal de cada una de las Oficinas y Unidades.

En espera de su atención a la presente, aprovecho la oportunidad para expresarle mi consideración y estima personal.

Atentamente,

MUNICIPALIDAD DISTRITAL DE PAPAYAL
GERENTE MUNICIPAL

Anexo 9. Ejecución de la Propuesta: Plan de Implementación del Modelo de Gestión de Riesgos para la Municipalidad Distrital de Papayal

Anexo 9.1. Carta de Comunicación a la Gerencia General de Implementación del Modelo

Papayal, 03 de septiembre 2020

Mg. César Ricardo Hilarión Pardo Neuman

Gerente Municipal

Municipalidad Distrital de Papayal

Tengo a bien dirigirme a usted, en la oportunidad de solicitar su apoyo para la implementación de un sistema de gestión de riesgos basado en la metodología MAGERIT para minimizar los riesgos de la implantación y uso de TI en la Municipalidad, con la participación de todas las oficinas y unidades involucradas en la seguridad informática de la institución, y de esta manera, estos sean participes en todas las etapas del proceso donde su información e intervención será de gran aporte para este proyecto que beneficia a todos los entes contralores del patrimonio público y por ende a los habitantes de la localidad.

Adjunto a este documento, se anexa el plan de implementación (Anexo 9.2.) de acuerdo a los procesos incluidos al modelo diseñado en este proyecto.

Agradeciendo de antemano su colaboración se despide

_____

Manuel Esteban Mogollon Garcia

Estudiante de X Ciclo de Ingeniería de Sistemas

Universidad "Señor de Sipán"

Anexo 9.2. Plan de implementación de un modelo de gestión de seguridad informática

MUNICIPALIDAD DISTRITAL DE PAPAYAL

CREADA POR LEY N° 9667 | 25.NOVIEMBRE.1942

UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

Plan de Implementación

Código: PRO XXXXXXXX

Versión: 00

Vigencia: 07.09.2020

N°	Objetivo	Descripción	Tareas	Recursos	Personal a cargo	Periodo	Proporción de cumplimiento
1	Sensibilización de los actores acerca de la Seguridad Informática.	Dar a conocer a todos los funcionarios que laboran en la Municipalidad la importancia de la	Charla	- Proyector - Presentación multimedia - Salón de	- Manuel Mogollon (Investigador y Responsable	7 al 18 de septiembre 2020	11,1%

		Seguridad Informática para evitar los riesgos a los que están expuestos los activos informáticos de la institución.		reunión	de la UTI) - Gerencia Municipal		
2	Diagnóstico del Contexto Institucional con respecto a la seguridad informática.	Conocer la razón social y función básica de gestión operativa y administrativa de la Municipalidad, con el fin de conocer su relación con los activos que posee como base de apoyo a sus actividades y los riesgos a los que están expuestos.	- Entrevistas - Revisión de gestión operativa de periodos anteriores	- Grabadora - Lápiz y papel para apuntes	Manuel Mogollon (Investigador y responsable de la UTI)	14 al 30 de Septiembre 2020	22,2%

9.2. (Cont.)

N°	Objetivo	Descripción	Tareas	Recursos	Personal a cargo	Periodo	Proporción de cumplimiento
3	Analizar los riesgos.	Conocer los riesgos y las causas que podrían generar una situación crítica para los activos, ante las amenazas y vulnerabilidades.	- Identificación y Valoración de los activos - Identificación y Valoración de las amenazas - Identificación y Valoración de los activos - Identificación y Valoración de las vulnerabilidades	- Lápiz y papel para apuntes - Office Excel - Herramienta de Análisis y Gestión de Riesgo basada en MAGERIT denominada R-Box	Manuel Mogollon (Investigador y Responsable de la UTI)	1 al 16 de Octubre	33,3%
4	Evaluar los	Estimar de forma	- Estimación del	- Lápiz y papel	Manuel	19 al 23 de	44,4%

	riesgos.	cuantitativa los riesgos, indicando las medidas para su posterior tratamiento.	impacto de amenazas y vulnerabilidades en activos - Estimación del riesgo en activos	para apuntes - Office Excel - Herramienta de Análisis y Gestión de Riesgo basada en MAGERIT denominada R-Box	Mogollon (Investigador y Responsable de la UTI)	Octubre 2020	
5	Determinación de salvaguardas de activos de la institución.	Identificar las salvaguardas desplegadas en los activos de la Municipalidad, calificándolas por su eficacia frente a	- Checklist - Identificación y Valoración de los salvaguardas	- Lápiz y papel para apuntes - Office Excel -	Manuel Mogollon (Investigador y Responsable de la UTI)	19 al 23 de Octubre2020	55,5%

amenazas que pretenden mitigar.

9.2. (Cont.)

N°	Objetivo	Descripción	Tareas	Recursos	Personal a cargo	Periodo	Proporción de cumplimiento
6	Tratamiento del riesgo.	Determina la acción para tratar el riesgo en función de evitar, reducir, transferir y aceptar los riesgos.	Diseño de Instrumento de políticas de seguridad	- Lápiz y papel para apuntes - Office Excel	- Manuel Mogollon (Investigador y Responsable de la UTI) - Gerencia Municipal	26 al 30 de Octubre 2020	66,6%
7			Diseño del plan de implementación de políticas de seguridad			2 al 13 de noviembre 2020	77,7%
8			Ejecución del plan de implementación			2 al 19 de febrero de	88,8%

			de políticas de seguridad			2021	
9	Control y seguimiento.	Medir la efectividad del cumplimiento de políticas de seguridad.	Aplicar indicadores de gestión	- Lápiz y papel para apuntes - Office Excel	Manuel Mogollon (Investigador y Responsable de la UTI)	22 al 26 de febrero de 2021	100%

Elaborado por. Manuel Esteban Mogollon García Investigador Firma:	**Revisado por**: Manuel Esteban Mogollon García Responsable de la UTI Firma:	Aprobado por: César Ricardo Pardo Newman Gerente Municipal Firma:
	Revisado por: Mg. César Ricardo Pardo Newman Gerente Municipal Firma:	Fecha: Papayal, 05 de Septiembre de 2020

Anexo 10. Instrumento Normativo Propuesto sobre las Políticas de Seguridad Informática

Políticas de Seguridad Informática

1. Objetivo

Definir las políticas para el control de la seguridad informática de la Municipalidad Distrital de Papayal.

2. Alcance

Direccionar medidas que sean consideradas por la UTI y demás miembros de la institución para orientar la Seguridad Informática de una forma eficiente y eficaz.

3. Política de Seguridad

Objetivo

Canalizar los preceptos y líneas que orienten el buen desempeño de la seguridad informática hacia una óptima gestión, y de esta manera se minimicen los riesgos a los que se ven expuestos los activos de la Municipalidad Distrital de Papayal, lo cual brindará a la gerencia una herramienta de apoyo para garantizar la seguridad de la información.

Por tal motivo se establece: *El factor humano de la institución estará comprometido con los objetivos organizacionales y en consonancia con la gestión de riesgos y la seguridad informática de la Municipalidad Distrital de Papayal, y en función de ello, corresponderán a los preceptos establecidos en la institución que garanticen y promuevan llevar a buen término el cumplimiento de acciones y medidas dispuestas por la gestión de SI*.

4. Políticas Generales

1. No se admitirá personas ajenas no autorizas en el local de la UTI.
2. Los usuarios tendrán acceso a la PC a las que se encuentran autorizados. En caso de no estar asignado a una PC se hará la solicitud ante esto.

3. La documentación de los softwares pertenecientes a la Municipalidad, tales como tutoriales y manuales estarán resguardados por el responsable de la UTI.
4. Para entrar a la intranet de la Municipalidad Distrital de Papayal es necesario contar con una clave de acceso a la misma, cuya responsabilidad es de quien la usa.
5. Los usuarios tienen la plena responsabilidad de cuidar y proteger de los equipos informáticos a su cargo.
6. Todas las computadoras de escritorio o laptop deberán activar su clave de inicio.
7. No se podrá abrir más de una sesión, y si así se requiere, se necesita una autorización del jefe del área en que el usuario se encuentre.
8. Las claves de usuario tendrán una duración de hasta 120 días, sin embargo, el usuario puede cambiarla cuando considere conveniente.
9. Los usuarios dividirán sus aplicaciones bajo tipo pública y tipo privada.
10. Al no darle uso a una clave en un periodo de 90 días la misma será eliminada. Exceptuando situaciones de permisos por maternidad o enfermedad.
11. La Unidad de RR.HH., comunicará a la UTI la renuncia o retiro de empleados para que estos sean sacados de la base de datos de usuarios.
12. La limpieza y depuración de los discos duros (DD) se llevará a cabo en equipo con los usuarios de áreas implicadas como Base de Datos (BD).
13. Los usuarios tienen la plena responsabilidad de la información almacenada en los DD de cuidar y proteger de los equipos informáticos a su cargo.
14. Los usuarios son responsables de la información almacenada en sus DD, y en función de ello deben respaldar la misma bajo los estándares establecidos por la UTI.
15. Todas las computadoras de escritorio o laptop deberán activar el protector de pantalla.

16. La documentación física en papel inservible en la UTI es conveniente triturarla, o de lo contrario reutilizarla.
17. Para instalar un nuevo software será necesario contar con su licencia original.
18. Para ingresar o sacar hardware o software de propiedad de la Municipalidad se requiere de autorización escrita del gerente, jefes de área o del responsable de la UTI.
19. El responsable de la UTI será el encomendado de comunicar cualquier anormalidad en el área, así como cualquier problema eléctrico que surja, o de los equipos de climatización, para su respectiva reparación y/o mantenimiento.

5. Políticas de Seguridad a Nivel del Personal

1. Establecer los mecanismos requeridos en la difusión de las situaciones subestándares que menoscaban la seguridad informática en su área de trabajo, así como los riesgos que caracterizan a la misma.
2. Poner al tanto al responsable de la UTI sobre las amenazas y riesgos inherentes a la SI, para que estos sepan cómo responder ante una eventualidad.
3. Detallar las responsabilidades de los empleados en relación con la seguridad, crear planes de incentivo para aminorar la rotación de empleados en el área de UTI, y garantizar su retención en el puesto.
4. Informar desde la etapa de iniciación en la Institución, de manera que sean incorporadas en las descripciones de cargos y constituyan una de las bases para medir el cumplimiento de su desempeño.
5. Comprometer al empleado ante la confidencialidad de la información.

6. Entrenar personal de contingencia para colaborar con la UTI, en caso de falta o indisposición del responsable.
7. Incluir cursos, talleres y seminarios en los planes de capacitación para adiestrar a todo el personal en cuanto a la utilización de la plataforma informática de la Municipalidad.
8. Proveer y garantizar la suficiencia de fuerza laboral para la UTI.
9. Incluir cursos, talleres y seminarios en los planes de capacitación para adiestrar al responsable de la UTI sobre la gestión de riesgos en SI.
10. Todos los empleados de la Municipalidad recibirán una adecuada capacitación y actualización periódica referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo, utilización de dispositivos de almacenamiento entre otros.

6. Políticas de Seguridad a Nivel Físico

1. Se debe contar con servicio de vigilancia permanente para la UTI.
2. Renovar los equipos de climatización de la UTI.
3. Cuando suceda algún inconveniente en a la UTI por fuego, accidente eléctrico o casos fortuitos o de fuerza mayor, se debe notificar al personal de seguridad laboral.
4. No se permite consumir ningún tipo de alimento o bebida cerca de los equipos de computación.
5. Restringir el acceso a la UTI, donde solo se podrá entrar con autorización.
6. Se debe proveer de sistemas contraincendios a todas las instalaciones de la Municipalidad, con prioridad la UTI.
7. Se prohíbe fumar en a la UTI.

8. Restringir el acceso a las instalaciones de la Municipalidad luego de terminar el horario de trabajo, donde solo se podrá entrar con autorización.
9. Los equipos contra incendios deberán estar ubicados en lugares adecuados y deberán ser revisados de forma periódica para verificar su estado y cambiados cuando sea necesario.
10. Revisar y realizar mantenimiento a los extintores de incendios periódicamente. Del mismo modo se debe proveer y garantizar la localización de un extintor en cada área de la institución.
11. Se debe proveer de un generador de energía eléctrica que soporte la carga utilizada en la Municipalidad, para garantizar la continuidad de sus funciones caso de corte de esta por la empresa proveedora.
12. Se debe proveer de equipos para respaldar el abastecimiento de energía, tal como los UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas.
13. Se debe asegurar contra todo riesgo los equipos por una compañía de seguros.
14. Se llevará control diario de las condiciones ambientales para verificar que no afecten el funcionamiento de las instalaciones de procesamiento de información y equipos de respaldo eléctrico.
15. Al momento de llevar a cabo las actividades de mantenimiento a los equipos, debe estar presente el responsable de la UTI.
16. Se debe verificar periódicamente el funcionamiento de los equipos de ininterrupción de suministro de energía (UPS).
17. Planificar actividades de mantenimiento a los aires acondicionados de la UTI, y de las demás instalaciones en general de la Municipalidad.

8. Políticas de Seguridad a Nivel Lógico

1. Sólo el responsable de la UTI estará a cargo de la seguridad lógica de la estructura general de la red.
2. Sólo el responsable de la UTI estará a cargo de crear y otorgar las claves de usuario.
3. Se deben implementar medios contra ataques maliciosos como hackers o programas malignos.
4. Las eventualidades que dificultan el buen desempeño de la UTI, así como los activos informáticos deben ser registradas en una base de datos de incidentes.
5. Sólo el responsable de la UTI podrá instalar y actualizar las BD.
6. Implementar equipos firewall para el apoyo en la protección de la red.
7. Sólo el responsable de la UTI podrá instalar y realizar mantenimiento del sistema operativo.
8. Solo se otorgará claves de acceso a un software si el usuario tiene la habilidad de manejarlo.
9. Para acceder a la navegación de un software el usuario debe hacerlo mediante la secuencia del menú, y en caso de que el mismo no requiera utilizar un módulo dentro del sistema debe comunicarlo.

9. Políticas de Seguridades a Nivel de Sistemas

1. Se debe considerar la recuperación automática de la información en caso de falla del sistema.

2. Se debe considerar el rol de los usuarios según su actividad en los sistemas diseñados, de manera que estos puedan ser agrupados según su clase o tipo.
3. Realizar periódicamente reuniones con los usuarios de software y aplicaciones para el aseguramiento del buen desempeño en el uso de estos.
4. Se debe considerar la ejecución de los sistemas con datos privados a partir del nivel de usuario o un equipo en particular.
5. Es conveniente que las aplicaciones y software orientados a ingresar datos contemplen la opción para validarlos, primeramente.
6. Es conveniente que las aplicaciones y software orientados a ingresar, modificar y eliminar datos contemplen la opción para generar registro de verificación que permita auditarlos, tales como fecha, hora, entre otros.
7. Se debe considerar firmar un acta de entrega y recibimiento del sistema diseñado, como garantía de propiedad del autor, y su cesión para uso legitimado a la Municipalidad.
8. Se debe considerar las normas de la UTI para el diseño y desarrollo de los sistemas.
9. Se debe hacer entrega al responsable de la UTI la documentación de diseño lógico, preliminar y codificado, de los sistemas diseñados para la Municipalidad.

10. Políticas de Respaldos y Recuperación de Información

1. Los respaldos periódicos se deben mantener en lugares de amplia seguridad y localizados fuera de la UTI.
2. Se debe mantener en lugares de amplia seguridad y localizados dentro de la UTI los respaldos de archivos permanentes.

3. Los respaldos serán en distintos dispositivos de almacenamiento para la BD, aplicaciones, usuarios, archivos de documentos y archivos de SO.
4. Los archivos históricos estarán disponibles en línea hasta un lapso de 2 años.
5. Establecer el tiempo estipulado entre un respaldo y otro, de acuerdo con su importancia.
6. Posteriormente se resguardarán en servidores.

11. Políticas Relacionadas a los Equipos de Computación

1. Todo equipo informático de la institución que se considere que interviene en procesos claves y críticos, debe ubicarse estratégicamente en un lugar acondicionado y seguro.
2. Es responsabilidad del usuario la seguridad física del equipo informático a su cargo.
3. Todos los equipos informáticos que estén configurados a lo largo y extenso de la infraestructura de la red de la institución deben estar sujeto a los estándares e instalación de la UTI.
4. La UTI en coordinación con el Área de Control de Bienes Patrimoniales deberá crear una BD que contenga todos los equipos que posee la institución.
5. La UTI es la responsable de todas las operaciones de asignación y rotación de los equipos informáticos.

12. Políticas de Mantenimiento de Equipos

1. Los usuarios no están autorizados para realizar mantenimiento a los equipos informáticos de su responsabilidad.

2. Se debe actualizar y ajustar semestralmente el plan de mantenimiento preventivo a equipos informáticos para verificar su correspondencia ante las necesidades.
3. Se debe contratar organizaciones externas para complementar la práctica de mantenimiento preventivo y correctivo a los equipos informáticos, cuyo tiempo de garantía haya expirado.
4. Es responsabilidad de la UTI realizar y controlar el mantenimiento preventivo y correctivo de los equipos informáticos, de manera de garantizar su seguridad y adecuación.

13. Políticas de Actualización de los Equipos

1. Con frecuencia se debe aplicar mejoras a los equipos informáticos de la institución, y así garantizar una adecuada conservación y desempeño de estos.

14. Políticas de Accesos Remotos

1. La UTI será responsable de manejar las autorizaciones a otras personas que laboran en la institución para el uso de los recursos informáticos de la red.
2. Orientar el cumplimiento de los lineamientos de la UTI para este tipo de servicio.

15. Políticas del WWW

1. La UTI será responsable de aplicar la instalación y operatividad de los servidores WWW; y solo con páginas autorizadas por la Gerencia Municipal.

16. Política de Control de Virus y Uso de Software

1. Llevar a cabo la ejecución del programa antivirus antes de usar algún dispositivo de almacenamiento auxiliar.
2. No se debe utilizar software sin licencias adquiridas por la institución.
3. Generar la protección contra escritura de los dispositivos de almacenamiento auxiliar.
4. Garantizar el desempeño permanente y consecutivo de un antivirus instalado en los equipos de computación, cuya adecuación esté disponible en línea.

17. Políticas de Gestión a Nivel de Monitoreo, Indicadores, Comunicación y Difusión

1. Llevar un control y seguimiento eficaz de las políticas desarrolladas para garantizar la SI.
2. Realizar una planificación eficaz de la gestión de los riesgos, donde se incorpore anualmente un análisis y evaluación del riesgo.
3. Llevar a cabo la identificación de las amenazas que expongan la SI de los activos.
4. La reducción del nivel de riesgo en los activos que se integran a la SI en la Municipalidad debe ajustarse en un horizonte de corto, mediano o largo plazo a través de los indicadores que se formulan a continuación:
    - Indicador para medir el nivel de efectividad de los controles: permite saber si las medidas implementadas tienen el funcionamiento esperado.
    - Indicador para medir el entorno: para la verificación del comportamiento de ocurrencia y recurrencias de las amenazas.

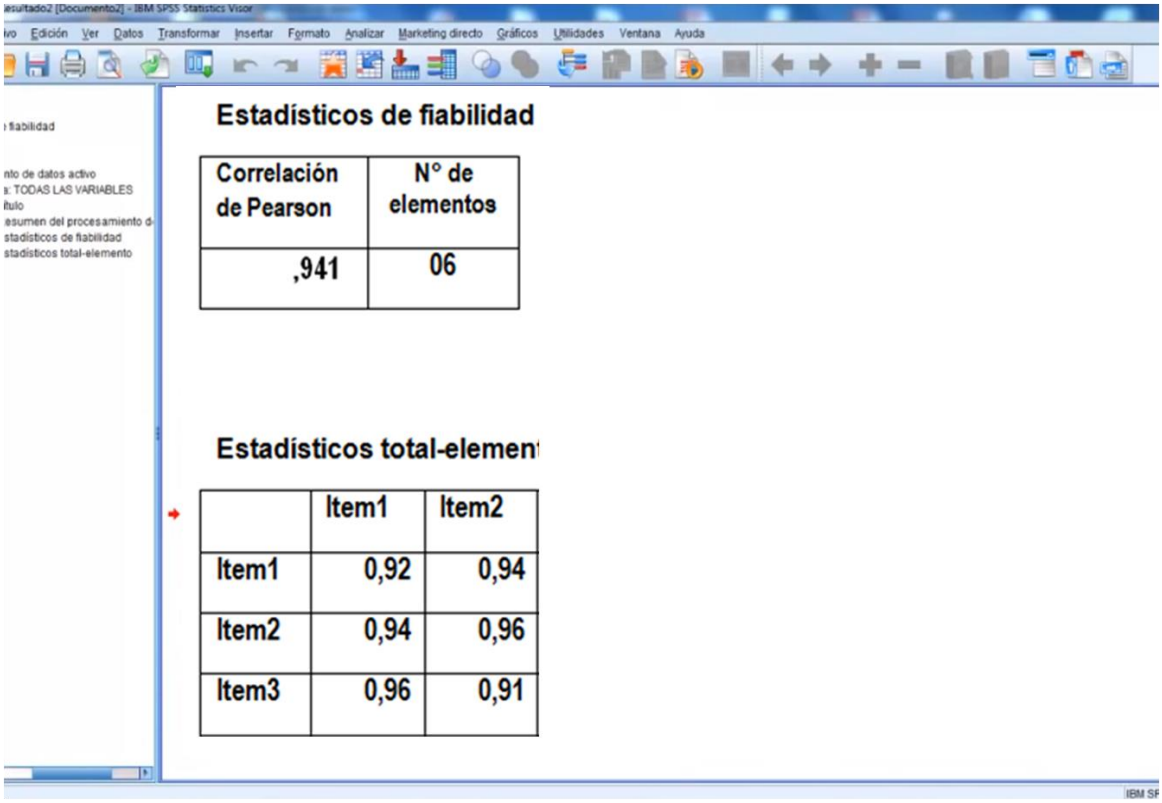
COMUNICACIONES ESCRITAS:

1. Entregar estrategias de difusión a todo el personal, consistente en un tríptico con la información relativa a las medidas de SI.
2. Informar mediante documentos (memorándums) enviados al personal o publicar en el periódico mural, la nueva estrategia de seguridad informática de la Municipalidad, conteniendo todas las líneas aquí expuestas.
3. Evaluar periódicamente el conocimiento y concepción de los empleados ante las medidas de SI.

18. Sanciones

1. Se castigará el quebrantamiento de las medidas de SI que son aplicadas malintencionadamente de acuerdo con las normativas del ente que le compete la administración de RR.HH. en la Municipalidad.
2. El funcionario que practicare una mala acción será suspendido en proporción al margen de daño ocasionado.

Anexo 11. Aplicación de prueba estadística con SSPS para correlación de coeficiente de Pearson en eficacia del modelo propuesto



Estadísticos de fiabilidad

Correlación de Pearson	N° de elementos
,941	06

Estadísticos total-elemen

	Item1	Item2
Item1	0,92	0,94
Item2	0,94	0,96
Item3	0,96	0,91

Anexo 12. Acta de revisión de similitud de la investigación

ACTA DE REVISIÓN DE SIMILITUD DE LA INVESTIGACIÓN

Yo, Mg. Mejía Cabrera Heber Ivan, docente del curso de xxxxxxxxxxxxxxxxxxxxxxxxxxx del Programa de Estudios de Ingeniería de Sistemas, y revisor de la investigación del estudiante, Manuel Esteban Mogollon Garcia, titulada:

DESARROLLO DE UN MODELO DE GESTIÓN DE RIESGOS BASADO EN LA METODOLOGÍA MAGERIT PARA MINIMIZAR LOS RIESGOS DE LA IMPLANTACIÓN Y USO DE TI EN UNA MUNICIPALIDAD DEL PERÚ

Se deja constancia que la investigación antes indicada tiene un índice d similitud del 9%, verificable en el reporte fina de análisis de originalidad mediante el software de similitud TURNITIN. Por lo que se concluye que cada una de las coincidencias detectadas no constituyen plagio y cumple con lo establecido en la Directiva sobre índice de similitud de los productos académicos y de investigación en la Universidad Señor de Sipán S.A.C., aprobada mediante Resolución de Directorio N° XXXXXX.

Pimentel, 02 de marzo de 2023

_____

Mg. Mejía Cabrera Heber Ivan

DNI N° XXXXXXXXXXX

NIVEL DE SIMILITUD

Reporte de similitud

NOMBRE DEL TRABAJO
Mogollon_Garcia_Manuel_Esteban_Turnitin.docx

AUTOR
Manuel Mogollon Garcia

RECUENTO DE PALABRAS
25615 Words

RECUENTO DE CARACTERES
134640 Characters

RECUENTO DE PÁGINAS
121 Pages

TAMAÑO DEL ARCHIVO
2.7MB

FECHA DE ENTREGA
Nov 7, 2023 12:10 PM GMT-5

FECHA DEL INFORME
Nov 7, 2023 12:11 PM GMT-5

19% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base d

- 18% Base de datos de Internet
- 2% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossr
- 6% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 8 palabras)