Universidad Nacional "Pedro Ruiz Gallo"

FACULTAD DE INGENIERÍA CIVIL, SISTEMAS Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

MODELO DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN EL HOSPITAL REGIONAL DE LAMBAYEQUE.

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTORES:

PUYÉN SANTOS VICENTE RAÚL

RIVAS PALACIOS BETTY GUILIANA

ASESOR:

DR. ING. ERNESTO KARLO CELI ARÉVALO

LAMBAYEQUE – PERU

2018

INFORMACIÓN GENERAL

Título de la investigación

Modelo de gestión de riesgos basados en la norma ISO/IEC 27005 y metodología MAGERIT para mejorar la gestión de seguridad de la información en el Hospital Regional de Lambayeque.

Código del proyecto

IS-2017-030

Responsables de la investigación

Autores

Puyén Santos Vicente Raúl
email: *rpuyensantos@outlook.com*

Rivas Palacios Betty Guiliana
email: *rivasp.bg@gmail.com*

Asesor

Dr. Ing. Ernesto Karlo Celi Arévalo

email: *eceli@unprg.edu.pe*

Orientación de la investigación

Línea de investigación

Gobierno y gestión de tecnología de información

Lugar de ejecución de la investigación

Hospital Regional de Lambayeque, Lambayeque - Perú

Lambayeque, Diciembre del 2018

Vicente Raúl Puyen Santos
Bachiller en Ingeniería de Sistemas

Betty Guiliana Rivas Palacios
Bachiller en Ingeniería de Sistemas

Dr. Ing. Ernesto Karlo Celi Arévalo
Asesor

Mg. Ing. Pilar Del Rosario Ríos Campos
Presidente de jurado

Mg. Ing. Pedro Miguel Jacinto Mejía
Secretario de jurado

Mg. Ing. Jesús Bernardo Olavarría Paz
Vocal de jurado

AGRADECIMIENTOS

Agradecer a Dios por bendecirme la vida, por guiarme a lo largo del tiempo, ser el apoyo y fortaleza en aquellos momentos más difíciles que he tenido.
Gracias a mis padres: Casimiro y Lita, por ser uno de los promotores de mis sueños, por confiar y creer en mis expectativas, por los consejos, valores y principios que me han inculcado. Así mismo, agradecer a mi esposa Cecilia, por el apoyo incondicional brindado, el amor y dedicación hacia mí en cada momento de mi vida y especialmente a mi hija Valentina, la bendición de mi hogar y la razón de seguir superándome día a día.
Agradecer a mi docente de la Escuela Profesional de Ingeniería de Sistemas de la UNPRG, el Ing. Celi Arévalo, por haber compartido sus conocimientos a lo largo de la preparación de mi profesión, y por su valioso apoyo y aporte en la realización del proyecto de investigación.

Agradezco en primer lugar a Dios por permitirme lograr cada uno de los objetivos trazados a lo largo de mi vida.

A mi madre, Betty, mis hermanas y hermanos por ser ejemplo de lucha y por ser quienes me incentivan a crecer día a día.

A mi familia y amigos que me motivaron a culminar este objetivo profesional.

A nuestro asesor el Dr. Ing. Celi Arévalo, por su guía, apoyo y gentileza al compartir su tiempo y conocimientos para culminar con éxito esta investigación.

DEDICATORIA

El presente proyecto de investigación lo dedico a Dios, por ser el inspirador y darme las fuerza para obtener una de mis metas más anheladas.

A mis padres, por su amor, trabajo y sacrificio en toda mi vida, gracias a ustedes he logrado llegar hasta aquí. He sido el orgullo y el privilegio de ser su hijo, son los mejores padres.

A mis hermanas (os) y sobrinos(as) por estar siempre presentes, por el apoyo moral, que me brindaron a lo largo de esta etapa de mi vida.

A mis esposa e hija, que son los pilares de mi nuevo hogar y son el motor y la fuerza para salir siempre triunfador en todas mis metas trazadas.

A todas las personas que me han apoyado y han hecho que el trabajo se realice con éxito, en especial a aquellos que nos compartieron sus conocimientos.

Esta investigación está dedicada a Dios por darme fortaleza espiritual para trabajar continuamente por cumplir los objetivos trazadas, a mi familia que siempre me motivo a seguir adelante y aquellas amistades que me animaron a desarrollar esta investigación.

RESUMEN

El actual avance tecnológico conlleva a una mayor exposición de riesgos asociados a la información que administra una organización o institución, pública o privada; a raíz de esto, dichas organizaciones enfocan sus mayores esfuerzos en conservar la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información que administran, bajo controles que permitan garantizar la seguridad de la misma; siendo de esta manera, la información, considerada como su activo principal.

Partiendo de la premisa en la que se indica que la información, es el activo de vital importancia para las organizaciones o instituciones, es necesario gestionar la seguridad de la misma, a través de la identificación y análisis de activos de información, determinación de activos críticos, identificación de vulnerabilidades y amenazas en aquellos activos críticos y la propuesta de controles que ayuden a mitigar los riesgos a los que se encuentren expuestos.

El uso adecuado de los modelos de gestión de riesgos para la seguridad de la información promueve una cultura de seguridad de la información en toda la organización o institución, creando entre sus clientes la confianza y mostrando su potencial y capacidad entre su competencia.

Esta investigación propone la mejora de la gestión de seguridad de la información en el Hospital Regional de Lambayeque, aplicando un modelo de gestión de riesgos basado en la norma ISO 27005 y la metodología MAGERIT.

ABSTRACT

The current technological advance leads to a greater exposure of risks associated with the information managed by a public or private organization or institution; as a result of this, said organizations focus their greatest efforts in preserving the confidentiality, integrity, availability, authenticity and traceability of the information they administer, under controls that allow guaranteeing the security thereof; being in this way, the information, considered as its main asset.

Starting from the premise that indicates that information is the asset of vital importance for organizations or institutions, it is necessary to manage the security of it, through the identification and analysis of information assets, determination of critical assets, identification of vulnerabilities and threats in those critical assets and the proposal of controls that help to mitigate the risks to which they are exposed.

The proper use of the risk management models for information security promotes a culture of information security throughout the organization or institution, creating confidence among its clients and showing their potential and capacity among their competitors.

This research proposes the improvement of information security management in the Regional Hospital of Lambayeque, applying a risk management model based on the ISO 27005 standard and the MAGERIT methodology.

INTRODUCCIÓN

Desde hace varios años el énfasis que se está dando mundialmente a la seguridad de la información, sobre todo para la protección de la información, es cada vez mayor, por lo que se vienen elaborando distintas normas internacionales que permiten controlar y mitigar los riesgos asociados a la seguridad de la información de manera uniforme e integrada y se vienen desarrollando diversas herramientas y metodologías que permiten analizar y controlar los riesgos asociados a la seguridad de la información.

La escasa cultura en gestión de riesgos para los activos de la información, conlleva a que las instituciones desconozcan el valor de la importancia real de sus activos de la información, impidiendo que puedan identificar las vulnerabilidades que podrían ser aprovechadas por distintas amenazas, que podrían impactar sustancialmente en la continuidad de los procesos del negocio y afectar a los principios de la seguridad de la información.

En la actualidad, las organizaciones e instituciones se vuelven más competitivas y se apoyan con mayor frecuencia en la tecnología para ofrecer sus productos y/o servicios, volviéndose susceptibles a ataques informáticos, fugas de información y otros incidentes en la seguridad de la información; por tal motivo, se brinda mayor importancia en resguardar la información que administran, a través de una adecuada gestión de seguridad de la información.

Para proteger la información, las instituciones deben mantener su confidencialidad, integridad y disponibilidad, a través de la aplicación de políticas de seguridad que incluyan tanto las medidas preventivas como las acciones a tomar, para proteger esta y los soportes donde se almacena, desde que se crea hasta que se destruye.

La adecuada gestión de la seguridad de la información, permite a las organizaciones administrar sus riesgos, entre los que tenemos: riesgos físicos como son los diversos desastres naturales, los riesgos de control de accesos a la información y los que provienen

del uso de los sistemas de información, en donde se tienen a los diferentes ataques informáticos y múltiples fugas de información ya sea por personal interno, como externo a la organización; garantizando la protección de su, información, dentro de su marco competitivo; manteniendo niveles altos en su imagen reputacional, que genera confianza en sus clientes..

Por estos motivos es que las principales autoridades la administración y/o dirección de las organizaciones e instituciones se abocan a proteger cada día más y mejor su información, para preservarlas de los diferentes ataques que puedan sufrir, no solo con herramientas que las contrarresten, sino también creando cultura de seguridad de la información en toda su organización.

El Hospital Regional de Lambayeque maneja una gran cantidad de información de suma importancia, entre las que se tienen información personal, financiera y de temas médicos de sus pacientes e incluso los de su personal, por tal motivo requiere que ésta sea protegida de cualquier tipo de riesgo de amenazas entre las que podemos mencionar: infección por malware, incidentes de seguridad, fuga intencional de datos, uso irresponsable de la tecnología, compartir información de estado de salud y estudios de pacientes, equipamiento médico vulnerable, sistemas operativos desactualizados, entre otros. En resumen, el HRL debe gestionar los riesgos asociados a su activo de información, de manera que se puedan implementar controles de seguridad destinados a proteger su información y los soportes que la almacenan, procesan y transfieren; con la finalidad de mantener una adecuada gestión de la información y así brindar un mejor soporte a los servicios administrativos, clínicos y por lo tanto un mejor servicio en la atención.

El objetivo de la presente investigación es proponer el desarrollo de un modelo de gestión de riesgos para la seguridad de la información basado en la norma ISO 27005 y la metodología MAGERIT, que permita una mejor gestión de la seguridad de la información en el Hospital Regional de Lambayeque. Para conseguir este propósito, el trabajo de investigación se encuentra estructurado de la siguiente manera:

En el Capítulo I, se describe el planteamiento del proyecto de investigación, el cual incluye la descripción de la problemática por la que atraviesa el Hospital Regional de

Lambayeque al no contar con un sistema de gestión de seguridad de información implementado y las posibles causas y efectos que generan dichos problemas. Así mismo, se formula el problema científico, la hipótesis que permite responder el problema científico planteado y se definen los objetivos de la investigación, así como el alcance de la investigación y limitaciones correspondientes.

En el Capítulo II, se especifican los antecedentes del proyecto de investigación, que sirven de base para la formulación del modelo de gestión de riesgos de seguridad de la información que se ha propuesto; estos proyectos enmarcados como antecedentes, corresponden al desarrollo de tesis que referencian el uso de las normas internacionales como ISO 27005:2011, ISO/IEC 27001:2013, 27002:2013, la metodología MAGERIT y el marco de trabajo COBIT para la gestión de seguridad de la información, que en algunos casos se han aplicado a instituciones hospitalarias; de igual forma se especifican artículos científicos relacionados al gobierno de las tecnologías y sistemas de información, proceso de gestión de riesgos en el desarrollo de software, la gestión del riesgo en la seguridad de información e implementación de sistemas nacionales de información de salud interoperables, por mencionar a los más resaltantes. Por último se considera una base teórica respecto que permita tener un mayor entendimiento en lo que consiste la gestión de seguridad de la información, el sistema de gestión de seguridad de la información, sistema de gestión de riesgos, marcos de referencia para implementar un sistema de gestión de riesgos, norma ISO para la calidad de un producto y definiciones de términos técnicos.

En el Capítulo III, realizamos una descripción detallada del método de Investigación, indicando las técnicas de recolección de datos utilizadas en nuestra investigación. Así como la descripción del modelo de gestión de riesgos propuesto y detallando la metodología a seguir, con el fin de mejorar la seguridad de la información, en el cual señalamos las cuatro fases de la metodología y sus respectivas actividades:

A. Identificación de los activos y sus amenazas
B. Análisis y evaluación
C. Tratamiento de los riesgos
D. Seguimiento y monitoreo de riesgos y de la seguridad de la información

Finalmente en este capítulo realizamos una propuesta de evaluación de calidad de nuestro modelo de gestión de riesgos, el cual es una adaptación del estándar ISO/IEC 25010 Calidad del producto software.

En el Capítulo IV, se presentan los resultados de la investigación, abordando las siguientes etapas establecidas para el desarrollo:

- Análisis de la situación actual de la gestión de la seguridad de los activos de la información relacionados con los sistemas de información de gestión hospitalaria, en donde se identifica, seleccionan y analizan los activos críticos dentro del servicio de gestión hospitalaria.
- Análisis de la situación actual de las políticas de seguridad de información del Ministerio de Salud sobre los activos de la información relacionados con los sistemas de información de gestión hospitalaria del Hospital Regional de Lambayeque.
- Análisis de la los datos recolectados por medio de las encuestas a los usuarios y administradores jefatura responsables de los sistemas de información de gestión hospitalaria del Hospital Regional de Lambayeque
- Modelo de gestión de riesgos, en donde se describen los componentes y sus interrelaciones entre sí para conformar nuestro modelo de gestión de riesgos de seguridad de información propuesto como proyecto de investigación.
- Desarrollo de la Metodología de gestión de riesgos. A través de un ejemplo se detalla cómo se gestionarían los riesgos en el Hospital Regional de Lambayeque con la aplicación de nuestro modelo de gestión de riesgos y el empleo de la metodología asociada, a raíz de esto se aprecia el desarrollo de cada etapa que comprende la metodología de gestión de riesgos, tomando como referencia un activo de información que tiene actualmente el Hospital Regional de Lambayeque.
- Valoración del modelo de gestión de riesgos basado en las normas ISO/ 27005 y metodología MAGERTI propuesto, por medio de la herramienta de valoración de juicio de expertos en seguridad de la información en base a los criterios de suficiencia, claridad, coherencia, relevancia.

En el Capítulo V, realizamos una discusión de los resultados obtenidos en nuestra investigación.

En el Capítulo VI, se plantean las conclusiones referentes al logro de los objetivos planteados en la investigación y las recomendaciones asociadas a los resultados obtenidos de aplicar el modelo de gestión de riesgos de seguridad de la información así como de la metodología que emplea, en el Hospital Regional de Lambayeque.

En el Capítulo VII, indicamos las referencias bibliográficas que hemos utilizado para el desarrollo de nuestra investigación.

En el Capítulo VIII, presentamos una lista de documentación anexada que forma parte de nuestra investigación, documentación que nos permitió realizar un tratamiento de información y obtener los resultados en nuestra investigación.

INDICE

INDICE DE TABLAS

INDICE DE ILUSTRACIONES

CAPITULO I. PLANTEAMIENTO DEL ESTUDIO

1.1. Descripción de la problemática

Actualmente el Hospital Regional de Lambayeque maneja un gran volumen de información derivada de la atención de todos sus pacientes e información de gestión institucional y personal de trabajo, información que debe ser procesada de forma continua para brindar un servicio adecuado a los pacientes y para la gestión del mismo hospital.

El Ministerio de Salud reconoció que la información es un activo importante, por lo cual requiere de protección, para lo cual requiere del compromiso de los directivos para asegurar la efectiva gestión de la seguridad de la información.

Dentro de este contexto el Hospital Regional de Lambayeque, se evidenció que la gestión de la información no forma parte de un proyecto de seguridad de la información en la que se puedan gestionar los riesgos a los que podría estar expuesta la información del hospital a los diferentes tipos de robo de información o ataques que involucren a la disponibilidad, confidencialidad e integridad de la información personal de pacientes y trabajadores, la cual podría ser vulnerada.

El Hospital Regional de Lambayeque, actualmente no cuenta con un sistema de gestión de riesgos que le permita:

- Identificar todos los activos de información a los cuales se tienen que proteger en base a su importancia y criticidad.
  Conocer la importancia de los activos de la información permitirá realizar una priorización sobre los controles para el tratamiento de los riesgos de la seguridad de la información.
- Identificar los posibles escenarios de riesgos, es decir identificar las potenciales amenazas que pueden materializarse para atacar un activo de información. En el escenario de riesgo se describe la relación amenaza-vulnerabilidad. Este es un trabajo que debe realizarse en cada área o por cada proceso, con las personas que participan en ello.

- Realizar una valoración sobre los impactos y probabilidades de ocurrencia de las amenazas, de tal forma que se pueda estimar los niveles de exposición al riesgo y por tanto establecer brechas de seguridad.

Es importante para el Hospital Regional de Lambayeque concientizar a su personal sobre la relevancia de la gestión de riesgos para los activos de la información, porque permite valorarlos e identificar oportunamente las vulnerabilidades que podrían ser aprovechadas por diversas amenazas, impactando sustancialmente en la continuidad de los procesos del negocio y en los principios de la seguridad de la información del HRL.

Desarrollar una metodología que permita implementar el modelo de gestión de riesgos para este proyecto, con el fin de orientar al personal calificado del Hospital Regional de Lambayeque en la gestión de riesgos alineada a las políticas de la institución, que permita la implementación de un sistema de gestión de seguridad de la información adecuado, que salvaguarde y garantice la continuidad de sus procesos y activos de la información

1.1.1. Efectos del problema

El problema descrito inicialmente, nos permite que identifiquemos los efectos que describimos a continuación:

- Dentro del Hospital Regional de Lambayeque se tiene un alto volumen de activos de la información que si no son valorados adecuadamente, no se podría determinar cuáles son los más importantes en la organización, de manera que se puedan gestionar los riesgos asociados y al cual se priorice la implementación de medidas para su protección.

- Al no tener identificados las vulnerabilidades de los activos de información, no se tendría conocimiento de los riesgos de seguridad de información asociados a dichos activos, de manera que se puedan

implementar los mecanismos de protección adecuados para su mitigación.

- Al no tener identificados las amenazas que afectan a los activos de información, no se tendría conocimiento de los riesgos de seguridad de información asociados a dichos activos, de manera que se puedan implementar los mecanismos de protección adecuados para su mitigación.

- Si no se realiza una estimación del nivel de riesgo asociado a los activos de información, no podemos determinar un adecuado mecanismo de protección para mitigar las amenazas identificadas.

- En caso de no elegir adecuadamente los mecanismos de protección para la mitigación de los riesgos asociados a los activos de información, las amenazas existentes continuarían aprovechándose de las vulnerabilidades que se tienen y por ende el riesgo residual podrían continuar a un mismo nivel que el riesgo inherente identificado.

1.2. Planteamiento del problema empírico

El Hospital Regional de Lambayeque no realiza una gestión de riesgos asociada a los activos de información, lo cual no permite que se pueda preservar la disponibilidad, confidencialidad, integridad, trazabilidad y autenticidad de la información, y por lo tanto, no se tiene un adecuado sistema de gestión de la seguridad de la información.

1.3. Formulación del problema científico

¿En qué medida un modelo de gestión de riesgo basado en las normas ISO 27005 y la metodología MAGERIT, contribuye al cumplimiento de las políticas de

seguridad de la información planteadas por el Ministerio de Salud y mejorar la gestión seguridad de la información en el Hospital Regional de Lambayeque?

1.4. Hipótesis

Un modelo para la gestión de riesgos de la seguridad de la información basado en las normas ISO 27005 y la metodología MAGERIT contribuye al cumplimiento de las políticas de seguridad de la información planteadas por el Ministerio de Salud y mejora la gestión de la seguridad de la información en el Hospital Regional de Lambayeque

Por lo tanto el diseño para la contrastación de la hipótesis, es un modelo descriptivo, como se muestra a continuación:

$$M_1: \quad O_1 \longrightarrow O_2 \; O_3 \; Y$$

Donde:

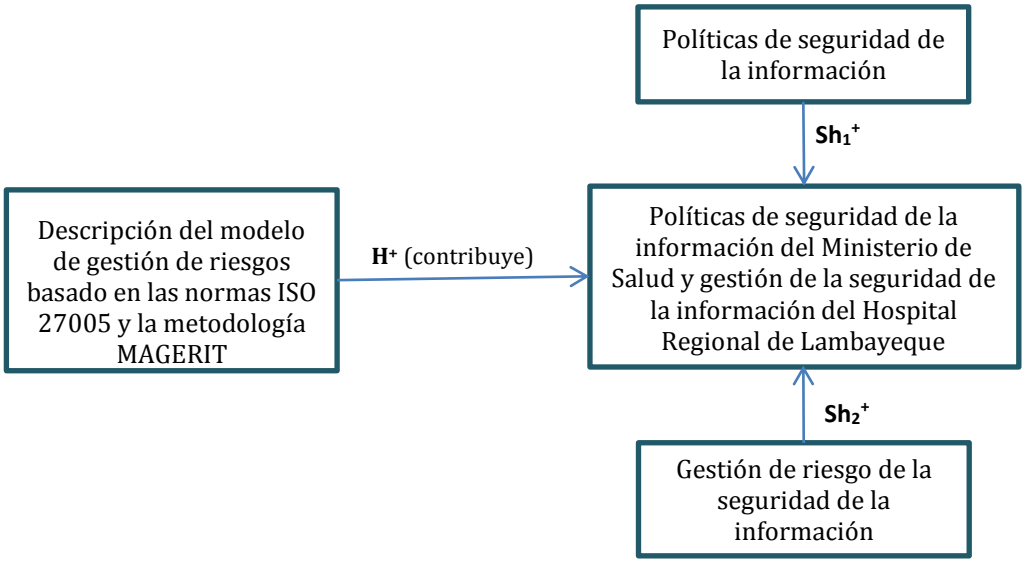
O_1: Descripción del modelo de gestión de riesgos basado en las normas ISO 27005 y la metodología MAGERIT

Y: Políticas de seguridad de la información del Ministerio de Salud y gestión de la seguridad de la información del Hospital Regional de Lambayeque

O_2: Análisis del cumplimiento de las políticas de seguridad de la información del Ministerio de Salud

O_3: Valoración del juicio de expertos para calificar la validez y utilidad del modelo de gestión de riesgo

Modelo conceptual de la investigación:



Desglose del planteamiento de hipótesis:

- Sub hipótesis 1: con respecto cumplimiento de las políticas de seguridad de la información del Ministerio de Salud:

  H_i: El modelo de gestión de riesgos basado en las normas ISO 27005 y la metodología MAGERIT contribuye al cumplimiento de políticas del Ministerio de Salud

  H_0: El modelo de gestión de riesgos basado en las normas ISO 27005 y la metodología MAGERIT no contribuye al cumplimiento de políticas del Ministerio de Salud

- Sub hipótesis 2: con respecto a la mejora de la gestión de seguridad de la información en el Hospital Regional de Lambayeque:

  H_i: El modelo de gestión de riesgos basado en las normas ISO 27005 y la metodología MAGERIT contribuye con la mejora de la gestión de seguridad de la información del Hospital Regional de Lambayeque

  H_0: El modelo de gestión de riesgos basado en las normas ISO 27005 y la metodología MAGERIT no contribuye con la mejora de la gestión de seguridad de la información del Hospital Regional de Lambayeque

1.5. Objetivos de la investigación

1.5.1. Objetivo general

Adecuar un modelo de gestión de riesgos de la seguridad de la información, tomando como referencia la ISO /IEC 27005 y la metodología MAGERIT, que permita cumplir las políticas planteadas por el Ministerio de Salud para mejorar la gestión de riesgos de los activos de la información del Hospital Regional de Lambayeque.

1.5.2. Objetivos específicos

- Determinar el cumplimiento de las políticas de seguridad de la información propuestas por el ministerio de Salud como parte de la gestión de riesgos de seguridad de la información del Hospital Regional de Lambayeque.

- Determinar la validez y utilidad del modelo de gestión de riesgos propuesto, para mejorar la gestión de riesgos de seguridad de la información del Hospital Regional de Lambayeque.

1.6. Alcances y limitaciones

En la elaboración del presente trabajo de investigación, se toma en cuenta los siguientes alcances:

- La investigación se realizará en el sector de gestión hospitalaria que posea un sistema de información en el Hospital Regional de Lambayeque, ubicado en la ciudad de Chiclayo.
- El análisis y evaluación de riesgos serán realizado para los activos de información críticos identificados como "priorizados" en la etapa de identificación de nuestra metodología, de manera que al proponerse mecanismos de protección, se tenga prioridad sobre aquellos activos de mayor importancia para el Hospital Regional de Lambayeque.
- La investigación se centrará en la elaboración de un modelo de gestión de riesgos de la información en base a la metodología MAGERIT V3 y a la ISO/IEC 27005.

Se toma en cuenta las siguientes limitaciones:

- Contamos con limitaciones de recursos humanos y tiempo para abarcar todos los procesos del Hospital Regional de Lambayeque, para esta investigación.
- Los usuarios involucrados en los procesos de estudio no cuentan con disponibilidad para brindarnos mayor detalle sobre los procesos involucrados. Existen procesos no documentados por las áreas funcionales.
- No existen procesos definidos por las áreas funcionales.
- Los procesos identificados no han sido automatizados.

CAPITULO II. DISEÑO TEÓRICO

2.1. Estado del arte

La gestión de la seguridad de la información cobra mayor relevancia a razón del paso de los años, debido a que las empresas e instituciones toman mayor conciencia en la importancia de controlar los riesgos a los que se exponen sus activos de información; es así que se muestran algunas de las investigaciones halladas, en donde se refleja el interés que toman las diversas instituciones en el uso de estándares internaciones y buenas prácticas en gestión de riesgos para fortalecer sus sistema de gestión de seguridad de la información:

Se ha determinado en investigaciones preliminares, que el uso de estándares internacionales como la ISO/IEC 27001:2013 e ISO/IEC 27002:2013, la incorporación de buenas prácticas en materia de seguridad de información y la aplicación de la Metodología MAGERIT v.3.0 para el análisis y evaluación de riesgos, repercuten directamente en una efectiva gestión de riesgos de seguridad de la información, la cual garantiza el cumplimiento de los pilares de seguridad de la información: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad (Baca, V. 2016). Diseño de un sistema de gestión de la seguridad de la información para la Unidad de gestión educativa local – Chiclayo, Revista Ingeniería: Ciencia, tecnología e innovación. Lambayeque.

Como antecedente a nuestra actual investigación, se concluye que la implementación de estándares internacionales como la ISO 27002 e ITIL, proporcionan diferentes ventajas a cualquier institución, como son: Aumento de la seguridad efectiva de los

sistemas de información, correcta planificación y gestión de la seguridad, garantías de continuidad del negocio, mejora continua a través del proceso de auditoría interna, incremento de los niveles de confianza en nuestros clientes y socios, aumento del valor comercial y mejora de la imagen de la organización (Miranda, K. 2013), Guía metodológica para Implementar un sistema de gestión de seguridad en instituciones, Universidad de Piura. Piura.

Como parte de la investigación, se concluye que es muy útil incorporar un enfoque de gestión de riesgos en las arquitecturas basadas en servicios (SOA), mediante el uso del estándar ISO / IEC 27005, por la razón en que estos tipos de servicios al ofrecer nuevas oportunidades para la interconexión de sistemas, introduce nuevas vulnerabilidades, y por lo tanto, nuevos riesgos (Lalanne V., Munier M., Gabillon A. 2013). Gestión de riesgos de seguridad de la información en un mundo de servicios. Conferencia internacional ASE / IEEE sobre privacidad, seguridad, riesgo y confianza. Francia.

Se concluye que para establecer los niveles de riesgos de los activos de información, se debe definir un proceso de análisis de riesgos de activos de información, en el contexto de un SGSI alineado al estándar ISO/IEC 27001:2005, siendo muy importante la sensibilización a los usuarios, en los concerniente al uso de buenas prácticas en seguridad de información y adopción de estándares establecidos. El proceso podría utilizar el marco referencial Magerit (Metodología de análisis y gestión de riesgos de tecnologías de información), e incorporar el Análisis de impacto de negocio(BIA), el cual tiene por objetivo evaluar el impacto sobre los procesos de negocio, debido a la no disponibilidad de los servicios de tecnologías de información, lo que posteriormente se deriva en la obtención del nivel de criticidad para cada activo de información, lo cual es indispensable para establecer el nivel de riesgo de los mismos (Sotelo, M. & Torres, J. & Rivera, J. 2012). Un Proceso práctico de análisis de riesgos de activos de información.

Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una guía de Implementación, permite la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. Con un plan de tratamiento de riesgos, se permitió la

disminución de los niveles de riesgos con respecto a los activos de información, considerados amenazas y vulnerabilidades en la institución. Finalmente con un plan de capacitación y concienciación puesto en marcha en la institución, se puede incrementar el porcentaje de conocimiento por parte del personal en temáticas orientadas a políticas, estrategias de seguridad que beneficien a la institución, teniendo como resultado un personal comprometido con la seguridad en favor de la institución (Alcántara, J. 2015). Elaboración de una guía de implementación de la seguridad basada en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P en la ciudad de Chiclayo.

Se concluye que es muy importante que toda institución que fomente una educación transformadora e innovadora a través del uso de tecnologías de información, como primer paso identifique los riesgos implicados, de manera que se pueda tomar importancia en: i) proteger a los niños en los medios digitales, ii)el deber de la escuela en educar a la familia y a la comunidad en relación a las tecnologías de información, iii) capacitar a los profesores para agregar tecnologías en sus prácticas, entre otros (Prioste, C. 2016). Tecnología, educación e innovación: riesgos y oportunidades. J. Eng. Technol. Vol.5, N°2, 72.-81

2.2. Base teórica

2.2.1 Gestión de los riesgos corporativos

Las diversas entidades en el contexto actual, luchan por competir en un mercado en el cual quien genera mayor valor agregado ya sea en sus productos o servicios, es quien tiene mayor probabilidad de sobrevivir a largo plazo en el mercado. Toda esta competencia genera incertidumbre entre los empresarios, lo cual nos lleva un análisis profundo de los riesgos a los que pueda exponerse.

De esta manera es que la gestión de riesgos, es quien trata mantener controlada la incertidumbre que genera la competencia y los riesgos que puedan estar presentándose, al igual que identificar de conveniente las oportunidades que le brinda los diversos escenarios de competencia diaria.

El informe COSO nos define la gestión de riesgos corporativos, como: "…un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos…" (Ambrosone, 2007, p.6)

Su finalidad es la de lograr alcanzar los objetivos de la entidad, las que se clasifican en:

- Estrategia: se refieren a los objetivos a alto nivel, que son alineados a la misión de la entidad.
- Operaciones: cuyos objetivos vinculados se relacionan al uso eficiente de los recursos.
- Información: hace referencia a los objetivos de fiabilidad de la información proporcionada.
- Cumplimiento: estos objetivos están relacionados al cumplimiento de normas y leyes a los que estén afectos.

De igual manera COSO nos permite identificar diversos componentes que intervienen en la gestión de riesgos corporativos:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos
- evaluación de riesgos
- Respuesta al riesgo
- Actividades de control
- información y comunicación
- Supervisión

La gestión de riesgos corporativos incluye las siguientes capacidades:

- Alinear el riesgo aceptado y la estrategia; después de una evaluación de los escenarios que presenta la entidad, el alta dirección evalúa el riesgo que puede aceptar la entidad, estableciendo los objetivos estratégicos y gestionando los riesgos asociados.
- Mejorar las decisiones de respuesta a los riesgos; la gestión de riesgos corporativos permite identificar los riesgos y evaluar si estos se pueden evitar, reducir, compartir o aceptar.
- Reducir las sorpresas y pérdidas operativas; permite que los potenciales eventos sean identificados oportunamente y establecer estrategias para combatirlos, eludirlos o atenuarlos, reduciendo las sorpresas no deseadas y pérdidas eventuales.
- Identificar y gestionar la diversidad de riesgos para toda la entidad; permitiendo plantear estrategias para la mitigación de los riesgos atenuando o anulando el impacto que puedan generar.
- Aprovechar las oportunidades; al identificar adecuadamente los potenciales eventos, se pueden aprovechar las oportunidades que puedan presentarse de modo proactivo.

- Mejorar la dotación de capital; para evaluar eficazmente las necesidades de la entidad.

2.2.2 Seguridad de información

Tam, F.(2009), lo define como la característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organización y herramientas especializadas a efectos que dicha información cumpla los criterios de confidencialidad, integridad y disponibilidad.

2.2.2.1 Criterios de la seguridad de información

Tam, F.(2009). Lima, en la Circular N° G-140-2009 define a los criterios de seguridad de información de la siguiente manera:

- Confidencialidad: La información debe ser accesible sólo a aquellos que se encuentren debidamente autorizados.
- Integridad: La información debe ser completa, exacta y válida.
- Disponibilidad: La información debe estar disponible en forma organizada para los usuarios autorizados cuando sea requerida.

Amutio, M & Candau, J & Mañas, J (2012).Madrid, adicionalmente considera como criterios de seguridad de información a los siguientes:

- Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

2.2.3 Sistema de gestión de seguridad de información

Alcántara, J. (2015) define el sistema de gestión de seguridad de información como el concepto central sobre el que se construye ISO 27001. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Villena, M. (2006) lo define como una forma sistemática de administrar la información sensible de una institución, para que permanezca segura. Abarca a las personas, los procesos y las tecnologías de información. La forma total de la seguridad de la información, y la integración de diferentes iniciativas de seguridad necesitan ser administradas para que cada elemento sea completamente efectivo. Aquí es donde entra el sistema de gestión de seguridad de la información que permite coordinar esfuerzos de seguridad con mayor efectividad.

2.2.4 Sistema de gestión de riesgos

2.2.4.1 El riesgo

Cañas, L. (2009) la define como la probabilidad de que, la ocurrencia de un suceso adverso afecte a la entidad e impacte en su habilidad para lograr sus objetivos estratégicos y por ende la capacidad de cumplir su misión y visión.

Soldano, A. (2009) define al riesgo como la probabilidad de que una amenaza se convierta en un desastre. Para poder "medir" el riesgo la expresión más generalizada es el producto de la probabilidad de la ocurrencia del evento considerado por las consecuencias esperadas.

Es el grado esperado de pérdida de los elementos en riesgo debido a la presencia de peligros. Puede ser expresado en términos de perdidas, personas heridas, daños materiales e interrupción de actividad económica (Salazar, Cortez & Mariscal,2002).

Es la expresión probabilidad e impacto de un evento con el potencial de influenciar el logro de los objetivos de una organización. La frase "probabilidad e impacto de un evento" implica que, como mínimo, un análisis cualitativo o cuantitativo es necesario para tomar una decisión teniendo en cuenta los riesgos mayores o las amenazas que puedan existir para lograr los objetivos de una organización (Bueno, Correa & Echeverry, 2010).

El equipo de investigación, define al riesgo como la probabilidad de materialización de amenazas, que afectan la economía, reputación y activos de información de una organización, y es originada en determinado tiempo, por distintos factores contemplados en el catálogo de amenazas de la metodología MAGERIT.

2.2.4.1.1 Factores de riesgos

Tam, F.(2009). Lima, en la Resolución S.B.S N° 2116-2009 clasifica a los factores de riesgo en:

- Procesos internos: Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que pueden tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos.

- Personal: Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje,

fraude, robo, paralizaciones, apropiación de información sensible, entre otros.

- Tecnología de información: Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos.

- Eventos externos: Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores.

2.2.4.1.2 Tipos de riesgo

Tam, F.(2009). Lima define los siguientes tipos de riesgo:

- Riesgo estratégico: Forma como se administra la empresa, directrices de la alta gerencia.
- Riesgo de crédito: Es la posibilidad de pérdida por la incapacidad o falta de voluntad de los deudores, contrapartes, o terceros obligados, para cumplir sus obligaciones contractuales registradas dentro o fuera del balance.
- Riesgo estratégico: Es la posibilidad de pérdidas por decisiones de alto nivel asociadas a la creación de ventajas competitivas sostenibles. Se encuentra relacionado a fallas o debilidades en el análisis del mercado, tendencias e incertidumbre del entorno, competencias claves de la empresa y en el proceso de generación e innovación de valor.

- Riesgo operacional: Es la posibilidad de pérdidas debido a procesos inadecuados, fallas del personal, de la tecnología de información, o eventos externos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y de reputación.

- Riesgo técnico: Es la posibilidad de pérdidas o modificación adversa del valor de los compromisos contraídos en virtud de los contratos de seguros, de reaseguros y de coaseguros. En el caso de los seguros de no vida, se consideran las fluctuaciones relacionadas con la frecuencia, la severidad, y la liquidación de los siniestros. Para el caso de los seguros de vida, esto puede incluir la posibilidad de pérdidas por variaciones en el nivel, la tendencia o la volatilidad de las tasas de mortalidad, longevidad, invalidez, morbilidad, renovación o rescate de los contratos de seguros, entre otros parámetros y supuestos, así como de los gastos de ejecución de dichas obligaciones.

– Riesgo de reputación: La posibilidad de pérdidas por la disminución en la confianza en la integridad de la institución que surge cuando el buen nombre de la institución es afectado. El riesgo de reputación puede presentarse a partir de otros riesgos inherentes en las actividades de una institución.

2.2.3.1.3. **Contribuciones de la gestión de riesgos**

La gestión de riesgos en la seguridad de la información, debe contribuir a:

- Identificación de riesgos.
- evaluación de riesgos: Consecuencias para el riesgo y Probabilidad de ocurrencia.
- Comunicación y entendimiento de estos riesgos: probabilidades y consecuencias.
- Orden de prioridad para el tratamiento de los riesgos.
- Priorización de las acciones para reducir la ocurrencia de riesgos.

- Participación de los interesados para la toma de decisiones de la gestión de riesgos y su estado.
- Eficacia y monitoreo del tratamiento del riesgo.
- monitoreo y revisión del riesgo y la gestión del riesgo.
- Captura de información para mejorar el enfoque de la gestión del riesgo.
- Educación de directores y personal acerca de los riesgos y las acciones para mitigarlas.

2.2.4.2 Gestión de riesgos de tecnologías de la información

Es el proceso en el que se tratan los riesgos, para obtener un beneficio. Se centra en identificar y tratar riesgos, con el fin de añadir valor, aumentando la probabilidad de éxito o reduciendo la de fallo o incertidumbre. Debe ser un proceso continuo y de constante desarrollo, que se lleve a cabo en toda la estrategia, tratando los riesgos de actividades pasadas, presentes y futuras. Debe estar integrado en la cultura de la empresa, con políticas y programas dirigidos por la alta dirección. Debe convertir la estrategia en objetivos tácticos, asignando responsabilidades a los empleados por la gestión del riesgo, promoviendo así la eficiencia operacional (Bueno, Correa & Echeverry, 2010).

2.2.4.2.1 Proceso de la gestión de riesgos de tecnologías de la información

Ambrosone, M. (2007) define que el sistema de gestión de riesgos corporativos, en el marco COSO ERM, está conformado por ocho componentes relacionados entre sí, los cuales se listan brevemente a continuación:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos
- evaluación de riesgos
- Respuesta al riesgo

- Información y comunicación
- Supervisión

2.2.4.2.2 Etapas de la gestión del riesgo de TI

Tomando como referencia al ciclo de Deming (PHVA) en relación al estándar ISO 27005 e ISO 31000 en la gestión de riesgos, se listan las siguientes etapas con el objetivo de cumplir los principios de la seguridad de la información.

- **Planificar:** En esta etapa se establecen los objetivos, procesos y procedimientos para el proceso de gestión de riesgos.
- **Hacer:** En esta etapa se realiza la implementación de los controles, procesos, valoración y tratamiento de los riesgos.
- **Verificar:** En esta etapa se realiza la medición del desempeño de los procesos de seguridad de la información y se informa sobre los resultados obtenidos.
- **Actuar:** Establecer las políticas para la gestión de riesgos tecnológicos e implementar los cambios requeridos para la mejora de los procesos, se verifican los cambios y el cumplimiento de los indicadores que fueran establecidos desde la planificación.

Tabla 1.- Comparación entre ISO 27005 - ISO 31000

PHVA	ISO27005		ISO 31000
Planear			Mandato y compromiso de la dirección
	Definir plan de gestión de riesgos		Diseño del marco de trabajo para la gestión de riesgos
	Establecimiento del contenido		Entender la organización y su contexto
			Definir responsabilidades
			Recursos
			Integración con procesos

<table>
<tr><td rowspan="5"></td><td colspan="2"></td><td rowspan="10"></td><td colspan="2">Establecer mecanismos de comunicación</td></tr>
<tr><td>Identificación del riesgo</td><td rowspan="3">Valoración riesgo</td><td colspan="2" rowspan="4"></td></tr>
<tr><td>Estimación del riesgo</td></tr>
<tr><td>evaluación del riesgo</td></tr>
<tr><td colspan="2">Desarrollar el plan de tratamiento del riesgo</td></tr>
<tr><td colspan="2">Aceptación del riesgo</td><td colspan="2"></td></tr>
<tr><td rowspan="3">Hacer</td><td colspan="2"></td><td colspan="2">Establecer políticas para la gestión de riesgo</td></tr>
<tr><td colspan="2">Implementar el plan de tratamiento</td><td>Implementación del marco de trabajo para la gestión de riesgos</td><td>Implementar el proceso de gestión de riesgos</td></tr>
<tr><td colspan="2">Implementar plan de comunicación del riesgo</td><td colspan="2"></td></tr>
<tr><td>Verificar</td><td colspan="2">monitoreo y revisión del riesgo</td><td colspan="2">monitoreo y revisión del marco de trabajo</td></tr>
<tr><td>Actuar</td><td colspan="2">Mantener y mejorar el proceso de gestión</td><td colspan="2">Mejora continua del marco de trabajo</td></tr>
</table>

Fuente: Ramírez, A., Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005, pág 59

2.2.4.2.3 Componentes de la gestión del riesgo de tecnología de la información

El plan de tratamiento en la gestión de riesgos de seguridad de la información tiene distintos componentes importantes, tales como:

- **Agente de amenaza**: Entidad humana o no humana que explota una vulnerabilidad
- **Amenaza**: Todo hecho que potencialmente puede producir daño en los activos de una entidad.
- **Vulnerabilidad**: Debilidad que deja una puerta abierta y puede ser explotada por el actor de la amenaza;
- **Resultados**: El resultado de la explotación de una vulnerabilidad;

- **Impacto**: Consecuencias de los resultados no deseados. No confunda los resultados con los impactos.

2.2.4.3 Apetito y tolerancia al riesgo

Podemos definir al apetito al riesgo al nivel de exposición al riesgo que una organización se encuentra dispuesta a aceptar, con los cuales opera sin mayores problemas.

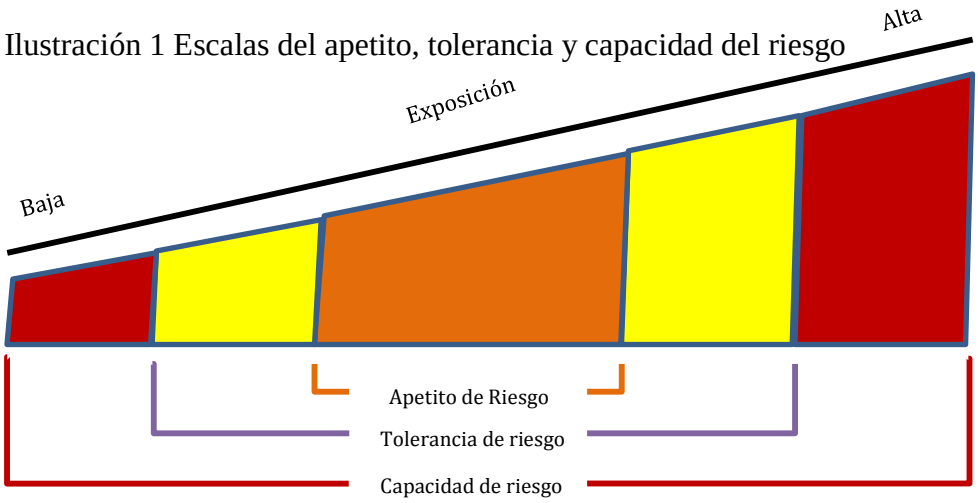
COSO define al apetito del riesgo como "el riesgo que está dispuesto a aceptar a aceptar en la búsqueda de la misión/visión de la entidad".

British Estándar 31100 se refiere al apetito del riesgo como "la cantidad y tipo de riesgo que una organización está preparada para afrontar, aceptar o tolerar".

Mientras que la **tolerancia al riesgo**, se considera a los límites de riesgo en los que una organización encuentra una adecuada seguridad, por lo cual no considera necesario la implementación de medidas de control que le permitan mantener asegurado su cotidiano funcionamiento.

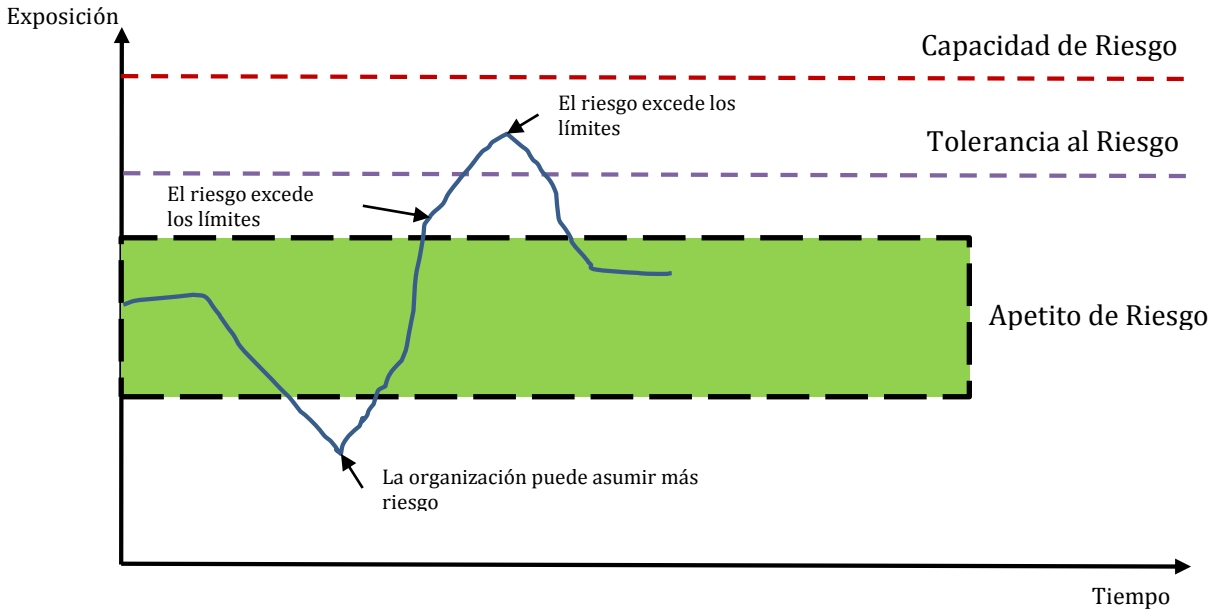
> COSO la define como el nivel aceptable de variación en los resultados o actuaciones de la compañía relativas a la consecución o logro de sus objetivos.
>
> El Instituto de auditores interno de España (2013) presentan las siguientes definiciones de apetito y tolerancia del riesgo:
>
> - **Apetito de riesgo:** Nivel de riesgo que la empresa quiere aceptar, aquel con el que se siente cómoda.
> - **Tolerancia de riesgo:** Desviación respecto al nivel en el que la empresa se siente cómoda. Sirve de alerta para evitar llegar al nivel que establece su capacidad.
> - **Capacidad de riesgo:** Nivel máximo de riesgo que la empresa puede soportar.

Ilustración 1 Escalas del apetito, tolerancia y capacidad del riesgo



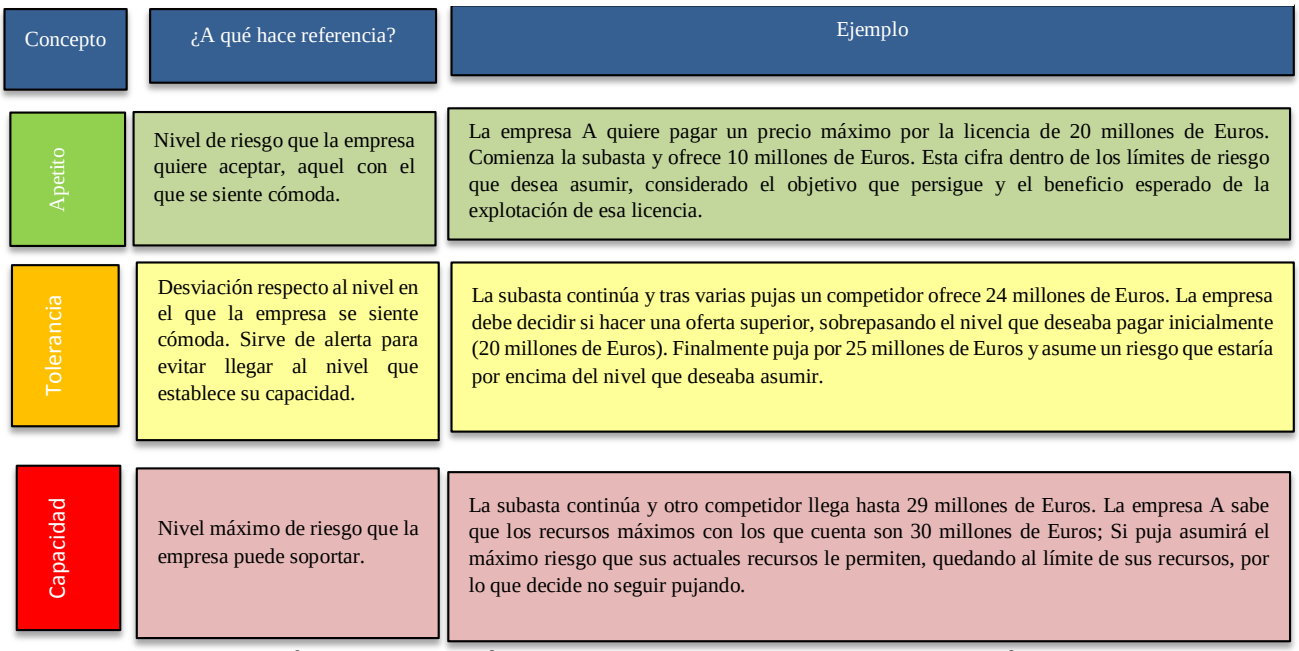
Fuente: Buenas prácticas en gestión de riesgo. Fábrica del pensamiento. Pág. 7

Ilustración 2 Apetito de riesgo en base al tiempo y exposición del riesgo



Fuente: Buenas prácticas en gestión de riesgo. Fábrica del pensamiento. Pág. 17

Ilustración 3 Ejemplos sobre apetito, tolerancia y capacidad de riesgos



Concepto	¿A qué hace referencia?	Ejemplo
Apetito	Nivel de riesgo que la empresa quiere aceptar, aquel con el que se siente cómoda.	La empresa A quiere pagar un precio máximo por la licencia de 20 millones de Euros. Comienza la subasta y ofrece 10 millones de Euros. Esta cifra dentro de los límites de riesgo que desea asumir, considerado el objetivo que persigue y el beneficio esperado de la explotación de esa licencia.
Tolerancia	Desviación respecto al nivel en el que la empresa se siente cómoda. Sirve de alerta para evitar llegar al nivel que establece su capacidad.	La subasta continúa y tras varias pujas un competidor ofrece 24 millones de Euros. La empresa debe decidir si hacer una oferta superior, sobrepasando el nivel que deseaba pagar inicialmente (20 millones de Euros). Finalmente puja por 25 millones de Euros y asume un riesgo que estaría por encima del nivel que deseaba asumir.
Capacidad	Nivel máximo de riesgo que la empresa puede soportar.	La subasta continúa y otro competidor llega hasta 29 millones de Euros. La empresa A sabe que los recursos máximos con los que cuenta son 30 millones de Euros; Si puja asumirá el máximo riesgo que sus actuales recursos le permiten, quedando al límite de sus recursos, por lo que decide no seguir pujando.

Fuente: Buenas prácticas en gestión de riesgo. Fabrica del pensamiento. Pág. 18

2.2.4.4 Brechas de seguridad

Las brechas de la seguridad muestran las vulnerabilidades importantes dentro de una institución, porque deja puertas abiertas a distintos mecanismos que pueden infiltrarse y vulnerar la información, para sustraerla, corromperla y utilizarla en con el objetivo de perjudicar a la empresa afectada.

Algunas de las brechas más comunes que suelen estar expuestas las empresas, son:

- **Ataques mediante emails**: El emisor suplanta la identidad e invita al usuario a descargarse un archivo, de esta forma instala el malware en nuestro equipo y cifra su información, y solicita un rescate para recuperarla.
- **Comunicaciones inseguras y robo de información**: Las empresas pueden sufrir la sustracción de información sensible, con fines delictivos o de competencia desleal.

- **Software desactualizado**: El software que no cuenta con un soporte y mantenimiento adecuado, es vulnerable ya que no cuenta con las actualizaciones necesarias para su correcto funcionamiento.
- **Falta de comunicación sobre las políticas de seguridad**: Todos los empleados deben saber cuáles son las políticas de seguridad establecidas que deben de seguirse para contribuir a la seguridad de la Empresa.
- **Accesos no autorizados**: Los empleados no cuentan con las restricciones suficientes para ingresar a zonas donde se resguardan activos importantes, o políticas de que limiten el uso de la información a la que tienen acceso, o incluso política para el control de accesos remotos a las redes interna de la institución.

2.2.5 Marcos de referencia para implementar un sistema de gestión de riesgos

2.2.5.1 ISO 27005: Gestión de riesgos de la seguridad de la información

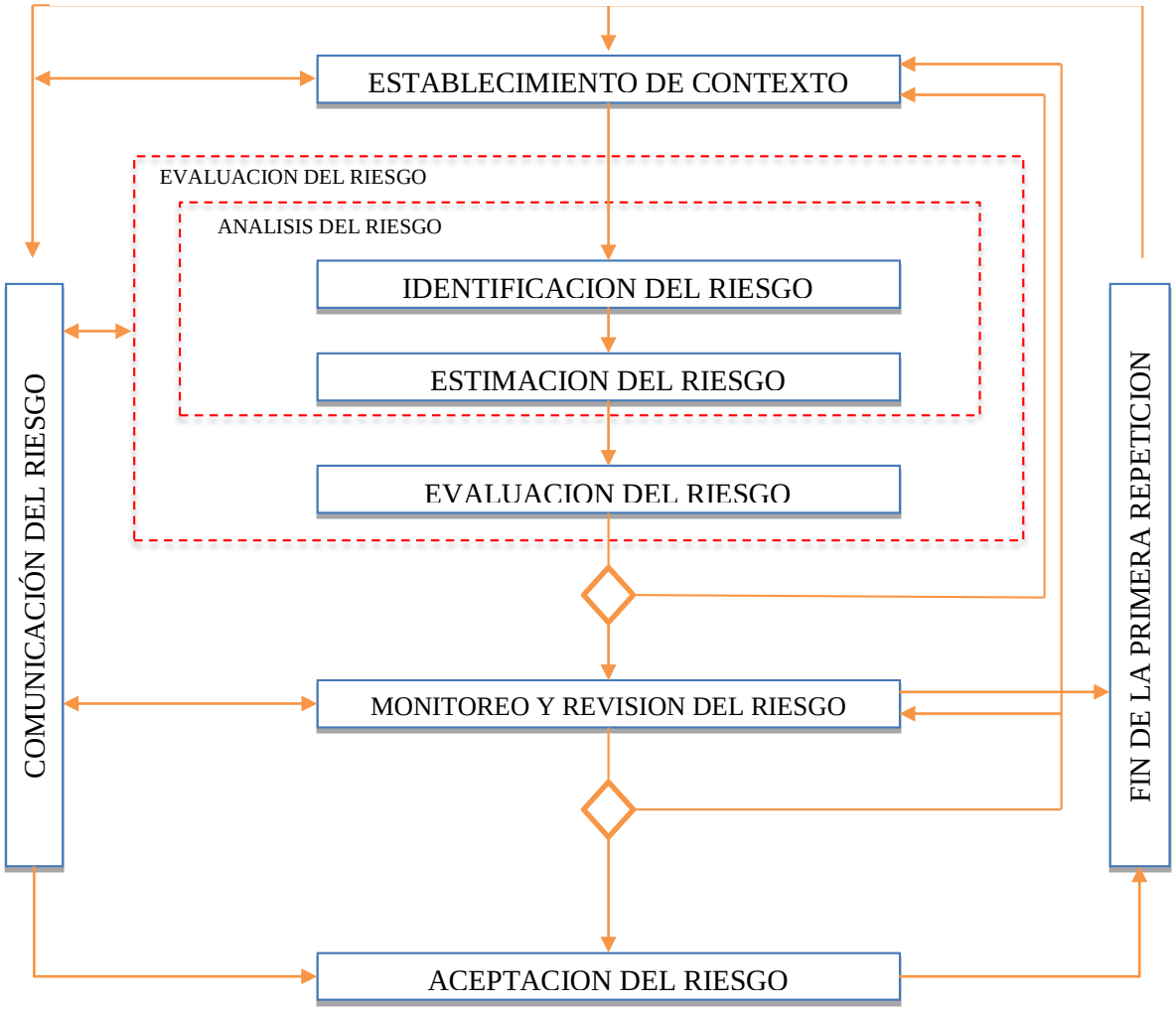
La gestión de riesgos en la seguridad de la información debería es parte integral de todas las actividades de seguridad de la información, y se debería aplicar a la implementación y funcionamiento continuo en un sistema de gestión de seguridad de la información.

La norma ISO 27005, es la norma internacional que se ocupa de brindar las directrices para realizar la gestión de riesgos de seguridad de la información, la cual puede aplicarse a las todo tipo de instituciones.

La norma ISO 27005, no recomienda ninguna metodología específica para realizar la gestión de riesgos de la seguridad de la información bajo las directrices ya establecidas, por lo cual queda abierta la posibilidad de elegir dicha metodología a la institución misma.

El proceso de gestión de riesgos en la seguridad de la información se puede aplicar a la organización en su totalidad, un aparte de ella, un sistema de información existente o planificada, o a los mecanismos de protección.

Ilustración 4 Proceso de la gestión de riesgos en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o del tratamiento del riesgo.



Fuente: ISO/IEC 27005:2011 Information technology – Security techniques information security risk management

En un sistema de gestión de seguridad de información:

Primero se establece el contexto, luego se valora el riesgo, si ésta suministra información suficiente para determinar las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada se sigue el tratamiento del riesgo.

Si la información no es suficiente, se lleva a cabo otra iteración de la valoración del riesgo.

La eficiencia del tratamiento del riesgo depende de los resultados de la valoración del riesgo, es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable del riesgo residual. En esta situación se puede requerir otra iteración de valoración del riesgo con cambios en los parámetros del contexto.

La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la organización, principalmente para la implementación de mecanismos de protección que requieren de aprobaciones de presupuestos.

Durante todo el proceso de gestión de riesgos de seguridad de la información es importante que los riesgos y su tratamiento se comuniquen a los directores y al personal operativo.

Tabla 2 .- Tareas a realizar por cada fase del ciclo de Deming

PLANIFICACIÓN	− Establecimiento del contexto. − Valoración del riesgo. − Desarrollo del plan de tratamiento. − Aceptación del riesgo.
HACER	− Implementar acciones y controles. (Implementación del plan de tratamiento del riesgo)
VERIFICAR	− Revisión de las valoraciones y tratamiento del riesgo. (monitoreo y revisión continuos del riesgo)
ACTUAR	− Se llevan a cabo todas las acciones incluyendo la aplicación adicional de gestión del riesgo en seguridad de la información. (Mantener y mejorar el proceso de gestión)

Fuente: Fuente: ISO/IEC 27005:2011 Information technology – Security techniques information security risk management

2.2.5.2 MAGERIT

La Secretaría de Estado de Administración Pública (2012), menciona que MAGERIT implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de información.

MAGERIT (Metodología de análisis y gestión de riesgos), es un método formal para investigar los riesgos que soportan los sistemas de información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos, con el fin de preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

MAGERIT ha sido elaborada por un equipo interdisciplinar del comité técnico de seguridad de los sistemas de información y tratamiento automatizado de datos personales, SSITAD, del consejo superior de informática, en España, y nos proporciona un catálogo de amenazas, un catálogo de salvaguardas y una forma de cálculo para evaluar los riesgos de seguridad de la información, a diferencia de la ISO 27005, en la cual nos señala el marco general en sus directrices.

Esta metodología (MAGERIT) se compone de cuatro fases:

1. Planificación del Proyecto de riesgo; en el cual se realizan las estimaciones iniciales de los riesgos que pueden afectar al sistema de la información.

2. Análisis de riesgo; en esta fase se estima el impacto que tendrán los riesgos en la organización.
3. gestión de riesgo: de tal manera que se determinen las posibles soluciones para cada riesgo.

4. Selección de mecanismos de protección; se eligen los mecanismos que implementarán las soluciones de la fase anterior.

El proceso de gestión de los riesgos que vulneran los controles de seguridad de información comprende 2 etapas: Análisis de riesgos y tratamiento de riesgos:

- **Análisis de riesgos**, que permite identificar los riesgos que tiene la organización y estimar el impacto que podría pasar, en caso los riesgos lleguen a materializarse.
- **Tratamiento de los riesgos**, que permite organizar la defensa concienzuda y prudente de la organización para mitigar el nivel de exposición de los riesgos identificados, defendiéndola para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

  El análisis de riesgos considera los siguientes elementos:

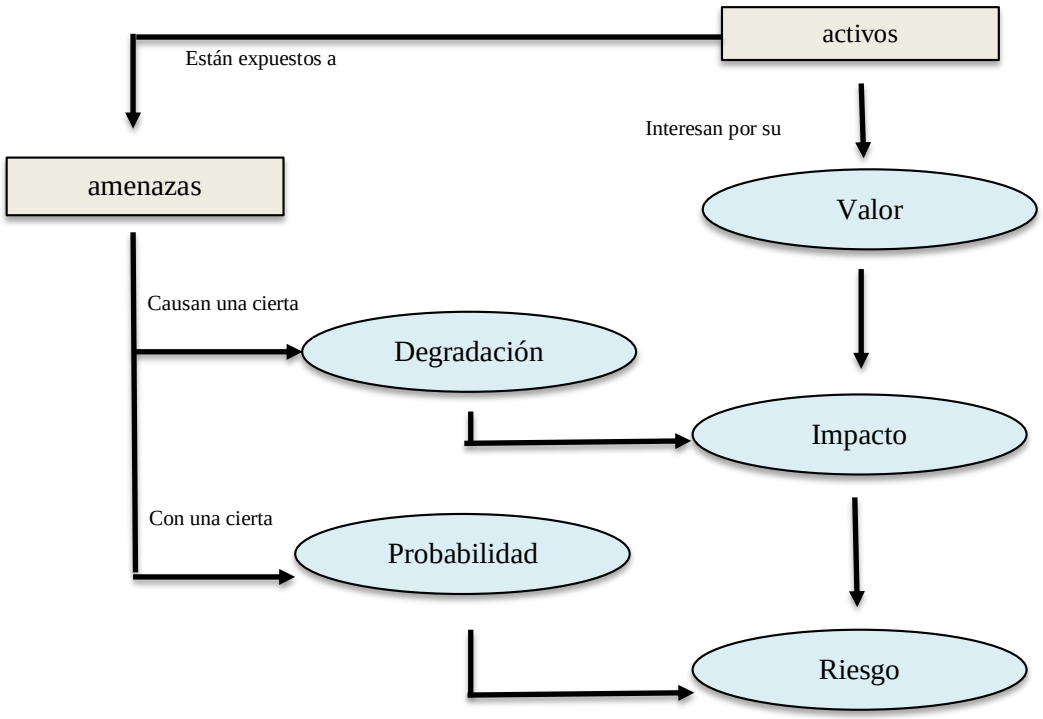
- **Activos**, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la organización
- **Amenazas**, que son situaciones que pueden suceder a los activos causando un perjuicio a la organización
- **Mecanismos de protección** (o contra medidas / salvaguardas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- **El Impacto**: Lo que podría pasar
- **El riesgo**: Lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y luego poder emprender la fase de tratamiento.

Ilustración 5 Elementos del análisis de riesgos potenciales



Fuente: Secretaría de Estado de Administración Pública (2012). *MAGERIT-versión 3.0. Metodología de análisis y gestión de riesgos de los sistemas de información.*

La Metodología del análisis y tratamiento del riesgo (MAR) comprende:

MAR.1: Caracterización de los activos

MAR.11 – Identificación de los activos

MAR.12 – Dependencias entre activos

MAR.13 – Valoración de los activos

MAR.2: Caracterización de las amenazas

MAR.21 – Identificación de las amenazas

MAR.22 – Valoración de las amenazas

MAR.3: Caracterización de las salvaguardas

MAR.31 – Identificación de las salvaguardas pertinentes

MAR.32 – Valoración de las salvaguardas

MAR.4: Estimación del estado de riesgo

MAR.41 – Estimación del impacto

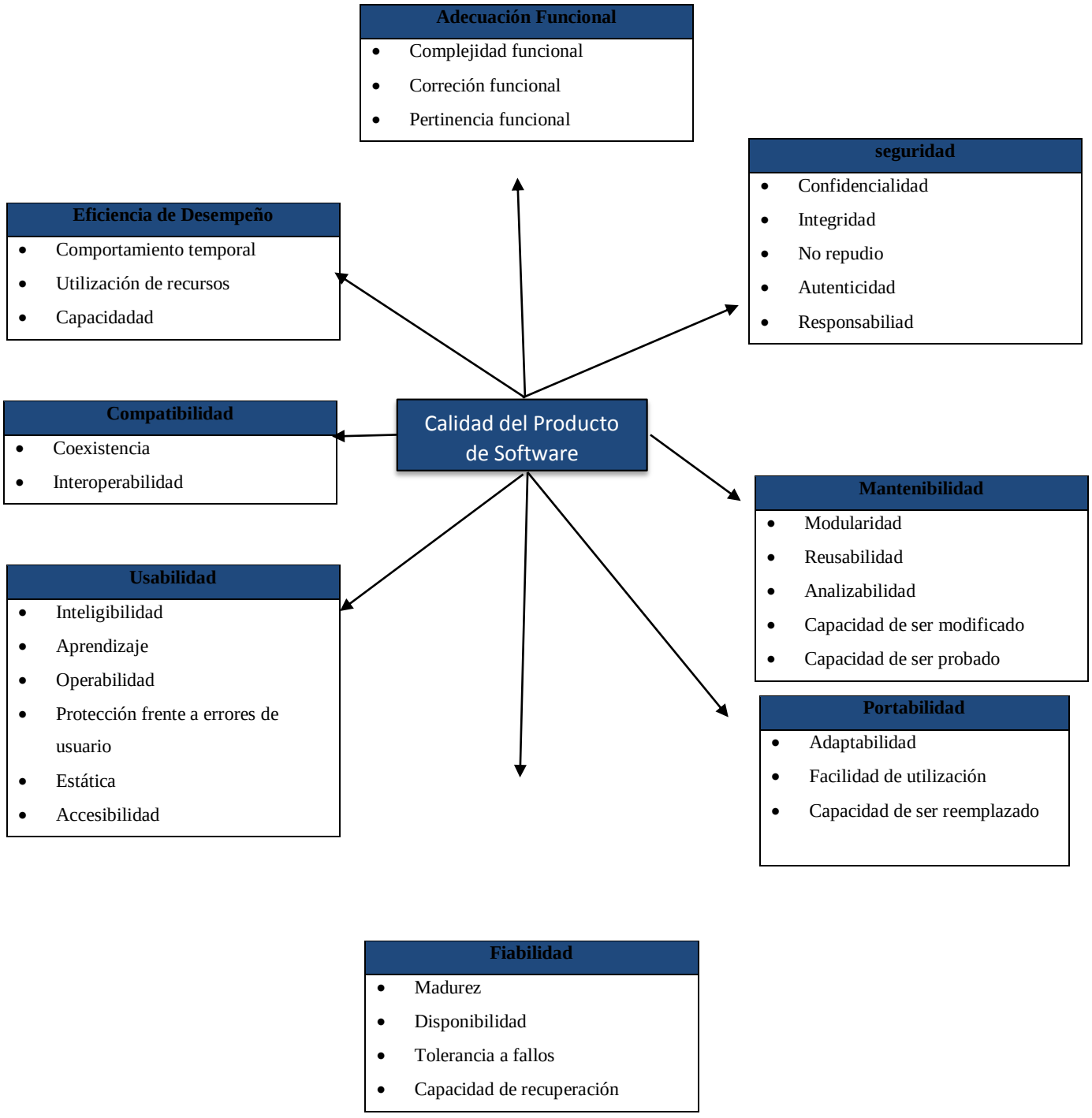
MAR.42 – Estimación del riesgo

2.2.6 Norma ISO para la Calidad de un Producto

ISO 25010 Calidad del Producto Software

El modelo propuesto por la ISO 25010, determina las características de calidad que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado. El modelo de calidad del producto definido por la ISO/IEC 25010 se encuentra compuesto por las ocho características de calidad que se detallan a continuación:

Ilustración 6 Características de la calidad del producto software



Fuente: Recuperado de https://iso25000.com/index.php/normas-iso-25000/iso-25010

– Adecuación Funcional: Cuando la funcionalidad un producto de software cubre las necesidades de un usuario, que fueron definidas al momento de requerirse dicha implementación.

- Eficiencia de desempeño: Característica que representa el desempeño de funciones que realiza el producto de software con el empleo del menor número posible de recursos.
- Compatibilidad: Capacidad que tiene el producto de software o en su defecto la capacidad que tienen algunos de sus componentes, para compartir y/0 consumir recursos comunes bajo un estándar universal (por ejemplo XML, JSON) proveniente de otro software independiente.
- Usabilidad: Capacidad del producto de software de tener una interfaz amigable de cara al usuario, que permita entender su funcionalidad, permita su utilización por usuarios con determinadas características y discapacidades, operarlo y controlarlo con facilidad y sobre todo tenga validaciones que proteja a los usuarios de cometer errores al momento del registro de información u otras situaciones.
- Fiabilidad: Capacidad del producto de software para satisfacer las necesidades del usuario cuando se usa bajo condiciones normales, estar operativo y accesible para su uso cuando se requiera, operar en presencia de fallos de hardware o software y recuperar los datos directamente afectados y reestablecer el estado deseado del sistema en caso de fallos.
- seguridad: Capacidad del software de mantener la confidencialidad, integridad, autenticidad y trazabilidad de la información
- Mantenibilidad: Capacidad de un producto de software de ser modificado de forma efectiva y eficiente sin degradar su desempeño, ser probado para evaluar su correcta funcionalidad, facilidad de diagnosticar deficiencias o fallos en el software a raíz de la realización de un determinado cambio.
- Portabilidad: Característica del producto o componente de software de ser transferido de forma efectiva y eficiente de un entorno hardware, software, operacional o de utilización a otro entorno.

2.2.6 Definiciones de Términos Técnicos:

- **Activos:** Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware),

comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

- **Amenazas:** Son las cosas que les pueden pasar a los activos, causados por el perjuicio a la organización.
- **Análisis del riesgo**: Uso sistemático de la información para identificar fuentes y estimar riesgo
- **Control**: Herramienta de la gestión del riesgo, incluido políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal
- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad los usuarios de los servicios de acceso, podemos tener suplantación de identidad.
- **Comité de seguridad de la información**: Son responsables de entregar las directrices para conformar la política de seguridad de la información de la Institución. Fomentar planes de difusión, capacitación y formación de la cultura de seguridad de la información.
- **Confidencialidad:** O que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autoriza-dos. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.
- **Custodio**: Son los encargados de confianza para realizar la protección y resguardo de los activos de información, y cuidando que se apliquen las políticas y directrices para la seguridad de la información.
- **Dimensión de activos de información**: Son los principios básicos y fundamentales que posee la información, los cuales consisten en

mantener la integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad de la información.

- **Disponibilidad:** O disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.
- **Evaluación de riesgo**: Proceso que determina el nivel de riesgo
- **Gerencia de sistemas y tecnologías**: Es responsable de velar por la seguridad informática de los activos de la información, según su clasificación, la seguridad física e integridad de los sistemas y dispositivos, salvo aquellos expresamente asignados a otra área responsable. Así también es responsable de velar por el cumplimiento pertinente de esta política y sus principios rectores durante la generación, procesamiento, eliminación y custodia de la información que esté asociada a los equipos y/o personal bajo su administración.
- **Gestión del riesgo**: Es el proceso de análisis, evaluación y tratamiento de los riesgos en la seguridad de la información
- **Incidente de seguridad de la información**: Es indicado por una o varias series de eventos inesperados y no deseados que tienen una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de la información.
- **Integridad:** Mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de la organización.
- **MAGERIT:** Metodología para la gestión de riesgos de activos de información
- **Mecanismos de protección** (o contra medidas / salvaguardas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.
- **Nivel de riesgo:** Grado de criticidad de exposición del riesgo

- **Oficial de seguridad de la información**: Es responsable de implementar y supervisar el cumplimiento de la presente política de seguridad de la información y de asesorar en materia de seguridad de la información a los integrantes de la institución que así lo requieran.
- **Plan de seguridad:** Conjunto de proyectos de seguridad que permiten materializar las decisiones de tratamiento de riesgos
- **Política**: Dirección general y formal expresada por la gerencia
- **Propietario de la información**: Persona (s) responsables del mantenimiento y clasificación de los activos de la información. Se encarga además de definir los usuarios que deberán tener permisos de accesos a los activos de información de acuerdo a sus funciones y competencias.
- **Riesgo**: Combinación de la probabilidad de un evento y sus consecuencias
- **Seguridad de la información**: Preservación de la confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas.
- **Tratamiento del riesgo** : proceso de selección e implementación de medidas para mitigar el riesgo
- **Trazabilidad:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad.
- **Usuario**: Persona (s) autorizada a interactuar con los activos de información y sus datos.
- **Valoración de activo**: Es el grado de importancia en base a las dimensiones que posee la información que contiene.

- **Vulnerabilidad**: Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas

CAPITULO III. MÉTODO DE LA INVESTIGACIÓN

3.1. Descripción del método de investigación

a) Según el nivel de investigación: Descriptiva, porque se utilizarán los datos directamente del contexto real, definiendo las características, categorías, observaciones, etc, sobre la gestión de riesgos de la seguridad de la información en el Hospital Regional de Lambayeque, sin intervenir en los procesos actuales.

b) Según el propósito de la investigación: Aplicada , porque está orientada a la solución de problemas, y en nuestro caso, el modelo propuesto para la gestión de riesgos de seguridad de información, plantea una solución al problema actual al no realizarse una gestión de riesgos asociada a los activos de información en el Hospital Regional de Lambayeque, aportando con nuestra investigación un proceso metodológico y una matriz de riesgos como herramienta para la gestión de riesgos de seguridad de la información.

c) Según el diseño de investigación: No experimental, porque los investigadores no someterán deliberada o intencionalmente a determinadas condiciones el objeto de estudio, si no que se analizará tal y como se en cuenta en el contexto actual. Respecto a los 3 tipos de diseño No experimental: a) Transeccional o Transversal, b) longitudinal o evolutivo y c) Manipulación de variables, nuestro proyecto corresponde a la investigación Transeccional porque la recolección de datos se realizó en el período de realización de la investigación, sin tomar en cuenta datos históricos, debido a que no existen. Con el propósito de describir y analizar su comportamiento e incidencia en un cierto momento.

d) Según el enfoque de la investigación: Mixta, porque reúne características tanto del enfoque cualitativo como cuantitativo, ya que partimos de una realidad de nuestro caso de estudio (delimitado) para recolectar datos y plantear una

propuesta de modelo de gestión de riesgos para la seguridad de la información basada en las teorías de la gestión de riesgos, el cual será valorado por los expertos en seguridad de información en base a su experiencia.

3.2 Técnicas de recolección de datos

Los instrumentos que hemos utilizado con el fin de recabar información para el desarrollo y análisis de nuestra investigación, son las siguientes:

3.2.1 Observación participante

La Jefatura de la División de tecnologías de la información nos mostró solo un formulario en el sistema de asignación de camas del HRL, el cual permite al usuario, gestionar el proceso de asignación y liberación de camas a los pacientes, así como validar el tiempo en que estuvo asignada una cama un paciente, del cual indicaron no contar con documentación, al igual que los otros sistemas de gestión hospitalaria (SIGHOR, GALEN PLUS, SIGBIO) que posee el Hospital Regional de Lambayeque.

Se observó la falta revisión de documentos de identificación a los visitantes, al momento de ingresar a la División de tecnologías de la información del HRL. Para el caso especial de los investigadores, de todas las veces que se ha ingresado a la División de tecnologías de la información, en ningún momento fueron solicitados los fotochecks asignados.

Se pudo observar que los responsables de los sistemas de gestión hospitalarias en el HRL, mostraron una actitud negativa y reacia frente a la importancia de mantener documentada la operativa y funcionalidad de los sistemas a través de manuales/ metodologías de usuario, la elaboración y uso de una política de gestión de seguridad de la información y la implementación de un sistema de gestión de riesgos de seguridad de la información. Infiriendo que ellos no son responsables de la implementación de estos mecanismos en mención, cuando al respecto deberían formar parte de una gestión de riesgos de seguridad de la información.

La finalidad de aplicar esta técnica, es para mantener una percepción general de cómo se encuentra la gestión de seguridad de la información respecto a la seguridad física y ambiental.

3.2.2 **Revisión documental**:

Se revisaron los diversos documentos del Hospital Regional de Lambayeque, proporcionados por los responsables de los sistemas de gestión hospitalarios en el HRL, entre los que fueron considerados: manuales de usuarios, inventarios de hardware y software y diversa documentación organizacional. Con la finalidad de tomar conocimiento de la operatividad de los sistemas, los mecanismos de protección de seguridad de la información considerados en la implementación de los sistemas, la estructura organizacional del HRL, entre otros aspectos.

3.2.3 Encuesta:

Aplicamos esta técnica para poder indagar respecto de las opiniones, actitudes y sugerencias sobre la seguridad de la información que poseen los usuarios de los sistemas de hospitalización, responsables y encargados de la gestión de estos sistemas de información en el Hospital Regional de Lambayeque.

Con la finalidad de evidenciar los conocimientos generales sobre seguridad de la información que se tiene por parte de los usuarios y responsables de los sistemas de información del Hospital Regional de Lambayeque.

Elaboramos 03 formatos de encuesta con preguntas generales sobre de la seguridad de la información enfocadas a su realidad laboral; éstas fueron dirigidas a diferentes tipos de usuario, los mismos que representan una muestra significativa de los usuarios que se relacionan directamente con los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque, tales como SIGHOR, Galen Plus, sistema de Asignación de Camas, SIGBIO.

Formato 001: Encuesta dirigida a los usuarios de los diversos sistemas de información de gestión hospitalaria del HRL.

Formato 002: Encuesta dirigida a los encargados y supervisores de los sistemas de gestión hospitalaria de la División de tecnologías de la información del HRL

Formato 003: Encuesta dirigida a la Jefatura de la División de tecnologías de la información del HRL encargada de la gestión de los sistemas de gestión hospitalaria

3.2.4 Entrevista:

Aplicamos esta técnica con el fin de indagar por medio de varias conversaciones con los responsables de la gestión de los sistemas de gestión hospitalaria que posee el Hospital Regional de Lambayeque, sobre la gestión de la seguridad de la información, cómo es que se aplica o no en su institución, y la importancia de mitigar los riesgos asociados a la seguridad de la información.

Las entrevistas fueron realizadas con la jefatura, los encargados y supervisores de los sistemas de gestión hospitalaria de la división de tecnologías de la información del HRL, con la finalidad de obtener un mayor detalle acerca de los procesos que actualmente se llevan a cabo para gestionar la seguridad de la información de sus activos.

Solicitamos adicionalmente al personal entrevistado, una serie de documentos para iniciar el desarrollo de nuestra investigación, que listamos en el siguiente checklist:

Tabla 3.- Check list para la recolección de datos

DOCUMENTACIÓN SOLICITADA	DOCUMENTADO			NO POSEE
	SI	PARCIAL	NO	
Organigrama del HRL	-	-	X	-
Organigrama de la División de tecnologías de información	-	-	X	-
Manual de Organización y Funciones	-	-	-	X
Políticas de seguridad de la información del HRL	-	-	-	X
Procedimientos formales utilizados para la asignación y devolución de activos de información asignados al personal del HRL.	-	-	-	X
Lista de Tareas para concientizar al personal sobre la gestión de la seguridad de la información del HRL	-	-	-	X
Listado de los sistemas de gestión hospitalaria actuales en el HRL	-	X	-	-
Manual de Usuario de los sistemas de gestión hospitalaria:				
SIGHOR	X	-	-	-
Galen Plus	-	X	-	-
Asignación de Camas	-	-	-	X
SIGBIO	X	-	-	-
Documentación (Formatos o Manuales técnicos) con los que registran los cambios y mejoras en los desarrollos de los sistemas de gestión hospitalaria.				
SIGHOR	-	-	-	X
Galen Plus	-	-	-	X
Asignación de Camas	-	-	-	X
SIGBIO	-	-	-	X
Inventario de los activos de información clasificados	-	-	-	X
Inventario de los Equipos Informáticos clasificados	-	X	-	-

Fuente: Elaboración propia

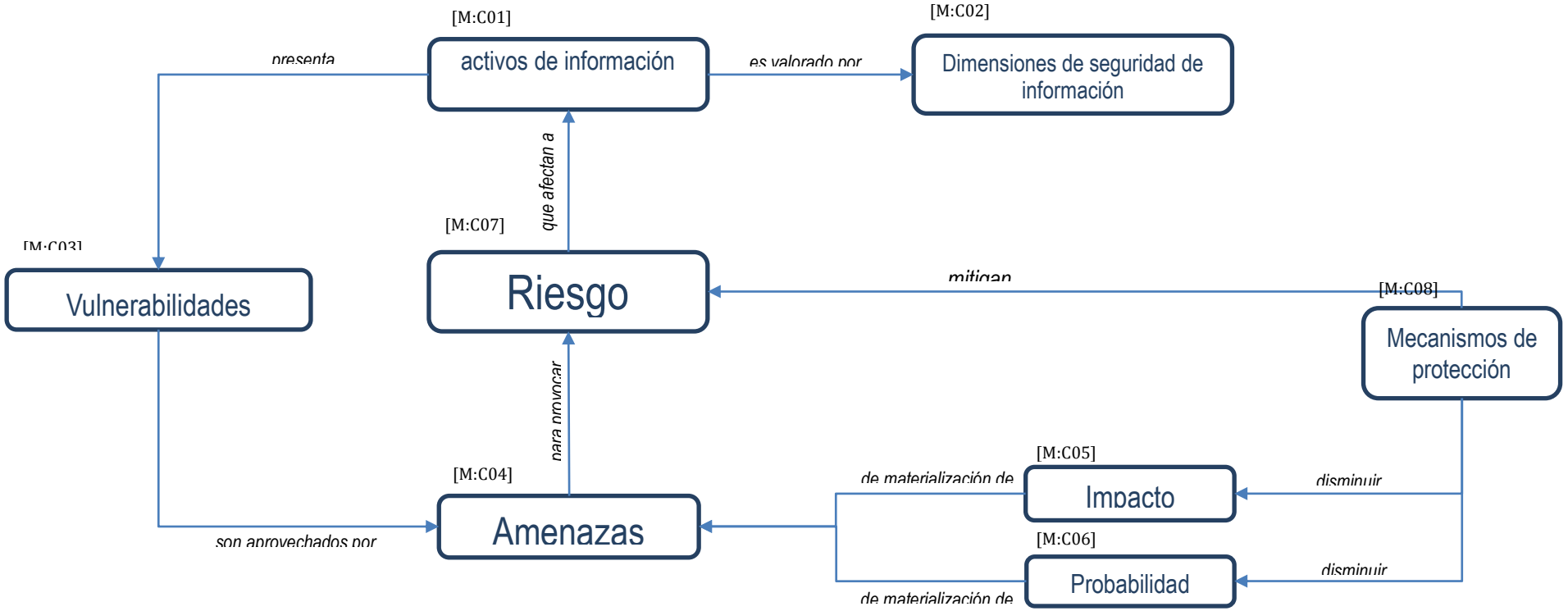
3.2.5 Juicio de expertos para la validación de instrumentos:

Aplicamos esta técnica con el fin de obtener una opinión informada de especialistas en materia de gestión de riesgos, sobre el modelo de gestión de riesgos que se propone en esta investigación

3.3 Modelo de gestión de riesgos propuesto

Teniendo como base el modelo PDCA estándar, nuestra propuesta se adecua y plantea las fases de identificación, análisis y evaluación tratamiento y el seguimiento y monitoreo para la gestión de riesgos de seguridad de la información en los activos de la información, la cual se lleva a la práctica con la Metodología propuesta que se pasa a describir líneas más abajo.

Ilustración 7 Modelo de gestión de riesgos propuesto



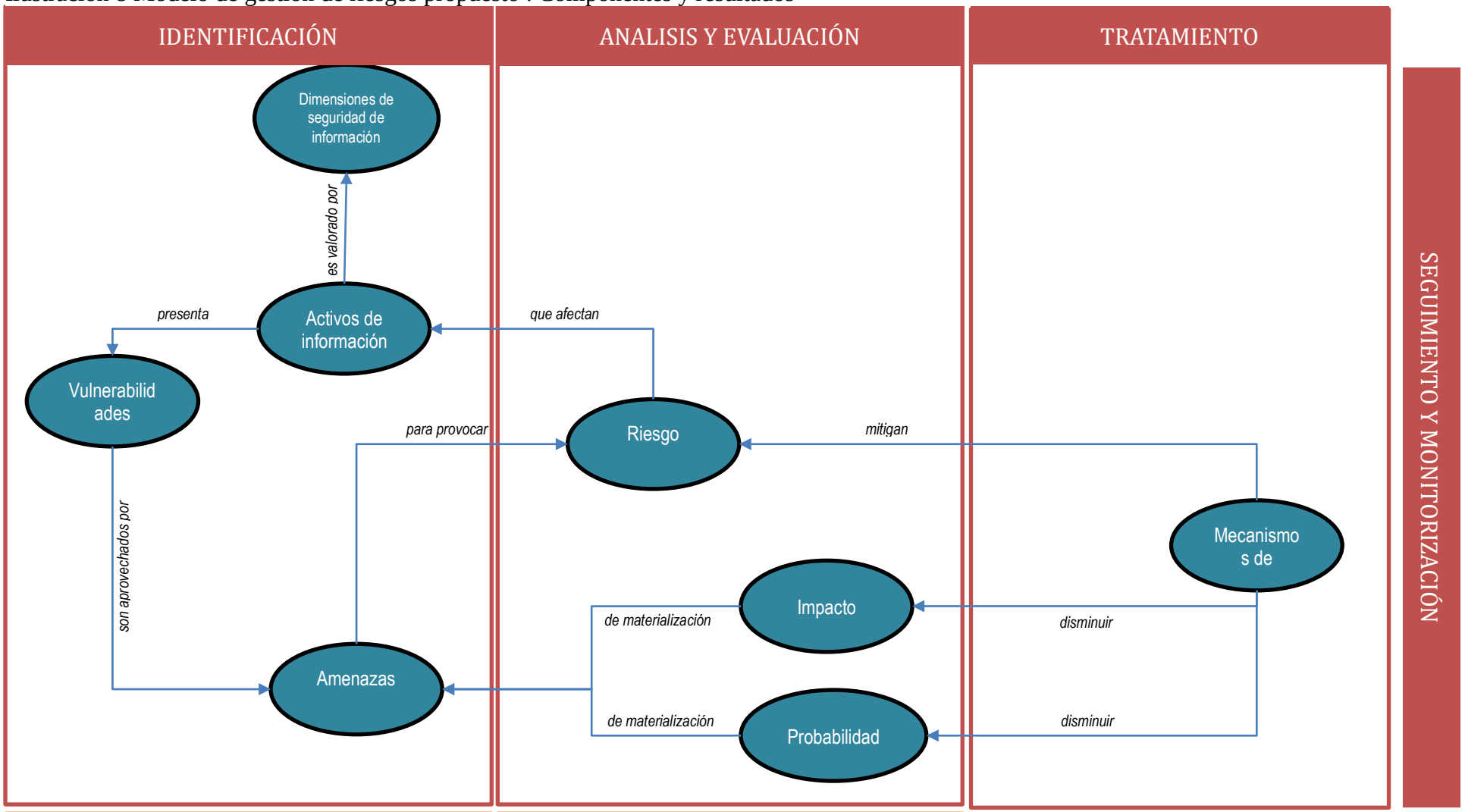
Fuente: Elaboración propia

Tabla 4.- Componentes del modelo de gestión de riesgo

COMPONENTES DEL MODELO DE GESTIÓN DE RIESGO	
M:C01	ACTIVOS DE LA INFORMACIÓN
M:C02	DIMENSIONES DE LA SEGURIDAD DE INFORMACIÓN
M:C03	VULNERABILIDADES
M:C04	AMENAZAS
M:C05	IMPACTO
M:C06	PROBABILIDAD
M:C07	RIESGO
M:C08	MECANISMOS DE PROTECCIÓN

Fuente: Elaboración propia

Ilustración 8 Modelo de gestión de riesgos propuesto : Componentes y resultados



RESULTADOS:
Inventario de activos de información
Matriz de riesgos:
-Valoración de dimensiones
-Priorización de activos
-Identificación de vulnerabilidades
-Identificación de amenazas

RESULTADOS:
Matriz de riesgos:
-Ponderación de probabilidad de materialización de amenazas
-Ponderación de impacto de amenazas
-Determinación del nivel de riesgos.

RESULTADOS:
Listado de propuesta de Mecanismos de protección
Criterios para medir la efectividad de los mecanismos de protección

Fuente : Elaboración propia

3.4 Metodología para la gestión de riesgos desarrollada

La metodología que estamos presentando, es una adaptación de la metodología Magerit V.3, que sigue las directrices de la ISO/IEC 27005 gestión de riesgos de tecnologías de la información, en la que buscamos establecer los lineamientos específicos que permita gestionar de manera adecuada los activos asociados a la tecnología de información en la institución del Hospital Regional del Lambayeque.

La metodología comprende 4 etapas: Identificación de activos y sus amenazas, análisis y evaluación de riesgos en los activos de información, Tratamiento de riesgos en los activos de información y seguimiento y monitoreo de riesgos en activos de información.

3.4.1 Etapas de la metodología para la gestión de riesgos de la seguridad de la información

La metodología para la gestión de riesgos de seguridad de la información comprende 4 etapas: Identificación de activos y sus amenazas, análisis y evaluación de riesgos para los activos de información, tratamiento de los riesgos y seguimiento y monitoreo de riesgos de seguridad de la información.

Ilustración 9. Etapas de la metodología de gestión de riesgos de la seguridad de la información

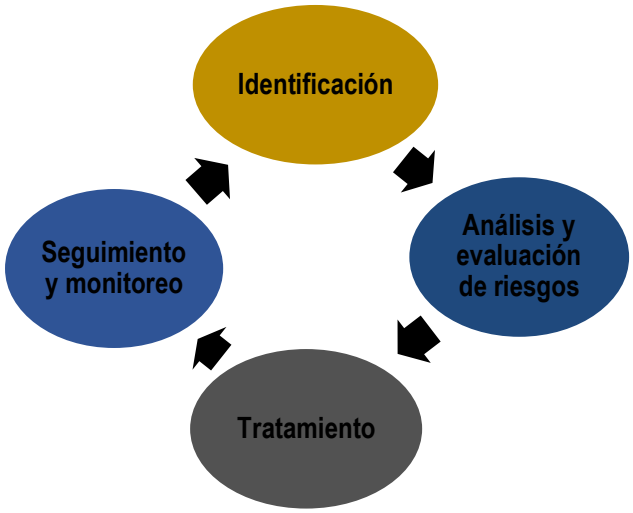
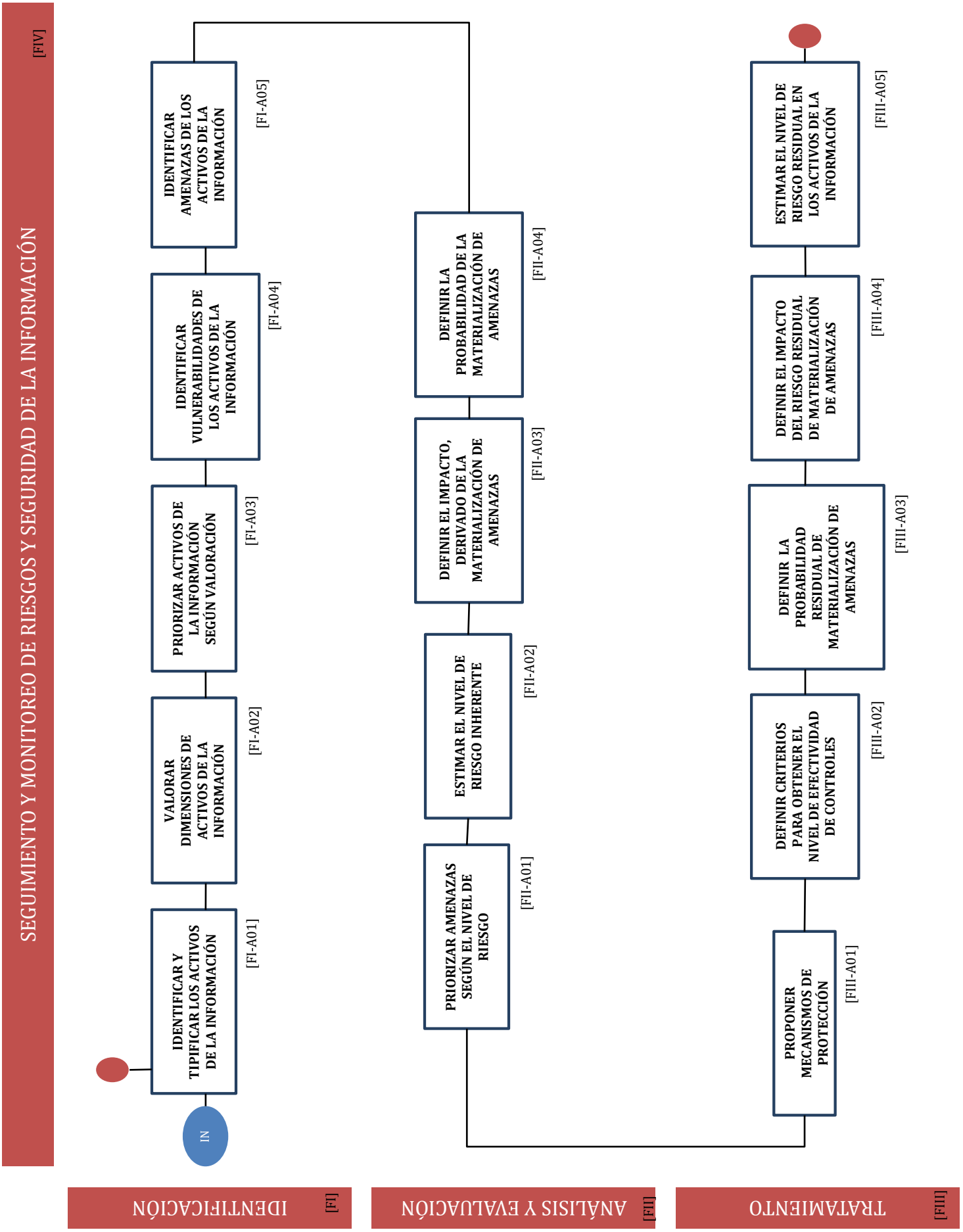


Ilustración 10 Metodología propuesta para la gestión de riesgos



Fuente : Elaboración propia

Tabla 5.- Actividades de metodología para la gestión de riesgos

ACTIVIDADES DE METODOLOGÍA PARA LA GESTIÓN DE RIESGOS	
FI	FASE IDENTIFICACIÓN
FI-A01	IDENTIFICAR Y TIPIFICAR LOS ACTIVOS DE LA INFORMACIÓN
FI-A02	VALORAR DIMENSIONES DE ACTIVOS DE LA INFORMACIÓN
FI-A03	PRIORIZAR ACTIVOS DE LA INFORMACIÓN SEGÚN VALORACIÓN
FI-A04	IDENTIFICAR VULNERABILIDADES DE LOS ACTIVOS DE LA INFORMACIÓN
FI-A05	IDENTIFICAR AMENAZAS DE LOS ACTIVOS DE LA INFORMACIÓN
FII	FASE ANÁLISIS Y EVALUACIÓN
FII-A01	PRIORIZAR AMENAZAS SEGÚN EL NIVEL DE RIESGO
FII-A02	ESTIMAR EL NIVEL DE RIESGO INHERENTE
FII-A03	DEFINIR EL IMPACTO, DERIVADO DE LA MATERIALIZACIÓN DE AMENAZAS
FII-A04	DEFINIR LA PROBABILIDAD DE LA MATERIALIZACIÓN DE AMENAZAS
FIII	FASE DE TRATAMIENTO
FIII-A01	PROPONER MECANISMOS DE PROTECCIÓN
FIII-A02	DEFINIR CRITERIOS PARA OBTENER EL NIVEL DE EFECTIVIDAD DE CONTROLES
FIII-A03	DEFINIR LA PROBABILIDAD RESIDUAL DE MATERIALIZACIÓN DE AMENAZAS
FIII-A04	DEFINIR EL IMPACTO DEL RIESGO RESIDUAL DE MATERIALIZACIÓN DE AMENAZAS
FIII-A05	ESTIMAR EL NIVEL DE RIESGO RESIDUAL EN LOS ACTIVOS DE LA INFORMACIÓN
FIV	FASE DE SEGUIMIENTO Y MONITOREO

Fuente: Elaboración propia

3.4.1.1 Etapa de identificación

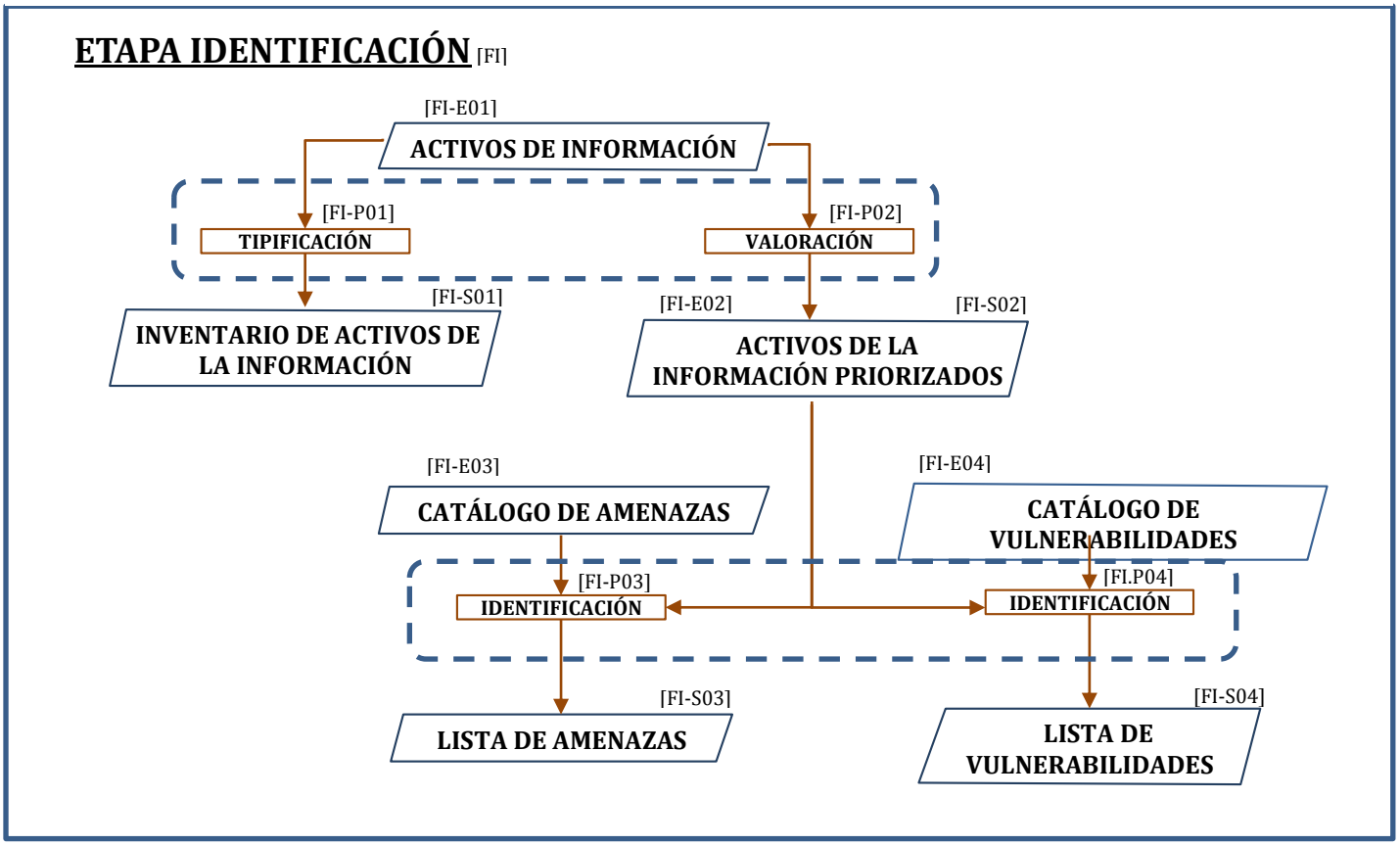
En esta fase inicial vamos a identificar los activos de información con los que dispone el Hospital Regional de Lambayeque, de manera que puedan ser tipificados en base a sus características físicas en: Datos/información, información impresa, personal, instalaciones, redes de comunicaciones, equipamiento auxiliar, soporte de información, equipos informáticos, aplicaciones informáticas y servicios auxiliares. El registro de los activos de información identificados será realizado mediante el uso del Anexo N° 04: Formato de inventario de activos, teniéndose como guía el Anexo N° 09: Manual de Usuario para el uso del Inventario de activos.

Una vez que hemos identificado los activos de información del HRL, los tenemos que valorar en base a los criterios definidos para cada dimensión (acápite 4.3 Desarrollo de la Metodología de gestión de riesgos, ítem 4.3.1.2 Valoración de dimensiones de

activos de información): Confidencialidad, integridad, disponibilidad, trazabilidad y autenticidad. El resultado de ésta valoración permite tener inventariado los activos de información priorizados, de manera que se puedan identificar sobre ellos, las amenazas y vulnerabilidades asociadas. La valoración de activos de información, será realizado mediante el uso del Anexo N° 05: Formato matriz de riesgo, teniéndose como guía el Anexo N° 10: Manual de usuario para el uso de la matriz de riesgos.

Seguidamente y tomando como referencia el Catálogo de Vulnerabilidades (Anexo N° 06: Catálogo de vulnerabilidades) y el Catálogo de amenazas (Anexo N° 07: Catálogo de amenazas), tenemos que identificar las posibles amenazas que pueden aprovechar las vulnerabilidades existentes sobre los activos de información priorizados. El registro de las amenazas y vulnerabilidades identificadas sobre los activos de información priorizados será realizado mediante el uso del Anexo N° 05: Formato matriz de riesgo, teniéndose como guía el anexo N° 10: Manual de usuario para el uso de la matriz de riesgos.

Ilustración 11 Diagrama de la etapa de identificación de la gestión de riesgo



Fuente: Elaboración propia

Tabla 6.- Etapa de identificación

ETAPA		ENTRADA		PROCESO		SALIDA	
FI	IDENTIFICACIÓN	FI-E01	ACTIVOS DE LA INFORMACIÓN	FI-P01	TIPIFICACIÓN	FI-S01	INVENTARIO DE ACTIVOS DE LA INFORMACIÓN
		FI-E01	ACTIVO DE LA INFORMACIÓN	FI-P02	VALORACIÓN	FI-S02	ACTIVOS D ELA INFORMACIÓN PRIORIZADOS
		FI-E02	ACTIVOS D ELA INFORMACIÓN PRIORIZAADOS	FI-P03	IDENTIFICACIÓN	FI-S03	LISTA DE AMENAZAS
		FI-E03	CATALOGO DE AMENAZAS		IDENTIFICACIÓN		
		FI-E02	ACTIVOS D ELA INFORMACIÓN PRIORIZAADOS	FI-P04	IDENTIFICACIÓN	FI-S04	LISTA DE VULNERABILIDADES
		FI-E04	CATALOGO DE VULNERABILIDADES		IDENTIFICACIÓN		

Fuente: Elaboración propia

Esta etapa representa la piedra angular del proceso, porque permite identificar los activos de información que administra el Hospital Regional de Lambayeque a través de los procesos de la división de tecnología y procesos, valorar y saber la importancia de los activos de información e identificar sus posibles amenazas.

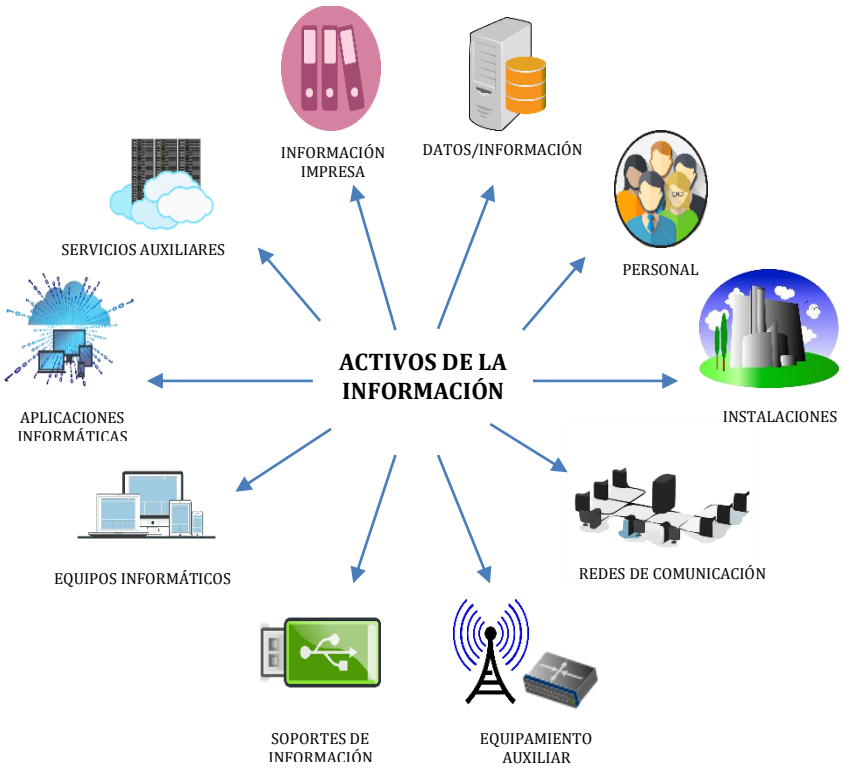
- Identificación y tipificación de activos de la información
- Valoración de dimensiones de activos de información
- Priorización de activos de la información
- Identificar vulnerabilidades sobre activos de información.
- Identificar amenazas posibles sobre activos de la información

1. Identificación y tipificación de activos de información:

Se deben identificar los activos de información del Hospital Regional Lambayeque y tipificarse en base a las siguientes definiciones: Datos/información, información impresa, servicios auxiliares, aplicaciones informáticas, equipos informáticos, soporte de información, equipamiento auxiliar, las redes de comunicaciones, las instalaciones o las personas.

Los criterios a considerarse para tipificar un activo de información, son los siguientes:

Ilustración 12 tipos de activos de la información



Fuente: Elaboración propia

Los diferentes tipos de activos se agruparán de acuerdo al código asignado:

Tabla 7.- Tipificación de activos

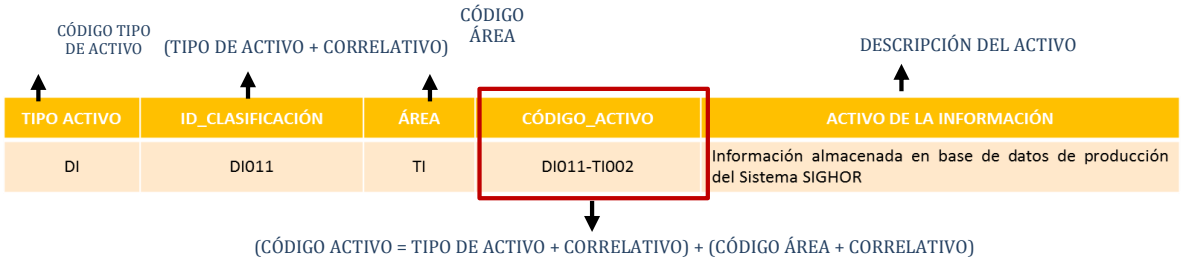
TIPIFICACION DE ACTIVOS	
TIPO ACTIVO	**DESCRIPCIÓN DEL TIPO DE ACTIVO**
DI	Datos/información
II	información impresa
SA	Servicios auxiliares que se necesitan para poder organizar el sistema
AI	Aplicaciones informáticas (software) que permiten manejar los datos
EI	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios
SI	Los soportes de información que son dispositivos de almacenamiento de datos
EA	El equipamiento auxiliar que complementa el material informático

RC	**Las redes de comunicaciones que permiten intercambiar datos**
IE	**Las instalaciones que acogen equipos informáticos y de comunicaciones**
PP	**Las personas que explotan u operan todos los elementos anteriores citados**

Fuente: Elaboración propia

Cada uno de los activos identificados dentro de la tipificación señalada, serán identificados por medio de un "código de activo", el cual se asignará tomando en cuenta los siguientes parámetros:

Ilustración 13 Tipificación de los activos de la información



Fuente: elaboración propia

a. **Datos/información:** Información almacenada en equipos o soportes de información o será transferido de un lugar a otro por los medios de transmisión de datos. Entre los que tenemos:
   - Ficheros, carpetas, documentos virtuales(archivos excel, word, PDF, ppt, Outlook, etc)
   - Copia de respaldo
   - Datos de configuración
   - Datos de control de acceso (contraseñas)
   - Datos de validación de credenciales (licencias de software)
   - Registro de actividad (Log)
   - Código fuente
   - Código ejecutable
   - Datos de prueba
   - información almacenada en base de datos de prueba
   - información almacenada en Base de datos de producción

b. **Información impresa:** Refiere a toda la información impresa en documentos físicos, entre los que tenemos:
    - Documentos almacenado en archivadores
    - Informes, memorándum, requerimientos, conformidad, etc que se hallan impreso

c. **Servicios auxiliares que se necesitan para poder organizar el sistema:** Función que satisface una necesidad de los usuarios (del servicio). La lista no limitativa puede contemplar:
    - Servicio de acceso (Lista de roles y perfiles asignados a usuarios)
    - Servicios subcontratados (Por ejemplo: correo electrónico, servicio web (alojamiento y dominio), etc.)
    - Transferencia de ficheros (ftp)

d. **Aplicaciones informáticas (software) que permiten manejar los datos:** Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.), refiriéndose a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios. No preocupa en este apartado el denominado "código fuente"
    - Desarrollo propio(in house)
    - Desarrollo subcontratado
    - sistema de gestión de dominios (Active directory)
    - sistema de gestión de base de datos (el aplicativo)
    - sistema operativo
    - Ofimática
    - Gestor de máquinas virtuales
    - sistema Backup
    - SPSS estadístico
    - Antivirus
    - Aplicaciones de desarrollo de software (open source y licenciados)
    - Aplicaciones de software instalados en equipos médicos
    - Entre otros

e. **Los equipos informáticos (hardware) que permiten hospedar los datos, aplicaciones y servicios**: Representan los datos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

- Servidores principales y alternos
- Equipos de cómputo de colaboradores (fijos y portátiles)
- Informática móvil
- Medios de impresión y escaneo
- Soporte de red (módems, switch, router, cortafuegos físicos, access point)
- Centralita telefónica (análogo)
- Entre otros (equipo médico con TI)

f. **Los soportes de información que son dispositivos de almacenamiento de datos:** se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

- Discos duros internos y externos
- Cederrón (CR-ROM)
- Memorias USB
- DVD
- Tarjeta de memoria cámaras fotográficas
- DVR (disco de almacenamiento de cámaras de seguridad)
- Entre otros

g. **El equipamiento auxiliar que complementa el material informático:** En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

- UPS
- Generadores eléctricos
- Aire acondicionado
- Cableado eléctrico

- Cableado de red
- Antenas
- Entre otros

h. **Las redes de comunicaciones que permiten intercambiar datos**: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.
   - Red inalámbrica
   - Red local
   - Por satélite
   - Internet
   - Entre otros

i. **Las instalaciones que acogen equipos informáticos y de comunicaciones:** En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.
   - Edificio
   - Cuarto de servidores
   - Instalaciones del servidor de respaldo
   - Instalaciones que alojan los backups
   - Entre otros

j. **Las personas que explotan u operan todos los elementos anteriores citados:** En este epígrafe aparecen las personas relacionadas con los sistemas de información
   - Usuarios externos
   - Usuarios internos
   - Administradores de sistemas
   - Administradores de comunicaciones
   - Administradores de BBDD
   - Administradores de seguridad
   - Desarrolladores/programadores

- Subcontratas
- Proveedores
- Entre otros.

Con la finalidad de reforzar la aplicación de la presente metodología, se han identificado los activos de información del Hospital Regional Lambayeque, específicamente a los que comprenden los sistemas de gestión hospitalaria, y se ha seleccionado el activo de información: base de datos de producción del sistema SIGHOR; el mismo que sería utilizado como base para ejemplificar todas las actividades que comprende la metodología propuesta por el equipo investigador. A continuación, se ejemplifica la actividad de identificación y tipificación de activos de información:

2. **Valoración de dimensiones de los activos de información:** La finalidad de esta etapa está en saber cuáles son los activos más importantes o más valiosos para la institución, de manera que se pueda ahondar en la implementación de mayores niveles de protección, en base a la exposición de las amenazas que presente su respectiva dimensión. El enfoque MAGERIT determina las siguientes dimensiones para un respectivo activo:

   - **Confidencialidad de la información:**
     ¿Qué daño causaría si los datos los conociera quien no debe? o ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
     Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.

   - **Integridad de los datos:**
     ¿Qué perjuicio causaría que los datos estuvieran dañados o corruptos? o ¿Qué importancia tendría que los datos fueran modificados fuera de control?
     Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.
     Y, recíprocamente, los daños carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

- **Disponibilidad:**

  ¿Qué perjuicio causaría que un servicio no pueda tenerlo o no pueda utilizarse? o ¿Qué importancia tendría que el activo no estuviera disponible?

  Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.

  Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño.

  La disponibilidad es una característica que afecta a todo tipo de activos.

  A menudo la disponibilidad requiere un tratamiento por escalones, desde breves interrupciones sin importancia, pasando por interrupciones que causan daños considerables y llegando a interrupciones que no admiten recuperación: la organización está acabada.

- **Autenticidad:**

  ¿Qué importancia se tendría que quien accede al servicio no sea realmente quien se cree?

  La autenticidad de los usuarios de un servicio es lo contrario de la oportunidad de fraude o uso no autorizado de un servicio.

  Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.

  Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

- **Trazabilidad**

  ¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?, ¿Qué importancia tendría que no quedara constancia del acceso a los datos?, ¿Qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Abriría las puertas al fraude, incapacitaría a la organización para perseguir delitos y podría suponer incumplimiento de obligaciones legales.

A continuación se muestra un cuadro con los valores que pueden tomar los activos de información, cuya escala debería ser común para todas las dimensiones que presenta un activo, permitiendo comparar riesgos. Se ha elegido una escala detallada de diez valores, dejando un valor 0 como determinante de lo que sería un valor despreciable (a efectos de riesgo) y un valor 10 como valor Extremo, la tabla de valores se correlacionan como se indica a continuación:

Tabla 8.- Tabla de valores trazabilidad

VALOR		**CRITERIO**
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Elaboración propia

Cada activo deberá tener una valoración en cada uno de las cinco dimensiones de seguridad de la información, por ejemplo:

Tabla 9.- Valoración de cada dimensión de seguridad

activo de la información	disponibilidad	Confidenciabilidad	Integridad	Autenticidad	Trazabilidad
Serv. BD	8	7	8	7	7

Fuente: Elaboración propia

3. **Priorización de activos de información:** Conociendo el valor de importancia de cada activo de información en base a la dimensión que presente, podemos determinar aquellos que necesitan de mayor cuidado y protección contra amenazas, puesto que implicaría un mayor impacto a la organización, en caso sus vulnerabilidades sean explotadas. En esta actividad se definirán los activos más importantes, para los cuales se identificarán las amenazas a las que podrían estar expuestas. Podría considerarse aquellos activos valorados como medio, alto, muy alto y extremo, el sustento para que una valoración de nivel MEDIO forme parte del proceso de priorización es porque este nivel podría estar expuesto a que tarde o temprano aborde o cambie a niveles altos de riesgo.

Se calculará el valor de los activos de la información, realizando un promedio simple de las dimensiones

Tabla 10.- Priorización de activos de información

activo de la información	disponibilidad	Confidenciabilidad	Integridad	Autenticidad	Trazabilidad	VALOR
Serv. BD	8	7	8	7	7	7

Fuente: Elaboración propia

4. **Identificar y valorar vulnerabilidades sobre activos de la información:** Se debe identificar las vulnerabilidades que poseen los activos de la información y que podrían causarles daños o inconsistencias, considerando los valores dependiendo del nivel de importancia como se indica en el ítem anterior. Para cada vulnerabilidad se presenta un cuadro como el siguiente:

5. **Identificar amenazas posibles sobre los activos de información**: se debe determinar las amenazas que ocurren o podrían ocurrir y que podrían causar daño a

un activo de información considerado con valoración importante según el ítem anterior. Para cada amenaza se presenta un cuadro como el siguiente:

Tabla 11.- Identificación de amenazas

Tipo de activos:	**Dimensiones:**
- Que se pueden ver afectados por este tipo de amenazas	de seguridad que se pueden ver afectados por este tipo de amenazas, ordenadas de más a menos relevante
Descripción: Complementaria o más detallada de la amenaza	

Fuente: Elaboración propia

a. **De origen natural:** Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.

➢ **Fuego**

Tabla 12.- Tipo de amenaza: Fuego

Tipo de activos:	**Dimensiones:**
- Equipos informáticos(hardware) - Soportes de información - Equipamiento auxiliar - Instalaciones	Disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema	

Fuente: Elaboración propia

➢ **Daños por agua**

Tabla 13.- Tipo de amenaza: Daños por agua

Tipo de activos:	**Dimensiones:**
-Equipos informáticos	

(hardware) -Soporte de información -Equipamiento auxiliar -Instalaciones	Disponibilidad
Descripción: Inundaciones: posibilidad de que el agua acabe con recursos del sistema	

Fuente: Elaboración propia

➢ **Desastres Naturales**

Tabla 14.- Tipo de amenaza: Desastres naturales

Tipo de activos:	**Dimensiones:**
-Equipos informáticos(hardware) -Soporte de información -Equipamiento auxiliar -Instalaciones	Disponibilidad
Descripción: Otros incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, contaminación, fenómenos climáticos,Se excluyen desastres específicos tales como incendios(fuego) e inundaciones(Daños por agua) Se excluye al personal por cuanto se ha previsto una amenaza específica para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	

Fuente: Elaboración propia

b. **De origen industrial:** Sucesos que pueden ocurrir de forma accidental o deliberada, derivados de la actividad humana.

➢ Fuego

Tabla 15.- Tipo de amenaza: Fuego origen industrial

Tipo de activos:	**Dimensiones:**
-Equipos informáticos(hardware) -Soportes de información -Equipamiento auxiliar -Instalaciones	Disponibilidad
Descripción: Incendios: posibilidad de que el fuego acabe con recursos del sistema, origen accidental o deliberado	

Fuente: Elaboración propia

➢ Daños por agua

Tabla 16.- Tipo de amenaza: Daño por agua origen industrial

Tipo de activos:	**Dimensiones:**
-Equipos informáticos(hardware) -Soporte de información -Equipamiento auxiliar -Instalaciones	Disponibilidad
Descripción: Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema, origen accidental o deliberado	

Fuente: Elaboración propia

➢ Contaminación mecánica

Tabla 17.- Tipo de amenaza: Contaminación mecánica

Tipo de activos:	**Dimensiones:**
- Equipos informáticos(hardware) - Soporte de información - Equipamiento auxiliar	Disponibilidad
Descripción:	

Polvo, suciedad

Fuente: Elaboración propia

➢ Avería de origen físico o lógico

Tabla 18.- Tipo de amenaza: Avería de origen físico o lógico

Tipo de activos:	**Dimensiones:**
-Aplicaciones(software) -Equipos informáticos (hardware) -Soportes de información -Equipamiento auxiliar	Disponibilidad
Descripción: Fallo en los equipos y/o fallo en los programas. Puede ser debido a un defecto de origen durante el funcionamiento del sistema.	

Fuente: Elaboración propia

➢ Corte del suministro eléctrico

Tabla 19.- Tipo de amenaza: Corte del suministro eléctrico

Tipo de activos:	**Dimensiones:**
-Equipos informáticos (hardware) -Soportes de información(electrónicos) -Equipamiento auxiliar	Disponibilidad
Descripción: Cese de la alimentación de potencia	

Fuente: Elaboración propia

➢ Condiciones inadecuadas de temperatura o humedad

Tabla 20.- Tipo de amenaza: Condiciones inadecuadas de temperatura o humedad

Tipo de activos:	**Dimensiones:**
-Equipos informáticos (hardware) -Soportes de información -Equipamiento auxiliar	disponibilidad
Descripción: Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad.	

Fuente: Elaboración propia

➢ Fallo de servicios de comunicaciones

Tabla 21.- Tipo de amenaza: Fallo de servicios de comunicaciones

Tipo de activos:	**Dimensiones:**
-Redes de comunicaciones	disponibilidad
Descripción: Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	

Fuente: Elaboración propia

➢ Degradación de los soportes de almacenamiento de la información

Tabla 22.- Tipo de amenaza: Degradación de los soportes de almacenamiento

Tipo de activos:	**Dimensiones:**
-Soportes de información	disponibilidad
Descripción: Como consecuencia del paso del tiempo (avería del hardware, falla de funcionamiento del hardware.	

Fuente: Elaboración propia

c. **Errores y fallos no intencionales:** Fallos no intencionales causado por las personas. El origen es humano accidental

➢ Errores de los usuarios

Tabla 23.- Tipo de amenaza: Errores y fallos no intencionales

Tipo de activos:	**Dimensiones:**
-Datos/información -Servicios -Aplicaciones (software) -Soporte de información	integridad confidencialidad disponibilidad
Descripción: Equivocaciones de las personas cuando usan los servicios, datos, etc	

Fuente: Elaboración propia

➢ Errores del administrador

Tabla 24.- Tipo de amenaza: Errores del administrador

Tipo de activos:	**Dimensiones:**
-Datos/información -Servicios -Aplicaciones (software) -Soporte de información	integridad confidencialidad disponibilidad
Descripción: Equivocaciones de las personas con responsabilidad de instalación y operación	

Fuente: Elaboración propia

➢ Errores de monitorización

Tabla 25.- Tipo de amenaza: Errores de monitorización

Tipo de activos:	**Dimensiones:**
-Registros de actividad	Integridad(trazabilidad)
Descripción: Inadecuado registro de actividades: falta de registros, registros incompletos	

Fuente: Elaboración propia

➢ Errores de configuración

Tabla 26.- Tipo de amenaza: Errores de configuración

Tipo de activos:	**Dimensiones:**
-Datos de configuración	Integridad
Descripción: Introducción de datos de configuración erróneos	

Prácticamente todos los activos dependen de su configuración y está de la diligencia del administrador: privilegios de acceso, flujo de actividades, registro de actividad, encaminamiento etc.

Fuente: Elaboración propia

➢ Deficiencias en la organización

Tabla 27.- Tipo de amenaza: Deficiencias en la organización

Tipo de activos:	**Dimensiones:**
-Personal	disponibilidad
Descripción: Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión sobre la ocurrencia de incidentes. Acciones descoordinadas, errores por omisión, etc.	

Fuente: Elaboración propia

➢ Difusión de software dañino

Tabla 28.- Tipo de amenaza: Difusión de software dañino

Tipo de activos:	**Dimensiones:**
- Aplicaciones (software)	disponibilidad integridad confidencialidad
Descripción: Propagación inocente de virus, espías(spyware), gusanos, troyanos, etc.	

Fuente: Elaboración propia

➢ Errores de reencaminamiento

Tabla 29.- Tipo de amenaza: Errores de reencaminamiento

Tipo de activos:	**Dimensiones:**
- Servicios - Aplicaciones(software) - Redes de comunicaciones	confidencialidad
Descripción: Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	

Fuente: Elaboración propia

➢ Errores de secuencia
➢ Escapes de información
➢ Alteración accidental de la información
➢ Destrucción de la información
➢ Fugas de información
➢ Vulnerabilidades de los programas
➢ Errores de mantenimiento/ actualización de programas
➢ Caídas del sistema por agotamiento de recursos
➢ Pérdida de equipos
➢ Indisponibilidad del personal

d. Ingeniería Social

- Causadas por las personas de forma accidental: Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- Causadas por las personas de forma deliberada: Las personas con acceso al sistema de información pueden ser causa de problemas intencionados

e. Extorción

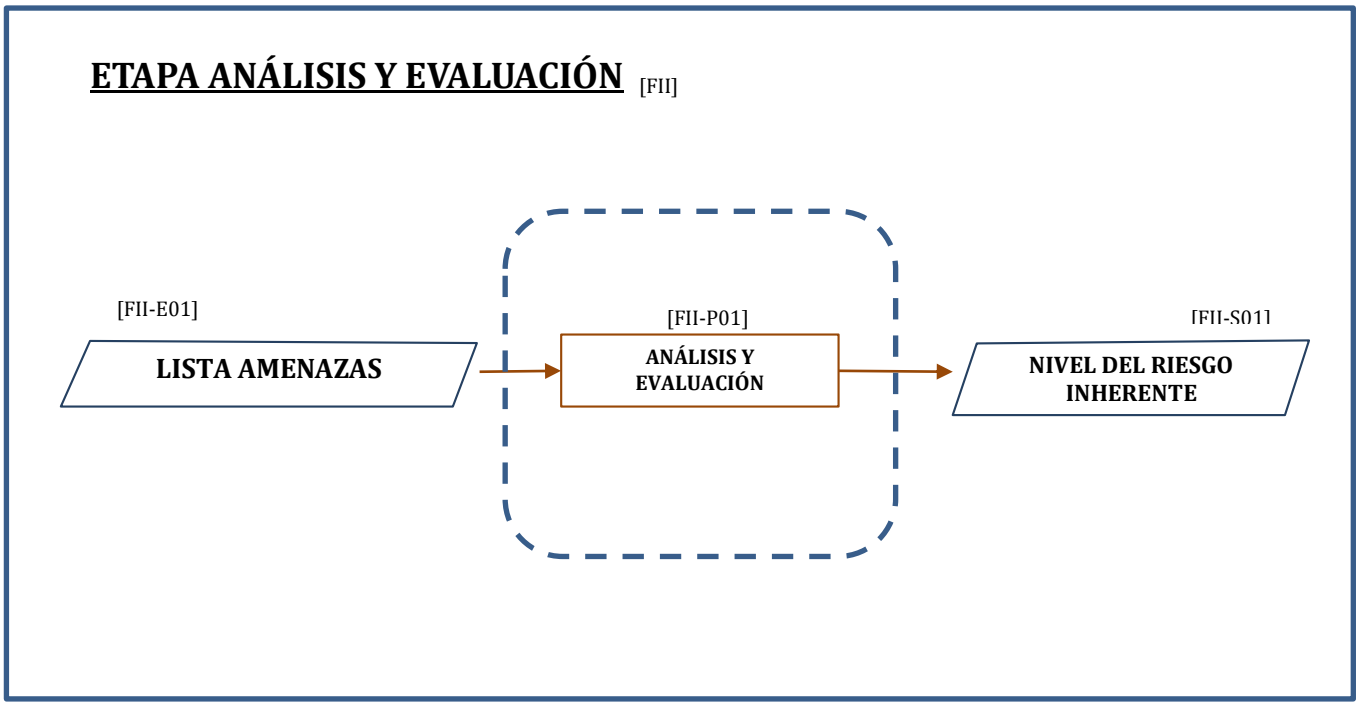
Causada por personas que sustraen información con el fin de sobornar a su víctima y obtener a cambio un beneficio económico.

3.4.1.2 Etapa análisis y evaluación

En la Fase de análisis y evaluación, tenemos que obtener el nivel de riesgo asociado a un activo de información priorizado. El nivel de riesgo lo calculamos en base a los niveles de probabilidad de materialización de las amenazas identificadas y los niveles de impacto al materializarse dichas amenazas (acápite 4.3 Desarrollo de la metodología de gestión de riesgos, 4.3.2.3 Estimar el nivel de riesgo inherente).

El cálculo del nivel de riesgo inherente, será realizado mediante el uso del Anexo N° 05: Formato matriz de riesgo, teniéndose como guía el Anexo N° 10: Manual de usuario para el uso de la matriz de riesgos.

Ilustración 14 Diagrama de la etapa de análisis y evaluación



Fuente: Elaboración propia

Tabla 30.- Actividades en Análisis y evaluación

ETAPA		ENTRADA		PROCESO		SALIDA	
FII	ANÁLISIS Y EVALUACIÓN	FII-E01	LISTA DE AMENAZAS	FII-P01	ANALISIS Y EVALUACIÓN	FII-S01	**NIVEL DE RIESGO INHERENTE**

Fuente: Elaboración propia

En esta etapa se estima el nivel de riesgo inherente de las amenazas asociadas a los activos de información identificados y se propone los respectivos mecanismos de protección para proteger cada activo de información.

1. **Definir probabilidad de materialización de amenaza sobre un activo de información:** Identificada las amenazas que pueden causar daño a un activo de información, debemos estimar la probabilidad de ocurrencia de materialización de dichas amenazas, en razón a las vulnerabilidades que se tengan:
   MAGERIT nos proporciona niveles de probabilidad que podemos utilizar para estimar la probabilidad de ocurrencia de una amenaza, los niveles se listan a continuación:

   Tabla 31.- Niveles de probabilidad de materialización de amenazas

PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS
5- MA: Prácticamente seguro
4- A: Probable
3- M: Posible
2- B: Poco probable
1- MB: Muy raro

   Fuente: Elaboración propia

2. **Definir impacto de materialización de amenaza sobre un activo de información:** Se tiene que estimar el nivel de impacto que pueda alcanzar una amenaza, al aprovechar las vulnerabilidades asociadas a un activo de información.

   MAGERIT nos proporciona niveles de impacto que podemos utilizar para estimar la probabilidad de ocurrencia de una amenaza; los niveles se listan a continuación:

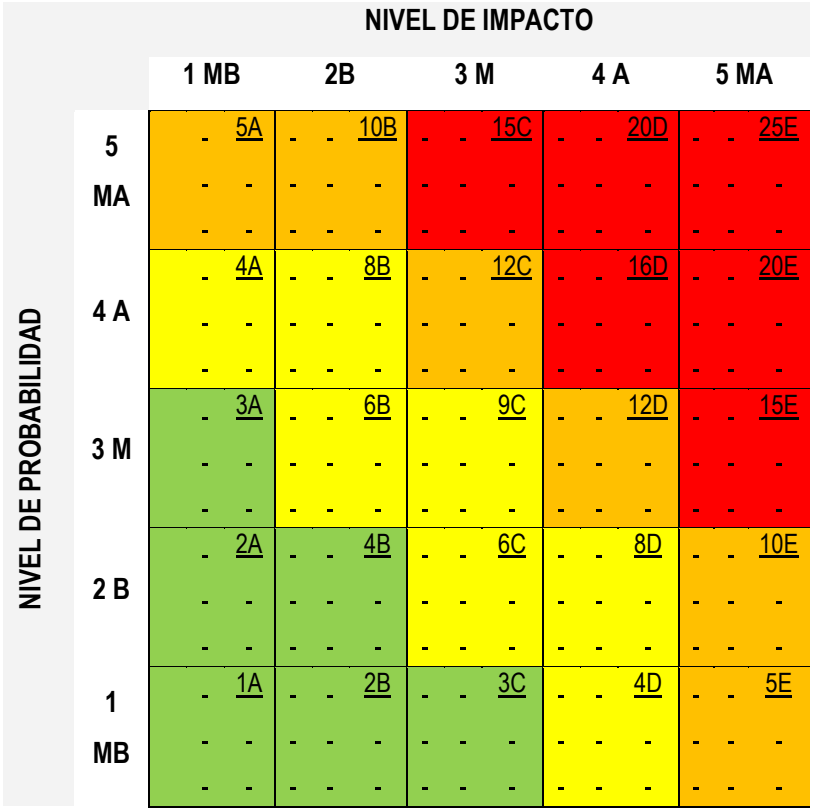
Tabla 32.- Niveles de impacto de amenazas

NIVELES DE IMPACTO
5- MA: Muy Alto
4- A: Alto
3- M: Medio
2- B: Bajo
1- MB: Muy bajo

Fuente: Elaboración propia

3. **Estimar el nivel de riesgo inherente:** El nivel de exposición al riesgo tal y como se encontró, antes de implementar medidas de mitigación, se obtiene a través de la multiplicación de los niveles de probabilidad e impacto, obteniéndose la siguiente matriz de riesgos:

Ilustración 15 Matriz de riesgos: Nivel de riesgo inherente



Fuente: elaboración propia

Finalmente se obtiene los siguientes niveles de riesgo:

Tabla 33.- Nivel de riesgo

COLORES	NIVEL DE RIESGO
	Extremo
	Alto
	Medio
	Bajo

Fuente: Elaboración propia

4. **Priorización de amenazas según su nivel de riesgo:** Como resultado de obtener los niveles de riesgo de impacto de amenaza a los que están expuesto los activos de información, podrán ser priorizados, de tal manera que puedan recibir un tratamiento especial para mitigar la exposición de sus riesgos, pudiéndose mitigar a primera instancia, aquellas amenazas que presenten niveles de riesgo inherente alto y extremo. Para aquellas amenazas que provoquen niveles Medio y Bajo, no es prioritario que se propongan mecanismos de protección, puesto que representan niveles bajo de exposición.

Nota: El resultado del cálculo para obtener Probabilidad y/o Impacto residual, obtenga valores menores o iguales a cero, la Probabilidad y/o Impacto residual tomarán el valor mínimo de 1.

Tabla 34.- Estrategia de tratamiento de riesgos

COLORES	NIVEL DE RIESGO	ESTRATEGIA DE TRATAMIENTO
	Extremo	Mitigar o Controlar (atención inmediata)
	Alto	Mitigar o Controlar
	Medio	Aceptar el riesgo
	Bajo	Aceptar el riesgo

Fuente: Elaboración propia

3.4.1.3 Etapa de tratamiento

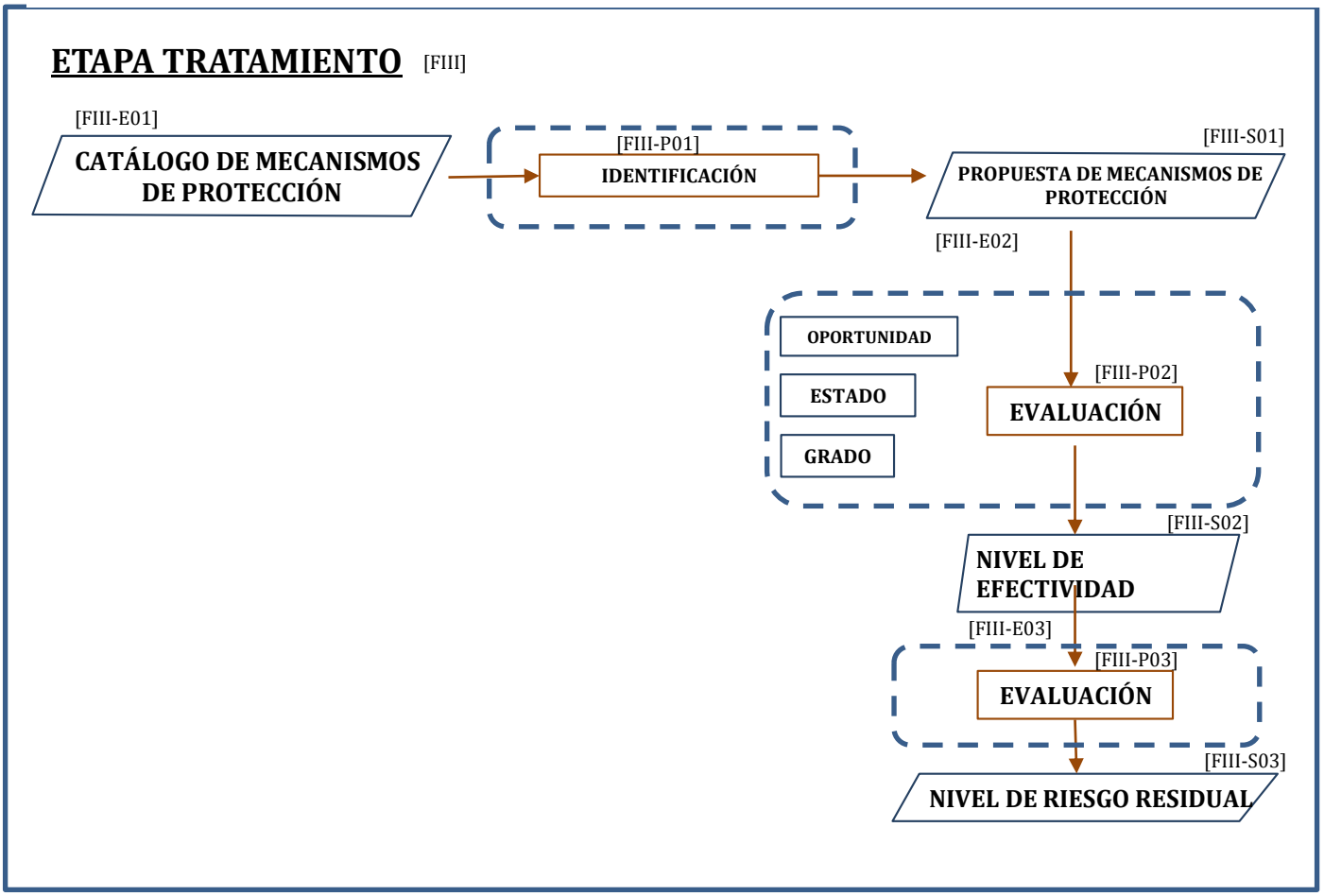
En la fase de tratamiento de riesgos, tomamos como referencia el Anexo N° 08: Catálogo de mecanismos de protección, de manera que podamos identificar y proponer los Mecanismos de protección aplicables para la mitigación de los riesgos identificados y asociados a los activos de información priorizados.

Las propuestas de mecanismos de protección, deben someterse a un proceso de evaluación, de manera que podamos obtener un nivel de efectividad de aplicación de mecanismos de protección (acápite 4.3 Desarrollo de la metodología de gestión de

riesgos, 4.3.3.2 Definir criterios para obtener niveles de efectividad de controles); éste proceso de evaluación deberá ser realizado en base a criterios de oportunidad, Estado de implementación y grado de implementación. Finalmente, en función al nivel de efectividad obtenida por cada mecanismo de protección, debemos calcular el nivel de riesgo residual (acápite 4.3 Desarrollo de la metodología de gestión de riesgos, 4.3.3.3 Definir probabilidad residual de materialización de amenazas, 4.3.3.4 Definir impacto residual de materialización de amenazas y 4.3.3.4 Definir el nivel de riesgo residual) asociado a los activos de información priorizados.

La fase de tratamiento de riesgos será realizado mediante el uso del Anexo N° 05: Formato matriz de riesgo, teniéndose como guía el Anexo N° 10: Manual de usuario para el uso de la matriz de riesgos.

Ilustración 16 Diagrama de la etapa de tratamiento



Fuente : elaboración propia

Tabla 35.- Actividades de tratamiento

ETAPA		ENTRADA		PROCESO		SALIDA	
FIII	TRATAMIENTO	FIII-E01	CATÁLOGO DE MECANISMOS DE PROTECCIÓN	FIII-P01	IDENTIFICACIÓN	FIII-S01	PROPUESTA DE MECANISMOS DE PROTECCIÓN
		FIII-E02	PROPUESTA DE MECANISMOS DE PROTECCIÓN	FIII-P02	EVALUACIÓN	FIII-S02	NIVEL DE EFECTIVIDAD
		FIII-E03	NIVEL DE EFECTIVIDAD	FIII-P03	EVALUACIÓN	FIII-S03	NIVEL DE RIESGO RESIDUAL

Fuente: Elaboración propia

Etapa de planteamiento de las medidas de seguridad que requiere una organización, de tal manera que se pueda mitigar los riesgos identificados en la etapa de Análisis y evaluación (riesgo residual)

1. **Proponer mecanismos de protección que permitan hacer frente a las amenazas:** Aquellas amenazas con niveles de exposición de riesgo Alto y Extremo deberán presentar mecanismos de protección, las mismas que serán evaluadas con la finalidad de mitigar los riesgos identificados.

   MAGERIT tipifica los mecanismos de protección de la siguiente manera:

   - Protecciones generales u horizontales
   - Protección de los datos / información
   - Protección de las claves criptográficas
   - Protección de los servicios
   - Protección de las aplicaciones (software)
   - Protección de los equipos (hardware)
   - Protección de las comunicaciones
   - Protección en los puntos de interconexión con otros sistemas
   - Protección de los soportes de información
   - Protección de los elementos auxiliares
   - Protección de las instalaciones
   - Mecanismos de protección relativas al personal
   - Mecanismos de protección de tipo organizativo
   - Continuidad de operaciones
   - Externalización
   - Adquisición y desarrollo

2. **Definir criterios para obtener niveles de efectividad de los mecanismos de protección:** Los mecanismos de protección propuestos para mitigar los riesgos deben tener niveles de efectividad ante las amenazas identificadas. La efectividad de los mecanismos de protección será medida a través de los siguientes criterios:
   - **Niveles de estado de mecanismos de protección**: se evaluaran si dichos mecanismos se encuentran implementados o no implementados.
   - **Niveles de oportunidad de propuesta de mecanismos de protección**: Se evaluarán si dichos mecanismos son: Preventivos, Detectivos o Correctivos
   - **Grado de implementación de mecanismos de protección** : El grado de implementación de mecanismos de protección considera los siguientes criterios: Manual, Semiautomático y Automatizado

De la combinación de estos criterios, se obtendrá los siguientes niveles de efectividad de los mecanismos de protección propuestos:

Tabla 36.- Niveles de efectividad

DESCRIPCION	VALOR
Óptimo	5
Bueno	4
Más que regular	3
Regular	2
Deficiente	1

Fuente: Elaboración propia

3. **Definir probabilidad residual de materialización de amenaza sobre un activo de información:** Los niveles de probabilidad residual bajarán en función del nivel de efectividad de mecanismos de protección de la siguiente manera:

Tabla 37.- Niveles de probabilidad residual

NIVEL DE EFECTIVIDAD DE MECANISMOS DE PROTECCIÓN		PROBABILIDAD RESIDUAL PMA(Probabilidad de Materialización de amenazas)
DESCRIPCION	**VALOR**	
Deficiente	1	PMA (menos) 0
Regular	2	PMA (menos) 1
Más que regular	3	PMA (menos) 2
Bueno	4	PMA (menos) 3
Óptimo	5	PMA (menos) 4

Fuente: Elaboración propia

4. **Definir impacto residual de materialización de amenaza sobre un activo de información:** Los niveles de impacto residual bajarán en función del nivel de efectividad de mecanismos de protección de la siguiente manera:

Tabla 38.- Niveles de impacto residual

NIVEL DE EFECTIVIDAD DE MECANISMOS DE PROTECCIÓN		IMPACTO RESIDUAL IMR: Impacto Residual
DESCRIPCION	**VALOR**	
Deficiente	1	IMR (menos) 0
Regular	2	IMR (menos) 1
Más que regular	3	IMR (menos) 2
Bueno	4	IMR (menos) 3
Óptimo	5	IMR (menos) 4

Fuente: Elaboración propia

5. **Estimar el Nivel de riesgo residual:** Es el nivel de riesgo de materialización de amenazas, después de haber implementado las medidas de control de riesgos, que lógicamente debería de haber disminuido, siempre y cuando sus mecanismos de protección hayan sido efectivos.

Ilustración 17 Matriz de riesgos: Nivel de riesgo residual

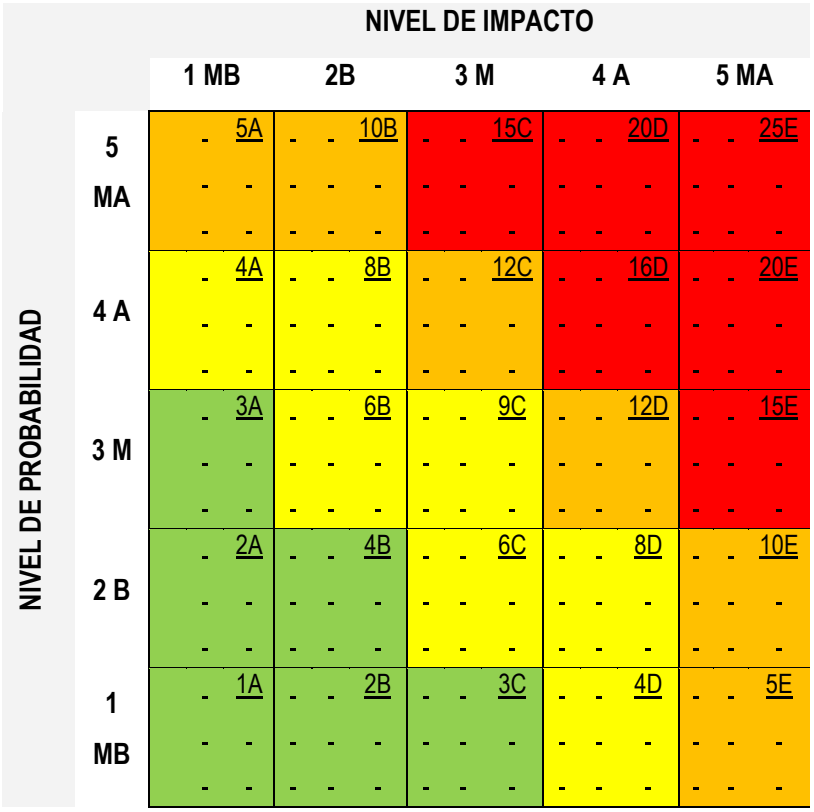


Tabla 39.- Niveles de riesgo residual

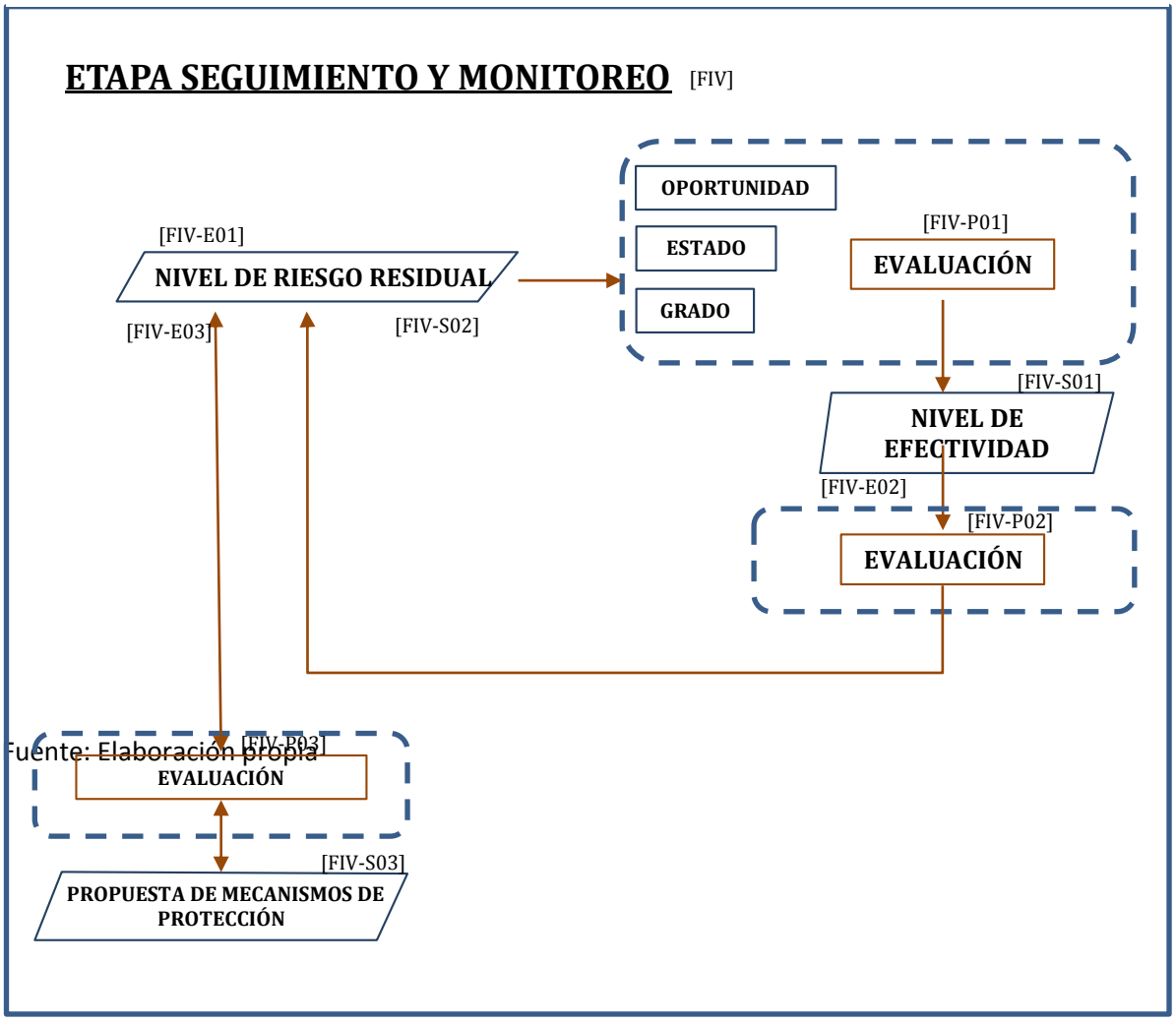
COLORES	NIVEL DE RIESGO
	Extremo
	Alto
	Medio
	Bajo

Fuente: Elaboración propia

3.4.1.4 Etapa de seguimiento y monitoreo

En la fase de Seguimiento y monitoreo, debemos tener como referencia el nivel de riesgo residual calculado en la etapa anterior, de manera que en el transcurso del tiempo, podamos contrastar que éste nivel de riesgo residual disminuya progresivamente. Cada vez que se evalúe y calcule el nivel de riesgo residual a través de periodos de tiempo transcurridos, deberá evaluarse la efectividad de los mecanismos de protección propuestos, con la finalidad de verificar si es necesario adicionar mecanismos de control para contener o disminuir niveles de riesgo asociados a los activos de información priorizados.

Ilustración 18 Diagrama de la etapa de seguimiento y monitoreo



Fuente: Elaboración propia

Fuente: Elaboración propia

Tabla 40.- Actividades de seguimiento y monitoreo

ETAPA		ENTRADA		PROCESO		SALIDA	
FIV	SEGUIMIENTO Y MONITOREO	FIV-E01	NIVEL DE RIESGO RESIDUAL	FIV-P01	EVALUACIÓN	FIV-S01	NIVEL DE EFECTIVIDAD
		FIV-E02	NIVEL DE EFECTIVIDAD	FIV-P02	EVALUACIÓN	FIV-S02	NIVEL DE RIESGO RESIDUAL
		FIV-E03	NIVEL DE RIESGO RESIDUAL	FIV-P03	EVALUACIÓN	FIV-S03	PROPUESTA DE MECANISMOS DE PROTECCIÓN

Fuente: Elaboración propia

En esta fase se realiza un seguimiento al nivel de efectividad obtenido de calificar los mecanismos de protección propuestas; a través del desarrollo de esta actividad, se obtiene el nivel de riesgo residual que presentan los activos de la información a lo largo del tiempo. En base al nivel de efectividad, se calcula la probabilidad e impacto residual cuyo producto da como resultado el nivel de riesgo residual. Este nivel de riesgo residual permite evaluar si el nivel de riesgo inherente está siendo mitigado.

3.5 Evaluación de calidad del modelo de gestión de riesgos propuesto

La calidad de un modelo de gestión de riesgos tiene por finalidad garantizar el cumplimiento de ciertas características referenciadas en la norma ISO/IEC 25010 respecto a la calidad del producto software, siendo contextualizadas en función a las necesidades de nuestro modelo propuesto, para evaluar su aplicabilidad.

Las características para garantizar la calidad de un modelo de gestión de riesgos, son las siguientes:

a) **Adecuación funcional:** Característica que tiene nuestro modelo de gestión de riesgos, cuya aplicación permite cumplir los requerimientos mínimos definidos en la política de seguridad de información del Ministerio de Salud.

b) **Compatibilidad:** Capacidad que tiene nuestro modelo de gestión de riesgos para ser aplicado en distintos servicios o instituciones del Ministerio de Salud.

c) **Usabilidad:** Capacidad que tiene nuestro modelo de gestión de riesgos para ser aplicado con facilidad, ser entendido, aprendido, usado por el usuario y que se adecuado a las necesidades del Hospital Regional Lambayeque respecto a la seguridad de la información.

d) **Fiabilidad:** Capacidad que tiene nuestro modelo de gestión de riesgos de ser fiable en su uso para cubrir las necesidades básicas del hospital, y que se puede ir complementándose y/o adaptándose a los requerimientos específicos del mismo Hospital Regional de Lambayeque, sin perder su fiabilidad en los resultados que arroje.

e) **Seguridad:** Capacidad que tiene nuestro modelo de gestión de riesgos, que permita implementar y mantener mecanismos de protección de seguridad de información para conservar la confidencialidad, integridad, disponibilidad, trazabilidad, y autenticidad de los datos y la información que administra, procesa y/o transfiere el Hospital Regional de Lambayeque.

f) **Mantenibilidad:** Capacidad que tiene nuestro modelo de gestión de riesgos cuya implementación, permita al Hospital Regional de Lambayeque realizar un control y seguimiento continuo del análisis de gestión de riesgos en la seguridad de la información.

g) **Portabilidad:** Capacidad que tiene nuestro modelo de gestión de riesgos para poder ser aplicado en distintas áreas o servicios de instituciones con diferente giro de negocio al de los hospitales del Ministerio de Salud.

CAPITULO IV. RESULTADOS

4.1. Situación actual de los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque

Actualmente el Hospital Regional de Lambayeque utiliza distintos sistemas de información como apoyo para brindar los servicios de gestión hospitalaria, dentro de los cuales encontramos a:

a. Sistema de gestión hospitalaria (Galen Plus o GalenHos); este sistema ha sido diseñado con el propósito de apoyar a la institución en el registro estandarizado de información de los empleados y pacientes, contribuir con una eficiente gestión de los procesos operativos críticos de un hospital, específicamente los de consulta externa, hospitalización, emergencia, archivo clínico y facturación, así como a optimizar el uso de los recursos de la institución. Este sistema cuenta con los siguientes módulos de trabajo:

- **Consulta Externa**: Incluye la administración de una base de datos de filiación así como también el registro de diagnósticos y procedimientos (según lo estipulado en la CIE 10 y en el Catálogo de Servicios de Ministerio de Salud). A diferencia de los módulos de hospitalización y emergencia, cuenta con un submódulo para la asignación de citas.

- **Hospitalización**: Considera la filiación de pacientes y registra diagnósticos y procedimientos. Además cuenta con un submódulo para la administración de camas hospitalarias.

- **Emergencia**: Al igual que Consulta Externa y Hospitalización, cuenta con filiación y registro de diagnósticos y procedimientos. Asimismo también permite la administración de las camas de observación en el servicio de emergencia.

- **Facturación**: Gestiona órdenes de servicio y fuentes de pago y de financiamiento; es el módulo encargado de administrar las cuentas corrientes de pacientes. Cuenta con un submódulo de caja que permite controlar los

cobros realizados a los pacientes y manejar los cierres o arqueos diarios de caja.

- **Archivo Clínico**: Módulo encargado de recibir solicitudes de historias clínicas para su búsqueda y monitorear las historias clínicas que se encuentran fuera del archivo.

b. Sistema web de guardias hospitalarias y control de raciones (SIGHOR)

El sistema web de guardias hospitalarias se ha desarrollado con el propósito de brindar servicios informáticos en lo que respecta a la programación de las guardias y/o turnos hospitalarios en el Hospital Regional de Lambayeque.

Este sistema está orientado a soportar los procesos de programación, cambio de turnos y/o guardias, evitar errores en la liquidación y programación total de horas mensuales, obteniendo beneficios tanto a nivel institucional como a nivel de personal que labora en dicha institución.

Así mismo, como parte de los entregables en la implementación de este sistema, el Hospital Regional de Lambayeque cuenta con un "Manual de usuario del SIGHOR", el mismo que establece los requerimientos mínimos de hardware y software que se deben tomar en cuenta, para tener una mejor funcionalidad del sistema.

El sistema SIGHOR cuenta con los siguientes módulos:

- **Módulo de mantenimiento:** Es a través de este módulo donde se agrega, consulta información, actualiza y/o elimina usuarios, empleados, departamentos, dependencias, actividades, tipo de trabajador, niveles remunerativos, tipo de guardia, grupos ocupacionales, guardias valorizadas, perfiles de usuario, opciones de menú y sub menú.

- **Módulo de creación de roles:** Este módulo permite crear la programación del rol de asistencia, programación de turnos y/o guardias para profesionales de la salud, otros profesionales de la salud – no

médicos, residentes, técnicos e internos de medicina; además la programación de ración a beneficiarios.

- **Módulo de roles pendientes:** Este módulo permite visualizar y editar la programación de roles pendientes para profesionales de la salud, otros profesionales de la salud - no médicos, residentes, técnicos, internos de medicina y ración a beneficiarios.

- **Módulo de roles aprobados:** Este módulo permite visualizar los roles de turnos y/o guardias que están aprobados para profesionales de la salud, otros profesionales de la salud - no médicos, residentes, técnicos, internos de medicina y otros beneficiarios. Para que un rol sea aprobado debe tener las siguientes validaciones: 1°: Revisa programación- Jefe de departamento, 2°: Responsable programación- Coordinador, 3°: Revisa U. de personal – Unidad de personal y 4°: Aprueba programación – Director de servicios de salud.

- **Módulo de nutrición:** Este módulo permite generar las raciones por servicio, roles hospitalarios que han sido aprobados y otros beneficiarios, también se puede visualizar las programaciones generadas de raciones y el reporte para el comedor.

- **Módulo de reportes:** Este módulo permite visualizar, imprimir y exportar los diferentes tipos de reportes de los roles consignados en este sistema.

- **Módulo de Movimientos:** Este módulo permite realizar los cambios de turno de las guardias que se van a realizar, estos cambios siempre se realizan entre el mismo tipo de guardia o turno.

c. Sistema de gestión de biopsias (SIGBIO):

El sistema de gestión de biopsias se ha desarrollado con el propósito de mejorar la gestión de los procesos que intervienen en el estudio de las biopsias, llevar un control del tiempo de estudio de éstas, generar informes para tomar desiciones y

realizar un seguimiento de los movimientos que se realizan en el sistema, obteniendo beneficios tanto a nivel institucional como a nivel de personal que labora en dicha institución.

Así mismo, como parte de los entregables en la implementación de este sistema, el Hospital Regional de Lambayeque cuenta con un "Manual de usuario del SIGBIO", el mismo que establece los requerimientos mínimos de hardware y software que se deben tomar en cuenta, para tener una mejor funcionalidad del sistema.

El sistema SIGBIO cuenta con los siguientes módulos:

- **Módulo de mantenimiento:** Es a través de este módulo donde se agrega, consulta información, actualiza y/o elimina usuarios, pacientes, marcadores, topografías, diagnósticos CCV, guía médico, muestras y biopsias.

- **Módulo de paciente:** Este módulo permite buscar al paciente y su historial, registrar la información de las muestras de la biopsia e imprimir las etiquetas de macroscopía y código de canastillas.

- **Módulo patología quirúrgica:** Este módulo permite modificar la información de recepción de biopsias, registrar el estudio macroscópico y microscópico de las biopsias del área de Patología quirúrgica e imprimir los informes para entregar a los pacientes.

- **Módulo citología especial:** Este módulo permite modificar la información de recepción de las biopsias, registrar el estudio macroscópico y microscópico de las biopsias del área de Citología especial e imprimir los informes para entregar a los pacientes.

- **Módulo citología cérvico vaginal:** Este módulo permite modificar la información de recepción de las biopsias, registrar el estudio macroscópico y microscópico de las biopsias del área de Citología cérvico vaginal e imprimir los informes para entregar a los pacientes.

- **Módulo inmunohistoquímica:** Este módulo permite modificar la información de recepción de las biopsias, registrar el estudio macroscópico y microscópico de las biopsias del área de Inmunohistoquímica e imprimir los informes para entregar a los pacientes.

- **Módulo monitoreo:** Este módulo permite realizar un seguimiento de los movimientos que se registran en el sistema y también tener un control de ellos, esto se ve reflejado en las siguientes opciones: Bitácora, Control de seguridad de la ISO/IEC 27001, Asigna Tecnólogo y Estado de biopsia.

- **Módulo guía médico:** Este módulo permite visualizar las diferentes guías en diversos formatos, como libros, url, imágenes, etc. Las cuales son de apoyo y orientación para el médico.

- **Módulo de reportes:** Este módulo permite visualizar e imprimir los diferentes informes y estadísticas que sirven para tomar decisiones dentro del servicio.

d. Sistema de asignación de camas: Este sistema ha sido diseñado con el propósito de tener una eficiente gestión en el control y asignación de camas a los pacientes, en el servicio hospitalario. En este sistema se visualizan la cantidad de camas por servicio para que sean asignadas a los pacientes que son ingresados para su hospitalización; cuando el paciente recibe un "alta", esta cama se libera y pasa a un estado de "limpieza o desinfección" para que luego se encuentre "disponible" para su próxima asignación a un nuevo paciente.

   Este sistema web es relativamente nuevo, pero aún no cuenta con documentación técnica para los desarrolladores, ni un manual para guía de los usuarios que a diario utilizan este sistema para gestionar las camas de los pacientes a que ingresarán o se encuentran ya hospitalizados.

La información respecto a la situación actual de la seguridad de la información en los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque, obtenida de las diversas técnicas de recolección de datos empleadas en este proyecto de investigación, se indicó que los administradores de sistemas de información, enfocan sus esfuerzos en cubrir criterios de seguridad de la información al momento de la creación de usuarios, dado que estos son asociados a un perfil correspondiente, en función a lo que requieran las áreas usuarias; sin embargo, no existe evidencia del análisis técnico sobre los perfiles asignados a los usuarios, de manera que estén alineados a los niveles de autorización y función que desempeñen en la institución, a fin que se realice un adecuado acceso y manejo de la información con la que se trabaje a través de los sistemas. De igual manera, no se evidencia que exista una revisión periódica de dichos accesos, ni otra medida adicional de seguridad.

4.2. Situación de las políticas de seguridad de información del Ministerio de Salud en el Hospital Regional de Lambayeque

El Ministerio de Salud es la institución que regula y supervisa al Hospital Regional de Lambayeque a través del cumplimiento de sus políticas institucionales establecidas, entre las que se definen políticas de seguridad de la información. Ante esta situación, se realizó un breve análisis de la situación actual en el Hospital Regional Lambayeque, respecto al cumplimiento de estas políticas:

a. La información es un activo institucional: el Ministerio de Salud indica que la información es un activo con valor para la institución, y como tal requiere una protección adecuada, así mismo resalta la importancia de implementar un compromiso con el desarrollo, el mantenimiento de sistemas de información y el tratamiento de información no automatizada.

   Actualmente el HRL no cuenta con una política de gestión de inventario de activos de información que brinde mayor detalle sobre la exposición a la que se encuentran y el tratamiento que deben de tener por sus responsables.

b. Compromiso de la alta dirección y de los órganos del Ministerio de Salud: el Ministerio de Salud requiere que el alta dirección de todas sus dependencias demuestran liderazgo y compromiso respecto del sistema de gestión de seguridad de la información asegurando los requisitos del sistema, los recursos y comunicando la importancia de una efectiva gestión de seguridad de la información a toda la institución.

   Actualmente el HRL no precisa de un claro compromiso por parte de la alta dirección, en asignar los recursos necesarios para implementar un sistema de gestión de seguridad de la información en el HRL y para capacitar al personal en temas relacionados a la gestión de seguridad de la información.

c. La seguridad de la información es el soporte de los procesos y procedimientos institucionales: el Ministerio de Salud insta a preservar la confidencialidad, integridad y disponibilidad de la información que se requiere, se procesa y genera.

   Actualmente en el Hospital Regional de Lambayeque no se evidencia un análisis y evaluación de los potenciales riesgos asociados a los activos de información, que puedan afectar la confidencialidad, integridad y disponibilidad de la información que se requiera, procese o genere.

d. Personal involucrado con la seguridad de la información: el Ministerio de Salud mediante sus lineamientos establece los niveles de autoridad y responsabilidad en el sistema de gestión de seguridad de la información, para defender y reportar su desempeño a la alta dirección.

   Actualmente el Hospital Regional de Lambayeque, no cuenta con una estructura orgánica que desempeñe funciones relacionadas a la seguridad de la información, del mismo modo, no se imparten capacitaciones, círculos de calidad y/o concientiza al personal a cerca de la importancia de la seguridad

de la información y el impacto de materialización de los riesgos asociados al incumplimiento de políticas y/o controles de seguridad de la información.

e. Prevención de riesgos y aplicación de mecanismos de protección: el Ministerio de Salud indica que los responsables de la información deben identificar, evaluar y tratar de manera ineludible los riesgos de seguridad de la información, aplicando formalmente la metodología de riesgos de acuerdo a lo señalado en la Norma Técnica Peruana ISO/IEC 27001 vigente.

   Actualmente el Hospital Regional de Lambayeque, no cuenta con una estructura orgánica que desempeñe funciones relacionadas a la seguridad de la información, la misma que incluye la identificación, evaluación y tratamiento de los riesgos asociados a activos de información.

f. Mantener la seguridad de la información en niveles óptimos: El Ministerio de Salud indica evaluar el desempeño, efectividad y conveniencia del sistema de gestión de seguridad de la información en relación a sus objetivos institucionales y que los problemas de seguridad de la información se reporten, investiguen y resuelvan mediante mecanismos de protección establecidos en la Norma Técnica Peruana ISO/IEC 27001 vigente y se acarrean responsabilidades administrativas, civiles y/o penales conforme al marco legal vigente.

   La Gestión de seguridad de la información en el Hospital Regional de Lambayeque, actualmente no es evaluado a través de un proceso de auditorías internas y/o externas, a fin de identificarse debilidades en dicha gestión y reforzar el cumplimiento de políticas y controles que permitan preservar la seguridad de la información. De igual manera no cuenta con un procedimiento establecido para la gestión de incidentes de seguridad de la información.

g. El bien público en salud respeta los datos personales individuales: el Ministerio de Salud indica que la disponibilidad de datos personales y diagnóstico de los pacientes debe restringirse a los casos dispuestos por políticas públicas y el tratamiento de dicha información se realice con respeto

y discreción, difundiéndose solo como información estadística y en forma anónima.

El Hospital Regional de Lambayeque actualmente no cuenta con políticas de seguridad de la información asociada a la protección de datos personales, en la que se establezcan lineamientos para conservar la privacidad de datos personales por medio de medidas técnicas, organizativas y normativas, y establecer criterios para clasificar y etiquetar la información contenida en sus activos de información.

h. El tratamiento de datos personales requiere el consentimiento de su titular: el Ministerio de Salud indica que se deben prevalecer los principios de confidencialidad, integridad y disponibilidad de la información de los datos personales, a través de la implementación de medidas técnicas, organizativas y normativas establecidas en la directiva de seguridad de la información.

El Hospital Regional de Lambayeque actualmente no cuenta con políticas de seguridad de la información asociada a la protección de datos personales, en la que se establezcan lineamientos para conservar la privacidad de datos personales por medio de medidas técnicas, organizativas y normativas, y establecer criterios para clasificar y etiquetar la información contenida en sus activos de información.

Análisis de encuestas para recolección de datos

Se realizaron tres tipos de encuesta para la recolección de datos a fin de realizar el análisis de la seguridad de la información en el contexto actual del Hospital Regional de Lambayeque, teniendo en cuenta las políticas planteadas por el Ministerio de Salud:

- La información es un activo institucional
- Compromiso de la alta dirección y de los órganos del ministerio de salud
- La seguridad de la información es el soporte de procesos y procedimientos institucionales
- Personal involucrado con la seguridad de la información

- Prevención de riesgos y aplicación de controles
- Mantener la seguridad de la información en niveles óptimos

4.2.1 Encuesta a usuarios de los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque:

a) La información es un activo de información

Tabla 41.- Pregunta 3- Usuarios de los sistemas

PREGUNTA N° 3	SI	NO
Cuenta con carpetas u unidades compartidas, en la intranet.	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, se cuenta con carpetas o unidades compartidas en la intranet.

Tabla 42.- Pregunta 6- Usuarios de los sistemas

PREGUNTA N° 6	SI	NO
Cuenta con información institucional compartida en unidades virtuales (Drive, Dropbox, etc)	29%	71%

Fuente: Elaboración propia

Comentario: El 29% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios cuentan con información institucional compartida en unidades virtuales (Drive, Dropbox, etc). Mientras que el 71% afirma que los usuarios no cuentan con información institucional compartida en unidades virtuales.

Tabla 43.- Pregunta 7- Usuarios de los sistemas

PREGUNTA N° 7	SI	NO
Cuenta con cuenta de correo propio de la institución	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios tienen cuentas de correo propio de la institución.

b) Compromiso de la alta dirección y de los órganos del ministerio de salud

Tabla 44.- Pregunta 20- Usuarios de los sistemas

PREGUNTA N° 20	SI	NO
Recibe orientación o charlas eventuales para seguir normas de seguridad de la información	14%	86%

Fuente: Elaboración propia

Comentario: El 14% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios reciben orientación o charlas eventuales para seguir normas de seguridad de la información. Mientras que el 86% manifiesta que no reciben tales orientaciones o charlas eventuales.

c) La seguridad de la información es el soporte de procesos y procedimientos institucionales

Tabla 45.- Pregunta 1- Usuarios de los sistemas

PREGUNTA N° 1	SI	NO
Cuenta con accesos propios para ingresar a los equipos informáticos (pc/laptos)	100%	0

Fuente: Elaboración propia

Comentario:

El 100% de la muestra afirma que el Hospital Regional Lambayeque cuenta con accesos propios para ingresar a los equipos informáticos.

Tabla 46.- Pregunta 2- Usuarios de los sistemas

PREGUNTA N° 2	SI	NO
Cambia las contraseñas en los equipos asignados	86%	14%

Fuente: Elaboración propia

Comentario: El 86% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios cambian cada 2-3 meses, las contraseñas en los equipos de cómputo asignados. Mientras que el 14% afirma que no cambian las contraseñas en los equipos de cómputo asignados.

d) Personal involucrado con la seguridad de la información

Tabla 47.- Pregunta 14- Usuarios de los sistemas

PREGUNTA N°14	SI	NO
Sigue las políticas de creación de contraseñas de la institución	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios siguen las políticas de creación de contraseñas de la institución.

e) Prevención de riesgos y aplicación de controles

Tabla 48.- Pregunta 10- Usuarios de los sistemas

PREGUNTAN°10	SI	NO
Existe alguna restricción de acceso a los ambientes en el que guardan sus archivos físicos	57%	43%

Fuente: Elaboración propia

Comentario: El 57% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios tienen alguna restricción de acceso a los ambientes en el que guardan sus archivos físicos. Mientras que el 43% afirma que no tienen restricciones de acceso a estos ambientes.

Tabla 49.- Pregunta 11- Usuarios de los sistemas

PREGUNTA N° 11	SI	NO
Existe alguna restricción de acceso a los ambientes en el que se encuentra su equipo informático	0	100%

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios no tienen alguna restricción de acceso a los ambientes en el que se encuentra su equipo informático.

Tabla 50.- Pregunta 12- Usuarios de los sistemas

PREGUNTA N° 12	SI	NO
Tiene acceso a dispositivos de impresión	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios tienen acceso a los dispositivos de impresión.

Tabla 51.- Pregunta 13- Usuarios de los sistemas

PREGUNTA N° 13	SI	NO
Tiene acceso a dispositivos de impresión de otras áreas.	14%	86%

Fuente: Elaboración propia

Comentario: El 14% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios tienen acceso a dispositivos de impresión de otras áreas, mientras que el 88% manifiesta que no cuentan con dichos accesos.

Tabla 52.- Pregunta 15- Usuarios de los sistemas

PREGUNTA N° 15	SI	NO
Presenta problemas usuales para ingresar a sus conexiones de internet	29%	71%

Fuente: Elaboración propia

Comentario: El 29% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios presentan problemas usuales de conexión de internet. Mientras que el 71% manifiesta que no presentan problemas de conexión a internet.

Tabla 53.- Pregunta 16- Usuarios de los sistemas

PREGUNTA N° 16	SI	NO
Presenta problemas usuales para ingresar a sus equipos informáticos	0	100%

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios no presentan problemas usuales para ingresar a sus equipos informáticos.

Tabla 54.- Pregunta 17- Usuarios de los sistemas

PREGUNTA N° 17	SI	NO
Comparte usuarios en el acceso de los sistemas información	0	100%

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios no comparten sus cuentas de usuarios con otros colaboradores, para acceder a los sistemas de información. Es decir cada usuario tiene su propia cuenta de acceso a los sistemas de información.

Tabla 55.- Pregunta 18- Usuarios de los sistemas

PREGUNTA N° 18	SI	NO
Presenta problemas usuales para ingresar a sus sistemas de información	0	100%

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios no presentan problemas usuales para ingresar a sus sistemas de información.

Tabla 56.- Pregunta 19- Usuarios de los sistemas

PREGUNTA N° 19	SI	NO
Presenta problemas para compartir o enviar información	0	100%

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios no presentan problemas para compartir información por medio de unidades compartidas o enviar información a través del correo institucional.

f) Mantener la seguridad de la información en niveles óptimos

Tabla 57.- Pregunta 4- Usuarios de los sistemas

PREGUNTA N° 4	SI	NO
Cuenta con permisos para guardar información en dispositivos externos (memorias usb, cd,s)	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, el personal cuenta con permisos de acceso para guardar información en dispositivos externos (memorias USB, CD's, etc).

Tabla 58.- Pregunta 5- Usuarios de los sistemas

PREGUNTA N° 5	SI	NO
Cuenta con permisos para acceder de forma remota a sus equipos informáticos	71%	29%

Fuente: Elaboración propia

Comentario: El 71% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios cuentan con permisos para acceder de forma remota a sus equipos informáticos. Mientras que el 29% afirma que no cuentan con los permisos mencionados.

Tabla 59.- Pregunta 8- Usuarios de los sistemas

PREGUNTA N° 8	SI	NO
Cuenta con un límite máximo para el tamaño de archivos enviados vía email	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que en el Hospital Regional de Lambayeque, los usuarios cuentan con un límite máximo para el tamaño de archivos enviados vía email.

4.2.2 Encuesta a responsables de la administración y mantenimiento de los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque

a) La información es un activo institucional

Tabla 60.- Pregunta 5- Responsables de administración

PREGUNTA N°5	SI	NO	N/A
Cuentan con un inventario actualizado de los activos de la información del Hospital Regional de Lambayeque	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que el Hospital Regional de Lambayeque cuenta con un inventario actualizado de software y hardware. Sin embargo el Hospital Regional de Lambayeque no cuenta con una Política de seguridad de la información que incluya normas y controles relacionados a la gestión de activos de información, ni una metodología que brinde los lineamientos para realizar un Inventario de activos de información y la gestión de riesgos asociados a los activos de la información.

Tabla 61.- Pregunta 13- Responsables de administración

REGUNTA N° 13	SI	NO	N/A
Los usuarios cuentan con unidades virtuales para compartir información	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra manifiesta que los usuarios cuentan con unidades virtuales para compartir información.

b) Compromiso de la alta dirección y de los órganos del Ministerio de Salud

Tabla 62.- Pregunta 1- Responsables de administración

PREGUNTA N° 1	SI	NO	N/A
Existen políticas de seguridad de la información documentadas para el Hospital Regional de Lambayeque	25%	50%	25%

Fuente: Elaboración propia

Comentario: El 50% de los encuestados afirman que en el Hospital Regional de Lambayeque no existen políticas de seguridad de la información documentadas para el Hospital Regional de Lambayeque. El 25% afirma que sí existen políticas de seguridad de la información; en cambio el 25% restante afirman no tener conocimiento de la existencia de políticas de seguridad de la información.

El HRL no cuenta con una Política de seguridad de la información aprobada formalmente por un Comité de seguridad de la información u otro organismo de gestión y control designado en el Hospital Regional de Lambayeque; En muy pocas ocasiones se ejecutan actividades asociadas a seguridad de información, que no va más allá que la aplicación de controles, como buenas prácticas.

c) La seguridad de la información es el soporte de procesos y procedimientos institucionales

Tabla 63.- Pregunta 6- Responsables de administración

PREGUNTA N° 6	SI	NO	N/A
La asignación de los perfiles de accesos se realiza mediante un procedimiento establecido.	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que si se asignan perfiles de acceso mediante un procedimiento establecido. En el Hospital Regional de Lambayeque si se asignan perfiles de acceso a los usuarios, en los sistemas de información, como buenas prácticas; pero no se cuenta con matrices de asignación de perfiles y acceso a usuarios hacia los sistemas de información.

Tabla 64.- Pregunta 7- Responsables de administración

PREGUNTA N° 7	SI	NO	N/A
La restricción de los perfiles de acceso de los exempleados se realiza :			
El mismo día en que se retira de la institución	0	0	0
Entre 1 a 3 días luego que se retira de la institución	75%	0	0
Hasta una semana después de retirarse de la institución	0	0	0
Otros	25%	0	0

Fuente: Elaboración propia

Comentario: El 75% de la muestra afirma que la baja de usuarios, se realiza entre 1 a 3 días de cesado un colaboradores y el 25% afirma que el plazo es más de una semana después del cese laboral de un colaborador.
En el Hospital Regional de Lambayeque no se realizan correctamente todas las bajas de usuario en los sistemas de información, es más no existe un procedimiento establecido que guie la gestión de accesos y perfiles de usuarios.

Tabla 65.- Pregunta 8- Responsables de administración

PREGUNTA N° 8	SI	NO	N/A
Cuenta con políticas para la creación de contraseñas de los usuarios	75%	25%	0

Fuente: Elaboración propia

Comentario: El 75% de la muestra manifiesta que si se cuenta con políticas para la creación de contraseña de los usuarios, mientras que el 25% manifiesta que no existen tales políticas.
Los sistemas de información del Hospital Regional de Lambayeque si cuentan con controles mínimos para crear contraseñas seguras, pero no hay Políticas de seguridad de información con directivas de creación, uso, actualización, confidencialidad entre otros aspectos aplicados a contraseñas seguras.

Tabla 66.- Pregunta 9- Responsables de administración

PREGUNTA N° 9	SI	NO	N/A
Cuenta con políticas para la actualización de contraseñas de los usuarios	50%	50%	0

Fuente: Elaboración propia

Comentario: El 50% de la muestra manifiesta que si se cuenta con políticas para la actualización de contraseña de los usuarios, mientras que el 50% manifiesta que no existen tales políticas.

Los sistemas de información del Hospital Regional de Lambayeque si cuentan con controles mínimos para crear contraseñas seguras, pero no hay Políticas de seguridad de información con directivas de creación, uso, actualización, confidencialidad, entre otros aspectos aplicados a una contraseña segura.

Tabla 67.- Pregunta 14- Responsables de administración

PREGUNTA N° 14	SI	NO	N/A
Existen tipos de accesos para la administración usuarios en el uso de carpetas virtuales	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra manifiesta que existen tipos de accesos para la administración de usuarios en el uso de carpetas virtuales.

Tabla 68.- Pregunta 16- Responsables de administración

PREGUNTA N° 16	SI	NO	N/A
Existen perfiles de acceso para el uso de sistemas informáticos.	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que existen perfiles de acceso para el uso de sistemas informáticos. En el Hospital Regional de Lambayeque si se asignan perfiles de acceso a los usuarios, en los sistemas de información, como buenas prácticas; pero no se realiza correctamente la baja respectivo de dichos accesos al momento de los ceses laborales o por motivos de absentismos de los colaboradores; tampoco existen lineamientos de un procedimiento establecido que guie la gestión de accesos y perfiles de usuarios.

d) Personal involucrado con la seguridad de la información

Tabla 69.- Pregunta 3- Responsables de administración

PREGUNTA N° 3 Cada cuanto tiempo se realizan charlas preventivas para el manejo de la seguridad de la información en los usuarios.	SI	NO	N/A
Cada 2 o 3 meses	0	0	0
Cada 4 o 6 meses	25%	0	0
Anualmente	25%	0	0
Otro	50%	0	0

Fuente: Elaboración propia

Comentario: El 50% de la muestra afirma que no se realizan charlas preventivas para el manejo de la seguridad de información en el Hospital Regional de Lambayeque;

mientras que el 25% menciona que se realiza entre 4 a 6 meses; sin embargo el 25% restante afirma que dichas charlas se realizan anualmente.
En las entrevistas desarrolladas con el personal del Hospital Regional de Lambayeque, nos informaron que el Hospital Regional de Lambayeque no cuenta con una Política de seguridad de la información, tampoco se elabora un Plan de Capacitaciones anuales a los colaboradores del Hospital, y por último, no se Concientiza a los usuario, sobre la importancia de la seguridad de la información, como una línea de defensa, para mitigar riesgos asociados.

e) Prevención de riesgos y aplicación de controles

Tabla 70.- Pregunta 10- Responsables de administración

PREGUNTA N° 10	SI	NO	N/A
Cuenta con restricciones de acceso para el ingreso en ambientes con equipos informáticos	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra manifiesta que el Hospital Regional de Lambayeque cuenta con restricciones de acceso para el ingreso en ambientes con equipos informáticos.
El Hospital Regional de Lambayeque si cuenta con medidas de control para restringir el acceso a áreas administrativas a través del personal de vigilancia; así mismo en las puertas de ingreso a las instalaciones de *tecnologías de la información* cuentan con etiquetas que prohíben el acceso a personal no autorizado. Del mismo modo el acceso al DataCenter está controlado a través de un sistema biométrico de Huella digital, para permitir el acceso solo a personal autorizado. Sin embargo el Hospital Regional de Lambayeque no cuenta con normas y controles establecidos formalmente a través de una Política de seguridad de la información aplicado específicamente a la seguridad física y ambiental.

Tabla 71.- Pregunta 17- Responsables de administración

PREGUNTA N° 17	SI	NO	N/A
Se realiza el control de accesos y tráfico de los usuarios de los sistemas informáticos.	75%	25%	0

Fuente: Elaboración propia

Comentario: El 75% de la muestra afirma que existen controles de acceso a los usuarios en los sistemas informáticos. Sin embargo en el Hospital Regional de Lambayeque, no existen responsables de la revisión de accesos en los sistemas de información, de manera que se puedan validar si la lista de personal considerado en planilla es la que se encuentra registrado en los sistemas de información con accesos vigentes, garantizando de ésta manera que todo personal que no esté laborando en el Hospital Regional de Lambayeque haya sido dado de baja en los sistemas de información.

Tabla 72.- Pregunta 18- Responsables de administración

PREGUNTA N° 18	SI	NO	N/A
Realizan mantenimientos preventivos de equipos informáticos	75%	25%	0

Fuente: Elaboración propia

Comentario: El 75% de la muestra afirma en el Hospital Regional de Lambayeque se realizan los mantenimientos preventivos de equipos informáticos.

Tabla 73.- Pregunta 19- Responsables de administración

PREGUNTA N° 19	SI	NO	N/A
Realizan supervisión de equipos de redes	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que si se realiza supervisión de equipos de redes

Tabla 74.- Pregunta 20- Responsables de administración

PREGUNTA N° 20	SI	NO	N/A
Realizan backups de correos electrónicos eventualmente	25%	75%	0

Fuente: Elaboración propia

Comentario: El 25% de la muestra, afirma que en el Hospital Regional de Lambayeque se realizan eventualmente, backups completos de las bases de datos. Sin embargo, en el Hospital Regional de Lambayeque no existe una bitácora del registro de esos backups de manera que se pueda identificar el responsable de la realización de ésta actividad, fecha y hora de realización y motivos de realización de ésta actividad. De igual manera no se puede evidenciar el resguardo de éstos backups fuera de las instalac7iones de tecnologías de la información, incluso en otras instalaciones fuera del edificio donde se ubica el área de tecnologías de la información.

Tabla 75.- Pregunta 21- Responsables de administración

PREGUNTA N° 21	SI	NO	N/A
Realizan backups de la información equipos informáticos eventualmente	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma en el HRL se realizan eventualmente, backups de la información de los equipos informáticos.

Tabla 76.- Pregunta 22- Responsables de administración

PREGUNTA N° 22	SI	NO	N/A
Se realizan backups completos de las bases de datos	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma en el HRL se realizan eventualmente, backups completos de las bases de datos. Sin embargo, en el HRL no existe una bitácora del registro de esos backups de manera que se pueda identificar el responsable de la realización de ésta actividad, fecha y hora de realización y motivos de realización de ésta actividad. De igual manera no se puede evidenciar el resguardo de éstos backups fuera de las instalaciones de TI, incluso en otras instalaciones fuera del edificio donde se ubica el área de TI.

Tabla 77.- Pregunta 23- Responsables de administración

PREGUNTA N° 23	SI	NO	N/A
Se realizan backups incrementales de las bases de datos	75%	25%	0

Fuente: Elaboración propia

Comentario: El 75% de la muestra afirma en el HRL se realizan eventualmente, backups incrementales de las bases de datos; Sin embargo, en el HRL no existe una bitácora del registro de esos backups de manera que se pueda identificar el responsable de la realización de ésta actividad, fecha y hora de realización y motivos de realización de ésta actividad. De igual manera no se puede evidenciar el resguardo de éstos backups fuera de las instalaciones de TI, incluso en otras instalaciones fuera del edificio donde se ubica el área de TI.

Tabla 78.- Pregunta 24- Responsables de administración

PREGUNTA N° 24	SI	NO	N/A
Realizan backups de los sistemas informáticos	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma en el HRL se realizan backups de los sistemas d información; Sin embargo, en el HRL no existe una bitácora del registro de esos backups de manera que se pueda identificar el responsable de la realización de ésta actividad, fecha y hora de realización y motivos de realización de ésta actividad. De igual manera no se puede evidenciar el resguardo de éstos backups fuera de las instalaciones de tecnologías de la información, incluso en otras instalaciones fuera del edificio donde se ubica el área de tecnologías de la información.

Tabla 79.- Pregunta 25- Responsables de administración

PREGUNTA N° 25	SI	NO	N/A
Cuentan con un ambiente de desarrollo de los sistemas informáticos	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que se cuenta con un ambiente de desarrollo de los sistemas informáticos

Tabla 80.- Pregunta 26- Responsables de administración

PREGUNTA N° 26	SI	NO	N/A
Cuentan con un ambiente de pruebas de los sistemas informáticos	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra afirma que se cuenta con un ambiente de prueba de los sistemas informáticos

Tabla 81.- Pregunta 27- Responsables de administración

PREGUNTA N° 27	SI	NO	N/A
Los sistemas de la información eventualmente pierden conexión	25%	75%	0

Fuente: Elaboración propia

Comentario: El 25% de la muestra confirma que los sistemas de información eventualmente pierden conexión. El Hospital Regional de Lambayeque no cuenta con Políticas de seguridad de la información respecto a la gestión de Incidentes, tampoco cuenta con un procedimiento de comunicación, atención y respuesta a Incidentes de seguridad de la información

Tabla 82.- Pregunta 28- Responsables de administración

PREGUNTA N° 28	SI	NO	N/A
Eventualmente se presentan cambios no autorizados en los sistemas informáticos	0	100%	0

Fuente: Elaboración propia

Comentario: El 100% afirma que en el Hospital Regional de Lambayeque no se presenta eventualmente cambios no autorizados en los sistemas informáticos. En el Hospital Regional de Lambayeque no se cuenta con un procedimiento para la atención de requerimientos de implementación y/o cambios en los sistemas de información solicitada por los usuarios.

Tabla 83.- Pregunta 30- Responsables de administración

PREGUNTA N° 30	SI	NO	N/A
Se realizan , pruebas/ simulaciones de los principales incidentes que pudieran afectar la seguridad de la información	50%	50%	0

Fuente: Elaboración propia

Comentario: El 50% de la muestra afirma que si se realizan pruebas/ simulaciones de los principales incidentes que pudieran afectar la seguridad de la información, mientras que el 50% restante manifiesta que dichas pruebas no se realizan.

f) Mantener la seguridad de la información en niveles óptimos

Tabla 84.- Pregunta 2- Responsables de administración

PREGUNTA N° 2	SI	NO	N/A
Se valida el cumplimiento de las políticas de seguridad de la información por parte de los responsables y usuarios	50%	50%	0

Fuente: Elaboración propia

Comentario: El 50% de la muestra afirma que en el HRL se valida el cumplimiento de políticas de seguridad de la información; en cambio el 50% menciona que no se validan controles de seguridad de la información.

El HRL no cuenta con una Política de seguridad de la información, sobre la cual se definan controles de seguridad de la información, ni responsables en la ejecución y/o validación de los mismos. Así mismo, tampoco se elabora un Plan de trabajo anual, que permita tener un cronograma de actividades para realizar la validación del cumplimiento de controles definidos en la Política de seguridad de la información. Actualmente en el HRL, en la medida de lo posible, entre las actividades cotidianas, el personal realiza labores de control de SI, que no va más allá que un mantenimiento de equipos, administración de un firewall, acceso biométrico a las instalaciones del Data Center, el cual consideran como validación de controles de SI.

Tabla 85.- Pregunta 4- Responsables de administración

PREGUNTA N° 4	SI	NO	N/A
Realizan supervisiones del control de las políticas de seguridad de la información del HRL	50%	50%	0

Fuente: Elaboración propia

Comentario: El 50% de la muestra afirma que en el HRL se valida el cumplimiento de políticas de seguridad de la información; en cambio el 50% menciona que no se validan controles de seguridad de la información.

El HRL no cuenta con una Política de seguridad de la información, sobre la cual se definan controles de seguridad de la información, ni responsables en la ejecución y/o validación de los mismos. Así mismo, tampoco se elabora un Plan de trabajo anual, que permita tener un cronograma de actividades para realizar la validación del cumplimiento de controles definidos en la Política de seguridad de la información. Actualmente en el HRL, en la medida de los posible, entre las actividades cotidianas, el personal realiza labores de control de SI, que no va más allá que un mantenimiento de equipos, administración de un firewall, acceso biométrico a las instalaciones del Data Center, administración de accesos a carpetas compartidas, restricciones al uso de redes inalámbricas, el cual consideran como validación de controles de SI.

Tabla 86.- Pregunta 11- Responsables de administración

PREGUNTA N° 11	SI	NO	N/A
Todos los usuarios cuentan con permisos de acceso remoto a sus equipos informáticos	0	100%	0

Fuente: Elaboración propia

Comentario: El 100% afirma que los usuarios del HRL no cuentan con permisos de acceso remoto a sus equipos informáticos. Sin embargo en las entrevistas desarrolladas, nos informaron que hay veces, muy pocas veces, en que si se dan permisos especiales a usuarios para conectarse de manera remota a través de TeamWeaber.

El HRL no cuenta con políticas de seguridad de la información donde se brinden lineamientos del uso de protocolos seguros para realizar conexiones remotas a través de VPN, de manera que la información o las tramas de datos que viajan en dichas conexiones queden completamente cifradas a través de protocolos como HTTPS, RPD, SSL, TLS, entre otros.

Tabla 87.- Pregunta 12- Responsables de administración

PREGUNTA N° 12	SI	NO	N/A
Los usuarios tienen permisos de uso de medios externos	0	100%	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra manifiesta que los usuarios no tienen permisos del uso de medios extraíbles.

Los administradores de la División de Tecnologías de Información indican que actualmente se cuenta con restricciones para los usuarios, en el uso de medios externos dentro del Hospital Regional de Lambayeque; sin embargo los usuarios indican que hacen uso efectivo de estos medios de almacenamiento de información. Por lo que se infiere que esta medida restrictiva no es aplicada, ni controlada de manera efectiva.

Tabla 88.- Pregunta 15- Responsables de administración

PREGUNTA N° 15	SI	NO	N/A
Existen restricciones para el acceso de redes inalámbricas	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% de la muestra manifiesta que existen restricciones para el acceso a conexiones inalámbricas.

Tabla 89.- Pregunta 29- Responsables de administración

PREGUNTA N° 29	SI	NO	N/A
Se mantiene un control de los accesos remotos en los sistemas de la información	100%	0	0

Fuente: Elaboración propia

Comentario: El 100% afirma que los usuarios del HRL mantienen un control de accesos remotos en los sistemas de información. Sin embargo en las entrevistas desarrolladas, nos informaron que hay veces, muy pocas veces, en que si se dan permisos especiales a usuarios para conectarse de manera remota a través de TeamWeaber.

El Hospital Regional de Lambayeque no cuenta con políticas de seguridad de la información donde se brinden lineamientos del uso de protocolos seguros para realizar conexiones remotas a través de VPN, de manera que la información o las tramas de datos que viajan en dichas conexiones queden completamente cifradas a través de protocolos como HTTPS, RPD, SSL, TLS, entre otros.

4.2.3 Encuesta a la jefatura de División de tecnologías de la información del Hospital Regional de Lambayeque

a) La información es un activo institucional

Tabla 90.- Pregunta 1- Jefatura de tecnologías de la información

PREGUNTA N° 1	SI	NO
¿El responsable del área de TI es el encargado de hacer el inventario de los activos de la información de todo el HRL?	0	100%

Fuente: Elaboración propia

Comentario: La División de tecnologías de la información no se encarga de realizar el inventario de los activos de información de todo el HRL, así mismo, en el desarrollo de las entrevistas, nos comunicaron que ninguna área realza ésta actividad. Por lo tanto, se concluye que el HRL no ha establecido los lineamientos, responsables, directrices de una Política de seguridad de información

b) Compromiso de la alta dirección y de los órganos del ministerio de salud

Tabla 91.- Pregunta 6- Jefatura de tecnologías de la información

PREGUNTA N° 6	SI	NO
Existen políticas para mantener el control y seguridad de los activos de la información documentadas	0	100%

Fuente: Elaboración propia

Comentario: No se tiene establecido una política de control de acceso lógico y físico, que resguarden los activos de información del Hospital Regional de Lambayeque

Tabla 92.- Pregunta 12- Jefatura de tecnologías de la información

PREGUNTA N° 12	SI	NO
Cuentan con presupuesto asignado para implementar políticas de gestión de seguridad de la información	0	100%

Fuente: Elaboración propia

Comentario: No se ha concretado una comunicación efectiva con el Directorio, para afianzar políticas y gestión de riesgos en seguridad de la información

c) La seguridad de la información es el soporte de procesos y procedimientos institucionales

Tabla 93.- Pregunta 2- Jefatura de tecnologías de la información

PREGUNTA N° 2	SI	NO
Cada cuanto tiempo realizan el inventario de activos de la información	0	0

Fuente: Elaboración propia

Comentario: No se tiene definido el periodo de realización y/o actualización de un inventario de activos de información

Tabla 94.- Pregunta 3- Jefatura de tecnologías de la información

PREGUNTA N° 3	SI	NO
Quien registra el inventario también se encarga de registra los cambios y/o actualización del inventario	100%	0

Fuente: Elaboración propia

Comentario: El área de tecnologías de la información registra y actualiza el inventario de hardware y software.

Tabla 95.- Pregunta 9- Jefatura de tecnologías de la información

PREGUNTA N° 9	SI	NO
Existen procedimientos a seguir en caso se detecten problemas en la seguridad de la información	0	100%

Fuente: Elaboración propia

Comentario: No existen procedimientos formales de respuesta ante la ocurrencia de problemas de seguridad de la información.

d) Personal involucrado con la seguridad de la información

Tabla 96.- Pregunta 7- Jefatura de tecnologías de la información

PREGUNTA N° 7	SI	NO
Cada cuanto tiempo se realizan capacitaciones a los usuarios, para reforzar medidas de seguridad	0	0

Fuente: Elaboración propia

Comentario: No se efectúan capacitaciones al personal del HRL en temas de seguridad de la información.

e) Prevención de riesgos y aplicación de controles

Tabla 97.- Pregunta 4- Jefatura de tecnologías de la información

PREGUNTA N° 4	SI	NO
El responsable de TI, se encarga de brindar y restringir accesos a los usuarios	0	100%

Fuente: Elaboración propia

Comentario: No se tiene establecido un procedimiento para brindar y restringir accesos a los nuevos usuarios, usuarios según su rotación y usuarios cesados en el HRL

Tabla 98.- Pregunta 5- Jefatura de tecnologías de la información

PREGUNTA N° 5	SI	NO
El responsable de TI, se encarga de administrar los accesos a los usuarios	0	100%

Fuente: Elaboración propia

Comentario: No se tiene establecido un procedimiento para brindar y restringir accesos a los nuevos usuarios, usuarios según su rotación y usuarios cesados en el HRL

Tabla 99.- Pregunta 10- Jefatura de tecnologías de la información

PREGUNTA N 10	SI	NO
Se han detectado las problemas con la seguridad de la información del HRL	100%	0

Fuente: Elaboración propia

Comentario: Se han detectado algunos problemas con las seguridad de la información del HRL, pero no se ha realizado un estudio profundo de causas, ni se ha evaluado el nivel de riesgo y afectación, tampoco se ha recopilado las evidencias respectivas.

Tabla 100.- Pregunta 11- Jefatura de tecnologías de la información

PREGUNTA N° 11	SI	NO
Se han determinado las principales causas de los problemas de seguridad de la información en el HRL	100%	0

Fuente: Elaboración propia

Comentario: Se han detectado algunos problemas con las seguridad de la información del HRL, pero no se ha realizado un estudio profundo de causas, ni se ha evaluado el nivel de riesgo y afectación, tampoco se ha recopilado las evidencias respectivas.

f) Mantener la seguridad de la información en niveles óptimos

Tabla 101.- Pregunta 8- Jefatura de tecnologías de la información

PREGUNTA N° 8	SI	NO
Cada cuanto tiempo se realizan observaciones del cumplimiento de las medidas de seguridad establecidas.	0	0

Fuente: Elaboración propia

Comentario: No existe un área que se encargue de realizar las funciones de Auditoría Interna para evaluar la gestión de activos de información, ni un procedimiento establecidos para requerir la evaluación de Auditorías externas.

4.3. Modelo de gestión de riesgos

En el modelo de gestión de riesgos propuesto, se consideraron los siguientes entregables en cada una de sus etapas:

Identificación de riesgos:

a. La elaboración de un Catálogo de activos de la información, el cual se indica la tipificación de los activos de la información, su clasificación de acuerdo a cada uno de los servicios a los que se encuentra asignados, y los detalles técnicos de cada uno de ellos.

   Este entregable se encuentra en el Anexo 4 Formato de activos de la información Del cual pudimos identificar 187 activos de la información relacionados a los sistemas de gestión hospitalaria que maneja el Hospital Regional de Lambayeque (GalenPlus, SIGHOR; Asignación de camas y SIGBIO)

b. La Valoración de las dimensiones y priorización de los activos de la información identificados.

Se realizó la valoración de todos los activos de la información en la matriz de gestión de riesgos elaborada por los investigadores, en base a las dimensiones de la seguridad de la información (integridad, confidencialidad, disponibilidad, trazabilidad y autenticidad), teniendo como resultado 31 activos priorizados.

Tabla 102.- Cantidad de activos de información priorizados

ACTIVOS DE LA INFORMACIÓN	CANTIDAD
PRIORIZADOS	**31**
NO PRIORIZADOS	**152**
TOTAL DE ACTIVOS DE LA INFORMACIÓN	**183**

Fuente: Elaboración propia

El criterio para la priorización de los activos de información, en referencia a la valoración de las dimensiones de la seguridad de la información de los activos de la información, fue el considerar como activos priorizados, aquellos cuyo promedio de valoración se encuentre n entre los valores 3, 4 y 5 (Más que regular, regular y deficiente)

Tabla 103.- Indicador de nivel de valoración

INDICADOR DE NIVEL DE VALORACION	
5	Deficiente
4	Regular
3	Más que regular
2	Bueno
1	Óptimo

Fuente: Elaboración propia

De los 31 activos Priorizados podemos realizar un análisis de las valoraciones en cada una de las dimensiones:

Tabla 104.- Análisis de valoración de cada dimensión

VALOR DE DIMENSION		CRITERIO DE VALORACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD
10	Extremo	Daño extremadamente grave	0%	0%	0%	3%	0%

9	Muy Alto	Daño muy grave	0%	0%	0%	0%	0%
6-8	Alto	Daño grave	77%	10%	58%	97%	10%
3-5	Medio	Daño importante	23%	90%	42%	0%	90%
1-2	Bajo	Daño menor	0%	0%	0%	0%	0%
0	Despreciable	Irrelevante a efectos prácticos	0%	0%	0%	0%	0%

Fuente: Elaboración propia

Confidencialidad:

El 77% del total de activos de información priorizados está expuesto a un daño grave en referencia a los criterios de CONFIDENCIALIDAD

El 23% del total de activos de información priorizados está expuesto a un daño importante en referencia a los criterios de CONFIDENCIALIDAD

Integridad

El 10% del total de activos de información priorizados está expuesto a un daño grave en referencia a los criterios de INTEGRIDAD

El 90% del total de activos de información priorizados está expuesto a un daño importante en referencia a los criterios de INTEGRIDAD

Disponibilidad

El 58% del total de activos de información priorizados está expuesto a un daño grave en referencia a los criterios de DISPONIBILIDAD

El 42% del total de activos de información priorizados está expuesto a un daño importante en referencia a los criterios de DISPONIBILIDAD

Trazabilidad

El 3% del total de activos de información priorizados está expuesto a un daño extremadamente grave en referencia a los criterios de TRAZABILIDAD

El 97% del total de activos de información priorizados está expuesto a un daño grave en referencia a los criterios de TRAZABILIDAD

Autenticidad

El 10% del total de activos de información priorizados está expuesto a un daño grave en referencia a los criterios de AUTENTICIDAD

El 90% del total de activos de información priorizados está expuesto a un daño

importante en referencia a los criterios de AUTENTICIDAD

Tabla 105 Clasificación y tipificación de los activos de la información

ID ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO
DI003-TI005	Datos/información	- Datos de configuración del servidor de base de datos
DI004-TI001	Datos/información	- Datos de control de acceso (Políticas para contraseñas)
DI006-TI005	Datos/información	- Registro de actividad (Log) del servidor de base de datos
DI009-TI001	Datos/información	- Información almacenada en base de datos de prueba Galen Plus
DI009-TI002	Datos/información	- Información almacenada en base de datos de prueba SIGHOR
DI009-TI003	Datos/información	- Información almacenada en base de datos de prueba del sistema de Asignación de camas
DI009-TI004	Datos/información	- Información almacenada en bbase de datos de prueba del sistema SIGBIO
DI011-TI001	Datos/información	- Información almacenada en base de datos de producción del sistema Galen Plus
DI011-TI002	Datos/información	- Información almacenada en base de datos de producción del sistema SIGHOR
DI011-TI003	Datos/información	- Información almacenada en base de datos de producción del sistema de Asignación de Camas
DI011-TI004	Datos/información	- Información almacenada en base de datos de producción del sistema SIGBIO
SA002-TI001	Servicios auxiliares que se necesitan para poder organizar el sistema	- Servicios subcontratados (Por ejemplo: correo electrónico, servicio web (alojamiento y dominio), etc.)
AI001-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Desarrollo propio(in house)
AI002-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Desarrollo subcontratado
AI008-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Sistema backup de BD

AI011-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Aplicaciones de desarrollo de software (open source y licenciados)
SI004-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Memorias USB
SI006-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Tarjeta de memoria cámaras fotográficas
IE002-TI001	Las instalaciones que acogen equipos informáticos y de comunicaciones	- Cuarto de servidores
PP002-SS001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CI001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-SO001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-NE001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CQ001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CO001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CE001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-ME001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-PE001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CG001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CS001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos

Fuente: Elaboración propia

c. Identificación de vulnerabilidades en los activos de la información, considerando el Catálogo de vulnerabilidades elaborado (Anexo N° 06: Catálogo de vulnerabilidades), se analizó cada uno de los activos de la información priorizados, para determinar en ellos las vulnerabilidades que presentan, del cual obtuvimos:

Las vulnerabilidades encontradas en los activos priorizados en los sistemas de gestión de riesgos del Hospital Regional de Lambayeque:

Tabla 106 Lista de vulnerabilidades y frecuencia por activo de información

VULNERABILIDAD	DESCRIPCION DE VULNERABILIDADES	FRECUENCIA	PORCENTAJE
5.1.1	Falta de políticas para la seguridad de la información	**31**	16%
6.1.1	No cuentan con responsables asignados para la seguridad de la información	12	6%
7.2.2	Escasa concienciación, educación y capacitación en seguridad de la información	11	6%
7.3.1	No existe comunicación inmediata sobre los ceses, rotaciones o cambios de puesto de trabajo del personal	5	3%
8.1.1	No cuentan con un inventario de activos actualizado	12	6%
8.2.1	No existe directrices para una buena clasificación de activos de información	**16**	8%
9.1.2	Existe un débil control para el acceso redes y servicios asociados	1	1%
9.2.3	No realizan la gestión de los roles de los usuarios con privilegios especiales	2	1%
9.2.5	No realizan la validación y seguimiento sobre los privilegios de los usuarios en los roles asignados	12	6%
9.3.1	No existe concientización del usuario para mantener la confidencialidad de sus contraseñas	12	6%
9.4.2	Falta de control de acceso a los sistemas y aplicaciones mediante un procedimiento seguro de logeo	2	1%
11.1.1	No se ha definido y utiliza perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica	6	3%
11.1.2	No han establecido controles ingreso en áreas restringidas	1	1%
11.1.4	No han establecido procedimientos para la protección de los activos de amenazas externas y/o ambientales	1	1%

11.1.6	No se tiene un control para restringir el ingreso de personas no autorizadas a las instalaciones de procesamiento de información.	1	1%
12.1.1	No se tiene documentado los procesos operativos y servicios que soportan a los sistemas de información	9	5%
12.1.4	No existe una diferenciación entre los ambientes asignados para el área de desarrollo, pruebas y producción.	10	5%
12.2.1	No existe control para la detección, prevención y recuperación ante afectaciones de malware	1	1%
12.3.1	No cuentan con un lugar seguro e independiente para reguardar las copias de seguridad.	1	1%
12.4.1	No cuentan con una bitácora de eventos de actividades	5	3%
12.6.1	No se tiene identificadas las vulnerabilidades técnicas de los sistemas de información, para evaluar de manera oportuna el grado de exposición de la organización	**16**	8%
12.7.1	No se realiza la planificación de controles de auditoria en sus sistemas de información, con el fin de mantener la continuidad del negocio	2	1%
14.2.2	No existen procedimientos para mantener un registro sobre el control de cambios realizados en los sistemas	2	1%
14.2.5	No se cuenta con una metodología de Desarrollo Seguro, en el que se tengan presentes los controles que garanticen la seguridad de la información en cada etapa de desarrollo del software, de manera que se pueda solucionar las vulnerabilidades o fallas identificadas.	2	1%
14.3.1	No existe la seguridad de contar con datos consistentes para realizar casos de prueba en el ambiente de pruebas	4	2%
16.1.3	No se informa las debilidades sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a proveedores que utilizan los sistemas y servicios de información de la organización	1	1%
18.2.1	No se realizan Auditorías internas y externas para supervisar y revisar las políticas de la seguridad de la información establecidas	**14**	7%

Fuente: Elaboración propia

De los activos de información priorizados, se detectó que en el 16% de los activos de la información No cuenta con políticas de seguridad de la información; 8% de los activos de la información No cuentan con directrices para una buena clasificación de los activos

de la información y No tienen identificadas las vulnerabilidades de los sistemas de información; 7% de sus activos de la información no realizan auditorías internas y externas.

d. Identificación de amenazas de los activos de la información, considerando el Catálogo de amenazas elaborado (Anexo N° 07: Catálogo de amenazas), se analizó cada uno de los activos de la información priorizados, para determinar en ellos las vulnerabilidades que presentan, del cual obtuvimos:

Las amenazas encontradas en los activos priorizados en los sistemas de gestión de riesgos del Hospital Regional de Lambayeque:

Tabla 107 Lista de amenazas y su frecuencia por activo de la información

AMENAZAS	DESCRIPCIÓN DE AMENAZAS	FRECUENCIA	PORCENTAJE
A.3	Desastres naturales	6	1%
B.1	Fuego	6	1%
B.2	Daños por agua	6	1%
B.4	Avería de origen físico o lógico	6	1%
C.1	Errores en los usuarios	27	7%
C.2	Errores del administrador	14	3%
C.3	Errores de monitorización (log)	13	3%
C.4	Errores de configuración	6	1%
C.5	Deficiencias en la organización	**31**	8%
C.9	Escapes de información	**28**	7%
C.10	Alteración accidental de información	**31**	8%
C.11	Destrucción de la información	**30**	7%
C.12	Fugas de información	27	7%
C.13	Vulnerabilidad d los programas	11	3%
C.14	Errores de mantenimiento / actualización de programas	3	1%
C.16	Pérdida de equipos	12	3%
C.17	Indisponibilidad del personal	12	3%
D.1	Manipulación de registros de Monitorización (log)	1	0%
D.2	Manipulación de la configuración	1	0%
D.3	Suplantación de identidad del usuario	5	1%
D.4	Abuso de privilegios de acceso	1	0%
D.6	Difusión de software dañino	3	1%
D.9	Acceso no autorizado	17	4%
D.10	Análisis de tráfico	3	1%
D.11	Repudio	12	3%

D.12	Interceptación de información	6	1%
D.13	Modificación deliberada de información	3	1%
D.14	Destrucción de información	1	0%
D.15	Divulgación de información	4	1%
D.17	Manipulación de equipos	3	1%
D.19	Robo	13	3%
D.22	Indisponibilidad del personal	1	0%
D.24	Bloqueo de base de datos bajo petición de rescate	10	2%
D.25	Bloqueo de servidores bajo petición de rescate	1	0%
D.27	Ataque telefónico (Persuación)	12	3%
D.28	Ataque email (suscripciones/cupones descuento)	13	3%
D.29	Estafa cibernética	13	3%
D.30	Keylogers	12	3%

Fuente: Elaboración propia

De los datos obtenidos, se detectó que en los activos de la información se encuentran expuestos a las siguientes amenazas: El 8% cuenta con deficiencias en la organización y están expuestas a la alteración accidental de la información, 7% se expone a la destrucción de la información y el 7% muestra que se expone a escapes de información

Análisis y evaluación de riesgos:

e. Ponderación de la probabilidad de materialización y determinación de del nivel de riesgos, el cual detallamos en el punto 4.3.2 de la metodología para la gestión de riesgos, del cual obtenemos:

Tabla 108 Análisis del nivel de riesgo inherente

NIVEL DE RIESGO INHERENTE						
Probabilidad / Impacto	3- M: Medio	4- A: Alto	Total general	% P. Medio	%P. Alto	% Total
3- M: Posible	0	30	30	0	97	**97**
4- A: Probable	1	0	1	3	0	**3**
Total general	1	30	31	3	0	**100**

Fuente: Elaboración propia

Determinando mediante el análisis de los activos de la información priorizados en cuatro sistemas de gestión hospitalaria utilizador por el HRL que sus activos de información

presentan un nivel de riesgo inherente del 97% resultado de una posible probabilidad y un alto Impacto (riesgo inherente ALTO) en la institución; y solo un 3% resultan probables con impacto medio (riesgo inherente alto).

Tratamiento de riesgos:

f. Listado de mecanismos de protección, considerando el Catálogo de mecanismos de protección elaborado (Anexo N° 08: Catálogo de mecanismos de protección), se analizó cada uno de los activos de la información priorizados, para realizar la propuesta de mecanismos de protección que puedan mitigar los riesgos ocasionados por las vulnerabilidades y amenazas que presentan, del cual obtuvimos:

Los mecanismos de protección propuestas para los activos priorizados en los sistemas de gestión de riesgos del Hospital Regional de Lambayeque:

Tabla 109 Lista de Mecanismos de protección y su frecuencia por activos de la información

MECANISMOS DE PROTECCIÓN	**DESCRIPCION DE** MECANISMOS DE PROTECCIÓN	**FRECUENCIA**	**PORCENTAJE**
AP01	Protección de las aplicaciones informáticas	8	3%
AP02	Copias de seguridad (backup)	8	3%
AP04	Se aplican perfiles de seguridad	20	7%
CC01	gestión de claves criptográficas	1	0%
CC02	gestión de las claves de cifra de información	2	1%
CC06	gestión de certificados	5	2%
CO03	Se aplican perfiles de seguridad	13	5%
CO04	Aseguramiento de la disponibilidad	9	3%
CO05	Autenticación del canal	1	0%
CO06	Protección de la integridad de los datos intercambiados	1	0%
DI01	Clasificación de la información	1	0%
DI03	Aseguramiento de la integridad	22	8%
DI04	Cifrado de la información	13	5%
EQ03	Se aplican perfiles de seguridad	12	4%
EX02	Acuerdos para el intercambio de información y software	3	1%
EX05	Personal subcontratado	1	0%

FF01	Protección de las instalaciones	1	0%
FF02	Diseño de las instalaciones	1	0%
FF03	Defensa en profundidad	1	0%
FF04	Control de los accesos físicos	1	0%
FF05	Aseguramiento de la disponibilidad	1	0%
GH01	Identificación y autenticación	1	0%
GH02	Control de acceso lógico	12	4%
GH03	Segregación de tareas	1	0%
GH04	Gestión de incidencias	1	0%
GH05	Herramientas de seguridad	1	0%
GH06	Herramienta contra código dañino	2	1%
GH07	IDS/IPS: Herramienta de detección / prevención de intrusión	1	0%
GH08	Herramienta de chequeo de configuración	1	0%
GH09	Herramienta de análisis de vulnerabilidades	1	0%
GH10	Herramienta de monitorización de tráfico	1	0%
GH11	DLP: Herramienta de monitorización de contenidos	1	0%
GH12	Herramienta para análisis de logs	1	0%
GH13	Honey net / honey pot	1	0%
GH14	Verificación de las funciones de seguridad	1	0%
GH15	Gestión de vulnerabilidades	1	0%
GH16	Registro y auditoría	1	0%
OP03	Plan de recuperación de desastres	1	0%
OR01	Organización	13	5%
OR02	Gestión de riesgos	19	7%
OR03	Planificación de la seguridad	22	8%
OR04	Inspecciones de la seguridad	16	6%
PP02	Formación y concienciación	14	5%
SI01	Protección de los soportes de información	2	1%
SI05	Destrucción de soportes	2	1%
SS02	Aseguramiento de la disponibilidad	12	4%
SS04	Se aplican perfiles de seguridad	16	6%
SS06	Gestión de cambios (mejoras y sustituciones)	5	2%
SS08	Protección de servicios y aplicaciones web	1	0%
SS09	Protección del correo electrónico	1	0%

SS10	Protección del directorio	1	0%
SS11	Protección del servidor de nombres de dominio DNS	1	0%

Fuente: Elaboración propia

De los datos obtenidos, podemos indicar que de los mecanismos de protección propuestos el 8% indican la necesidad de una planificación de la seguridad y Aseguramiento de la integridad; 7% requiere de la aplicación de perfiles de seguridad y 7% necesita realizar una gestión de riesgos.

g. Criterios para medir la efectividad de los mecanismos de protección

Tabla 110 Análisis estado y tipo de mecanismos de protección

Estado mecanismos / Tipo de mecanismos	% Detectivo	% Preventivo	% Total
Implementado	0%	32%	32%
No implementado	10%	58%	68%
Total	10%	90%	100%

Fuente: Elaboración propia

Se identifica que el 10% de los mecanismos de protección propuestos son detectivos y el 90% son preventivos.

Así mismo, el 32% de los mecanismos de protección propuesto se encuentra implementados y el 68% no se encuentran implementados.

Tabla 111 Análisis nivel de efectividad

NIVEL DE EFECTIVIDAD		%ACTIVOS
1	Deficiente	68%
5	Optimo	32%

Fuente: Elaboración propia

Actualmente el 68% de los mecanismos de protección propuestos no se encuentran implementados, lo cual muestra un nivel de efectividad "deficiente", así mismo los mecanismos de protección propuestos que encuentran implementados genera un nivel de efectividad en la mitigación de los riesgos del 32%.

el nivel de efectividad de los mecanismos de protección aumentará a medida que los propuestos mecanismos de protección se vayan implementando.

4.4. Desarrollo de la metodología de gestión de riesgos

4.5.1 Identificación de activos y sus amenazas

4.5.1.3 Tipificación de activos de la información

De la lista de inventario de activos de la información se toman los activos que se registrarán en la matriz de riesgos, considerando los siguientes datos generales:

Tabla 112 Tipificación para los activos de la información

DATOS DEL ACTIVO	**ID ACTIVO**
	TIPO DE ACTIVO
	NOMBRE DEL ACTIVO

Fuente: Elaboración propia

- **ID ACTIVO**: Indica el código del activo de la información.
- **TIPO DE ACTIVO**: Indica la descripción del tipo de activo de la información.
- **NOMBRE DEL ACTIVO**: Indica la descripción del activo de la información.

Tabla 113 Ejemplo: Identificación de datos del activo DI011-TI002

ID ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO
DI011-TI002	Datos/información	- información almacenada en base de datos de producción del sistema SIGHOR

Fuente: Elaboración propia

Tabla 114 Resultados obtenidos sobre la tipificación de activos de la información

ID ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO

DI001-SS001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-CI001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-SO001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-NE001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-CQ001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-CO001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-CE001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-ME001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-PE001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-CG001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI001-CE001	Datos/información	- Ficheros, carpetas, documentos virtuales
DI002-TI001	Datos/información	- Copia de respaldo de la información compartida en ficheros virtuales
DI003-TI001	Datos/información	- Datos de configuración del Activy Directory
DI003-TI002	Datos/información	- Datos de configuración del Firewall
DI003-TI003	Datos/información	- Datos de configuración del Servidor de correos
DI003-TI004	Datos/información	- Datos de configuración del Antivirus Magement
DI003-TI005	Datos/información	- Datos de configuración del Servidor de Base de Datos
DI004-TI001	Datos/información	- Datos de control de acceso (Políticas para Contraseñas)
DI005-TI001	Datos/información	- Datos de validación de credenciales (licencias de software)
DI006-TI001	Datos/información	- Registro de actividad (Log) del Activy Directory

DI006-TI002	Datos/información	- Registro de actividad (Log) del Firewall
DI006-TI003	Datos/información	- Registro de actividad (Log) del Servidor de Correos
DI006-TI004	Datos/información	- Registro de actividad (Log) del Antovirus management
DI006-TI005	Datos/información	- Registro de actividad (Log) del Servidor de Base de Datos
DI007-TI001	Datos/información	- Código fuente del Sistema Galen Plus
DI007-TI002	Datos/información	- Código fuente del Sistema SIGOR
DI007-TI003	Datos/información	- Código fuente del Sistema de Asignación de Camas
DI007-TI004	Datos/información	- Código fuente del Sistema SIGBIO
DI008-TI001	Datos/información	- Código ejecutable SIGHOR
DI008-TI002	Datos/información	- Código ejecutable GALEN PLUS
DI008-TI003	Datos/información	- Código ejecutable Sistema de asignación de camas
DI008-TI004	Datos/información	- Código ejecutable Sistema SIGBIO
DI009-TI001	Datos/información	- Información almacenada en Base de Datos de prueba Galen Plus
DI009-TI002	Datos/información	- Información almacenada en Base de Datos de prueba SIGHOR
DI009-TI003	Datos/información	- Información almacenada en Base de Datos de prueba del Sistema de Asignación de Camas
DI009-TI004	Datos/información	- Información almacenada en Base de Datos de prueba del Sistema SIGBIO
DI011-TI001	Datos/información	- Información almacenada en Base de datos de producción del Sistema Galen Plus
DI011-TI002	Datos/información	- Información almacenada en Base de datos de producción del Sistema SIGHOR
DI011-TI003	Datos/información	- Información almacenada en Base de datos de producción del Sistema de Asignación de Camas
DI011-TI004	Datos/información	- Información almacenada en Base de datos de producción del Sistema SIGBIO

II001-SS001	Información impresa	- Documentos almacenado en archivadores
II001-CI001	Información impresa	- Documentos almacenado en archivadores
II001-SO001	Información impresa	- Documentos almacenado en archivadores
II001-NE001	Información impresa	- Documentos almacenado en archivadores
II001-CQ001	Información impresa	- Documentos almacenado en archivadores
II001-CO001	Información impresa	- Documentos almacenado en archivadores
II001-CE001	Información impresa	- Documentos almacenado en archivadores
II001-ME001	Información impresa	- Documentos almacenado en archivadores
II001-PE001	Información impresa	- Documentos almacenado en archivadores
II001-CG001	Información impresa	- Documentos almacenado en archivadores
II001-CS001	Información impresa	- Documentos almacenado en archivadores
II001-TI001	Información impresa	- Documentos almacenado en archivadores
II002-SS001	Información impresa	- Información confidencial que se hallan impreso
II002-CI001	Información impresa	- Información confidencial que se hallan impreso
II002-SO001	Información impresa	- Información confidencial que se hallan impreso
II002-NE001	Información impresa	- Información confidencial que se hallan impreso
II002-CQ001	Información impresa	- Información confidencial que se hallan impreso
II002-CO001	Información impresa	- Información confidencial que se hallan impreso
II002-CE001	Información impresa	- Información confidencial que se hallan impreso
II002-ME001	Información impresa	- Información confidencial que se hallan impreso
II002-PE001	Información impresa	- Información confidencial que se hallan impreso
II002-CG001	Información impresa	- Información confidencial que se hallan impreso

II002-CS001	Información impresa	- Información confidencial que se hallan impreso
II002-TI001	Información impresa	- Información confidencial que se hallan impreso
SA001-TI001	Servicios auxiliares que se necesitan para poder organizar el sistema	- Servicio de Acceso (Lista de roles y perfiles asignados a usuarios)
SA002-TI001	Servicios auxiliares que se necesitan para poder organizar el sistema	- Servicios subcontratados (Por ejemplo: Correo electrónico, Servicio web (Alojamiento y Dominio), etc.)
SA003-TI001	Servicios auxiliares que se necesitan para poder organizar el sistema	- Transferencia de ficheros (ftp)
AI001-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Desarrollo propio(in house)
AI002-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Desarrollo subcontratado
AI003-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Sistema de gestión de Dominios (Active Directory)
AI004-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Sistema de gestión de base de datos (el aplicativo)
AI005-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Sistema operativo
AI006-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Ofimática
AI008-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Sistema Backup de BD
AI010-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Antivirus
AI011-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Aplicaciones de desarrollo de software (open source y licenciados)
AI012-TI001	Aplicaciones informáticas (software) que permiten manejar los datos	- Aplicaciones de software instalados en equipos médicos
EI001-TI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Servidores principales y alternos
EI002-SS001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-SS002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-SS003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-SS004	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-SO001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-SO002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-SO003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)

EI002-CI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CI002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CI003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-NE001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-NE002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI0002-CQ001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI0002-CQ002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI0002-CQ003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CO001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CO002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CE001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CE002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-ME001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-ME002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-ME003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-PE001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-PE002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-PE003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CG001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CG002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CG003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CG004	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)

EI002-CS001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CS002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CS003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CS004	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CS005	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-CS006	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI003	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI004	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI005	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI006	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI007	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI008	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI009	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI010	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI011	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI012	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI013	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI014	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI002-TI015	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (fijos)
EI003-TI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de

		colaboradores (portátiles)
EI003-TI002	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Equipos de cómputo de colaboradores (portátiles)
EI005-TI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-SS001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-CI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-SO001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-NE001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-CQ001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-CO001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-CE001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-ME001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-PE001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-CG001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI005-CS001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Medios de impresión y escaneo
EI006-TI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Soporte de red (módems, switch, router, cortafuegos físicos, access point)
EI007-TI001	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	- Centralita telefónica (análogo)
SI001-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Discos duros internos
SI002-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Discos duros externos
SI003-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Cederrón (CR-ROM)
SI004-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Memorias USB
SI005-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- DVD
SI006-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- Tarjeta de memoria cámaras fotográficas
SI007-TI001	Los soportes de información que son dispositivos de almacenamiento de datos	- DVR (disco de almacenamiento de cámaras de seguridad)
EA001-TI001	El equipamiento auxiliar que complementa el material informático	- UPS
EA002-TI001	El equipamiento auxiliar que complementa el material informático	- Generadores eléctricos
EA003-TI001	El equipamiento auxiliar que complementa el material informático	- Aire acondicionado del cuarto de servidores
EA004-TI001	El equipamiento auxiliar que complementa el material informático	- Cableado eléctrico del cuarto de servidores
EA005-TI001	El equipamiento auxiliar que complementa el material informático	- Cableado de red

EA006-TI001	El equipamiento auxiliar que complementa el material informático	- Antenas
RC001-TI001	Las redes de comunicaciones que permiten intercambiar datos	- Red inalámbrica
RC002-TI001	Las redes de comunicaciones que permiten intercambiar datos	- Red local
RC004-TI001	Las redes de comunicaciones que permiten intercambiar datos	- Internet
IE001-TI001	Las instalaciones que acogen equipos informáticos y de comunicaciones	- Edificio
IE002-TI001	Las instalaciones que acogen equipos informáticos y de comunicaciones	- Cuarto de servidores
IE003-TI001	Las instalaciones que acogen equipos informáticos y de comunicaciones	- Instalaciones del servidor de respaldo
IE004-TI001	Las instalaciones que acogen equipos informáticos y de comunicaciones	- Instalaciones que alojan los Backups
PP001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios externos
PP002-SS001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CI001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-SO001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-NE001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CQ001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CO001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CE001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-ME001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-PE001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CG001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-CS001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP002-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Usuarios internos
PP003-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Administradores de sistemas
PP004-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Administradores de comunicaciones
PP005-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Administradores de BBDD
PP007-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Desarrolladores/programadores
PP008-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Subcontratas relacionados con los servicios / sistemas de información
PP009-TI001	Las personas que explotan u operan todos los elementos anteriores citados	- Proveedores relacionados con los servicios / sistemas de información

Fuente Elaboración propia

4.5.1.2 Valoración de dimensiones de activos de información

De acuerdo a los conceptos de las dimensiones de seguridad de la información de los activos de información, en cada una de las

dimensiones mencionadas se colocará una valoración de **0 – 10** considerando los parámetros de valoración de la dimensión según del cuadro 1:

Tabla 115 Dimensiones de la seguridad de la información

DIMENSIONES DE SEGURIDAD DE LA INFORMACION	**CONFIDENCIALIDAD**
	INTEGRIDAD
	DISPONIBILIDAD
	TRAZABILIDAD
	AUTENTICIDAD

Fuente: Elaboración propia

Tabla 116 Escala de valoración dimensiones del activo.

VALOR DE DIMENSION	
10	Extremo
9	Muy Alto
6-8	Alto
3-5	Medio
1-2	Bajo
0	Despreciable

Fuente: Elaboración propia.

Tabla 117 Ejemplo: Valoración dimensiones del activo DI011-TI002

ID ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD
DI011-TI002	6	5	6	6	5

Fuente: Elaboración propia

Tabla 118 Resultados de la valoración de las dimensiones de seguridad obtenidos

ID ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD
DI001-SS001	3	0	2	2	1
DI001-CI001	3	0	2	2	1

DI001-SO001	3	0	2	2	1
DI001-NE001	3	0	2	2	1
DI001-CQ001	3	0	2	2	1
DI001-CO001	3	0	2	2	1
DI001-CE001	3	0	2	2	1
DI001-ME001	3	0	2	2	1
DI001-PE001	3	0	2	2	1
DI001-CG001	3	0	2	2	1
DI001-CE001	3	0	2	2	1
DI002-TI001	1	1	2	2	1
DI003-TI001	1	2	6	6	1
DI003-TI002	1	1	6	6	2
DI003-TI003	2	2	3	4	1
DI003-TI004	3	6	8	6	4
DI003-TI005	6	4	7	7	4
DI004-TI001	4	3	8	6	8
DI005-TI001	3	2	4	2	3
DI006-TI001	3	2	4	3	4
DI006-TI002	4	2	4	3	2
DI006-TI003	3	2	2	3	2
DI006-TI004	3	3	4	4	2
DI006-TI005	5	5	8	6	5
DI007-TI001	4	3	6	5	3
DI007-TI002	4	3	6	5	3
DI007-TI003	4	3	6	5	3
DI007-TI004	4	3	6	5	3
DI008-TI001	5	3	6	5	3
DI008-TI002	5	3	6	5	3
DI008-TI003	5	3	6	5	3
DI008-TI004	5	3	6	5	3
DI009-TI001	6	5	6	6	5

DI009-TI002	6	5	6	6	5
DI009-TI003	6	5	6	6	5
DI009-TI004	6	5	6	6	5
DI011-TI001	6	5	6	6	5
DI011-TI002	6	5	6	6	5
DI011-TI003	6	5	6	6	5
DI011-TI004	6	5	6	6	5
II001-SS001	5	1	5	7	3
II001-CI001	5	1	5	7	3
II001-SO001	5	1	5	7	3
II001-NE001	5	1	5	7	3
II001-CQ001	5	1	5	7	3
II001-CO001	5	1	5	7	3
II001-CE001	5	1	5	7	3
II001-ME001	5	1	5	7	3
II001-PE001	5	1	5	7	3
II001-CG001	5	1	5	7	3
II001-CS001	5	1	5	7	3
II001-TI001	5	1	5	7	3
II002-SS001	6	4	4	5	3
II002-CI001	6	4	4	5	3
II002-SO001	6	4	4	5	3
II002-NE001	6	4	4	5	3
II002-CQ001	6	4	4	5	3
II002-CO001	6	4	4	5	3
II002-CE001	6	4	4	5	3
II002-ME001	6	4	4	5	3
II002-PE001	6	4	4	5	3
II002-CG001	6	4	4	5	3
II002-CS001	6	4	4	5	3
II002-TI001	6	4	4	5	3
SA001-TI001	2	5	6	7	4
SA002-TI001	5	6	6	7	4
SA003-TI001	4	6	6	7	4
AI001-TI001	5	6	5	8	4
AI002-TI001	5	5	8	10	5
AI003-TI001	6	5	6	5	4
AI004-TI001	4	4	5	8	4
AI005-TI001	4	4	4	5	4
AI006-TI001	3	3	2	3	3
AI008-TI001	7	6	6	8	4
AI010-TI001	4	4	3	4	3
AI011-TI001	5	5	7	6	5

AI012-TI001	2	4	5	5	4
EI001-TI001	4	5	5	4	3
EI002-SS001	4	3	5	5	4
EI002-SS002	4	3	5	5	4
EI002-SS003	4	3	5	5	4
EI002-SS004	4	3	5	5	4
EI002-SO001	4	3	5	5	4
EI002-SO002	4	3	5	5	4
EI002-SO003	4	3	5	5	4
EI002-CI001	4	3	5	5	4
EI002-CI002	4	3	5	5	4
EI002-CI003	4	3	5	5	4
EI002-NE001	4	3	5	5	4
EI002-NE002	4	3	5	5	4
EI0002-CQ001	4	3	5	5	4
EI0002-CQ002	4	3	5	5	4
EI0002-CQ003	4	3	5	5	4
EI002-CO001	4	3	5	5	4
EI002-CO002	4	3	5	5	4
EI002-CE001	4	3	5	5	4
EI002-CE002	4	3	5	5	4
EI002-ME001	4	3	5	5	4
EI002-ME002	4	3	5	5	4
EI002-ME003	4	3	5	5	4
EI002-PE001	4	3	5	5	4
EI002-PE002	4	3	5	5	4

EI002-PE003	4	3	5	5	4
EI002-CG001	4	3	5	5	4
EI002-CG002	4	3	5	5	4
EI002-CG003	4	3	5	5	4
EI002-CG004	4	3	5	5	4
EI002-CS001	4	3	5	5	4
EI002-CS002	4	3	5	5	4
EI002-CS003	4	3	5	5	4
EI002-CS004	4	3	5	5	4
EI002-CS005	4	3	5	5	4
EI002-CS006	4	3	5	5	4
EI002-TI001	4	3	5	5	4
EI002-TI002	4	3	5	5	4
EI002-TI003	4	3	5	5	4
EI002-TI004	4	3	5	5	4
EI002-TI005	4	3	5	5	4
EI002-TI006	4	3	5	5	4
EI002-TI007	4	3	5	5	4
EI002-TI008	4	3	5	5	4
EI002-TI009	4	3	5	5	4
EI002-TI010	4	3	5	5	4
EI002-TI011	4	3	5	5	4
EI002-TI012	4	3	5	5	4
EI002-TI013	4	3	5	5	4
EI002-TI014	4	3	5	5	4
EI002-TI015	4	3	5	5	4

EI003-TI001	4	3	5	5	4
EI003-TI002	4	3	5	5	4
EI005-TI001	4	3	5	5	4
EI005-SS001	4	3	5	5	4
EI005-CI001	4	3	5	5	4
EI005-SO001	4	3	5	5	4
EI005-NE001	4	3	5	5	4
EI005-CQ001	4	3	5	5	4
EI005-CO001	4	3	5	5	4
EI005-CE001	4	3	5	5	4
EI005-ME001	4	3	5	5	4
EI005-PE001	4	3	5	5	4
EI005-CG001	4	3	5	5	4
EI005-CS001	4	3	5	5	4
EI006-TI001	4	4	5	5	3
EI007-TI001	4	5	6	6	3
SI001-TI001	4	3	5	5	4
SI002-TI001	4	2	3	2	2
SI003-TI001	5	4	5	5	4
SI004-TI001	6	5	6	6	6
SI005-TI001	5	4	5	5	4
SI006-TI001	6	5	6	6	5
SI007-TI001	5	5	6	6	5
EA001-TI001	4	3	5	5	4
EA002-TI001	4	3	5	5	4
EA003-TI001	4	3	5	5	4
EA004-TI001	4	3	5	5	4
EA005-TI001	4	3	5	6	4
EA006-TI001	1	1	2	1	2
RC001-TI001	4	3	5	6	4
RC002-TI001	4	3	4	5	4
RC004-TI001	4	4	4	6	3
IE001-TI001	4	3	3	5	4
IE002-TI001	4	3	7	7	7
IE003-TI001	4	3	5	8	4
IE004-TI001	4	4	5	5	3
PP001	8	4	4	5	4

PP002-SS001	8	5	4	6	5
PP002-CI001	8	5	4	6	5
PP002-SO001	8	5	4	6	5
PP002-NE001	8	5	4	6	5
PP002-CQ001	8	5	4	6	5
PP002-CO001	8	5	4	6	5
PP002-CE001	8	5	4	6	5
PP002-ME001	8	5	4	6	5
PP002-PE001	8	5	4	6	5
PP002-CG001	8	5	4	6	5
PP002-CS001	8	5	4	6	5
PP002-TI001	8	5	4	6	5
PP003-TI001	3	3	4	5	3
PP004-TI001	3	3	4	5	4
PP005-TI001	3	4	4	6	3
PP007-TI001	3	6	5	8	3
PP008-TI001	3	5	6	5	3
PP009-TI001	3	5	6	5	3

Fuente: Elaboración propia

4.5.1.3 Priorización de activos de la información

Para la priorización de los activos de información, bajo el criterio de los investigadores, se propone una equivalencia entre el promedio **del valor de las dimensiones de seguridad de la información** y el **indicador de nivel de valoración** que se detalla líneas abajo.

Tabla 119 Priorización de los activos de la información

ACTIVO PRIORIZADO	***INDICADOR DEL NIVEL DE VALORACION***
	INDICADOR

Fuente: Elaboración propia

- **INDICADOR DEL NIVEL DE VALORACION**: De acuerdo a la valoración del activo calculado, se realiza la equivalencia del valor de dimensión respecto del indicador de nivel de valoración, como se señala en el cuadro 2; devolviendo la descripción del valor de dimensión.

Tabla 120 Equivalencia del indicador del nivel de valoración respecto del valor de la dimensión de un activo.

INDICADOR DE NIVEL DE VALORACION		VALOR DE DIMENSION		CRITERIO
5	Deficiente	10	Extremo	Daño extremadamente grave
		9	Muy Alto	Daño muy grave
4	Regular	.6-8	Alto	Daño grave
3	Más que regular	.3-5	Medio	Daño importante
2	Bueno	.1-2	Bajo	Daño menor
1	Óptimo	0	Despreciable	Irrelevante a efectos prácticos

Fuente: Elaboración propia

- **INDICADOR**: Por criterio de los investigadores el valor del **indicador del nivel de valoración** equivalente al Valor de la dimensión que sean mayores a "3" se considerarán PRIORITARIOS, por lo cual se devolverá la señalización de **priorizar** si dicha equivalencia se encuentra en los parámetros del cuadro 3, caso contrario se considerarán activos no priorizados

Tabla 121 Indicador de nivel de valoración de los activos que se priorizarán.

PRIORIZACION DE ACTIVOS POR NIVEL DE VALORACION:	
INDICADOR DE NIVEL DE VALORACION	
5	Deficiente
4	Regular
3	Más que regular

Fuente: Elaboración propia.

Tabla 122 Ejemplo: Priorización del activo DI011-TI002

ID ACTIVO	VALORACIÓN DE ACTIVO	INDICADOR
DI011-TI002	6	PRIORIZAR

Fuente: Elaboración propia

Al realizar la priorización de los activos de la información relacionados con los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque, se obtuvo como resultado 31 activos de la información priorizados

Tabla 123 Resultados de los activos de la información priorizados según su valoración

	VALORACION DEL ACTIVO		ACTIVO PRIORIZADO
ID ACTIVO	´(PROM DE DIMENSIONES)	*INDICADOR DEL NIVEL DE VALORACION*	INDICADOR
DI003-TI005	6	Alto	Priorizar
DI004-TI001	6	Alto	Priorizar
DI006-TI005	6	Alto	Priorizar
DI009-TI001	6	Alto	Priorizar
DI009-TI002	6	Alto	Priorizar
DI009-TI003	6	Alto	Priorizar
DI009-TI004	6	Alto	Priorizar
DI011-TI001	6	Alto	Priorizar
DI011-TI002	6	Alto	Priorizar
DI011-TI003	6	Alto	Priorizar
DI011-TI004	6	Alto	Priorizar
SA002-TI001	6	Alto	Priorizar
AI001-TI001	6	Alto	Priorizar
AI002-TI001	7	Alto	Priorizar
AI008-TI001	6	Alto	Priorizar
AI011-TI001	6	Alto	Priorizar
SI004-TI001	6	Alto	Priorizar
SI006-TI001	6	Alto	Priorizar
IE002-TI001	6	Alto	Priorizar
PP002-SS001	6	Alto	Priorizar
PP002-CI001	6	Alto	Priorizar
PP002-SO001	6	Alto	Priorizar
PP002-NE001	6	Alto	Priorizar
PP002-CQ001	6	Alto	Priorizar
PP002-CO001	6	Alto	Priorizar
PP002-CE001	6	Alto	Priorizar
PP002-ME001	6	Alto	Priorizar
PP002-PE001	6	Alto	Priorizar
PP002-CG001	6	Alto	Priorizar
PP002-CS001	6	Alto	Priorizar
PP002-TI001	6	Alto	Priorizar

Fuente: Elaboración propia

4.5.1.4 Identificar y valorar vulnerabilidades sobre activos de información.

En cada uno de los activos registrados, se analizarán las vulnerabilidades que éstos puedan contener, para lo cual en cada una de las celdas denominadas V_1, V_2, V_3 … V_n se seleccionarán las vulnerabilidades que

contiene el activo analizado (Estas vulnerabilidades se encuentras descritas y listadas en el Catálogo de vulnerabilidades)

Tabla 124 Vulnerabilidades de los activos de la información

VULNERABILIDADES	**V_1**
	V_2
	V_n

Fuente: Elaboración propia

Tabla 125 Ejemplo: Identificación de vulnerabilidades del activo DI011-TI002

ID ACTIVO	V1	V1	V3	V4	V5	V6	V7
DI011-TI002	5.1.1	7.3.1	8.2.1	11.1.1	12.1.1	12.1.4	12.6.1

Fuente: Elaboración propia

Tabla 126 Resultados obtenidos de las vulnerabilidades identificadas asociadas a los activos de la información

	VULNERABILIDADES													
ID ACTIVO	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14
DI003-TI005	5.1.1	12.1.1	8.2.1	12.6.1										
DI004-TI001	5.1.1	9.1.2	12.6.1											
DI006-TI005	5.1.1	12.4.1	12.6.1											
DI009-TI001	5.1.1	8.2.1	12.1.1	12.1.4	12.6.1	14.3.1								
DI009-TI002	5.1.1	8.2.1	12.1.1	12.1.4	12.6.1	14.3.1								
DI009-TI003	5.1.1	8.2.1	12.1.1	12.1.4	12.6.1	14.3.1								
DI009-TI004	5.1.1	8.2.1	12.1.1	12.1.4	12.6.1	14.3.1								
DI011-TI001	5.1.1	7.3.1	8.2.1	11.1.1	12.1.1	12.1.4	12.6.1							
DI011-TI002	5.1.1	7.3.1	8.2.1	11.1.1	12.1.1	12.1.4	12.6.1							
DI011-TI003	5.1.1	7.3.1	8.2.1	11.1.1	12.1.1	12.1.4	12.6.1							
DI011-TI004	5.1.1	7.3.1	8.2.1	11.1.1	12.1.1	12.1.4	12.6.1							
SA002-TI001	5.1.1	7.3.1	8.2.1	9.3.1	12.2.1	12.6.1								
AI001-TI001	5.1.1	8.2.1	9.4.2	12.1.4	12.4.1	12.6.1	12.7.1	14.2.2	14.2.5	18.2.1				
AI002-TI001	5.1.1	8.2.1	9.4.2	12.1.4	12.4.1	12.6.1	12.7.1	14.2.2	14.2.5	18.2.1				
AI008-TI001	5.1.1	8.2.1	11.1.1	12.3.1	12.4.1									
AI011-TI001	5.1.1	8.2.1	12.4.1	12.6.1										
SI004-TI001	5.1.1	8.2.1	9.2.3											
SI006-TI001	5.1.1	8.2.1	9.2.3											
IE002-TI001	5.1.1	11.1.2	11.1.6	11.1.1	11.1.4									
PP002-SS001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1							

PP002-CI001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-SO001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-NE001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-CQ001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-CO001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-CE001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-ME001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-PE001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-CG001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-CS001	5.1.1	6.1.1	7.2.2	8.1.1	9.2.5	9.3.1	18.2.1								
PP002-TI001	5.1.1	6.1.1	8.1.1	9.2.5	12.6.1	16.1.3	18.2.1								

Fuente: Elaboración propia

4.5.1.5 Identificar amenazas posibles sobre activos de la información

En cada uno de los activos registrados, se analizarán las amenazas a las que se encuentran expuestas, para lo cual en cada una de las celdas denominadas A_1,A_2,A_3 … An se seleccionarán las amenazas a las que se encuentra expuesta el activo analizado (Estas amenazas se encuentras descritas y listadas en el Catálogo de amenazas)

Tabla 127 Amenazas de los activos de la información

AMENAZAS	**A_1**
	A_2
	A_n

Fuente: Elaboración propia

Tabla 128 Ejemplo: Identificación de amenazas del activo DI011-TI002

ID ACTIVO	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18
DI011-T002	A.3	B.1	B.2	B.4	C.1	C.3	C.2	C.4	C.5	C.9	C.10	C.11	C.12	C.13	D.3	D.9	D.19	D.24

Fuente: Elaboración propia

Tabla 129 Resultados obtenidos vulnerabilidades identificadas a las que estarían expuestos los activos de la información

	AMENAZAS																															
ID ACTIVO	A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	A30	A31	A32
DI003-TI005	C.2	C.4	C.5	C.10	C.11	D.13	D.24																									
DI004-TI001	C.5	C.9	C.10	C.12	D.9																											
DI006-TI005	C.1	C.2	C.3	C.5	C.10	C.11	C.13	D.9	D.10	D.12	D.19	D.24																				
DI009-TI001	C.1	C.2	C.3	C.5	C.9	C.10	C.11	C.12	D.9																							
DI009-TI002	C.1	C.2	C.3	C.5	C.9	C.10	C.11	C.12	D.9																							
DI009-TI003	C.1	C.2	C.3	C.5	C.9	C.10	C.11	C.12	D.9																							
DI009-TI004	C.1	C.2	C.3	C.5	C.9	C.10	C.11	C.12	D.9																							
DI011-TI001	A.3	B.1	B.2	B.4	C.1	**C.3**	C.2	C.4	C.5	C.9	C.10	C.11	C.12	C.13	D.3	D.9	D.19	D.24														
DI011-TI002	A.3	B.1	B.2	B.4	C.1	C.3	C.2	C.4	C.5	C.9	C.10	C.11	C.12	C.13	D.3	D.9	D.19	D.24														
DI011-TI003	A.3	B.1	B.2	B.4	C.1	C.3	C.2	C.4	C.5	C.9	C.10	C.11	C.12	C.13	D.3	D.9	D.19	D.24														

PP002-SO001	PP002-CI001	PP002-SS001	IE002-TI001	SI006-TI001	SI004-TI001	AI011-TI001	AI008-TI001	AI002-TI001	AI001-TI001	SA002-TI001	DI011-TI004
C.1	C.1	C.1	A.3	C.1	C.1	C.1	A.3	C.2	C.2	C.1	A.3
C.5	C.5	C.5	B.1	C.5	C.5	C.5	B.1	C.3	C.3	C.5	B.1
C.9	C.9	C.9	B.2	C.9	C.9	C.9	B.2	C.5	C.5	C.9	B.2
C.10	C.10	C.10	B.4	C.10	C.10	C.10	B.4	C.9	C.9	C.10	B.4
C.11	C.11	C.11	C.1	C.11	C.11	C.11	C.1	C.10	C.10	C.11	C.1
C.12	C.12	C.12	C.5	C.12	C.12	C.12	C.5	C.11	C.11	C.12	C.3
C.16	C.16	C.16	C.10	D.6	D.6	C.13	C.9	C.12	C.12	C.13	C.2
C.17	C.17	C.17	C.11	D.15	D.15	D.9	C.10	C.13	C.13	D.9	C.4
D.11	D.11	D.11	D.9	D.19	D.19	D.12	C.11	C.14	C.14	D.10	C.5
D.27	D.27	D.27	D.17			D.19	C.12	D.9	D.9	D.12	C.9
D.28	D.28	D.28					C.13	D.12	D.12	D.14	C.10
D.29	D.29	D.29					D.9	D.13	D.13	D.15	C.11
D.30	D.30	D.30					D.19	D.19	D.19	D.17	C.12
								D.24	D.24	D.19	C.13
										D.24	D.3
										D.28	D.9
										D.29	D.19
											D.24

PP002-TI001	PP002-CS001	PP002-CG001	PP002-PE001	PP002-ME001	PP002-CE001	PP002-CO001	PP002-CQ001	PP002-NE001
C.1	C.1	C.1	C.1	C.1	C.1	C.1	C.1	C.1
C.2	C.5	C.5	C.5	C.5	C.5	C.5	C.5	C.5
C.3	C.9	C.9	C.9	C.9	C.9	C.9	C.9	C.9
C.4	C.10	C.10	C.10	C.10	C.10	C.10	C.10	C.10
C.5	C.11	C.11	C.11	C.11	C.11	C.11	C.11	C.11
C.9	C.12	C.12	C.12	C.12	C.12	C.12	C.12	C.12
C.10	C.16	C.16	C.16	C.16	C.16	C.16	C.16	C.16
C.11	C.17	C.17	C.17	C.17	C.17	C.17	C.17	C.17
C.12	D.11	D.11	D.11	D.11	D.11	D.11	D.11	D.11
C.13	D.27	D.27	D.27	D.27	D.27	D.27	D.27	D.27
C.14	D.28	D.28	D.28	D.28	D.28	D.28	D.28	D.28
C.16	D.29	D.29	D.29	D.29	D.29	D.29	D.29	D.29
C.17	D.30	D.30	D.30	D.30	D.30	D.30	D.30	D.30
D.1								
D.2								
D.3								
D.4								
D.6								
D.9								
D.10								
D.11								
D.12								
D.15								
D.17								
D.19								
D.22								
D.24								
D.25								
D.27								
D.28								
D.29								
D.30								

Fuente: Elaboración propia

4.5.2 Análisis y evaluación de riesgos

4.5.2.1 Definir probabilidad de materialización de amenazas sobre activos de información

El responsable del análisis de la gestión de riesgos registrará el valor de la probabilidad de materialización de amenazas del activo de la información analizado, colocando un valor del 1 – 5 considerando la descripción de la tabla 130.

Tabla 130 Escala de valoración de la probabilidad de materialización de amenazas (PMA).

PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS		
5	MA	5-MA: Prácticamente seguro
4	A	4-A: Probable
3	M	3-M: Posible
2	B	2-B: Poco probable
1	MB	1-MB: Muy raro

Fuente: Elaboración propia.

4.5.2.2 Definir impacto de materialización de amenaza sobre un activo de información

El responsable del análisis de la gestión de riesgos registrará el valor del impacto de materialización de amenazas del activo de la información analizado, colocando un valor del 1 – 5 considerando la descripción de la tabla 131.

Tabla 131 Escala de valoración del niel de impacto de materialización (IMI).

NIVELES DE IMPACTO		
5	MA	5-MA: Muy Alto
4	A	4-A: Alto
3	M	3-M: Medio
2	B	2-B: Bajo
1	MB	1-MB: Muy Bajo

Fuente: Elaboración propia.

4.5.2.3 Estimar el nivel de riesgo inherente

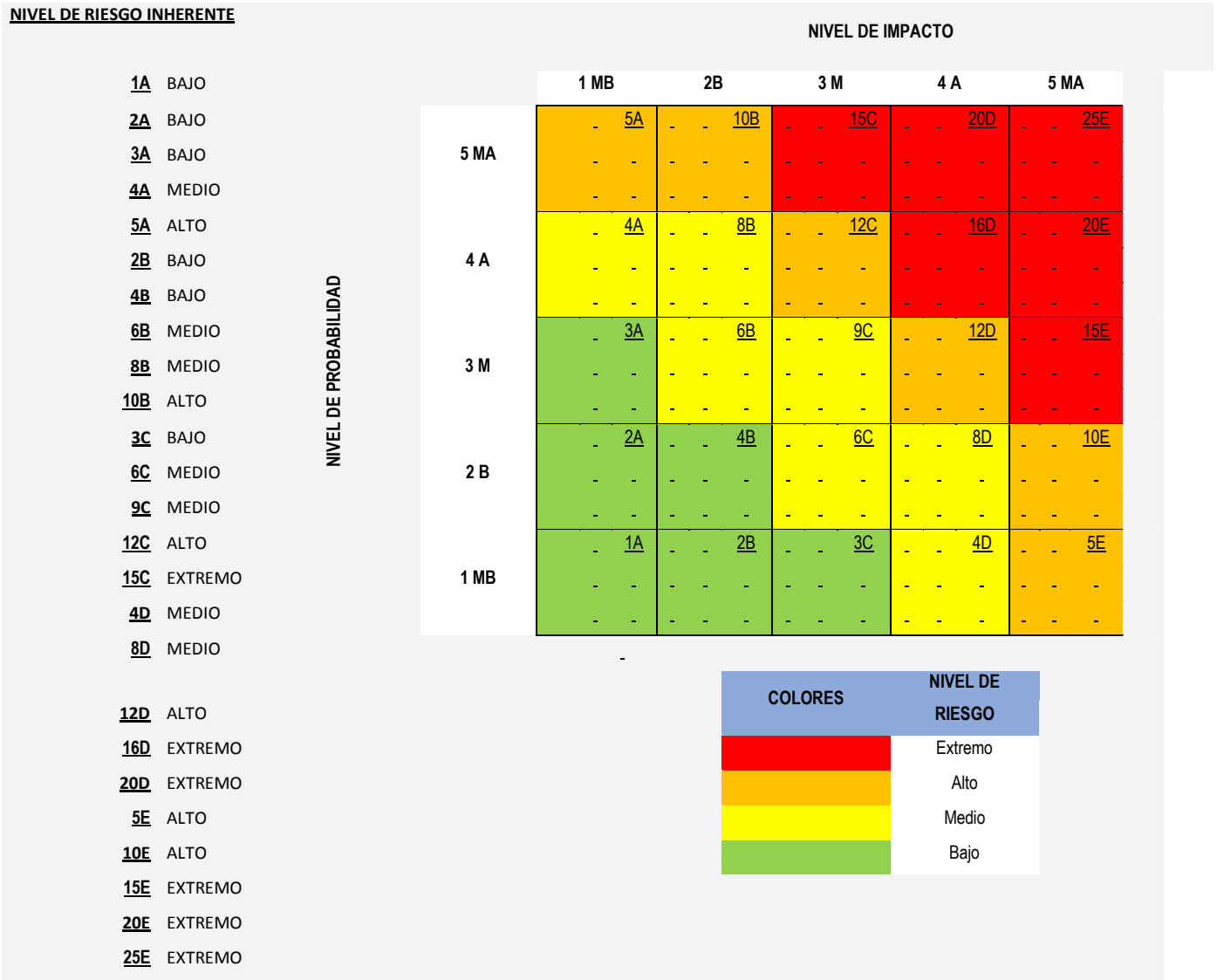
Una vez registrada la probabilidad de materialización de amenazas y el nivel de impacto de la amenaza, se devolverá en la celda la descripción del nivel de riesgo inherente según el cuadro 6 y teniendo en cuenta el cálculo realizado con la matriz mostrada.

Tabla 132 Escala de valoración del nivel de riesgo Inherente

OLORES	NIVEL DE RIESGO
	Extremo
	Alto
	Medio
	Bajo

Fuente: Elaboración propia

Fig 1. Matriz de riesgo Inherente.



Fuente: Elaboración propia.

Tabla 133 Ejemplo: Estimación de nivel de riesgo inherente para el análisis del activo DI011-TI002

ID ACTIVO	PROBABILIDAD DE MATERIALIZACION	IMPACTO DE MATERIALIZACIÓN			NIVEL DE RIESGO INHERENTE
DI011-TI002	3- M: Posible	4- A: Alto	D	12D	ALTO

Fuente: Elaboración propia

Tabla 134 Resultados de los niveles de riesgo inherente obtenidos

ID ACTIVO	PROBABILIDAD DE MATERIALIZACION	IMPACTO DE MATERIALIZACION	NIVEL DE RIESGO INHERENTE		
DI003-TI005	3- M: Posible	4- A: Alto	D	12D	ALTO
DI004-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
DI006-TI005	3- M: Posible	4- A: Alto	D	12D	ALTO
DI009-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
DI009-TI002	3- M: Posible	4- A: Alto	D	12D	ALTO
DI009-TI003	3- M: Posible	4- A: Alto	D	12D	ALTO
DI009-TI004	3- M: Posible	4- A: Alto	D	12D	ALTO
DI011-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
DI011-TI002	3- M: Posible	4- A: Alto	D	12D	ALTO
DI011-TI003	3- M: Posible	4- A: Alto	D	12D	ALTO
DI011-TI004	3- M: Posible	4- A: Alto	D	12D	ALTO
SA002-TI001	4- A: Probable	3- M: Medio	C	12C	ALTO
AI001-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
AI002-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
AI008-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
AI011-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
SI004-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
SI006-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
IE002-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-SS001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-CI001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-SO001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-NE001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-CQ001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-CO001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-CE001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-ME001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-PE001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-CG001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-CS001	3- M: Posible	4- A: Alto	D	12D	ALTO
PP002-TI001	3- M: Posible	4- A: Alto	D	12D	ALTO

Fuente: Elaboración propia

4.5.3 Tratamiento

4.5.3.1 Proponer mecanismos de protección que permitan hacer frente a las amenazas

En cada uno de los activos registrados, se analizarán los mecanismos de protección que puedan contrarrestar las amenazas y vulnerabilidades a las que se encuentran expuestas, para lo cual en cada una de las celdas denominadas S_1, S_2 … S_n, se seleccionarán las salvaguardas que según el criterio del analista puedan controlar estas amenazas (Estos mecanismos de protección se encuentras descritas y listadas en el Catálogo de mecanismos de protección)

Tabla 135 Mecanismos de protección

MECANISMOS DE PROTECCIÓN	**S_1**
	S_2
	S_n

Fuente: Elaboración propia

Tabla 136 Ejemplo: Identificación de mecanismos de protección del activo DI011-TI002

ID ACTIVO	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10
DI011-TI002	AP01	AP02	AP04	SS02	OR04	DI03	DI04	CO04	GH02	CC06

Fuente: Elaboración propia

Tabla 137 Resultados de los mecanismos de protección propuestos asociados a los activos de la información

	SALVAGUARDAS																									
ID ACTIVO	S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16	S17	S18	S19	S20	S21	S22	S23	S24	S25	S26
DI003-TI005	GH01	GH06	CC01	OR03																						
DI004-TI001	GH02	OR01	OR03	CC02	DI04																					
DI006-TI005	OR03	OR04	DI04																							

										EX02	
										GH02	
								EX02		EX05	
				CC06	CC06	CC06	CC06	OR04	GH02	EX02	
GH02	GH02	GH02	GH02	GH02	GH02	GH02	GH02	OR03	OR04	OR04	DI04
CO04	CO04	CO04	CO04	CO04	CO04	CO04	CO04	OR02	OR03	OR03	DI03
DI04	DI04	DI04	DI04	DI04	DI04	DI04	DI04	CO06	OR02	OR02	DI01
DI03	DI03	DI03	DI03	DI03	DI03	DI03	DI03	CO05	SS06	SS06	CC02
OR04	OR04	OR04	OR04	OR04	OR04	OR04	OR04	CO04	SS04	SS04	SS04
SS02	SS02	SS02	SS02	SS02	SS02	SS02	SS02	CO03	SS02	SS02	SS02
AP04	AP04	AP04	AP04	AP04	AP04	AP04	AP04	SS06	OR04	OR04	OR04
AP02	AP02	AP02	AP02	AP02	AP02	AP02	AP02	SS04	OR03	OR03	OR03
AP01	AP01	AP01	AP01	AP01	AP01	AP01	AP01	SS02	OR02	OR02	OR02
DI009-TI001	DI009-TI002	DI009-TI003	DI009-TI004	DI011-TI001	DI011-TI002	DI011-TI003	DI011-TI004	SA002-TI001	AI001-TI001	AI002-TI001	AI008-TI001

			OP03								
CC06			PP02	SS04	SS04	SS04	SS04	SS04	SS04	SS04	SS04
SS11			FF05	AP04	AP04	AP04	AP04	AP04	AP04	AP04	AP04
SS10			FF04	EQ03	EQ03	EQ03	EQ03	EQ03	EQ03	EQ03	EQ03
SS09	SI05	SI05	FF03	CO03	CO03	CO03	CO03	CO03	CO03	CO03	CO03
SS08	SI01	SI01	FF02	DI03	DI03	DI03	DI03	DI03	DI03	DI03	DI03
SS06	OR03	OR03	FF01	OR03	OR03	OR03	OR03	OR03	OR03	OR03	OR03
OR04	PP02	PP02	OR04	OR02	OR02	OR02	OR02	OR02	OR02	OR02	OR02
OR03	DI04	DI04	OR03	OR01	OR01	OR01	OR01	OR01	OR01	OR01	OR01
OR02	DI03	DI03	OR02	PP02	PP02	PP02	PP02	PP02	PP02	PP02	PP02
AI011-TI001	SI004-TI001	SI006-TI001	IE002-TI001	PP002-SS001	PP002-CI001	PP002-SO001	PP002-NE001	PP002-CQ001	PP002-CO001	PP002-CE001	PP002-ME001

PP002-PE001	PP02	OR01	OR02	OR03	DI03	CO03	EQ03	AP04	SS04																				
PP002-CG001	PP02	OR01	OR02	OR03	DI03	CO03	EQ03	AP04	SS04																				
PP002-CS001	PP02	OR01	OR02	OR03	DI03	CO03	EQ03	AP04	SS04																				
PP002-TI001	GH02	GH03	GH04	GH05	GH06	GH07	GH08	GH09	GH10	GH11	GH12	GH13	GH14	GH15	GH16	OR01	OR02	OR03	OR04	CO03	EQ03	AP04	SS04	SS06	EX02				

Fuente: Elaboración propia

4.5.3.2 Definir criterios para obtener niveles de efectividad de controles

Tabla 138 Criterios para la medición del nivel de efectividad

MECANISMOS DE PROTECCIÓN	ESTADO DE MECANISMOS DE PROTECCIÓN
	OPORTUNIDAD DE MECANISMOS DE PROTECIÓN
	GRADO DE IMPLEMENTACIÓN
	NIVEL DE EFECTIVIDAD

Fuente: Elaboración propia

- **ESTADO DE MECANISMO DE PROTECCIÓN**: Se registrará el Estado de mecanismos de protección en el que se encuentra los mecanismos de protección seleccionados para el control de las amenazas del activo analizado, según el cuadro 6, considerando los valores "**1**" en caso de estar implementado ó "**0**" de ser no implementado

Tabla 139 Escala de valoración de los estados de mecanismos de protección.

ESTADO DE MECANISMO DE PROTECCIÓN	
1	Implementado
0	No implementado

Fuente: Elaboración propia.

En caso de contar con más de un mecanismo de protección por activo analizado, en la matriz de riesgos se colocará el promedio de los valores registrados en el estado de mecanismos de protección.

- **OPORTUNIDAD DE MECANISMOS DE PROTECCIÓN**: Se registrará la oportunidad de la propuesta de los mecanismos de protección para el activo analizado, según el cuadro 7, considerando los valores "**1**" en caso de proponer una salvaguarda de naturaleza **preventiva** , "**2**" si la propuesta es de una salvaguarda de naturaleza **detectiva** ó "**3**" si la propuesta se consideran un mecanismo de protección c**orrectiva**

Tabla 140 Escala de valoración de oportunidades de propuesta de mecanismos de protección.

OPORTUNIDAD DE PROPUESTA DE MECANISMO DE PROTECCIÓN	
1	Preventivo
2	Detectivo
3	Correctivo

Fuente: Elaboración propia.

En caso de contar con más de un mecanismo de control por activo analizado, en la matriz de riesgos se colocará el promedio de los valores registrados en la oportunidad de propuesta de control de estos mecanismos de protección.

- **GRADO DE IMPLEMENTACIÓN**: Se registrará el grado de implementación de los mecanismos de protección para el activo analizado, según el cuadro 8, considerando los valores "**1**" en caso de proponer un

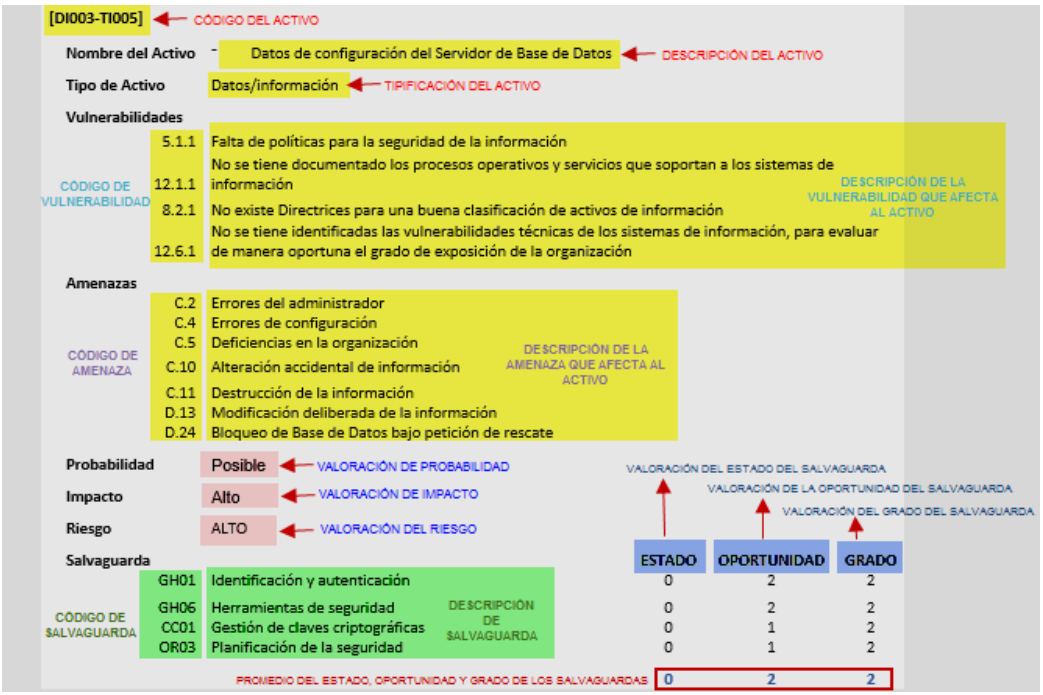
mecanismo de protección que requiera como mínimo una implementación **manual** , "**2**" si la propuesta es de un mecanismo de protección que deba ser s**emiautomatizada** ó "**3**" si la propuesta se consideran un mecanismo de protección implementada de forma a**utomatizada**

Tabla 141 Escala de valoración del grado de implementación de mecanismos de protección.

GRADO DE IMPLEMENTACION DE MECANISMOS DE PROTECCIÓN	
1	Manual
2	Semiautomatizado
3	Automatizado

Fuente: Elaboración propia.

En caso de contar con más de un mecanismo de protección por activo analizado, en la matriz de riesgos se colocará el promedio de los valores registrados en el grado de implementación de estos mecanismos de protección.



- **NIVEL DE EFECTIVIDAD**: Una vez que el responsable del registro del estado, oportunidad y grado del mecanismo de protección completó estos

tres datos, la celda de nivel de efectividad devolverá el valor del nivel de efectividad del mecanismo de protección señaladas para el activo analizado, de acuerdo a las combinaciones señaladas en el cuadro 9.

Tabla 142 Equivalencia de los niveles de efectividad de control de medidas de protección.

NIVELES DE EFECTIVIVDAD DE MEDIDAS DE PROTECCIÓN					
NIVELES DE ESTADO	NIVELES DE OPORTUNIDAD	GRADO	COMBINACIÓN	DESCRIPCIÓN	VALOR
No implementado	Preventivo	Manual	No implementadoPreventivoManual	1. Deficiente	1
No implementado	Preventivo	Semiautomatizado	No implementadoPreventivoSemiautomatizado	1. Deficiente	1
No implementado	Preventivo	Automatizado	No implementadoPreventivoAutomatizado	1. Deficiente	1
No implementado	Correctivo	Manual	No implementadoCorrectivoManual	1. Deficiente	1
No implementado	Correctivo	Semiautomatizado	No implementadoCorrectivoSemiautomatizado	1. Deficiente	1
No implementado	Correctivo	Automatizado	No implementadoCorrectivoAutomatizado	1. Deficiente	1
No implementado	Detectivo	Manual	No implementadoDetectivoManual	1. Deficiente	1
No implementado	Detectivo	Semiautomatizado	No implementadoDetectivoSemiautomatizado	1. Deficiente	1
No implementado	Detectivo	Automatizado	No implementadoDetectivoAutomatizado	1. Deficiente	1
Implementado	Correctivo	Manual	ImplementadoCorrectivoManual	2. Regular	2
Implementado	Correctivo	Semiautomatizado	ImplementadoCorrectivoSemiautomatizado	2. Regular	2
Implementado	Correctivo	Automatizado	ImplementadoCorrectivoAutomatizado	2. Regular	2
Implementado	Detectivo	Manual	ImplementadoDetectivoManual	3. Más que regular	3
Implementado	Detectivo	Semiautomatizado	ImplementadoDetectivoSemiautomatizado	3. Más que regular	3
Implementado	Detectivo	Automatizado	ImplementadoDetectivoAutomatizado	4. Bueno	4
Implementado	Preventivo	Manual	ImplementadoPreventivoManual	4. Bueno	4
Implementado	Preventivo	Semiautomatizado	ImplementadoPreventivoSemiautomatizado	5. Optimo	5
Implementado	Preventivo	Automatizado	ImplementadoPreventivoAutomatizado	5. Optimo	5

Fuente: Elaboración propia.

Tabla 143 Ejemplo: Estimación de nivel de efectividad de los mecanismos de protección para el activo DI011-TI002

ID ACTIVO	ESTADO DE MECANISMOS DE PROTECCIÓN	OPORTUNIDAD DE MECANISMOS DE PROTECCIÓN	GRADO DE IMPLEMENTACION	NIVEL DE EFECTIVIDAD
DI011-TI002	Implementado	Preventivo	Semiautomatizado	**5**

Fuente: Elaboración propia

Tabla 144 Resultados del nivel de efectividad obtenidos

ID ACTIVO	ESTADO DE CONTROL		OPORTUNIDAD DE CONTROL		GRADO DE IMPLEMENTACIÓN		NIVEL DE EFECTIVIDAD
DI003-TI005	0	No implementado	2	Detectivo	2	Semiautomatizado	**1**
DI004-TI001	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**

DI006-TI005	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
DI009-TI001	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI009-TI002	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI009-TI003	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI009-TI004	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI011-TI001	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI011-TI002	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI011-TI003	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
DI011-TI004	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
SA002-TI001	1	Implementado	1	Preventivo	2	Semiautomatizado	**5**
AI001-TI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
AI002-TI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
AI008-TI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
AI011-TI001	0	No implementado	2	Detectivo	2	Semiautomatizado	**1**
SI004-TI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
SI006-TI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
IE002-TI001	0	No implementado	2	Detectivo	2	Semiautomatizado	**1**
PP002-SS001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-CI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-SO001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-NE001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-CQ001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-CO001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-CE001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-ME001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-PE001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-CG001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-CS001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**
PP002-TI001	0	No implementado	1	Preventivo	2	Semiautomatizado	**1**

Fuente: Elaboración propia

4.5.3.2.1 Definir probabilidad residual de materialización de amenaza sobre un activo de información

Tomando en cuenta el valor del nivel de efectividad calculado anteriormente, es que se devuelve la probabilidad residual, teniendo en cuenta la equivalencia del cuadro 10, en el cual de acuerdo al valor del nivel de efectividad del mecanismo de protección, la probabilidad residual se halla como resultado del valor de la probabilidad de materialización de

amenazas (PMA) menos los valores (0-1) según la equivalencia del nivel de efectividad del mecanismo de protección del activo analizado

Tabla 145 Escala de valoración de la probabilidad residual.

NIVEL EFECTIVIDAD DE MECANISMO DE PROTECCIÓN		PROBABILIDAD RESIDUAL: PMA: Probabilidad de Materialización de amenazas
DESCRIPCIÓN	VALOR	
Deficiente	1	PMA (menos) 0
Regular	2	PMA (menos) 1
Más que regular	3	PMA (menos) 2
Bueno	4	PMA (menos) 3
Optimo	5	PMA (menos) 4

Fuente: Elaboración propia.

4.5.3.3 Definir impacto residual de materialización de amenaza sobre un activo de información

- Tomando en cuenta el valor del nivel de efectividad calculado anteriormente, es que se devuelve el impacto residual, teniendo en cuenta la equivalencia del cuadro 11, en el cual de acuerdo al valor del nivel de efectividad del mecanismo de protección, el impacto residual se halla como resultado del valor impacto de materialización (IMI) menos los valores (0-1) según la equivalencia del nivel de efectividad del mecanismo de protección del activo analizado

Tabla 146 Escala de valoración del impacto residual.

NIVEL EFECTIVIDAD DEL MECANISMO DE PROTECCIÓN		IMPACTO RESIDUAL IMI: Impacto Inherente
DESCRIPCIÓN	VALOR	
Deficiente	1	IMI (menos) 0
Regular	2	IMI (menos) 1
Más que regular	3	IMI (menos) 2
Bueno	4	IMI (menos) 3

Optimo	5	IMI (menos) 4

Fuente: Elaboración propia.

4.5.3.4 Definir el nivel de riesgo residual

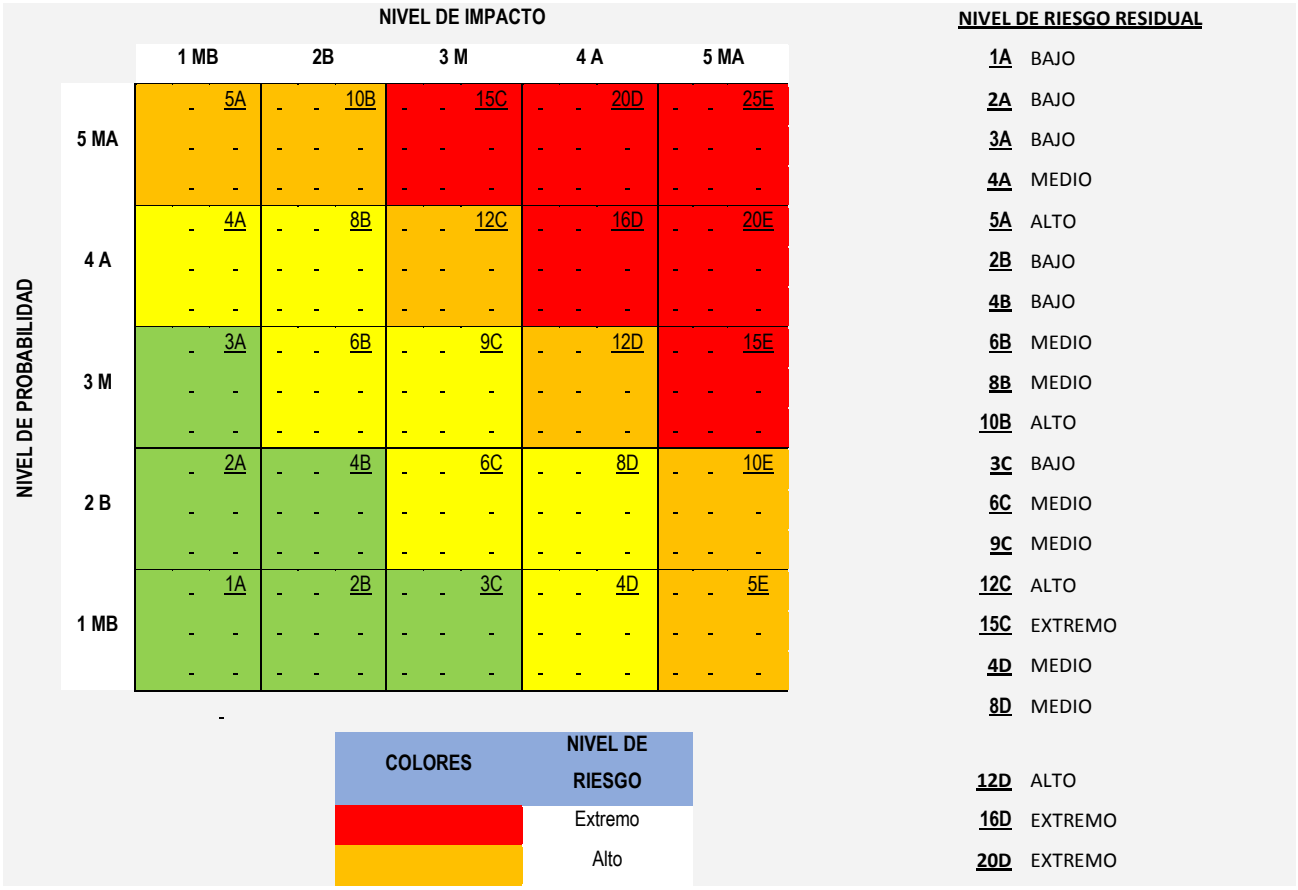
Con los valores de la probabilidad residual y el impacto residual es que se determina el nivel de riesgo residual considerando el cuadro 12 y tomando como referencia la matriz mostrada

Tabla 147 Escala de valoración del nivel de riesgo residual.

COLORES	NIVEL DE RIESGO RESIDUAL
	Extremo
	Alto
	Medio
	Bajo

Fuente: Elaboración propia.

Fig 2. Matriz de riesgo residual.



	Medio	**5E**	ALTO
	Bajo	**10E**	ALTO
		15E	EXTREMO
		20E	EXTREMO
		25E	EXTREMO

Fuente: Elaboración propia.

Tabla 148 Ejemplo: Estimación de nivel de riesgo residual para el análisis del activo DI011-TI002

ID ACTIVO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO RESIDUAL
DI011-TI002	1	1	BAJO

Fuente: Elaboración propia

Tabla 149 Resultados del nivel de riesgo residual obtenidos

	ANALISIS DE RIESGO RESIDUAL				
ID ACTIVO	PROBABILIDAD	IMPACTO	NIVEL DE RIESGO RESIDUAL		
DI003-TI005	3	4	D	12D	ALTO
DI004-TI001	1	1	A	1ª	BAJO
DI006-TI005	3	4	D	12D	ALTO
DI009-TI001	1	1	A	1ª	BAJO
DI009-TI002	1	1	A	1ª	BAJO
DI009-TI003	1	1	A	1ª	BAJO
DI009-TI004	1	1	A	1ª	BAJO
DI011-TI001	1	1	A	1ª	BAJO
DI011-TI002	1	1	A	1A	BAJO
DI011-TI003	1	1	A	1A	BAJO
DI011-TI004	1	1	A	1A	BAJO
SA002-TI001	1	1	A	1A	BAJO
AI001-TI001	3	4	D	12D	ALTO
AI002-TI001	3	4	D	12D	ALTO
AI008-TI001	3	4	D	12D	ALTO
AI011-TI001	3	4	D	12D	ALTO
SI004-TI001	3	4	D	12D	ALTO
SI006-TI001	3	4	D	12D	ALTO
IE002-TI001	3	4	D	12D	ALTO
PP002-SS001	3	4	D	12D	ALTO
PP002-CI001	3	4	D	12D	ALTO
PP002-SO001	3	4	D	12D	ALTO
PP002-NE001	3	4	D	12D	ALTO

PP002-CQ001	3	4	D	12D	ALTO
PP002-CO001	3	4	D	12D	ALTO
PP002-CE001	3	4	D	12D	ALTO
PP002-ME001	3	4	D	12D	ALTO
PP002-PE001	3	4	D	12D	ALTO
PP002-CG001	3	4	D	12D	ALTO
PP002-CS001	3	4	D	12D	ALTO
PP002-TI001	3	4	D	12D	ALTO

Fuente: Elaboración propia

4.5. Análisis de juicio de expertos

Se sometió a juicio de expertos en seguridad de la información, la valoración del modelo de gestión de riesgos diseñado, con el objetivo de verificar su validez y utilidad, en función a las características de suficiencia, claridad, coherencia y relevancia en las actividades que se realizan en cada etapa del modelo, bajo los siguientes indicadores:

CRITERIO	CALIFICACIÓN	INDICADOR
SUFICIENCIA Las actividades descritas que pertenecen a una misma etapa bastan para obtener la dimensión de ésta	1. No cumple con el criterio	Los ítems no son suficientes para medir el criterio
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes
CLARIDAD Las actividades se comprenden fácilmente, es decir, su sintáctica y semántica son adecuadas.	1 No cumple con el criterio	El ítem no es claro
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA Las actividades tienen relación lógica con la etapa que está midiendo.	1 No cumple con el criterio	El ítem no tiene relación lógica con la dimensión
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.

RELEVANCIA Las actividades son esenciales o importantes, es decir debe ser incluido.	1 No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Fuente: Elaboración propia

Las siguientes tablas muestran la valoración realizada por los expertos en seguridad de la información:

a. Etapa de identificación

- Suficiencia: Las actividades descritas son suficientes para explicar esta etapa.

Tabla 150 Resultados criterio suficiencia – etapa de identificación

ACTIVIDAD	SUFICIENCIA			PROMEDIO
Identificar y tipificar los activos de la información	4	4	3	4
Valorar las dimensiones de los activos de la información	4	4	3	4
Priorizar los activos de la información	4	4	4	4
Identificar amenazas de los activos de la información	4	3	4	4
Identificar amenazas de la información	4	3	4	4

Fuente: Elaboración propia

- Claridad: Las actividades de esta etapa se describieron de forma clara, con la semántica y sintaxis adecuada. Pero se debe mejorar la terminología utilizada en las actividades de identificación y tipificación.

Tabla 151Resultados criterio claridad – etapa de identificación

ACTIVIDAD	CLARIDAD			PROMEDIO
Identificar y tipificar los activos de la información	4	2	4	3
Valorar las dimensiones de los activos de la información	4	4	4	4
Priorizar los activos de la información	4	3	4	4

Identificar amenazas de los activos de la información	4	3	4	4
Identificar amenazas de la información	4	3	4	4

Fuente: Elaboración propia

- Coherencia: Las actividades descritas se encuentran completamente relacionado con esta etapa. No obstante, la actividad de identificación de amenazas de la información podría incluirse en la etapa de tratamiento.

Tabla 152Resultados criterio coherencia – etapa de identificación

ACTIVIDAD	COHERENCIA							PROMEDIO
Identificar y tipificar los activos de la información	4	4	4					4
Valorar las dimensiones de los activos de la información	4	4	4					4
Priorizar los activos de la información	4	4	4					4
Identificar amenazas de los activos de la información	4	4	4					4
Identificar amenazas de la información	4	1	4					3

Fuente: Elaboración propia

- Relevancia: Las actividades descritas son importantes para el desarrollo de esta etapa. En la actividad que corresponde a la valoración de dimensiones de activos de la información, se podrían considerar un número menor de dimensiones para su valoración.

Tabla 153 Resultados criterio relevancia – etapa de identificación

ACTIVIDAD	RELEVANCIA			PROMEDIO
Identificar y tipificar los activos de la información	4	4	4	4
Valorar las dimensiones de los activos de la información	4	4	2	3
Priorizar los activos de la información	4	4	4	4
Identificar amenazas de los activos de la información	4	4	4	4
Identificar amenazas de la información	4	4	4	4

Fuente: Elaboración propia

b. Etapa de análisis y evaluación

- Suficiencia: Las actividades descritas son suficientes para explicar esta etapa.

Tabla 154 Resultados criterio suficiencia – etapa de análisis y evaluación

ACTIVIDAD	SUFICIENCIA			PROMEDIO
Priorización de amenazas según el nivel de riesgo	4	4	4	4
Estimar el nivel de riesgo inherente	3	4	4	4
Definir Impacto derivado de la materialización de las amenazas	3	4	4	4
Definir Probabilidad de materialización de las amenazas	3	4	4	4

Fuente: Elaboración propia

- Claridad: Las actividades de esta etapa se describieron de forma clara, con la semántica y sintaxis adecuada.

Tabla 155 Resultados criterio claridad – etapa de análisis y evaluación

ACTIVIDAD	CLARIDAD			PROMEDIO
Priorización de amenazas según el nivel de riesgo	4	4	4	4
Estimar el nivel de riesgo inherente	3	4	4	4
Definir Impacto derivado de la materialización de las amenazas	3	4	4	4
Definir Probabilidad de materialización de las amenazas	3	4	4	4

Fuente: Elaboración propia

- Coherencia: Las actividades descritas se encuentran completamente relacionadas con esta etapa.

Tabla 156 Resultados criterio coherencia – etapa de análisis y evaluación

ACTIVIDAD	COHERENCIA			PROMEDIO
Priorización de amenazas según el nivel de riesgo	4	4	4	4
Estimar el nivel de riesgo inherente	3	4	4	4
Definir Impacto derivado de la materialización de las amenazas	3	4	4	4
Definir Probabilidad de materialización de las amenazas	3	4	4	4

Fuente: Elaboración propia

- Relevancia: Las actividades descritas son importantes para el desarrollo de esta etapa.

Tabla 157 Resultados criterio relevancia – etapa de análisis y evaluación

ACTIVIDAD	RELEVANCIA			PROMEDIO
Priorización de amenazas según el nivel de riesgo	4	4	4	4
Estimar el nivel de riesgo inherente	3	4	4	4
Definir Impacto derivado de la materialización de las amenazas	3	4	4	4
Definir Probabilidad de materialización de las amenazas	3	4	4	4

Fuente: Elaboración propia

c. Etapa de tratamiento

- Suficiencia: Adicionalmente a las actividades de definición de criterios para obtener el nivel de eficiencia de los mecanismos de protección, el impacto residual y estimación del nivel de riesgo residual, pueden complementarse con otras actividades para explicar de manera más detallada esta etapa.

Tabla 158 Resultados criterio suficiencia – etapa de tratamiento

ACTIVIDAD	SUFICIENCIA			PROMEDIO
Proponer mecanismos de protección	4	4	4	4
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	3	3	3
Definir la probabilidad residual de materialización de amenazas	4	4	3	4
Definir Impacto residual de materialización de amenazas	4	3	3	3
Estimar el nivel de riesgo residual	3	3	4	3

Fuente: Elaboración propia

- Claridad: Las actividades de esta etapa se describieron en forma clara, con la semántica y sintaxis adecuada. Pero en cuanto a las actividades de definición de criterios para obtener el nivel de eficiencia de los mecanismos de protección y estimación del nivel de riesgo residual, podrían mejorar la terminología que utilizan, para una mayor claridad.

Tabla 159 Resultados criterio claridad – etapa de tratamiento

ACTIVIDAD	CLARIDAD	PROMEDIO

Proponer mecanismos de protección	4	4	4	4
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	3	4	3
Definir la probabilidad residual de materialización de amenazas	4	3	4	4
Definir Impacto residual de materialización de amenazas	4	3	4	4
Estimar el nivel de riesgo residual	3	3	4	3

Fuente: Elaboración propia

- Coherencia: Las actividades descritas se encuentran completamente relacionado con esta etapa.

Tabla 160 Resultados criterio coherencia – etapa de tratamiento

ACTIVIDAD	COHERENCIA			PROMEDIO
Proponer mecanismos de protección	4	4	4	4
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	4	4	4
Definir la probabilidad residual de materialización de amenazas	4	4	4	4
Definir Impacto residual de materialización de amenazas	4	4	4	4
Estimar el nivel de riesgo residual	3	4	4	4

Fuente: Elaboración propia

- Relevancia: Las actividades descritas son importantes para el desarrollo de esta etapa.

Tabla 161 Resultados criterio relevancia – etapa de tratamiento

ACTIVIDAD	RELEVANCIA			PROMEDIO
Proponer mecanismos de protección	4	4	4	4
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	4	4	4
Definir la probabilidad residual de materialización de amenazas	4	4	4	4
Definir Impacto residual de materialización de amenazas	4	4	4	4
Estimar el nivel de riesgo residual	3	4	4	4

Fuente: Elaboración propia

d. Etapa de seguimiento y monitoreo

- Suficiencia: Adicionalmente a las actividades de definición de criterios para obtener el nivel de eficiencia de los mecanismos de protección, el impacto residual y estimación del nivel de riesgo residual, pueden complementarse con otras actividades para explicar de manera más detallada esta etapa.

Tabla 162 Resultados criterio suficiencia – etapa de seguimiento y monitoreo

ACTIVIDAD	SUFICIENCIA			PROMEDIO
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	3	3	3
Definir la probabilidad residual de materialización de amenazas	4	4	3	4
Definir Impacto residual de materialización de amenazas	4	3	3	3
Estimar el nivel de riesgo residual	3	3	4	3

Fuente: Elaboración propia

- Claridad: Las actividades de esta etapa se describieron en forma clara, con la semántica y sintaxis adecuada. Pero en cuanto a las actividades de definición de criterios para obtener el nivel de eficiencia de los mecanismos de protección y estimación del nivel de riesgo residual, podrían mejorar la terminología que utilizan, para una mayor claridad.

Tabla 163 Resultados criterio claridad – etapa de seguimiento y monitoreo

ACTIVIDAD	CLARIDAD			PROMEDIO
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	3	4	3
Definir la probabilidad residual de materialización de amenazas	4	3	4	4
Definir Impacto residual de materialización de amenazas	4	3	4	4
Estimar el nivel de riesgo residual	3	3	4	3

Fuente: Elaboración propia

- Coherencia: Las actividades descritas cuentan con una relación moderada con esta etapa.

Tabla 164 Resultados criterio coherencia – etapa de seguimiento y monitoreo

ACTIVIDAD	COHERENCIA			PROMEDIO
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	2	4	3
Definir la probabilidad residual de materialización de amenazas	4	2	4	3
Definir Impacto residual de materialización de amenazas	4	2	4	3

Estimar el nivel de riesgo residual	3	2	4	3

Fuente: Elaboración propia

- Relevancia: Las actividades descritas son importantes para el desarrollo de esta etapa.

Tabla 165 Resultados criterio relevancia – etapa de seguimiento y monitoreo

ACTIVIDAD	RELEVANCIA			PROMEDIO
Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección	3	4	4	4
Definir la probabilidad residual de materialización de amenazas	4	4	4	4
Definir Impacto residual de materialización de amenazas	4	4	4	4
Estimar el nivel de riesgo residual	3	4	4	4

Fuente: Elaboración propia

CAPITULO V. DISCUSIÓN DE RESULTADOS

En base a los objetivos específicos definidos y los resultados obtenidos en nuestra investigación en el Hospital Regional de Lambayeque, podemos deducir lo siguiente:

5.1. Del diagnóstico de la situación actual de la seguridad de la información:

– Los usuarios, administradores y responsables de los sistemas de gestión hospitalaria del Hospital Regional de Lambayeque, manifestaron en las entrevistas que participaron, que la alta dirección desconoce la importancia de la seguridad de la información y los riesgos en los que podría quedar expuesta la institución al no reguardar los activos de información que administra, procesa y custodia; de ello se desprende la falta de recursos asignados por parte de la alta dirección para implementar un sistema de gestión de seguridad de la información alineado a las políticas de seguridad de información definidos por el Ministerio de Salud, la falta de capacitación, concientización y compromiso del personal, para cumplir con las políticas de seguridad de la información del Ministerio de Salud.

- El modelo propuesto para la gestión de riesgos de la seguridad de la información, permite cumplir con la mayor cantidad de políticas de seguridad de la información definidos por el Ministerio de Salud, de lo cual se tiene:
  a. La información es un activo institucional: en nuestra metodología, se plantea la amplia gestión de los activos de la información desde su identificación, que se plasma en el inventario de activos de la información, hasta su tratamiento con la valoración y priorización, identificando los riesgos a las distintas amenazas, vulnerabilidades, y proponiendo los respectivos mecanismos de protección.

  b. Compromiso de la alta dirección y de los órganos del Ministerio de Salud: la aplicación de nuestra metodología sugiere que el directorio cree un comité o grupo de trabajo integrado por las áreas que éste designe como responsables, incluido algunos integrantes del directorio; de manera que cumpla el rol de organismo de control a quien se deba reportar la gestión de seguridad de la información, de igual manera se pueda designar un coordinador de seguridad de la información, establecer y aprobar el marco normativo con las políticas de seguridad de la información, que incluya los roles y responsabilidades de la seguridad de la información, lineamientos para resguardar la información y las respectivas sanciones administrativas ante las infracciones de las mismas; tomando como referencia la ISO27001 y la Norma Técnica Peruana 27005.

  c. La seguridad de la información es el soporte de los procesos y procedimientos institucionales: la aplicación de nuestra metodología permite que mediante el análisis de los activos de la información se valore cada una de las dimensiones de la seguridad de la información de cada uno de ellos, llegando a señalar el tipo de daño que podría sufrir, ésta valoración permite priorizarlos para determinar en ellos las amenazas, vulnerabilidades, riesgos y mecanismos de protección que puedan controlarlos.

  d. Personal involucrado con la seguridad de la información: en el desarrollo de nuestra metodología se sugiere la conformación de un grupo de trabajo que

mantenga coordinación con la alta dirección, y permita designar a los responsables de establecer y hacer cumplir las políticas la seguridad de la información para la gestión de activos de la información.

e. Prevención de riesgos y aplicación de mecanismos de protección: el desarrollo de nuestra metodología sugiere y muestra una herramienta que facilita al responsable de la gestión de la seguridad de la información sobre los activos de la información, de forma detallada la identificación, evaluación y tratamiento de los riesgos a los que se encuentran expuestos los activos de la información.

f. Mantener la seguridad de la información en niveles óptimos: mediante la aplicación de nuestra metodología a través de las etapas de identificación de vulnerabilidades y el tratamiento de riesgos, se logra cubrir éste lineamiento de la política de seguridad de la información del Ministerio de Salud; ya que se pudo identificar activos de información cuya vulnerabilidad corresponde a que no se realizan auditorías internas y externas para supervisar y revisar las políticas de la seguridad de la información establecidas, para los cuales se ha propuesto como mecanismo de protección la evaluación de Auditarías internas y externas.

g. El bien público en salud respeta los datos personales individuales: la aplicación de nuestra metodología a través de las etapas de identificación de vulnerabilidades y el tratamiento de riesgos, se logra cubrir éste lineamiento de la Política de seguridad de la información del Ministerio de Salud; ya que se pudo identificar activos de información cuya vulnerabilidad corresponde a "*No existe directrices para una buena clasificación de activos de información*", para los cuales se ha propuesto como mecanismo de protección la clasificación de dicha información.

h. El tratamiento de datos personales requiere el consentimiento de su titular: el alcance de nuestro modelo y metodología de gestión de riesgos asociados

a los activos de información, no aplica al consentimiento del tratamiento de datos personales por parte del titular.

5.2. Del alcance del modelo propuesto, su metodología, método de estimación y mecanismos de protección de riesgos:

En cuanto a los niveles de exposición al riego de los activos de la información podemos decir:

Se determinó mediante el análisis de los activos de la información de los cuatro sistemas de gestión hospitalaria utilizador por el HRL que sus activos de información presentan un nivel de riesgo inherente del 97% resultado de una posible probabilidad y un alto impacto (riesgo inherente ALTO) en la institución; y solo un 3% resultan probables con impacto medio (riesgo inherente ALTO).

Tabla 166 Análisis del nivel de riesgo inherente

NIVEL DE RIESGO INHERENTE						
Probabilidad / Impacto	3- M: Medio	4- A: Alto	Total general	% P. Medio	%P. Alto	% Total
3- M: Posible	0	30	30	0	97	**97**
4- A: Probable	1	0	1	3	0	**3**
Total general	1	30	31	3	0	**100**

Fuente: Elaboración propia

NIVEL DE RIESGO INHERENTE	
1A	BAJO
2A	BAJO
3A	BAJO
4A	MEDIO
5A	ALTO
2B	BAJO
4B	BAJO
6B	MEDIO
8B	MEDIO
10B	ALTO
3C	BAJO
6C	MEDIO
9C	MEDIO
12C	ALTO
15C	EXTREMO
4D	MEDIO
8D	MEDIO
12D	ALTO
16D	EXTREMO
20D	EXTREMO
5E	ALTO
10E	ALTO
15E	EXTREMO
20E	EXTREMO
25E	EXTREMO

NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO				
	1 MB	2B	3 M	4 A	5 MA
5 MA	5A	10B	15C	20D	25E
4 A	4A	8B	12C	16D	20E
3 M	3A	6B	9C	12D	15E
2 B	2A	4B	6C	8D	10E
1 MB	1A	2B	3C	4D	5E

COLORES	NIVEL DE RIESGO
	Extremo
	Alto
	Medio
	Bajo

Fuente: Elaboración propia

Por lo cual tenemos como resultado que el riesgo inherente del 100% de los activos priorizados presentan un nivel de riesgo inherente ALTO.

5.3 De la calificación efectuada por los expertos en seguridad de la información mediante la valoración de juicio de expertos:

Con respecto a los resultados obtenidos a la valoración realizada por los expertos en seguridad de la información, al modelo de gestión de riesgos propuesto, se puede considerar los siguientes aspectos:

- Etapa identificación: El desarrollo de esta etapa se realizó en forma clara y coherente, considerando las suficientes actividades que permitan la plena identificación de los activos de la información, sus vulnerabilidades y amenazas. Considerando que se podría mejorar la terminología específica que se utilizan en la etapa de identificación de los activos de la información. Las actividades que se consideran en esta etapa son relevante para el desarrollo del modelo de gestión de riesgos propuesto.

- Etapa análisis y evaluación: El desarrollo de esta etapa se realizó en forma clara y coherente, considerando suficientes actividades que permitan priorizar correctamente las amenazas según el nivel de riesgo y estimando el nivel de riesgo inherente en función de los niveles de probabilidad e impacto de materialización de amenazas. Las actividades que se consideran en esta etapa son relevantes para el desarrollo del modelo de gestión de riesgos propuesto.

- Etapa de tratamiento: El desarrollo de esta etapa se realizó en forma clara y coherente, considerando las suficientes actividades que permitan proponer mecanismos de protección ante amenazas, definir los criterios para obtener el nivel de eficiencia de estos mecanismos de protección, Las actividades que se consideran en esta etapa son relevantes para el desarrollo del modelo de gestión de riesgos propuesto. Sin embargo, se podría mejorar la terminología utilizada en esta etapa e incrementar algunas sub tareas que aporten claridad y suficiencia definir criterios que permitan medir la eficiencia de los mecanismos de control y estimar el riesgo residual.

- Etapa de seguimiento y monitoreo: El desarrollo de esta etapa se realizó en forma clara y coherente, considerando las suficientes actividades que permitan realizar un seguimiento de la propuesta de mecanismos de protección, considerando los criterios para medir el nivel de eficiencia de estos mecanismos de protección y el impacto y estimar el nivel de riesgo residual en forma periódica. Las actividades que se consideran en esta etapa son relevantes para el desarrollo y continuidad del modelo de gestión de riesgos propuesto. Sin embargo, se podría mejorar la terminología utilizada en esta etapa e incrementar algunas sub tareas que aporten claridad y suficiencia definir criterios que permitan medir la eficiencia de los mecanismos de control y estimar el riesgo residual.

CAPITULO VI. CONCLUSIONES Y RECOMENDACIONES

6.1 **CONCLUSIONES**:

- Del análisis realizado en nuestra investigación evidenció que Hospital Regional de Lambayeque no cuenta con normas, políticas o alguna estrategia para gestionar la seguridad de la información dentro de su institución. La utilización del modelo de gestión de riesgos basado en las normas ISO/IEC 27005 y la metodología MAGERIT propuesto, permitiría cumplir con 6 de los 8 lineamientos definidos en la política de seguridad de la información establecida por el Ministerio de Salud.

- De la valoración obtenida por los expertos en seguridad de la información, se puede concluir que el "Modelo de gestión de riesgos basados en la norma ISO/IEC 27005 y metodología MAGERIT para mejorar la gestión de la seguridad de la información en el Hospital Regional de Lambayeque", las fases del modelo presentado cuentan con un moderado - alto nivel de suficiencia, claridad, coherencia y relevancia, por lo tanto es un modelo válido para realizar la gestión de riesgos y de utilidad en el Hospital Regional de Lambayeque, es decir este modelo podría contribuir en la mejora de la gestión en la seguridad de la información de esta institución.

6.2 **RECOMENDACIONES**:

- Se recomienda que la alta dirección del Hospital Regional de Lambayeque en coordinación con los responsables de la seguridad de la información del establecimiento, den inicio al proceso de implementación de un sistema de gestión de la seguridad de la información por medio de un modelo para la gestión de riesgos

- Se recomienda que los responsables de la seguridad de la información del Hospital Regional de Lambayeque, aplique el modelo de gestión de riesgos basado en las normas ISO/IEC 27005 y la metodología MAGERIT propuesto, en los diferentes

servicios y procesos del hospital, con el fin de identificar y analizar amenazas latentes y vulnerabilidades, evaluar riesgos y proponer mecanismos de protección que puedan mitigarlos.

CAPITULO VII. REFERENCIA DE LAS FUENTES DE CONSULTA

Al-Safwani, N., Hassan y S., Katuk, N. (2014). A Multiple Attribute Decision Making for Improving Information Security Control Assessment. International Journal of Computer Applications. Volume 89 – No.3.

Alcántara, J. (2015). Guía de Implementación de la Seguridad basado en la Norma ISO/IEC 27001, para apoyar la Seguridad en los Sistemas Informáticos de la Comisaria del Norte P.N.P en la ciudad de Chiclayo. Universidad Católica Santo Toribio de Mogrovejo, Chiclayo

Ambrosone, M. (2007). La administración del riesgo empresarial: Una responsabilidad d todos – El enfoque COSO.

Amutio, M & Candau, J & Mañas, J (2012).Madrid. MAGERIT- versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Baca, V. (2016). Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local – Chiclayo. UGEL. Chiclayo

Barrantes, C. & Hugo, J. (2012) Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos. Universidad San Martin de Porras, Lima

Bueno, Correa & Echeverry, 2010. Administración de riesgos- una visión global y moderna.

Cañas, Luis (2009). Gestión de riesgos de negocio. Desarrollo e implementación de Sistemas de Gestión de Riesgos

Cárdenas, L., Martínez, H. y Becerra, L. (2016). Gestión de Seguridad de la Información: Revisión Bibliográfica. El profesional de la información, Vol. 25, n. 6

Duménigo, C., Vilaragut, J., Morales, J., Perez, A., Guerrero, M., McFarlane, T., Soler, K., Cruz, Y. y Batista, F.(2010).Estudios de casos con la utilización del enfoque de "matriz de riesgos" para prevenir accidentes en tratamientos de radioterapia.Núcleus. Vol. 48

Dussan, Ciro (2006).Políticas de Seguridad de Información

Fábrica del Pensamiento. (2013). Buenas Prácticas en Gestión de Riesgos. Instituto de Auditores Internos de España

Gaona, K. (2013). Aplicación de la metodología MAGERIT para el Análisis y Gestión de Riesgos de la Seguridad de la Información aplicado a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala, Cuenca

Gasca, G., Echeverri, J., Vega, V. y San Feliu, T.(2012).Similitud de Estándares y Modelos Según el Proceso de Gestión de Riesgos en el Desarrollo de Software.CISTI.646-650.

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

Haddad, H. y Romero B. (2009). Asset Identification for Security Risk Assessment in Web Applications. Int.J. of Software Engineering, IJSE. Vol.2 No.3.

Lalanne, V., Munier, M. y Gabillon, A. (2013). Information Security Risk Management in a World of Services. ASE/IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT 2013). 586-593.

Lemus, M., Pino, F. y Piattini, M.(2010).Hacia un Marco para el Gobierno de las Tecnologías y Sistemas de Información aplicable al Sector Bancario.CISTI.35-42.

Linares, V. (2014). Plan Estratégico Institucional del Hospital Regional De Lambayeque 2014-2018. Hospital Regional de Lambayeque

Miranda, K. (2013). Guía Metodológica para implementar un Sistema de Gestión de Seguridad en Instituciones. Universidad de Piura. Piura

Ministerio de Haciendas y Administraciones Públicas. (2012) MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I - Método. Madrid

Ministerio de Haciendas y Administraciones Públicas. (2012) MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos. Madrid

Ministerio de Haciendas y Administraciones Públicas. (2012) MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. Madrid

Ovies-Bernal DP, Agudelo-Londoño SM. Lecciones aprendidas en la implementación de sistemas nacionales de información de salud interoperables: una revisión sistemática. Rev Panam Salud Pública. 2014;35(5/6):415–23

Prioste, C. (2016). Tecnología, educación e innovación: riesgos y oportunidades. J. Eng. Technol. Vol.5, N°2, 72.-81

Ramirez, A. & Ortiz, Z (2011). Gestión de Riesgos Tecnológicos basados en la ISO 31000 e ISO 27005.Colombia

Resolución Ministerial 520-2016. Lineamientos Políticas de Seguridad de la Información MINSA

Sotelo, M. & Torres, J. & Rivera, J. (2012). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. Ugaz Burga (Organizador). IV Congreso Internacional de Computación y Telecomunicaciones, Lima – Perú

Salazar, Cortez & Mariscal, 2002. Gestión Comunitaria de riesgos.

Soldano, A. (2009). Conceptos sobre Riesgo

Tam, F.(2009). Lima. Circular SBS N° 140-2009.Gestión de la Seguridad de la Información

Tam, F.(2009). Lima, Resolución S.B.S N° 2116-2009.Reglamento para la gestión del Riesgo Operacional

Tam, F.(2009). Lima, en la Resolución S.B.S N° 37-2008.Reglamento de la Gestión Integral de Riesgos

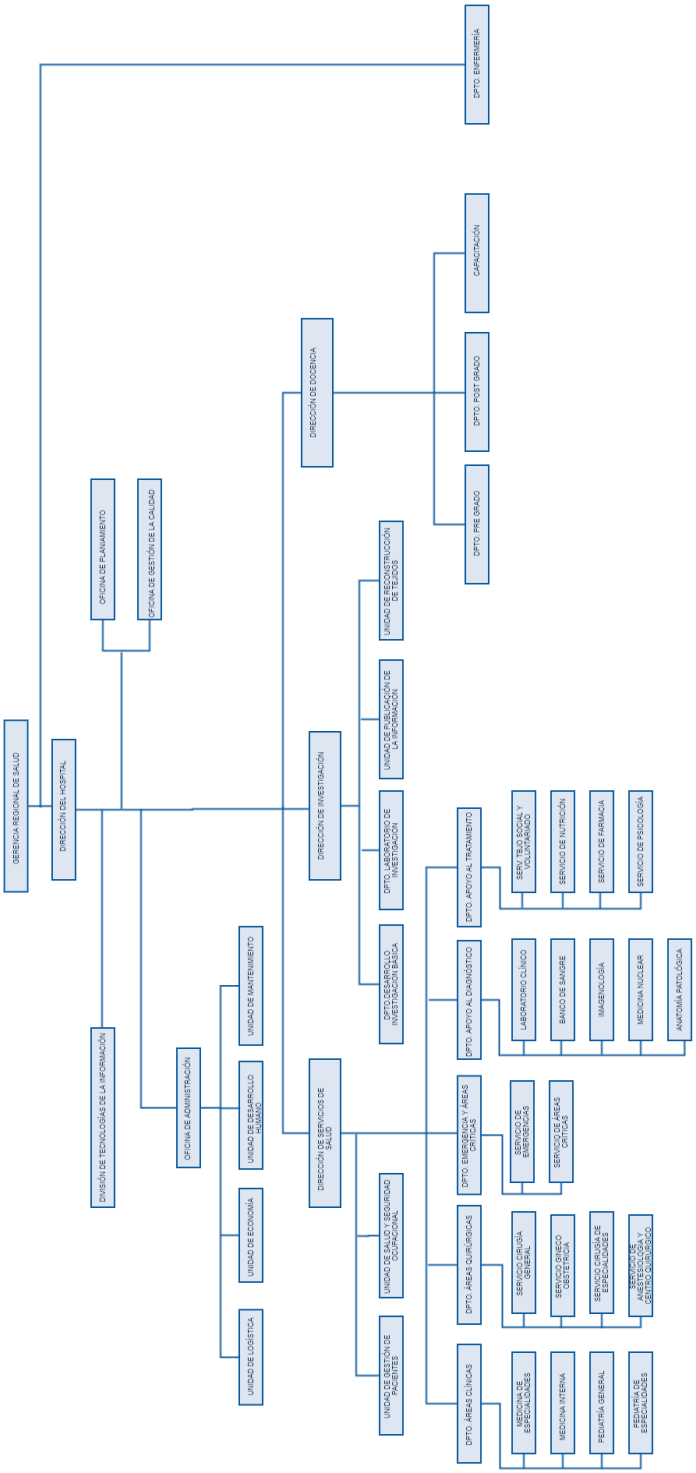
] Villena, M (2006). Sistema de Gestión de Información para una institución financiera. Tesis para optar el título de ingeniero informático.

Zavaleta, D. (2016). Implementación De Un Sistema De Gestión De Seguridad De La Información Aplicando NTP ISO/IEC 27001:2014 En El Sector Hospitalario. Universidad Privada Norbert Wiener. Lima

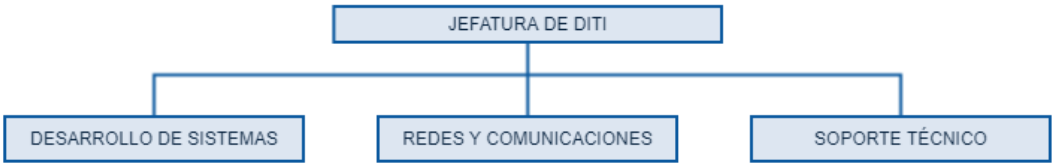
Zne-Jung L. y Li-Yun C.(2014). Apply Fuzzy Decision Tree to Information Security Risk Assessment. International Journal of Fuzzy Systems, Vol. 16, No. 2

CAPITULO VIII. ANEXOS

Anexo N° 01: Organigrama Hospital Regional de Lambayeque



Anexo N° 02: Organigrama de la División de tecnologías de la información del Hospital Regional de Lambayeque



Anexo N° 03: Formatos de encuesta personal Hospital Regional de Lambayeque

Formato N° 001: Encuesta dirigida a los usuarios de los sistemas de gestión hospitalaria

Modelo de Gestión de riesgos basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la Gestión de seguridad de la información en el Hospital Regional de Lambayeque.

FORMATO N°001
ENTREVISTA A USUARIOS:
FECHA:
AREA:

N°	CUESTIONARIO	SI	NO	N/A	OBSERVACIONES
1	Cuenta con accesos propios para ingresar a los equipos informáticos (pc/laptos)				
2	Cambia las contraseñas en los equipos asignados				
	¿Cada cuánto tiempo?				
3	Cuenta con carpetas u unidades compartidas, en la intranet.				
4	Cuenta con permisos para guardar información en dispositivos eternos (memorias usb, cd,s)				
5	Cuenta con permisos para acceder de forma remota a sus equipos informáticos				
6	Cuenta con información institucional compartida en unidades virtuales (Drive, Dropbox, etc)				
7	Cuenta con cuenta de correo propio de la institución				
8	Cuenta con un límite máximo para el tamaño de archivos enviados vía email				
9	Puede conectarse a alguna señal Wifi libre dentro de la institución				
10	Existe alguna restricción de acceso a los ambientes en el que guardan sus archivos físicos				
11	Existe alguna restricción de acceso a los ambientes en el que se encuentra su equipo informático				
12	Tiene acceso a dispositivos de impresión				
13	Tiene acceso a dispositivos de impresión de otras áreas.				
14	Sigue las políticas de creación de contraseñas de la institución				
15	Presenta problemas usuales para ingresar a sus conexiones de internet				
16	Presenta problemas usuales para ingresar a sus equipos informáticos				
17	Comparte usuarios en el acceso de los sistemas información				
18	Presenta problemas usuales para ingresar a sus sistemas de información				
19	Presenta problemas para compartir o enviar información				
20	Recibe orientación o charlas eventuales para seguir normas de seguridad de la información				

Formato N° 00: Encuesta dirigida a los administradores de los sistemas de gestión hospitalaria

FORMATO N°002
ENTREVISTA A ENCARGADO DE GESTION DE RIESGOS:
FECHA:
AREA:

N°	CUESTIONARIO	SI	NO	N/A	OBSERVACIONES
1	Existen políticas de seguridad de la información documentadas para el HRL				
2	Se valida el cumplimiento de las políticas de seguridad de la información por parte de los responsables y usuarios				
3	Cada cuanto tiempo se realizan charlas preventivas para el manejo de la seguridad de la información en los usuarios.				
	Cada 2 o 3 meses				
	Cada 4 o 6 meses				
	Anualmente				
	Otro				
4	Realizan supervisiones del control de las políticas de seguridad de la información del HRL				
5	Cuentan con un inventario actualizado de los activos de la información del HRL				
6	La asignación de los perfiles de accesos se realiza mediante un procedimiento establecido.				
7	La restricción de los perfiles de acceso de los exempleados se realiza :				
	El mismo día en que se retira de la institución				
	Entre 1 a 3 días luego que se retira de la institución				
	Hasta una semana después de retirarse de la institución				
	Otros				
8	Cuenta con políticas para la creación de contraseñas de los usuarios				
9	Cuenta con políticas para la actualización de contraseñas de los usuarios				
10	Cuenta con restricciones de acceso para el ingreso en ambientes con equipos informáticos				

11	Todos los usuarios cuentan con permisos de acceso remoto a sus equipos informáticos				
12	Los usuarios tienen permisos de uso de medios eternos				
13	Los usuarios cuentan con unidades virtuales para compartir información				
14	Existen tipos de accesos para la administración usuarios en el uso de carpetas virtuales				
15	Existen restricciones para el acceso de redes inalámbricas				
16	Existen perfiles de acceso para el uso de sistemas informáticos.				
17	Se realiza el control de accesos y tráfico de los usuarios de los sistemas informáticos.				
18	Realizan mantenimientos preventivos de equipos informáticos				
19	Realizan supervisión de equipos de redes				
20	Realizan backups de correos electrónicos eventualmente				
21	Realizan backups de la información equipos informáticos eventualmente				
22	Se realizan backups completos de las bases de datos				
23	Se realizan backups incrementales de las bases de datos				
24	Realizan backups de los sistemas informáticos				
25	Cuentan con un ambiente de desarrollo de los sistemas informáticos				
26	Cuentan con un ambiente de pruebas de los sistemas informáticos				
27	Los sistemas de la información eventualmente pierden conexión				
28	Eventualmente se presentan cambios no autorizados en los sistemas informáticos				
29	Se mantiene un control de los accesos remotos en los sistemas de la información				
30	Se realizan , pruebas/ simulaciones de los principales incidentes que pudieran afectar la seguridad de la información				

Formato N° 00: Encuesta dirigida a los jefatura de la división de tecnologías de la información del Hospital Regional de Lambayeque

Modelo de Gestión de riesgos basados en la norma ISO/IEC 27005 y metodología Magerit para mejorar la Gestión de seguridad de la información en el Hospital Regional de Lambayeque.

FORMATO N° 003
ENTREVISTA A GERENCIA:
FECHA:
AREA:

N°	CUESTIONARIO	SI	NO	N/A	OBSERVACIONES
1	¿El responsable del área de TI es el encargado de hacer el inventario de los activos de la información de todo el HRL?				
2	Cada cuanto tiempo realizan el inventario de activos de la información				
3	Quien registra el inventario también se encarga de registra los cambios y/o actualización del inventario				
4	El responsable de TI, se encarga de brindar y restringir accesos a los usuarios				
5	El responsable de TI, se encarga de administrar los accesos a los usuarios				
6	Existen políticas para mantener el control y seguridad de los activos de la información documentadas				
7	Cada cuanto tiempo se realizan capacitaciones a los usuarios, para reforzar medidas de seguridad				
8	Cada cuanto tiempo se realizan observaciones del cumplimiento de las medidas de seguridad establecidas.				
9	Existen procedimientos a seguir en caso se detecten problemas en la seguridad de la información				
10	Se han detectado las problemas con la seguridad de la información del HRL				
11	Se han determinado las principales causas de los problemas de seguridad de la información en el HRL				
12	Cuentan con presupuesto asignado para implementar políticas de Gestión de Seguridad de la información				

Anexo N° 04: Formato inventario de activos de la información

DATOS GENERALES												DETALLE DEL ACTIVO			SISTEMA OPERATIVO		BASE DE DATOS	DESARROLLO SW						PROGRAMAS OFFICE						NAVEGADOR			SW INSTITUCIONAL				REDES
TIPO DE ACTIVOS	ID CLASIFICACION	NOMBRE DEL ACTIVO	AREA	CODIGO DE ACTIVO	CANTIDAD	ESTADO DE OP	ID USUARIO RESPONSABLE	USUARIO RESPONSABLE	PUESTO DE TRABAJO	UBICACIÓN	DETALLE UBICACIÓN	MODELO	MARCA	SERIAL	SO	Código Licencia SO	BD	JDK	Cod Licencia	APACHE	Cod Licencia	JAVA	Cod Licencia	WOffice	Cod. Licencia	OpenOffice	Skype	PDF	Compresor	Chrome	Explorer	Mozilla	sistema Asignación Camas	SIGHOR	GALENUS	SIGBIO	Conexión Internet

Anexo N° 05: Formato matriz de riesgos

FASE IDENTIFICACIÓN															FASE ANÁLISIS Y EVALUACIÓN		
DATOS GENERALES			DIMENSIONES DE SEGURIDAD DE LA INFORMACION					VALORACION DEL ACTIVO	ACTIVO PRIORIZADO		VULNERABILIDADES			AMENAZAS			ANÁLISIS RIESGO INHERENTE		
ID ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD	´(PROM EDIO DE DIMENSIONES)	*INDICADOR DEL NIVEL DE VALORACION*	INDICADOR	V1	V2	... Vn	A1	A2	... An	PROBABILIDAD DE MATERIALIZACION	IMPACTO DE MATERIALIZACION	NIVEL DE RIESGO INHERENTE

FASE SEGUIMIENTO	ANALISIS DE LA EFICIENCIA Y EL RIESGO RESIDUAL EN SEGUIMIENTO	NIVEL DE RIESGO RESIDUAL
		IMPACTO RESIDUAL
		PROBABILIDAD RESIDUAL
		NIVEL DE EFECTIVIDAD
		GRADO
		OPORTUNIDAD DE CONTROL
		ESTADO DE CONTROL
FASE TRATAMIENTO	ANALISIS DE RIESGO RESIDUAL	**NIVEL DE RIESGO RESIDUAL**
		IMPACTO
		PROBABILIDAD
	ANÁLISIS NIVEL DE EFECTIVIDAD	**NIVEL DE EFECTIVIDAD**
		GRADO DE IMPLEMENTACIÓN
		OPORTUNIDAD DE MECANISMO DE PROTECCIÓN
		ESTADO DE MECANISMO DE PROTECCIÓN
	MECANISMOS DE PROTECCIÓN	**Descripción del mecanismo de protección aplicado**
		... Sn
		S3
		S2
		S1

Anexo N° 06: Catálogo de vulnerabilidades

CATALOGO VULNERABILIDADES			
5	**POLITICAS DE SEGURIDAD**		
	5.1	Directrices de la Dirección en seguridad de la información	
		5.1.1	Falta de políticas para la seguridad de la información
		5.1.2	No realizan la revisión de las políticas para la seguridad de la información
6	**ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACION**		
	6.1	Organización Interna	
		6.1.1	No cuentan con responsables asignados para la seguridad de la información
		6.1.2	No realizan la segregación de tareas
		6.1.3	No se tiene contacto con las autoridades
		6.1.4	No existe contacto con grupo de interés especial
		6.1.5	La Gestión de proyectos se realiza omitiendo la planificación de la seguridad de la información
	6.2	Dispositivos para movilidad y Teletrabajo	
		6.2.1	No cuentan con políticas para el uso de dispositivos móviles
		6.2.2	No existe controles para teletrabajo
7	**SEGURIDAD LIGADA A LOS RECURSOS HUMANOS**		
	7.1	Antes de la contratación	
		7.1.1	Falta de investigación sobre los antecedentes
		7.1.2	No especifican los términos y condiciones de trabajo
	7.2	Durante la contratación	
		7.2.1	No se especifican las responsabilidades de gestión
		7.2.2	Escasa concienciación, educación y capacitación en Seg. Información
		7.2.3	No cuentan con medidas de carácter disciplinario
	7.3	Cese o cambio de puesto de trabajo	
		7.3.1	No existe comunicación inmediata sobre los ceses, rotaciones o cambios de puesto de trabajo del personal
		7.3.2	
8	**GESTION DE ACTIVOS**		
	8.1	Responsabilidad sobre los Activos	
		8.1.1	No cuentan con un inventario de activos actualizado
		8.1.2	No cuentan con un inventario sobre los propietarios de los activos asignados
		8.1.3	No utilizan adecuadamente los activos de la información
		8.1.4	Deficiente o escaso control en el proceso de devolución de activos
	8.2	Clasificación de la información	
		8.2.1	No existe Directrices para una buena clasificación de activos de información
		8.2.2	No se etiqueta adecuadamente la información
		8.2.3	Realizan manipulaciones sobre los activos de la información, sin respetar el esquema de clasificación de la información adoptado por el HRL
	8.3	**Manejo de los soportes de almacenamiento**	
		8.3.1	No cuentan con procedimientos de Gestión para soportes extraíbles
		8.3.2	No cuentan con procedimientos para la eliminación de soportes extraíbles

		8.3.3	No cuentan con procedimientos para los soportes físicos en tránsito
9	**CONTROL DE ACCESOS**		
	9.1	Requisitos del negocio para el control de acceso	
		9.1.1	No cuentas con política para el control de accesos
		9.1.2	Existe un débil control para el acceso redes y servicios asociados
	9.2	Gestión de Accesos de Usuario	
		9.2.1	No realizan procedimientos de Gestión para las altas/ bajas del registro de usuarios
		9.2.2	Carente control de acceso a las redes y servicios asociados
		9.2.3	No realizan la gestión de los roles de los usuarios con privilegios especiales
		9.2.4	No existe controles para gestionar la asignación de información confidencial para la autenticación (Por ejemplo: aplica para autenticación multifactor, podría ser utilizando Token)
		9.2.5	No realizan la validación y seguimiento sobre los privilegios de los usuarios en los roles asignados
		9.2.6	Escaso control para retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio
	9.3	Responsabilidades de Usuario	
		9.3.1	No existe concientización del usuario para mantener la confidencialidad de sus contraseñas
	9.4	Control de acceso a sistemas y aplicaciones	
		9.4.1	No existe controles para restringir el acceso de los usuarios y el personal de mantenimiento de los sistemas, a la información y funciones de los sistemas de aplicaciones
		9.4.2	Falta de control de acceso a los sistemas y aplicaciones mediante un procedimiento seguro de logeo
		9.4.3	No realizan la gestión de contraseñas seguras de usuarios
		9.4.4	No se restringe el uso de software utilitario que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas
		9.4.5	No se restringe el acceso a código fuente de las aplicaciones de software
10	**CIFRADO**		
	10.1	**Controles criptográficos**	
		10.1.1	No cuentan con políticas que regule el uso de controles criptográficos para la protección de la información
		10.1.2	No se cuenta con políticas sobre el uso, protección y el ciclo de vida de las claves criptográficas a través de todo su ciclo de vida.
11	**SEGURIDAD FISICA Y AMBIENTAL**		
	11.1	Áreas seguras	
		11.1.1	No se ha definido y utiliza perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica
		11.1.2	No han establecido controles ingreso en áreas restringidas
		11.1.3	No mantienen la seguridad en oficinas, despachos y recursos
		11.1.4	No han establecido procedimientos para la protección de los activos de amenazas externas y/o ambientales
		11.1.5	No cuentan con ambientes seguros para realizar las funciones asignadas

		11.1.6	No se tiene un control para restringir el ingreso de personas no autorizadas a las instalaciones de procesamiento de información.
	11.2	Seguridad de los equipos	
		11.2.1	No cuentan con un inventario de equipos que muestre la ubicación real de los equipos
		11.2.2	Los equipos no se encuentran protegidos contra cortes de luz y otras interrupciones provocada por fallas en los suministros básicos de apoyo
		11.2.3	No cumplen las normas de cableado
		11.2.4	No realizan la programación del mantenimiento de equipos
		11.2.5	No cuentan con procedimientos de seguridad para la salida de equipos de la institución
		11.2.6	No cuentan con lineamientos establecidos para la protección de los activos fuera de las instalaciones de la institución
		11.2.7	No cuentan con procedimientos para reutilizar y/o desechar dispositivos de almacenamiento de información.
		11.2.8	Falta de seguimiento a las incidencias de los equipos reportadas por los usuarios, hasta su cierre.
		11.2.9	No se cuenta con políticas de puesto de trabajo despejado y bloqueo de pantallas de usuario
12	**SEGURIDAD EN LA OPERATIVA**		
	12.1	Responsabilidades y procedimientos de operación	
		12.1.1	No se tiene documentado los procesos operativos y servicios que soportan a los sistemas de información
		12.1.2	No se controlan los cambios que afectan a la seguridad de la información en la organización y procesos de negocio, las instalaciones y sistemas de procesamiento de información.
		12.1.3	No se monitorea las capacidades de procesamiento y almacenamiento en los equipos para garantizar el rendimiento adecuado de los sistemas
		12.1.4	No existe una diferenciación entre los ambientes asignados para el área de desarrollo, pruebas y producción.
	12.2	PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	
		12.2.1	No existe control para la detección, prevención y recuperación ante afectaciones de malware
	12.3	COPIAS DE SEGURIDAD	
		12.3.1	No cuentan con un lugar seguro e independiente para reguardar las copias de seguridad.
	12.4	REGISTRO DE ACTIVIDAD Y SUPERVISIÓN	
		12.4.1	No cuentan con una bitácora de eventos de actividades
		12.4.2	No cuentan con lineamientos para la protección del registro de la información
		12.4.3	No se registrar las actividades del administrador y del operador del sistema, así mismo, los registros asociados no se protegen y revisan de manera regular.
		12.4.4	No se sincronizan los relojes de todos los sistemas de procesamiento de información en relación a una fuente de sincronización única de referencia
	12.5	CONTROL DE SOFTWARE EN EXPLOTACIÓN	
		12.5.1	Inadecuada instalación de software de sistemas en usuarios de producción
	12.6	GESTIÓN DE LA VULNERABILIDAD TÉCNICA	

		12.6.1	No se tiene identificadas las vulnerabilidades técnicas de los sistemas de información, para evaluar de manera oportuna el grado de exposición de la organización
		12.6.2	No se restringe la instalación de software a los usuarios, sobre los equipos
	12.7	CONSIDERACIONES DE LAS AUDITORIAS DE LOS SISTEMAS DE LA INFORMACIÓN	
		12.7.1	No se realiza la planificación de controles de auditoria en sus sistemas de información, con el fin de mantener la continuidad del negocio
13	**SEGURIDAD EN LAS TELECOMUNICACIONES**		
	13.1	GESTIÓN DE LA SEGURIDAD EN LAS REDES	
		13.1.1	No cuentan con suficientes controles de red
		13.1.2	No cuentan con mecanismos establecidos para mantener la seguridad de los servicios en las redes
		13.1.3	Deficiente segregación de redes
	13.2	INTERCAMBIO DE INFORMACIÓN CON PARTES EXTERNAS	
		13.2.1	No existen políticas ni procedimientos para realizar intercambios de información.
		13.2.2	No se tienen acuerdos para la transferencia segura de información entre la organización y las partes externa
		13.2.3	No se cuentan con lineamientos para remitir información por mensajería electrónica, con la adecuada aprobación de los responsables de la información
		13.2.4	No se cuenta con acuerdos de confidencialidad y no divulgación de la información
14	**ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE LA INFORMACION**		
	14.1	REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE LA INFORMACIÓN	
		14.1.1	No realizan el análisis ni especificación de los requerisitos de seguridad suficientes en el desarrollo de sistemas de información
		14.1.2	No se tiene mecanismos de control para proteger la información los servicios de aplicaciones accesibles por redes públicas
		14.1.3	Deficiente protección de transacciones realizadas por medio de redes telemáticas
	14.2	SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE	
		14.2.1	No existen políticas para realizar desarrollos de forma ordenada y segura.
		14.2.2	No existen procedimientos para mantener un registro sobre el control de cambios realizados en los sistemas
		14.2.3	No existe un equipo que se encargue de realizar las validaciones técnicas sobre los desarrollos de sistemas realizados
		14.2.4	No existe control de cambio de modificaciones en los paquetes de software suministrados por terceros
		14.2.5	No se cuenta con una metodología de Desarrollo Seguro, en el que se tengan presentes los controles que garanticen la seguridad de la información en cada etapa de desarrollo del software, de manera que se pueda solucionar las vulnerabilidades o fallas identificadas.
		14.2.6	No se establece controles de acceso no autorizado a los entornos de labores de desarrollo e integración
		14.2.7	No cuentan con lineamientos para la gestión de los entregables (entrega de documentación técnica y funcional, evidencias de calidad de pruebas, fuentes de la aplicación de sw, control de cambios, etc) de los requerimientos tercerizados.

		14.2.8	No se realizan suficientes pruebas funcionales , que incluyan el pruebas integrales del flujo de información, durante el desarrollo de los sistemas
		14.2.9	No se realizan pruebas de aceptación, por parte del usuario, tras la puesta en producción del sistema de información.
	14.3	DATOS DE PRUEBA	
		14.3.1	No existe la seguridad de contar con datos consistentes para realizar casos de prueba en el ambiente de pruebas
15	**RELACIONES CON SUMINISTRADORES**		
	15.1	SEGURIDAD DE LA INFORMACIÓN EN LAS RELACIONES CON SUMINISTRADORES	
		15.1.1	No se tiene definido adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización al cual tendrían acceso y uso los proveedores y terceras personas
		15.1.2	No se tiene definida a las alternativas de solución para mitigar los riesgos asociados al acceso y uso de activos de información por parte de proveedores y terceras personas
		15.1.3	No se cuenta con una cadena de comunicación con los proveedores, que les permita seguir un flujo de comunicación con los vistos buenos de las jefaturas respectivas de la organización, a fin de garantizar la efectiva solicitud y entrega de activos de la información.
	15.2	GESTIÓN DE LA PRESTACIÓN DEL SERVICIO POR SUMINISTRADORES	
		15.2.1	No cuentan con un control de supervisión y validación de los servicios brindados por proveedores en las diferentes etapas de los entregables
		15.2.2	No realiza la Gestión para el control de cambios realizados por los proveedores de servicios tercerizados, manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos.
16	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN**		
	16.1	**GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN Y MEJORAS**	
		16.1.1	No se tiene definidas las responsabilidades ni procedimientos para la seguridad de la información dentro de las funciones del personal.
		16.1.2	No se informa oportunamente sobre el despliegue de un evento que afecta la seguridad de la información.
		16.1.3	No se informa las debilidades sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a proveedores que utilizan los sistemas y servicios de información de la organización
		16.1.4	No se realiza la evaluación de los eventos de seguridad de la información.
		16.1.5	No se tienen procedimientos documentados para dar respuestas a los incidentes de seguridad de la información reportados.
		16.1.6	No se utiliza el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
		16.1.7	No cuenta con el procedimiento para reunir las evidencias relevantes ante un evento no deseado en contra de la seguridad de la información
17	**ASPECTOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**		
	17.1	CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN	
		17.1.1	No cuenta con un programa de contingencia planificado para asegurar la continuidad de las funciones de los sistemas de información afectados ante un evento no deseado en contra la seguridad de la información.

		17.1.2	No se establece, documenta, implementa y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas
		17.1.3	No se verifica/revisa regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
	17.2	REDUNDANCIAS	
		17.2.1	No se tiene implementada la suficiente redundancia en las instalaciones de procesamiento de la información.
18	**CUMPLIMIENTO**		
	18.1	CUMPLIMIENTO DE LOS REQUISITOS LEGALES Y CONTRACTUALES	
		18.1.1	No tienen identificados las normas, decretos, leyes que garanticen el cumplimiento de las cláusulas de seguridad de la información descritas dentro de un acuerdo.
		18.1.2	No se tienen procedimientos para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilización de productos de software originales.
		18.1.3	Los registros de la organización no se protegen contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
		18.1.4	No existen controles que garantice la privacidad y la protección de la información personal , según lo requiere la legislación y las normativas pertinentes aplicables que correspondan
		18.1.5	No se utilizan controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
	18.2	REVISIONES DE LA SEGURIDAD DE LA INFORMACIÓN	
		18.2.1	No se realizan Auditorías internas y externas para supervisar y revisar las políticas de la seguridad de la información establecidas
		18.2.2	No se cumplen las normas ni políticas de seguridad de la información establecidas.
		18.2.3	No se acopia evidencias suficientes para la comprobación del cumplimiento de políticas de Seguridad de la Información

Anexo N° 07: Catálogo de amenazas

CATÁLOGO DE AMENAZAS		
A	**DE ORIGEN NATURAL**	
	A.1	Fuego
	A.2	Daños por agua
	A.3	Desastres Naturales
B	**DE ORIGEN INDUSTRIAL**	
	B.1	Fuego
	B.2	Daños por agua
	B.3	Contaminación mecánica
	B.4	Avería de origen físico o lógico
	B.5	Corte del suministro eléctrico
	B.6	Condiciones inadecuadas de temperatura o humedad
	B.7	Fallo de servicios de comunicaciones
	B.8	Degradación de los soportes de almacenamiento de la información
C	**ERRORES Y FALLOS NO INTENCIONALES**	
	C.1	Errores en los usuarios
	C.2	Errores del administrador
	C.3	Errores de monitorización (log)
	C.4	Errores de configuración
	C.5	Deficiencias en la organización
	C.6	Difusión de software dañino
	C.7	Errores de re encaminamiento
	C.8	Errores de secuencia
	C.9	Escapes de Información
	C.10	Alteración accidental de información
	C.11	Destrucción de la información
	C.12	Fugas de información
	C.13	Vulnerabilidad d los programas
	C.14	Errores de mantenimiento / actualización de programas
	C.15	Caídas del sistema por agotamiento de recursos
	C.16	Pérdida de equipos
	C.17	Indisponibilidad del personal
D	**ATAQUES INTENCIONADOS**	
	D.1	Manipulación de registros de Monitorización (log)
	D.2	Manipulación de la configuración
	D.3	Suplantación de identidad del usuario
	D.4	Abuso de privilegios de acceso

	D.5	Uso no previsto
	D.6	Difusión de software dañino
	D.7	Re encaminamiento de mensajes
	D.8	Alteración de secuencias
	D.9	Acceso no autorizado
	D.10	Análisis de tráfico
	D.11	Repudio
	D.12	Interceptación de información
	D.13	Modificación deliberada de información
	D.14	Destrucción de información
	D.15	Divulgación de información
	D.16	Manipulación de programas
	D.17	Manipulación de equipos
	D.18	Denegación de servicio
	D.19	Robo
	D.20	Ataque destructivo
	D.21	Ocupación enemiga
	D.22	Indisponibilidad del personal
	D.23	Bloqueo de ordenador bajo petición de rescate
	D.24	Bloqueo de Base de Datos bajo petición de rescate
	D.25	Bloqueo de Servidores bajo petición de rescate
	D.26	Ataques Web (enlaces maliciosos)
	D.27	Ataque Telefónico (Persuasión)
	D.28	Ataque Email (suscripciones/cupones descuento)
	D.29	Estafa cibernética
	D.30	Keylogers
	D.31	Software para re direccionar el nombre de dominio

PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS	
5- MA: Prácticamente seguro	**5- MA: Prácticamente seguro**
4- A: Probable	**4- A: Probable**
3- M: Posible	**3- M: Posible**
2- B: Poco probable	**2- B: Poco probable**
1- MB: Muy raro	**1- MB: Muy raro**

Anexo N° 08: Catálogo de mecanismos de protección

CATALOGO MECANISMOS DE PROTECCIÓN			
GH	**protecciones generales y horizontales**		
		GH01	Identificación y autenticación
		GH02	Control de acceso lógico
		GH03	Segregación de tareas
		GH04	Gestión de incidencias
		GH05	Herramientas de seguridad
		GH06	Herramienta contra código dañino
		GH07	IDS/IPS: Herramienta de detección / prevención de intrusión
		GH08	Herramienta de chequeo de configuración
		GH09	Herramienta de análisis de vulnerabilidades
		GH10	Herramienta de monitorización de tráfico
		GH11	DLP: Herramienta de monitorización de contenidos
		GH12	Herramienta para análisis de logs
		GH13	Honey net / honey pot
		GH14	Verificación de las funciones de seguridad
		GH15	Gestión de vulnerabilidades
		GH16	Registro y auditoría
DI	**protección de datos / información**		
		DI01	Clasificación de la Información
		DI02	Copias de seguridad de los datos (backup)
		DI03	Aseguramiento de la integridad
		DI04	Cifrado de la información
		DI05	Uso de firmas electrónicas
		DI06	Uso de servicios de fechado electrónico (time stamping)
CC	**protección de las claves criptográficas**		
		CC01	Gestión de claves criptográficas
		CC02	Gestión de las claves de cifra de información
		CC03	Gestión de las firmas de información
		CC04	Gestión de laves para contenedores criptográficos
		CC05	Gestión de claves de comunicaciones
		CC06	Gestión de certificados
SS	**protección de los servicios**		
		SS01	Protección de los servicios
		SS02	Aseguramiento de la disponibilidad
		SS03	Aceptación y puesta en operación
		SS04	Se aplican perfiles de seguridad

		SS05	Explotación
		SS06	Gestión de cambios (mejoras y sustituciones)
		SS07	Terminación
		SS08	Protección de servicios y aplicaciones web
		SS09	Protección del correo electrónico
		SS10	Protección del directorio
		SS11	Protección del servidor de nombres de dominio DNS
		SS12	Teletrabajo
		SS13	Voz sobre IP
AP	**protección de las aplicaciones (Sw)**		
		AP01	Protección de las aplicaciones informáticas
		AP02	Copias de seguridad (backup)
		AP03	Puesta en producción
		AP04	Se aplican perfiles de seguridad
		AP05	Explotación/Producción
		AP06	Cambios (actualizaciones y mantenimientos)
		AP07	Terminación
EQ	**protección de los equipos (Hw)**		
		EQ01	Protección de los equipos informáticos
		EQ02	Puesta en producción
		EQ03	Se aplican perfiles de seguridad
		EQ04	Aseguramiento de la disponibilidad
		EQ05	Operación
		EQ06	Cambios (actualizaciones y mantenimientos)
		EQ07	Terminación
		EQ08	Informática móvil
		EQ09	Reproducción de documentos
		EQ10	Protección de la centralita telefónica
CO	**protección de las comunicaciones**		
		CO01	Protección de las comunicaciones
		CO02	Entrada en servicio
		CO03	Se aplican perfiles de seguridad
		CO04	Aseguramiento de la disponibilidad
		CO05	Autenticación del canal
		CO06	Protección de la integridad de los datos intercambiados
		CO07	Protección criptográfica de la confidencialidad de los datos intercambiados
		CO08	Operación
		CO09	Cambios (actualizaciones y mantenimientos)
		CO10	Terminación
		CO11	Internet
		CO12	Seguridad Wireless
		CO13	Telefonía móvil
		CO14	Segregación de las redes de dominio

PI	**protección de los puntos de interconexión con otros sistemas**		
		PI01	Puntos de interconexión: conexiones entre zonas de confianza
		PI02	Sistema de protección perimetral
		PI03	Protección de los equipos de frontera
SI	**protección de los soportes de información**		
		SI01	protección de los soportes de información
		SI02	Aseguramiento de la disponibilidad
		SI03	Protección criptográfica del contenido
		SI04	Limpieza de contenidos
		SI05	Destrucción de soportes
EA	**protección de los elementos auxiliares**		
		EA01	Elementos auxiliares
		EA02	Aseguramiento de la disponibilidad
		EA03	Instalación
		EA04	Suministro eléctrico
		EA05	Climatización
		EA06	Protección de cableado
FF	**protección física (Instalaciones)**		
		FF01	Protección de las instalaciones
		FF02	Diseño de las instalaciones
		FF03	Defensa en profundidad
		FF04	Control de los accesos físicos
		FF05	Aseguramiento de la disponibilidad
		FF06	Terminación
PP	**Salvaguardas relativos al personal**		
		PP01	Gestión del personal
		PP02	Formación y concienciación
		PP03	Aseguramiento de la disponibilidad
OR	**Salvaguardas de tipo organizativo**		
		OR01	Organización
		OR02	Gestión de Riesgos
		OR03	Planificación de la seguridad
		OR04	Inspecciones de la seguridad
OP	**Continuidad de Operaciones**		
		OP01	Continuidad del negocio
		OP02	Análisis del impacto
		OP03	Plan de Recuperación de desastres
EX	**Externalización**		
		EX01	Relaciones Externas
		EX02	Acuerdos para el intercambio de información y software
		EX03	Acceso externo
		EX04	Servicios proporcionados por otras organizaciones
		EX05	Personal subcontratado
AD	**Adquisición y desarrollo**		

		AD01	Adquisición y desarrollo
		AD02	Servicios: Adquisición y desarrollo
		AD03	Aplicaciones: Adquisición y desarrollo
		AD04	Equipos: Adquisición y desarrollo
		AD05	Comunicaciones: Adquisición y desarrollo
		AD06	Soportes de información: Adquisición
		AD07	Productos certificados o acreditados

ESTADO DE CONTROL	
1	Implementado
0	No implementado

OPORTUNIDAD DE PROPUESTA DE CONTROL	
1	Preventivo
2	Detectivo
3	Correctivo

GRADO DE IMPLEMENTACION DE CONTROLES	
1	Manual
2	Semiautomatizado
3	Automatizado

Anexo N° 09: Manual de usuario para el uso del inventario de activos

MANUAL DE USUARIO PARA IDENTIFICACIÓN Y TIPIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN, Y EL LLENADO DEL INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

Caracterización del Documento

Nombre del Documento:	Manual para realizar la identificación y tipificación de los Activos de la Información del Hospital Regional de Lambayeque		
Nivel de Confidencialidad:	Este documento debe distribuirse al personal responsable de la Gestión de Riesgos de Seguridad de la Información y no debe ser conocido por personal ajeno a ésta.		
Codificación:	M-GR-002	Versión:	1.0
Fecha de última modificación:		Fecha de Creación:	
Responsable del documento:	<Personal responsable asignado, según las políticas de Seguridad de la Información>		
Aprobado por:	<Área/Comité responsable de la Seguridad del Información del HRL, según las Políticas de Seguridad de la Información>		

Control de Versiones

Versión	Fecha	Elaborador por	Observaciones
1.0			Primera versión del documento

OBJETIVO; Identificar adecuadamente los activos de la información, relacionados a los Sistemas de la Gestión Hospitalaria del Hospital Regional de Lambayeque, tomando en cuenta la metodología propuesta por los autores de la presente investigación, para posteriormente llenar de forma adecuada el Inventario de activos de la información.

I. IDENTIFICACIÓN Y TIPIFICACIÓN DE ACTIVOS DE LA INFORMACIÓN

Tomando en cuenta la diversidad de activos de información por su naturaleza y funcionalidad, éstos serán tipificados en 10 Categorías o Tipos de Activos los cuales definiremos brevemente:

Fig. 01: Identificación y Tipificación de Activos de la información.

Fuente: Elaboración propia.

a. **Datos/información:** Información almacenada en equipos o soportes de información o será transferido de un lugar a otro por los medios de transmisión de datos.

b. **Información impresa:** Refiere a toda la información impresa en documentos físicos.

c. **Servicios auxiliares que se necesitan para poder organizar el sistema:** Servicios que permiten cumplir una función que satisface una necesidad de los usuarios (del servicio/área).

d. **Aplicaciones informáticas (software) que permiten manejar los datos:** Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.), refiriéndose a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.

e. **Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios**: Representan los datos materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.

f. **Los soportes de información que son dispositivos de almacenamiento de datos:** se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.

g. **El equipamiento auxiliar que complementa el material informático:** En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.

h. **Las redes de comunicaciones que permiten intercambiar datos**: Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.

i. **Las instalaciones que acogen equipos informáticos y de comunicaciones:** En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.

j. **Las personas que explotan u operan todos los elementos anteriores citados:** En este epígrafe aparecen las personas relacionadas con los sistemas de información

Cada uno de los Tipos de Activos de información detallados previamente, se asociarán a un determinado código, en base a la siguiente lista:

TIPIFICACION DE ACTIVOS	
DI	Datos/información
II	Información impresa
SA	Servicios auxiliares que se necesitan para poder organizar el sistema
AI	Aplicaciones informáticas (software) que permiten manejar los datos
EI	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios
SI	Los soportes de información que son dispositivos de almacenamiento de datos
EA	El equipamiento auxiliar que complementa el material informático
RC	Las redes de comunicaciones que permiten intercambiar datos
IE	Las instalaciones que acogen equipos informáticos y de comunicaciones
PP	Las personas que explotan u operan todos los elementos anteriores citados

Fig. 02: Tipificación de Activos de la información.

Fuente: Elaboración propia.

De acuerdo al área o servicio en el que se encuentren asignados los activos de información identificados, se tomará en cuenta el código del área al que pertenece el activo:

CODIGO AREA	AREA
SS	SERVICIO SOCIAL
CI	UCI - UCIN
SO	SALUD OCUPACIONAL
NE	NEONATOLOGIA
CQ	CENTRO QUIRURGICO
CO	CENTRO OBSTETRICO
CE	CENTRAL DE ESTERILIZACION
ME	MEDICINA
PE	PEDIATRIA
CG	CIRUGIA
CS	CIRUGIA ESPECIALIDADES
TI	TECNOLOGIA DE LA INFORMACIÓN

Fig. 02: Áreas de Gestión Hospitalaria del Hospital Regional de Lambayeque.

Fuente: Elaboración propia.

Habiendo identificado plenamente el activo de información según su tipología y el área a la cual fue asignado, se procede a designarle un CÓDIGO DE ACTIVO, para que este pueda ser registrado y sea de fácil identificación y seguimiento dentro del Inventario de Activos de la Información.

El Código de Activo se conforma concatenando el **ID DE CLASIFICACIÓN DEL ACTIVO DE INFORMACIÓN, CÓDIGO DEL ÁREA Y CORRELATIVO DEL ACTIVO DE INFORMACIÓN**), según el siguiente formato:

<ID_CLASIFICACION> " - " <CÓDIGO DE ÁREA> < CORRELATIVO>

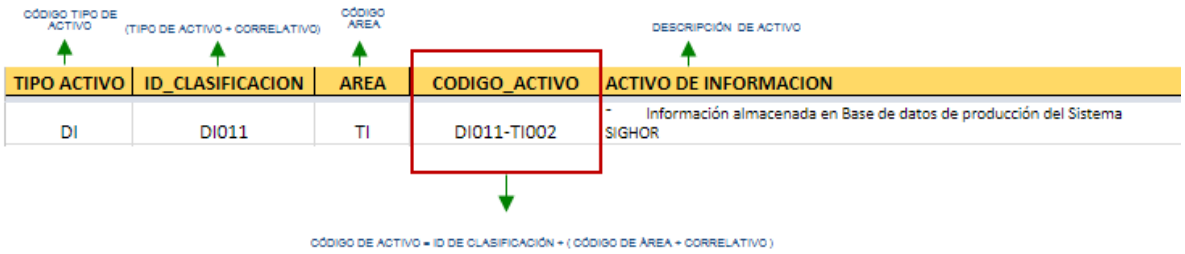


Fig. 03: Nomenclatura para Clasificación de Activos de la información.

Fuente: Elaboración propia.

II. LLENADO DE INVENTARIO DE ACTIVOS DE LA INFORMACIÓN

El inventario de activos de la información propuesto deberá ser llenado por el encargado de las Gestión de los activos de la información asignado, el cual deberá de mantenerse actualizado en el tiempo, en base a los lineamientos de la Política de Seguridad de la Información

Los datos que deberán registrarse se dividen en las siguientes categorías:

A. DATOS GENERALES, se registrarán datos referentes a la tipificación del activo, y al usuario asignado.

DATOS GENERALES	TIPO DE ACTIVOS
	ID CLASIFICACIÓN
	NOMBRE DEL ACTIVO
	ÁREA
	CÓDIGO DE ACTIVO
	CANTIDAD
	ESTADO DE OP
	ID USUARIO RESPONSABLE
	USUARIO RESPONSABLE
	PUESTO DE TRABAJO
	UBICACIÓN
	DETALLE UBICACIÓN

- TIPO DE ACTIVOS: Se seleccionará el Código del Tipo de Activo al cual hace referencia nuestro activo.

TIPIFICACIÓN ACTIVOS	
Datos/información	**DI**
Información impresa	**II**
Servicios auxiliares que se necesitan para poder organizar el sistema	**SA**
Aplicaciones informáticas (software) que permiten manejar los datos	**AI**
Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios	**EI**
Los soportes de información que son dispositivos de almacenamiento de datos	**SI**
El equipamiento auxiliar que complementa el material informático	**EA**
Las redes de comunicaciones que permiten intercambiar datos	**RC**
Las instalaciones que acogen equipos informáticos y de comunicaciones	**IE**
Las personas que explotan u operan todos los elementos anteriores citados	**PP**

Cuadro 01: Códigos para la Tipificación de Activos de la información.

Fuente: Elaboración propia.

- ID CLASIFICACION; Se ingresará el Código del Tipo de Activo con el correlativo respectivo, por ejemplo:

TIPO ACTIVO	ID CLASIFICACIÓN	NOMBRE DEL ACTIVO
DI	**DI001**	- Ficheros, carpetas, documentos virtuales
DI	**DI002**	- Copia de respaldo de la información compartida en ficheros virtuales
DI	**DI003**	- Datos de configuración del Activy Directory

Cuadro 02: Clasificación de los activos según el Tipo de Activos de la información.

Fuente: Elaboración propia.

- NOMBRE DEL ACTIVO; Se ingresa la descripción del activo que se está registrando

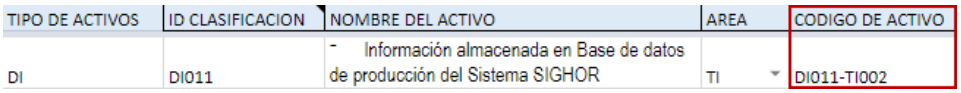
- ÁREA: se selecciona el código del área a la cual está asignado el activo

CÓDIGO ÁREA	**ÁREA**
SS	SERVICIO SOCIAL
CI	UCI - UCIN
SO	SALUD OCUPACIONAL
NE	NEONATOLOGÍA
CQ	CENTRO QUIRURGICO
CO	CENTRO OBSTÉTRICO
CE	CENTRAL DE ESTERILIZACIÓN
ME	MEDICINA
PE	PEDIATRÍA
CG	CIRUGÍA
CS	CIRUGIA ESPECIALIDADES
TI	TECNOLOGÍA DE LA INFORMACIÓN

Cuadro 03: Lista de los código de área del servicio de Gestión Hospitalaria de.del Hospital Regional de Lambayeque

Fuente: Elaboración propia.

- CÓDIGO DE ACTIVO: se selecciona el Código del activo que se registra



TIPO DE ACTIVOS	ID CLASIFICACION	NOMBRE DEL ACTIVO	AREA	CODIGO DE ACTIVO
DI	DI011	Información almacenada en Base de datos de producción del Sistema SIGHOR	TI	DI011-TI002

- CANTIDAD: Se selecciona la cantidad de Activos agrupados, en su defecto se colocará "**1**"

- ESTADO DE OPERATIVO; Se selecciona el código del estado en que se encuentra el activo, de acuerdo a la siguiente lista:

ESTADO	
1.OPERATIVO	OPE
2.DAÑADO	DAÑ
3.EN SERV.TÉCNICO	STC
4.PERDIDO*	PER
5.Otro	OTR

Cuadro 04: Clasificación de los estado de Activos de la información.

Fuente: Elaboración propia

- ID USUARIO RESPONSABLE: se indica el Código de trabajador al cual se asignó como responsable del activo, en su defecto se coloca el DNI del responsable asignado.

- USUARIO RESPONSABLE: Se indica el nombre completo del trabajador responsable del activo asignado

- PUESTO DE TRABAJO: Se ingresa la descripción del Puesto de trabajo al que está asignado el activo

- UBICACIÓN; Se indica el Número del Piso en el que se encuentra ubicado el activo, por ejemplo: "**Piso 3**" hace referencia a que el activo se encuentra en el tercer piso del edificio

- DETALLE UBICACIÓN: (opcional) se ingresa alguna referencia de la ruta de la ubicación del activo

B. DETALLE DEL ACTIVO: en el caso de equipos los activos han de señalar la Marca , modelo y Serie del fabricante

DETALLE DEL ACTIVO	MODELO
	MARCA
	SERIAL

C. SISTEMA OPERATIVO: en el caso de equipos que cuenten con Sistema operativo instalado

SISTEMA OPERATIVO	SO
	CÓDIGO LICENCIA SO

- SO: Se seleccionará el tipo de Sistema operativo que se encuentra instalado en el activo, según la lista.

- CÓDIGO DE LICENCIA SO: se registrará el código de la licencia del sistema operativo del Sistema operativo instalado en el activo

SISTEMA OPERATIVO	
1.Linux	Linux
2.Win 7	Win 7
3.Win 8	Win 8
4.Win 10	Win 10
5.Ios	IOS
6.WinSrv8	WinSrv9
7.WinSrv10	WinSrv11
8.WinSrv12	WinSrv13
9.WinSrv14	WinSrv15
10.Otros	Otro

Cuadro 05: Tipo de Sistemas Operativos.

Fuente: Elaboración propia

D. BASE DE DATOS: Se registrará la Base de datos instalada

BASE DE DATOS	BD

E. DESARROLLO SOFTWARE: se seleccionará de la lista si cuenta o no con el Software de desarrollo mencionado.
De igual manera se seleccionará de la lista si cuenta o no con la licencia del Software de desarrollo mencionado.

DESARROLLO SW	JDK
	COD LICENCIA
	APACHE
	COD LICENCIA
	JAVA
	COD LICENCIA

SOFTWARE DESARROLLO	
A. SI	Cuenta con el Sw
B. NO	No cuenta con el Sw

Cuadro 06: Indicador de tenencia de software de Desarrollo

Fuente: Elaboración propia

LICENCIA	
SI	Cuenta Licencia
NO	No cuenta con Licencia

Cuadro 07: Indicador de tenencia de Licencias para Software de Desarrollo.

Fuente: Elaboración propia

F. PROGRAMAS OFFICE: Se seleccionará la "**X**" de contar con el programa Office mencionado, en su defecto se mantendrá en vacío.
En el código de licencia se seleccionará de la lista si cuenta o no con el código de licencia.

PROGRAMAS OFFICE	WOFFICE
	COD. LICENCIA
	OPENOFFICE
	SKYPE
	PDF
	COMPRESOR

LICENCIA	
SI	Cuenta Licencia
NO	No cuenta con Licencia

Cuadro 08: Indicador de tenencia de licencia de software para Programas Office.

Fuente: Elaboración propia

G. NAVEGADOR: Se seleccionará la "**X**", de contar con el navegador de internet mencionado, en su defecto se mantendrá en vacío.

NAVEGADOR	Chrome
	Explorer
	Mozilla

H. SOFTWARE INSTITUCIONAL: Se seleccionará de la lista, si cuenta o no con el Software institucional mencionado instalado en el activo de referencia

SW INSTITUCIONAL	Sistema Asignación Camas
	SIGHOR
	GALENUS
	SIGBIO

SOFTWARE INSTITUCIONAL	
A. SI	Cuenta con el Sw
B. NO	No cuenta con el Sw

Cuadro 09: Indicador de tenencia de software institucional

Fuente: Elaboración propia

I. REDES: se seleccionará de la lista, el tipo de conexión a internet con el que se encuentra conectado el activo.

REDES	Conexión Internet

CONEXIÓN INTERNET	
1.CABLE	CA
2.WIFI	WI

Cuadro 10: Tipos de conexión a internet con el que cuentan los activos de la información.

Fuente: Elaboración propia

Anexo N° 10: Manual de usuario para el uso de la matriz de riesgos

MANUAL PARA EL LLENADO DE LA MATRIZ DE GESTIÓN DE RIESGOS DEL HOSPITAL REGIONAL DE LAMBAYEQUE

Caracterización del Documento

Nombre del Documento:	Manual para el llenado de la Matriz de Gestión de Riesgos de Seguridad de la Información del Hospital Regional de Lambayeque		
Nivel de Confidencialidad:	Este documento debe distribuirse al personal responsable de la Gestión de Riesgos de Seguridad de la Información y no debe ser conocido por personal ajeno a ésta.		
Codificación:	M-GR-001	Versión:	1.0
Fecha de última modificación:		Fecha de Creación:	
Responsable del documento:	<Personal responsable asignado, según las políticas de Seguridad de la Información>		
Aprobado por:	<Área/Comité responsable de la Seguridad del Información del HRL, según las Políticas de Seguridad de la Información>		

Control de Versiones

Versión	Fecha	Elaborador por	Observaciones
1.0			Primera versión del documento

OBJETIVO:

Proporcionar al usuario responsable del Análisis y Gestión de Riesgos de la seguridad de la información, los lineamientos necesarios para registrar los activos de información, asociarlos a los riesgos identificados, evaluar los riesgos y proponer mecanismos de protección, de manera que se pueda gestionar efectivamente los riesgos identificados sobre los activos de los Sistemas de Gestión Hospitalaria del Hospital Regional de Lambayeque.

1. **Registro de datos del activo**: Los activos que serán registrados en la Matriz de riesgos, son los mismos que han sido identificados en el Inventario de Activos de información. Los Datos del Activo comprende los siguientes campos: Id Activo, Tipo de Activo y Nombre de Activo.

DATOS DEL ACTIVO	**ID ACTIVO**
	TIPO DE ACTIVO
	NOMBRE DEL ACTIVO

A continuación, se detallan los siguiente campos de Datos del Activo:

- **ID ACTIVO**: Identificador único que indica el código del activo de información
- **NOMBRE DEL ACTIVO**: Indica la descripción del activo de la información.
- **TIPO DE ACTIVO**: Refiere a la tipificación del activo de información. Los activos de información se tipifican de la siguiente manera:

TIPIFICACION DE ACTIVOS	
DI	Datos/información
II	Información impresa
SA	Servicios auxiliares que se necesitan para poder organizar el sistema
AI	Aplicaciones informáticas (software) que permiten manejar los datos
EI	Los equipos informáticos (Hardware) que permiten hospedar los datos, aplicaciones y servicios
SI	Los soportes de información que son dispositivos de almacenamiento de datos
EA	El equipamiento auxiliar que complementa el material informático
RC	Las redes de comunicaciones que permiten intercambiar datos
IE	Las instalaciones que acogen equipos informáticos y de comunicaciones
PP	Las personas que explotan u operan todos los elementos anteriores citados

Ejemplo 01: Identificación de Datos del Activo DI011-TI002

ID ACTIVO	TIPO DE ACTIVO	NOMBRE DEL ACTIVO
DI011-TI002	Datos/información	- Información almacenada en Base de datos de producción del Sistema SIGHOR

2. **Dimensiones de Seguridad de la Información**: La Seguridad de la Información se puede valorar a través de 5 dimensiones y son las siguientes: Confidencialidad, Integridad, Disponibilidad, Trazabilidad y Autenticidad.

   Criterios para valorar las Dimensiones de Seguridad de la Información:

   Confidencialidad: Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Para poder valorar un activo de información a través de la dimensión "Confidencialidad", el responsable deberá plantearse la siguiente pregunta:

   ¿Qué importancia tendría que el dato fuera conocido por personas no autorizadas?
   En donde las posibles respuestas serían:

- Los datos reciben una alta valoración desde el punto de vista de confidencialidad cuando su revelación causaría graves daños a la organización.
- Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de confidencialidad cuando su conocimiento por cualquiera no supone preocupación alguna.

Integridad: Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. Para poder valorar un activo de información a través de la dimensión "Integridad", el responsable deberá plantearse la siguiente pregunta:

¿Qué importancia tendría que los datos fueran modificados fuera de control?
En donde las posibles respuestas serían:
- Los datos reciben una alta valoración desde el punto de vista de integridad cuando su alteración, voluntaria o intencionada, causaría graves daños a la organización.
- Y, recíprocamente, los datos carecen de un valor apreciable desde el punto de vista de integridad cuando su alteración no supone preocupación alguna.

Disponibilidad: Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. Para poder valorar un activo de información a través de la dimensión "Disponibilidad", el responsable deberá plantearse la siguiente pregunta:

¿Qué importancia tendría que el activo no estuviera disponible?
En donde las posibles respuestas serían:
- Un activo tiene un gran valor desde el punto de vista de disponibilidad cuando si una amenaza afectara a su disponibilidad, las consecuencias serían graves.
- Y recíprocamente, un activo carece de un valor apreciable desde el punto de vista de disponibilidad cuando puede no estar disponible frecuentemente y durante largos periodos de tiempo sin por ello causar mayor daño.

Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Para poder valorar un activo de información a través de la dimensión "Autenticidad", el responsable deberá plantearse la siguiente pregunta:

¿Qué importancia tendría que quien accede al servicio no sea realmente quien se cree?
En donde las posibles respuestas serían:
- Así, un servicio recibe una elevada valoración desde el punto de vista de autenticidad cuando su prestación a falsos usuarios supondría un grave perjuicio para la organización.
- Y, recíprocamente, un servicio carece de un valor apreciable desde el punto de vista de autenticidad cuando su acceso por cualquiera no supone preocupación alguna.

Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Para poder valorar un activo de información a través de la dimensión "Trazabilidad", el responsable deberá plantearse las siguientes preguntas:

¿Qué importancia tendría que no quedara constancia fehaciente del uso del servicio?
- Abriría las puertas al fraude, incapacitar a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

¿Qué importancia tendría que no quedara constancia del acceso a los datos?

- Abriría las puertas al fraude, incapacitar a la Organización para perseguir delitos y podría suponer el incumplimiento de obligaciones legales.

En base a las definiciones de Dimensiones de Seguridad de la información de los activos de información; se seleccionará una valoración del 0 al 10 para cada Dimensión, en base al siguiente cuadro:

VALOR DE DIMENSION	
10	Extremo
9	Muy Alto
.6-8	Alto
.3-5	Medio
.1-2	Bajo
0	Despreciable

Cuadro 1. Escala de Valoración Dimensiones del Activo.
Fuente: Elaboración propia.

Ejemplo 02: Valoración de Dimensiones del Activo de Información DI011-TI002

DIMENSIONES DE SEGURIDAD DE LA INFORMACION				
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD
6	5	6	6	5

3. **Valoración del Activo de Información**: Refiere al cálculo del promedio final de los valores seleccionados para cada Dimensión de Seguridad de la Información.

VALORACIÓN DEL ACTIVO	**Promedio (Valoración Confidencialidad + Valoración Integridad + Valoración Disponibilidad + Valoración Trazabilidad + Valoración Autenticidad)**

Ejemplo 03: Valoración del Activo DI011-TI002

DIMENSIONES DE SEGURIDAD DE LA INFORMACION					VALORACION DEL ACTIVO
CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TRAZABILIDAD	AUTENTICIDAD	(PROM DE DIMENSIONES)
6	5	6	6	5	6

4. **Activo Priorizado:** Un Activo priorizado, es aquel seleccionado en base a ciertos criterios, por el cual se identificarán los riesgos asociados. Un Activo priorizado comprende: El Indicador del Nivel de Valoración y el Indicador de Priorización.

ACTIVO PRIORIZADO	***INDICADOR DEL NIVEL DE VALORACION***
	INDICADOR DE PRIORIZACION

- Indicador del Nivel de Valoración: Los Niveles de valoración son cinco: 1) Óptimo; 2) Bueno; 3) Más que regular; 4) Regular; y 5) Deficiente. Los niveles de valoración comprenden a los valores de dimensión de seguridad de la información, en base a los siguientes rangos de valorización:

INDICADOR DE NIVEL DE VALORACION		VALOR DE DIMENSION		CRITERIO
5	Deficiente	10	Extremo	Daño extremadamente grave
		9	Muy Alto	Daño muy grave
4	Regular	.6-8	Alto	Daño grave
3	Más que regular	.3-5	Medio	Daño importante
2	Bueno	.1-2	Bajo	Daño menor
1	Óptimo	0	Despreciable	Irrelevante a efectos prácticos

Cuadro 2. Equivalencia del Indicador del Nivel de Valoración respecto del Valor de la Dimensión de un Activo.
Fuente: Elaboración propia

- Indicador de Priorización: Por criterio de los investigadores, el valor del **Indicador del Nivel de Valoración** equivalente al Valor de la dimensión que sean mayores a "3" se considerarán PRIORITARIOS, por lo cual se devolverá la señalización de **Priorizar** si dicha equivalencia se encuentra en los parámetros del Cuadro 3, caso contrario se considerarán Activos no Priorizados

PRIORIZACION DE ACTIVOS POR NIVEL DE VALORACION:	
INDICADOR DE NIVEL DE VALORACIÓN	
5	Deficiente
4	Regular
3	Más que regular

Cuadro 3. Indicador de nivel de Valoración de los Activos que se Priorizarán.
Fuente: Elaboración propia.

Ejemplo 04: Priorización del Activo DI011-TI002

VALORACION DEL ACTIVO	ACTIVO PRIORIZADO	
(PROM DE DIMENSIONES)	"INDICADOR DEL NIVEL DE VALORACION"	INDICADOR
6	Alto	Priorizar

5. **VULNERABILIDADES**: En cada uno de los activos registrados, se analizarán las Vulnerabilidades que éstos puedan contener, para lo cual en cada una de las celdas denominadas V1 … Vn se seleccionarán las Vulnerabilidades que contiene el activo analizado (Estas vulnerabilidades se encuentran descritas y listadas en el Catálogo de Vulnerabilidades)

VULNERABILIDADES	**V1**
	V2
	Vn

Ejemplo 05: Identificación de Vulnerabilidades del Activo DI011-TI002

VULNERABILIDADES													
V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14
5.1.1	7.3.1	8.2.1	11.1.1	12.1.1	12.1.4	12.6.1							

6. **AMENAZAS**: En cada uno de los activos registrados, se analizarán las Amenazas a las que se encuentran expuestas, para lo cual en cada una de las celdas denominadas A1 … An se seleccionarán las Amenazas a las que se encuentra expuesta el activo analizado (Estas amenazas se encuentras descritas y listadas en el Catálogo de Amenazas)

AMENAZAS	**A1**
	A2
	An

Ejemplo 06: Identificación de Amenazas del Activo DI011-TI002

AMENAZAS																									
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27
A.3	B.1	B.2	B.4	C.1	C.3	C.2	C.4	C.5	C.9	C.10	C.11	C.12	C.13	D.3	D.9	D.19	D.24									

7. **NIVEL DE RIESGO INHERENTE:**

NIVEL DE RIESGO INHERENTE	**PROBABILIDAD DE MATERIALIZACION**
	IMPACTO DE MATERIALIZACION
	NIVEL DE RIESGO INHERENTE

- **PROBABILIDAD DE MATERIALIZACION**: El responsable del análisis de la Gestión de riesgos registrará el Valor de la Probabilidad de materialización de amenazas del activo de la información analizado, colocando un valor del 1 – 5 considerando la descripción del cuadro 4

PROBABILIDAD DE MATERIALIZACIÓN DE AMENAZAS		
5	MA	5-MA: Prácticamente seguro
4	A	4-A: Probable
3	M	3-M: Posible
2	B	2-B: Poco probable
1	MB	1-MB: Muy raro

Cuadro 4. Escala de Valoración de la Probabilidad de Materialización de Amenazas (PMA).

Fuente: Elaboración propia.

- **IMPACTO DE MATERIALIZACION**: El responsable del análisis de la Gestión de riesgos registrará el Valor del Impacto de materialización de amenazas del activo de la información analizado, colocando un valor del 1 – 5 considerando la descripción del cuadro 5

NIVELES DE IMPACTO		
5	MA	5-MA: Muy Alto
4	A	4-A: Alto
3	M	3-M: Medio
2	B	2-B: Bajo
1	MB	1-MB: Muy Bajo

Cuadro 5. Escala de Valoración del Niel de Impacto de Materialización (IMI).

Fuente: Elaboración propia.

- **NIVEL DE RIESGO INHERENTE**: Una vez registrada la Probabilidad de Materialización de Amenazas y el Nivel de Impacto de la Amenaza, se devolverá en la celda la descripción del Nivel de Riesgo Inherente según el cuadro 6 y teniendo en cuenta el cálculo realizado con la matriz mostrada.

COLORES	NIVEL DE INHERENTE
	Extremo
	Alto
	Medio
	Bajo

Cuadro 6. Escala de Valoración del Nivel de Riesgo Inherente

Fuente: Elaboración propia

NIVEL DE RIESGO INHERENTE	
1A	BAJO
2A	BAJO
3A	BAJO
4A	MEDIO
5A	ALTO
2B	BAJO
4B	BAJO
6B	MEDIO
8B	MEDIO
10B	ALTO
3C	BAJO
6C	MEDIO
9C	MEDIO
12C	ALTO
15C	EXTREMO
4D	MEDIO
8D	MEDIO
12D	ALTO
16D	EXTREMO
20D	EXTREMO
5E	ALTO
10E	ALTO
15E	EXTREMO
20E	EXTREMO
25E	EXTREMO

NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO				
	1 MB	2B	3 M	4 A	5 MA
5 MA	5A	10B	15C	20D	25E
4 A	4A	8B	12C	16D	20E
3 M	3A	6B	9C	12D	15E
2 B	2A	4B	6C	8D	10E
1 MB	1A	2B	3C	4D	5E

COLORES	NIVEL DE RIESGO
	Extremo
	Alto
	Medio
	Bajo

Fig 2. Matriz de Riesgo Inherente.
Fuente: Elaboración propia.

Ejemplo 07: Estimación de Nivel de Riesgo Inherente para el análisis del activo DI011-TI002

PROBABILIDAD DE MATERIALIZACION	IMPACTO DE MATERIALIZACION	NIVEL DE RIESGO INHERENTE
3- M: Posible	4- A: Alto	ALTO

8. **MECANISMOS DE PROTECCION**: En cada uno de los activos registrados, se analizarán los mecanismos de protección que puedan contrarrestar las amenazas y vulnerabilidades a las que se encuentran expuestas, para lo cual en cada una de las celdas denominadas S1 … Sn, se seleccionarán los mecanismos que según el criterio del analista puedan controlar estas amenazas (Estos mecanismos se encuentras descritas y listadas en el Catálogo de Mecanismos de Protección)

MECANISMO DE PROTECCION	S1
	S2
	Sn

Ejemplo 08: Identificación de Mecanismos de Protección del Activo DI011-TI002

										SALVAGUARDAS					
S1	S2	S3	S4	S5	S6	S7	S8	S9	S10	S11	S12	S13	S14	S15	S16
AP01	AP02	AP04	SS02	OR04	DI03	DI04	CO04	GH02	CC06						

9. NIVEL DE RIEEFECTIVIDAD:

MECANISMOS DE PROTECCION	ESTADO
	OPORTUNIDAD
	GRADO DE IMPLEMENTACIÓN
	NIVEL DE EFECTIVIDAD

- **ESTADO** : Se registrará el Estado en el que se encuentra el mecanismo de protección seleccionado para el control de las amenazas del activo analizado, según el cuadro 6, considerando los valores "**1**" en caso de estar Implementado ó "**0**" de ser No implementado

ESTADO	
1	Implementado
0	No implementado

Cuadro 6. Escala de Valoración de los Estados de Mecanismo de Protección.
Fuente: Elaboración propia.

En caso de contar con más de un mecanismo de protección por activo analizado, en la matriz de riesgos se colocará el promedio de los valores registrados en el Estado de estos mecanismos.

- OPORTUNIDAD: Se registrará la Oportunidad de la propuesta de los mecanismos de protección para el activo analizado, según el cuadro 7, considerando los valores "**1**" en caso de proponer un mecanismo de naturaleza **Preventiva** , "**2**" si la propuesta es de un mecanismo de naturaleza **Detectiva** ó "**3**" si la propuesta se consideran un mecanismo de naturaleza **Correctiva**

OPORTUNIDAD DE PROPUESTA DE MECANISMOS DE PROTECCION	
1	Preventivo
2	Detectivo
3	Correctivo

Cuadro 7. Escala de Valoración de Oportunidad.
Fuente: Elaboración propia.

En caso de contar con más de un mecanismo de protección por activo analizado, en la matriz de riesgos se colocará el promedio de los valores registrados en la Oportunidad de Propuesta de estos mecanismos.

- **GRADO DE IMPLEMENTACIÓN**: Se registrará el Grado de Implementación de mecanismos de protección para el activo analizado, según el cuadro 8, considerando los valores "**1**" en caso de proponer un mecanismo que requiera como mínimo una implementación **Manual** , "**2**" si la propuesta es de un mecanismo de protección que deba ser **Semiautomatizada** ó "**3**" si la propuesta se considera un mecanismo de protección implementada de forma **Automatizada**

GRADO DE IMPLEMENTACION	
1	Manual
2	Semiautomatizado
3	Automatizado

Cuadro 8. Escala de Valoración del Grado de Implementación.
Fuente: Elaboración propia.

En caso de contar con más de un mecanismo de protección por activo analizado, en la matriz de riesgos se colocará el promedio de los valores registrados en el Grado de Implementación de estos mecanismos.

Mecanismos de protección		ESTADO	OPORTUNIDAD	GRADO
AP01	Protección de las aplicaciones informáticas	1	1	2
AP02	Copias de seguridad (backup)	1	1	2
AP04	Se aplican perfiles de seguridad	0	1	2
SS02	Aseguramiento de la disponibilidad	1	1	2
OR04	Inspecciones de la seguridad	0	2	2
DI03	Aseguramiento de la integridad	1	1	3
DI04	Cifrado de la información	1	1	2
CO04	Aseguramiento de la disponibilidad	1	1	3
GH02	Control de acceso lógico	1	1	2
CC06	Gestión de certificados	0	1	2
		1	1	2

- **NIVEL DE EFECTIVIDAD**: una vez que el responsable del registro del estado, nivel de oportunidad y grado de implementación de mecanismos de protección completó estos tres datos, la celda de Nivel de Efectividad devolverá el valor del Nivel de Efectividad de los mecanismos de protección señalados para el activo analizado, de acuerdo a las combinaciones señaladas en el cuadro 9.

NIVELES DE EFECTIVIDAD DE LOS MECANISMO DE PROTECCION					
NIVELES DE ESTADO	NIVELES DE OPORTUNIDAD	GRADO	COMBINACIÓN	DESCRIPCIÓN	VALOR
No implementado	Preventivo	Manual	No implementadoPreventivoManual	1. Deficiente	1
No implementado	Preventivo	Semiautomatizado	No implementadoPreventivoSemiautomatizado	1. Deficiente	1
No implementado	Preventivo	Automatizado	No implementadoPreventivoAutomatizado	1. Deficiente	1
No implementado	Correctivo	Manual	No implementadoCorrectivoManual	1. Deficiente	1
No implementado	Correctivo	Semiautomatizado	No implementadoCorrectivoSemiautomatizado	1. Deficiente	1
No implementado	Correctivo	Automatizado	No implementadoCorrectivoAutomatizado	1. Deficiente	1
No implementado	Detectivo	Manual	No implementadoDetectivoManual	1. Deficiente	1
No implementado	Detectivo	Semiautomatizado	No implementadoDetectivoSemiautomatizado	1. Deficiente	1
No implementado	Detectivo	Automatizado	No implementadoDetectivoAutomatizado	1. Deficiente	1
Implementado	Correctivo	Manual	ImplementadoCorrectivoManual	2. Regular	2
Implementado	Correctivo	Semiautomatizado	ImplementadoCorrectivoSemiautomatizado	2. Regular	2
Implementado	Correctivo	Automatizado	ImplementadoCorrectivoAutomatizado	2. Regular	2
Implementado	Detectivo	Manual	ImplementadoDetectivoManual	3. Más que regular	3
Implementado	Detectivo	Semiautomatizado	ImplementadoDetectivoSemiautomatizado	3. Más que regular	3
Implementado	Detectivo	Automatizado	ImplementadoDetectivoAutomatizado	4. Bueno	4
Implementado	Preventivo	Manual	ImplementadoPreventivoManual	4. Bueno	4
Implementado	Preventivo	Semiautomatizado	ImplementadoPreventivoSemiautomatizado	5. Optimo	5
Implementado	Preventivo	Automatizado	ImplementadoPreventivoAutomatizado	5. Optimo	5

Cuadro 9. Equivalencia de los niveles de Efectividad de los mecanismos de protección. Fuente: Elaboración propia.

Ejemplo 09: Estimación de nivel de efectividad de los mecanismos de protección para el activo l DI011-TI002

PROBABILIDAD DE MATERIALIZACION	IMPACTO DE MATERIALIZACION	NIVEL DE RIESGO INHERENTE		ESTADO DE CONTROL		OPORTUNIDAD DE CONTROL		GRADO DE IMPLEMENTACIÓN	NIVEL DE EFECTIVIDAD
3- M: Posible	4- A: Alto	ALTO	1	Implementado	1	Preventivo	2	Semiautomatizado	5

10. ANALISIS DE RIESGO RESIDUAL

ANALISIS DE RIESGO RESIDUAL	PROBABILIDAD
	IMPACTO
	NIVEL DE RIESGO RESIDUAL

- **PROBABILIDAD RESIDUAL**: Tomando en cuenta el valor del Nivel de Efectividad calculado anteriormente, es que se devuelve la Probabilidad Residual, teniendo en cuenta la equivalencia del cuadro 10, en el cual de acuerdo al valor del Nivel de Efectividad de las medidas de protección , la Probabilidad Residual se halla como resultado del Valor de la Probabilidad de Materialización de Amenazas (PMA) menos los valores (0-1) según la equivalencia del Nivel de Efectividad de los mecanismo de protección del activo analizado.

NIVEL EFECTIVIDAD		PROBABILIDAD RESIDUAL: PMA: Probabilidad de Materialización de amenazas
DESCRIPCIÓN	VALOR	
Deficiente	1	PMA (menos) 0
Regular	2	PMA (menos) 1
Más que regular	3	PMA (menos) 2
Bueno	4	PMA (menos) 3
Optimo	5	PMA (menos) 4

Cuadro 10. Escala de Valoración de la Probabilidad Residual.
Fuente: Elaboración propia.

- **IMPACTO RESIDUAL**: Tomando en cuenta el valor del Nivel de Efectividad calculado anteriormente, es que se devuelve el Impacto Residual, teniendo en cuenta la equivalencia del cuadro 11, en el cual de acuerdo al valor del Nivel de Efectividad de los mecanismo de protección, el Impacto Residual se halla como resultado del Valor Impacto de Materialización (IMI) menos los valores (0-1) según la equivalencia del Nivel de Efectividad de los mecanismos de protección del activo analizado

NIVEL EFECTIVIDAD		IMPACTO RESIDUAL IMI: Impacto Inherente
DESCRIPCIÓN	VALOR	
Deficiente	1	IMI (menos) 0
Regular	2	IMI (menos) 1
Más que regular	3	IMI (menos) 2
Bueno	4	IMI (menos) 3
Optimo	5	IMI (menos) 4

Cuadro 11. Escala de Valoración del Impacto Residual.
Fuente: Elaboración propia.

- **NIVEL DE RIESGO RESIDUAL:** Con los valores de la Probabilidad Residual y el Impacto Residual es que se determina el Nivel de Riesgo Residual considerando el cuadro 12 y tomando como referencia la matriz mostrada

COLORES	NIVEL DE RIESGO RESIDUAL
	Extremo
	Alto
	Medio
	Bajo

Cuadro 12. Escala de Valoración del Nivel de Riesgo Residual.
Fuente: Elaboración propia.

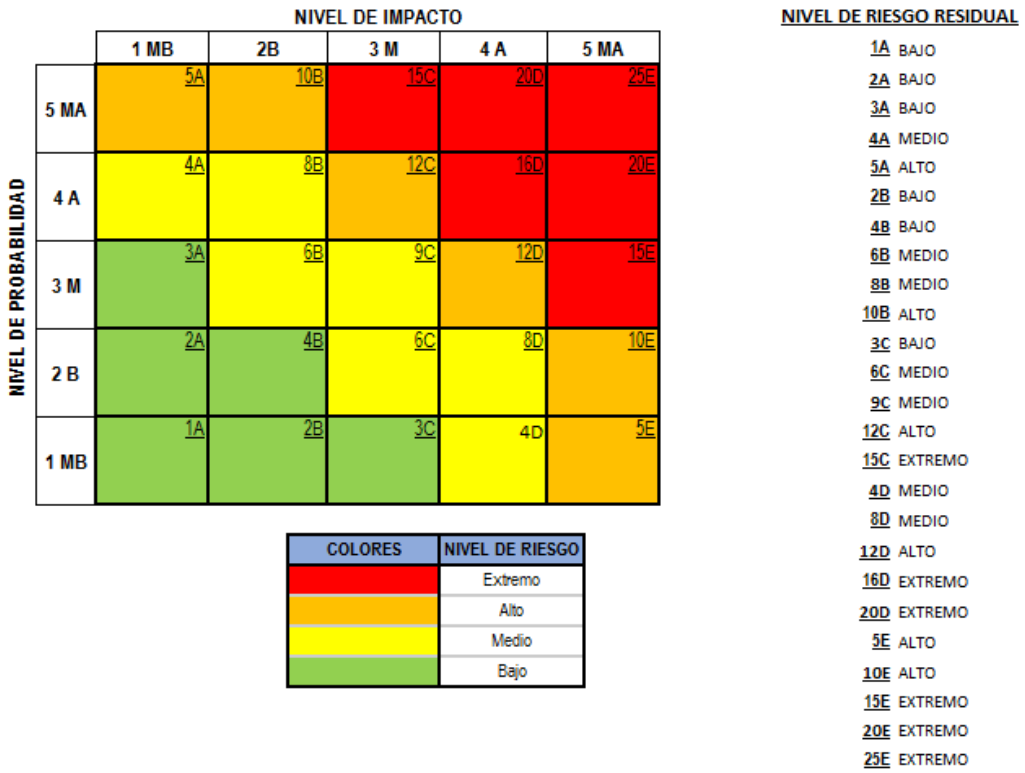


Fig 3. Matriz de Riesgo Residual.
Fuente: Elaboración propia.

Ejemplo 10: Estimación de Nivel de Riesgo Residual para el análisis del activo DI011-TI002

ANALISIS DE RIESGO RESIDUAL		
PROBABILIDAD	IMPACTO	NIVEL DE RIESGO RESIDUAL
1	1	BAJO

11. **SEGUIMIENTO**: Una vez puestos en marcha los mecanismo de protección sugeridos por medio de la matriz sobre los activos analizados para el control de las amenazas existentes, es que según el plazo (tiempo) establecido por las políticas de seguridad, se vuelve a realizar el análisis de los mecanismos de protección implementadas, en la pestaña de "Seguimiento", donde se vuelve a evaluar el Estado, Oportunidad, Grado de implementación así como el Nivel de Efectividad de los mecanismos de protección implementados y del mismo modo la Probabilidad, Impacto y Nivel de Riesgo Residual

SEGUIMIENTO	ESTADO
	OPORTUNIDAD
	GRADO DE IMPLEMENTACIÓN
	NIVEL DE EFECTIVIDAD
	PROBABILIDAD RESIDUAL
	IMPACTO RESIDUAL
	NIVEL DE RIESGO RESIDUAL

Anexo N° 11: Resolución de Políticas de seguridad de la información del Ministerio de Salud

MINISTERIO DE SALUD

No. 431-2015/MINSA

REPUBLICA DEL PERU

Resolución Ministerial

Lima, 9 de Julio del 2015

Visto, el Expediente N° 14-066417-001 que contiene el Informe N° 002-2015-OGEI-OIT-OFISEG/MINSA de la Oficina General de Estadística e Informática del Ministerio de Salud; y,

CONSIDERANDO:

Que, el artículo 9° de la Ley N° 29733, Ley de Protección de Datos Personales, establece que el titular del banco de datos personales y el encargado de su tratamiento deben adoptar las medidas técnicas, organizativas y legales necesarias para garantizar la seguridad de los datos personales. Las medidas de seguridad deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar y con la categoría de datos personales de que se trate;

Que, mediante Resolución Ministerial N° 520-2006/MINSA, del 30 de mayo de 2006, se aprobó el documento técnico "Lineamientos de Política de Seguridad de la Información del Ministerio de Salud", con el fin de preservar la integridad, disponibilidad y confidencialidad de la información del Ministerio de Salud, en todos sus medios de soporte y tratamiento;

Que, mediante Resolución Ministerial Nº 246-2007-PCM, se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª Edición" en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la Administración Pública;

Que, la Norma Técnica Peruana referida en el considerando precedente, señala que la Política de Seguridad de la Información, tiene como objetivo dirigir y dar soporte a la gestión de seguridad de la información en concordancia con los requerimientos de la institución, las leyes y las regulaciones; correspondiendo a la Alta Dirección establecer las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una Política de Seguridad en toda la organización;

Que, la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros recomienda la aplicación y el uso de la "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos.", de manera progresiva, en todas las entidades que integran el Sistema

Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, complementando así lo dispuesto por la Resolución Ministerial Nº 246-2007-PCM antes señalada;

Que, en tal sentido, mediante Resolución Ministerial Nº 129-2012-PCM, se aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", en todas las entidades integrantes del Sistema Nacional de Informática, estableciendo que su control deberá ser implementado de acuerdo a las recomendaciones de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información";

Que, mediante Resolución Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias N° 129-2014/CNB-INDECOPI, del Instituto Nacional de Defensa de la Competencia y Protección de la Propiedad Intelectual – INDECOPI, se deja sin efecto la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008" y se aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2ª edición."

Que, en atención a los cambios normativos referidos a la gestión de seguridad de la información, con el documento de Visto la Oficina General de Estadística e Informática propone la aprobación del Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud", resultando necesario emitir el acto resolutivo correspondiente;

Con el visado de la Directora General de la Oficina General de Asesoría Jurídica, del Director General de la Oficina General de Estadística e Informática y de la Secretaria General; y,

De conformidad con lo dispuesto en la Ley N° 29158, Ley Orgánica del Poder Ejecutivo; en la Ley N° 29733, Ley de Protección de Datos Personales y en el Decreto Legislativo N° 1161, Ley de Organización y Funciones del Ministerio de Salud;

SE RESUELVE:

Artículo 1.- Aprobar el Documento Técnico "Política de Seguridad de la Información del Ministerio de Salud - MINSA", que como Anexo forma parte integrante de la presente Resolución Ministerial.

Artículo 2.- Dejar sin efecto la Resolución Ministerial N° 520-2006/MINSA y cualquier otra disposición que se oponga a la presente Resolución Ministerial.

Artículo 3.- Disponer que la presente Resolución Ministerial se notifique a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

Artículo 4.- Disponer que la Oficina General de Comunicaciones publique la presente Resolución Ministerial en el Portal Institucional del Ministerio de Salud en la dirección electrónica: http://www.minsa.gob.pe/transparencia/dga_normas.asp

Regístrese, comuníquese y publíquese

S. RUIZ Z.

Zevala S.

ANÍBAL VELÁSQUEZ VALDIVIA
Ministro de Salud

Anexo N°12: Análisis de los indicadores de calidad para un modelo de gestión de riesgo tomando como referencia la norma ISO 25010

Los indicadores de calidad del producto software en la ISO 25010, han sido contextualizados para la evaluación de la calidad de nuestra propuesta de modelo de gestión de riesgos.

Característica de calidad: Adecuación funcional **Definición ISO 25010:** Cuando la funcionalidad un producto de software cubre las necesidades de un usuario, que fueron definidas al momento de requerirse dicha implementación **Contextualización para nuestro modelo de gestión de riesgos:** Característica que tiene nuestro modelo de gestión de riesgos, cuya aplicación permite cumplir los requerimientos mínimos definidos en la política de seguridad de información del Ministerio de Salud.
Característica de calidad: Eficiencia de desempeño **Definición ISO 25010:** Característica que representa el desempeño de funciones que realiza el producto de software con el empleo del menor número posible de recursos. **Contextualización para nuestro modelo de gestión de riesgos:** No aplica

Característica de calidad: Compatibilidad

Definición ISO 25010:

Capacidad que tiene el producto de software o en su defecto la capacidad que tienen algunos de sus componentes, para compartir y/0 consumir recursos comunes bajo un estándar universal (por ejemplo XML, JSON) proveniente de otro software independiente.

Contextualización para nuestro modelo de gestión de riesgos:

Capacidad que tiene nuestro modelo de gestión de riesgos para ser aplicado en distintos servicios o instituciones del Ministerio de Salud.

Característica de calidad: Usabilidad

Definición ISO 25010:

Capacidad del producto de software de tener una interfaz amigable de cara al usuario, que permita entender su funcionalidad, permita su utilización por usuarios con determinadas características y discapacidades, operarlo y controlarlo con facilidad y sobre todo tenga validaciones que proteja a los usuarios de cometer errores al momento del registro de información u otras situaciones.

Contextualización para nuestro modelo de gestión de riesgos:

Capacidad que tiene nuestro modelo de gestión de riesgos para ser aplicado con facilidad, ser entendido, aprendido, usado por el usuario y que se adecuado a las necesidades del Hospital Regional Lambayeque respecto a la seguridad de la información.

Característica de calidad: Fiabilidad

Definición ISO 25010:

Capacidad del producto de software para satisfacer las necesidades del usuario cuando se usa bajo condiciones normales, estar operativo y accesible para su uso cuando se requiera, operar en presencia de fallos de hardware o software y recuperar los datos directamente afectados y reestablecer el estado deseado del sistema en caso de fallos.

Contextualización para nuestro modelo de gestión de riesgos:

Capacidad que tiene nuestro modelo de gestión de riesgos de ser fiable en su uso para cubrir las necesidades básicas del hospital, y que se puede ir complementándose y/o adaptándose a los requerimientos específicos del mismo Hospital Regional de Lambayeque, sin perder su fiabilidad en los resultados que arroje.

Característica de calidad: seguridad

Definición ISO 25010:

Capacidad del software de mantener la confidencialidad, integridad, autenticidad y trazabilidad de la información

Contextualización para nuestro modelo de gestión de riesgos:

Capacidad que tiene nuestro modelo de gestión de riesgos, que permita implementar y mantener mecanismos de protección de seguridad de información para conservar la confidencialidad, integridad, disponibilidad, trazabilidad, y autenticidad de los datos y la información que administra, procesa y/o transfiere el Hospital Regional de Lambayeque.

Característica de calidad: Mantenibilidad

Definición ISO 25010:
Capacidad de un producto de software de ser modificado de forma efectiva y eficiente sin degradar su desempeño, ser probado para evaluar su correcta funcionalidad, facilidad de diagnosticar deficiencias o fallos en el software a raíz de la realización de un determinado cambio.

Contextualización para nuestro modelo de gestión de riesgos:
Capacidad que tiene un modelo de gestión de riesgos cuya implementación, permita a la organización realizar un control y seguimiento continuo del análisis de gestión de riesgos en la seguridad de la información.

Característica de calidad: Portabilidad

Definición ISO 25010:
Característica del producto o componente de software de ser transferido de forma efectiva y eficiente de un entorno hardware, software, operacional o de utilización a otro entorno.

Contextualización para nuestro modelo de gestión de riesgos:
Capacidad que tiene nuestro modelo de gestión de riesgos para poder ser aplicado en distintas áreas o servicios de instituciones con diferente giro de negocio al de los hospitales del Ministerio de Salud.

Anexo N°13: Fichas de análisis de los 3 primeros activos de la información priorizados

[DI003-TI005]

Nombre del Activo	- Datos de configuración del Servidor de Base de Datos
Tipo de Activo	Datos/información
Vulnerabilidades	
5.1.1	Falta de políticas para la seguridad de la información
12.1.1	No se tiene documentado los procesos operativos y servicios que soportan a los sistemas de información
8.2.1	No existe Directrices para una buena clasificación de activos de información
12.6.1	No se tiene identificadas las vulnerabilidades técnicas de los sistemas de información, para evaluar de manera oportuna el grado de exposición de la organización
Amenazas	
C.2	Errores del administrador
C.4	Errores de configuración
C.5	Deficiencias en la organización
C.10	Alteración accidental de información
C.11	Destrucción de la información
D.13	Modificación deliberada de la información
D.24	Bloqueo de Base de Datos bajo petición de rescate
Probabilidad	Posible
Impacto	Alto
Riesgo	ALTO

Mecanismo de Protección		**ESTADO**	**OPORTUNIDAD**	**GRADO**
GH01	Identificación y autenticación	0	2	2
GH06	Herramientas de seguridad	0	2	2
CC01	Gestión de claves criptográficas	0	1	2
OR03	Planificación de la seguridad	0	1	2
		0	**2**	**2**

[DI004-TI001]

Nombre del Activo	- Datos o políticas de control de acceso
Tipo de Activo	Datos/información
Vulnerabilidades	
5.1.1	Falta de políticas para la seguridad de la información
9.1.2	Existe un débil control para el acceso redes y servicios asociados
12.6.1	No se tiene identificadas las vulnerabilidades técnicas de los sistemas de información, para evaluar de manera oportuna el grado de exposición de la organización
Amenazas	
C.5	Deficiencias en la organización
C.9	Escapes de Información
C.10	Alteración accidental de información
C.12	Fugas de información
D.9	Acceso no autorizado
Probabilidad	Posible
Impacto	Alto
Riesgo	ALTO

Mecanismos de Protección		**ESTADO**	**OPORTUNIDAD**	**GRADO**
GH02	Control de acceso lógico	1	1	2
OR01	Organización	0	1	1
OR03	Planificación de la seguridad	0	1	2
CC02	Gestión de las claves de cifra de información	1	2	2
DI04	Cifrado de la información	1	1	2
		1	**1**	**2**

[DI006-TI005]

Nombre del Activo	- Registro de actividad (Log) del Servidor de Base de Datos
Tipo de Activo	Datos/información
Vulnerabilidades	
5.1.1	Falta de políticas para la seguridad de la información
12.4.1	No cuentan con una bitácora de eventos de actividades
12.6.1	No se tiene identificadas las vulnerabilidades técnicas de los sistemas de información, para evaluar de manera oportuna el grado de exposición de la organización
Amenazas	
C.1	Errores en los usuarios
C.2	Errores del administrador
C.3	Errores de monitorización (log)
C.5	Deficiencias en la organización
C.10	Alteración accidental de información
C.11	Destrucción de la información
C.13	Vulnerabilidad d los programas
D.9	Acceso no autorizado
D.10	Análisis de tráfico
D.12	Interceptación de información
D.19	Robo
D.24	Bloqueo de Base de Datos bajo petición de rescate
Probabilidad	**Posible**
Impacto	**Alto**
Riesgo	ALTO

Mecanismos de Protección		**ESTADO**	**OPORTUNIDAD**	**GRADO**
OR03	Planificación de la seguridad	0	1	2
OR04	Inspecciones de la seguridad	0	2	2
DI04	Cifrado de la información	0	1	2
		0	**1**	**2**

Anexo N°14: Formato encuesta de juicio de expertos para la valoración del modelo de gestión de riesgo

CUESTIONARIO PARA VALIDACIÓN DEL MODELO DE GESTIÓN DE RIESGOS BASADOS EN LA NORMA ISO/IEC 27005 Y METODOLOGÍA MAGERIT PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN EL HOSPITAL REGIONAL DE LAMBAYEQUE

ETAPA	ACTIVIDAD	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA	OBSERVACIONES
Identificación	Identificar y tipificar los activos de la información					
	Valorar las dimensiones de los activos de la información					
	Priorizar los activos de la información					
	Identificar amenazas de los activos de la información					
	Identificar amenazas de la información					
Análisis y evaluación	Priorización de amenazas según el nivel de riesgo					
	Estimar el nivel de riesgo inherente					
	Definir Impacto derivado de la materialización de las amenazas					
	Definir Probabilidad de materialización de las amenazas					
Tratamiento	Proponer mecanismos de protección					
	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección					
	Definir la probabilidad residual de materialización de amenazas					
	Definir Impacto residual de materialización de amenazas					
	Estimar el nivel de riesgo residual					
Seguimiento y monitoreo	Definir criterios para obtener el nivel de eficiencia de los mecanismos de protección					
	Definir la probabilidad residual de materialización de amenazas					
	Definir Impacto residual de materialización de amenazas					
	Estimar el nivel de riesgo residual					