UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE CIENCIAS DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO

PRESENTADA PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

Autores:

Céspedes Vega Charles Richard

Rivera Barboza Darwin Jair

Asesor:
Mg, Enrique Santos Nauca Torres

Línea de Investigación:

Desarrollo y gestión de los sistemas de información

Chiclayo – Perú

2020

Firma del asesor y jurado de tesis

_____
Mg. Enrique Santos Nauca Torres
ASESOR

_____
Ing. Jorge Tomás Cumpa Vásquez
PRESIDENTE

_____
Mg. Cilenny Cayotopa Ylatoma
SECRETARIO

_____
Mg. Enrique Santos Nauca Torres
VOCAL

Dedicatoria

Dedico, esta tesis a Dios, quien me bendice día a día

A mis padres, quienes se esfuerzan por darme lo mejor y por su apoyo incondicional.

Céspedes Vega Charles Richard

Dedico este trabajo a mi familia y seres queridos por estar siempre conmigo brindándome su apoyo en todo este largo y difícil camino.

Rivera Barboza Darwin Jair

Agradecimientos

Agradezco a dios, a mis padres quienes siempre me han apoyado incondicionalmente Asimismo, a mi asesor por su apoyo a la elaboración de este proyecto.

Céspedes Vega Charles Richard

Agradezco a Dios por cada una de las bendiciones que me ha regalado y ha estado siempre presente en mi vida, por mi familia, amigos y por cada una de las personas que ha puesto en mí camino para enseñarme algo nuevo.

Rivera Barboza Darwin Jair

Resumen

Los negocios implementan tecnologías de la información como soporte a los procesos que desarrollan diariamente; por tal motivo, se presenta la necesidad de implementar mecanismos de seguridad con el objetivo de asegurar la continuidad de los procesos básicos del negocio.

La presente investigación fue descriptiva, planteando como objetivo elaborar un modelo de gestión de riesgos de tecnologías de información basada en el estándar ISO 27005 y en la metodología MagerIT para el Hospital Privado Juan Pablo II de la ciudad de Chiclayo. El modelo consideró las principales etapas de la gestión de riesgos de tecnologías de información, en el que se incluyen el análisis de riesgos y el tratamiento de los riesgos. El proyecto se justificó por su aporte a la seguridad de los activos de información y el uso de la tecnología, permitiendo un mejor aprovechamiento de las ventajas que brindan en la productividad de las empresas

Finalmente, el modelo fue evaluado mediante el juicio de tres expertos que determinaron que el modelo propuesto permitió identificar y evaluar los escenarios de riesgos de tecnologías de información a los que está expuesto el hospital, calificándolo en un nivel aceptable.

Palabras clave: Riesgos, Tecnología de Información, MagerIT, Tolerancia al riesgo, ISO 27005.

Abstract

Companies implement information technologies to support the processes developed daily; for this reason, there is a need to implement security mechanisms in order to ensure the continuity of the basic flow of the business.

The present investigation was descriptive. The objective was defined to develop an information technology risk management model based on the ISO 27005 standard and the MagerIT methodology for the Juan Pablo II Private Hospital in the city of Chiclayo. The model considered the main stages of information technology risk management, including risk analysis and treatment. The project was justified for its contribution to the security of information assets and the use of technology, allowing a better use of the advantages that they offer in the productivity of companies.

Finally, the model was evaluated through the judgment of three experts who determined that the proposed one allowed identifying and evaluating the information technology risk scenarios to which the hospital is exposed, rating it to an acceptable level.

Keyeords: Risks, Information Technology, MagerIT, Risk Tolerance, ISO 27005

Índice

Índice de tablas

Índice de figuras

I. Introducción

En la actualidad las instituciones soportan sus procesos de negocio sobre una infraestructura tecnológica cada vez más cambiante, debido a los avances tecnológicos. Las empresas valoran cada vez más el papel que juegan las tecnologías de la información en el día a día de sus actividades (Ahmad, Maynard, & Park, 2014). Sin embargo, la incorporación de la tecnología de información como soporte en los procesos de negocio tiene como consecuencia necesidades de gobierno y gestión de este recurso, así como nuevos riesgos de seguridad que deben controlarse para asegurar la continuidad del negocio y la disponibilidad e integridad de la información.

Para Johnston y Warkentin (2010) dentro del clima de los negocios modernos, las organizaciones normalmente sufren de amenazas a sus datos, a la infraestructura de tecnología de la información y a la informática personal.

Es así que, para controlar estos riesgos, las empresas implementan estrategias de seguridad de la información mediante el establecimiento de un marco global que permita su desarrollo e institucionalización. Por tanto, la seguridad de la información tiene un papel muy importante en el apoyo a las actividades de la organización.

La seguridad de la información para Susanto (2012) significa proteger la información y los sistemas de información del acceso, uso, divulgación, alteración, modificación, lectura, inspección, grabación o destrucción no autorizada.

Es necesario implementar una metodología para la gestión de riesgos de Tecnologías de Información, existen numerosas metodologías para la gestión de riesgos de TI, como MagerIT, RiskIT, Octave, CobIT, etc. También existen estándares como la familia ISO 27000 e ISO 20000, que se utilizan en la gestión de riesgos de TI. Sin embargo, sus procedimientos o no son adecuadas para el tamaño de infraestructura de TI o no son adecuados para el grado de madurez de TI de las instituciones o su implementación requiere fuertes inversiones o simplemente no cuentan con herramientas flexibles y adecuadas al tipo de organizaciones de nuestro país, y específicamente a las del sector de salud.

El Hospital Privado Juan Pablo II de ciudad de Chiclayo, es una institución privada de salud que cuenta con una División de Tecnologías de la Información encargada de los servicios de instalación de software y atención de cambios de los sistemas informáticos en producción, a través de su división de desarrollo, y la de atención de incidentes y puesta en producción de las nuevas unidades de software mediante la Unidad de Soporte Técnico. El proyecto tuvo como objetivo elaborar un modelo de gestión de riesgos de tecnologías de información basado en la ISO/IEC 27005 para mitigar los riesgos operacionales en

tecnologías de información en el Hospital Privado Juan Pablo II, y como objetivos específicos (1) realizar el diagnóstico de los niveles de exposición a los riesgos de TI de los activos de TI de los procesos del hospital, (2) elaborar el modelo de gestión de riesgos operacionales en tecnologías de información, (3) evaluar el cumplimiento de los indicadores de calidad para un modelo de evaluación propuesto teniendo como referencia la ISO 27005 y (4) Validar el modelo elaborado con la opinión de expertos en la base del cumplimiento de los requisitos exigidos en los Lineamientos de Política de Seguridad de la Información basado en ISO/IEC 27005 y la metodología MagerIT

Los incidentes relacionados con el uso de las TI en el hospital Juan Pablo II cada vez son más frecuentes, y este servicio actualmente se brinda acudiendo directamente a cada una de las áreas del hospital en los que se ha generado el incidente. Esta metodología de trabajo está generando retrasos en el trabajo dentro del área de TI y elevando los costos para recuperar el normal funcionamiento de los sistemas del hospital.

La tesis formuló como pregunta de investigación ¿De qué manera un modelo de gestión de riesgos de tecnologías de información, basada en la ISO/IEC 27005 y permitiría mitigar los riesgos operacionales en el Hospital Privado Juan Pablo II de la ciudad de Chiclayo?

II. Marco teórico

2.1. Antecedentes del problema

De la revisión literaria, se describe a continuación los antecedentes tomados como referencia para el estudio, los que servirán de guía en el desarrollo de tesis

Antecedentes Internacionales

Arciniegas Duarte (2017) en su investigación titulada *"Análisis de riesgos en la empresa bilateral Call Center sede Bogotá bajo la metodología Magerit V3",* tuvo como objetivo identificar, analizar y evaluar los riesgos que se presentan en los activos de información en la compañía Bilateral Call Center sede Bogotá durante el año 2016, evaluando el nivel de madurez de la compañía bajo un marco de referencia que en este caso es la metodología Magerit V3, como medida de solución a los riesgos en activos de información. Riesgos que provocan pérdidas significativas en el negocio y para su control existen procesos que ayudan a reducir la materialización de éstos, ayudando a conservar la disponibilidad, integridad y confidencialidad de estos activos de información. Concluyendo en tener en cuenta la falta de implementación de sistemas de gestión de seguridad de la información y ausencia de documentación, se observa la posibilidad de brindar una

perspectiva para adentrarse de una manera cualitativa sobre los impactos que los riesgos podrían originarse en la compañía.

Gaona (2013) en su tesis titulada "*Aplicación de Metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito SA en la ciudad de Machala*" propone analizar los procesos que actualmente se realizan en la empresa, los activos que tiene y la identificación de las carencias de seguridad que existan. Se utiliza la metodología MAGERIT como referencia de una serie de pasos estructurados para el análisis y la gestión de riesgos. Concluyendo en que la empresa tendrá un documento encaminado a la seguridad, que será el inicia en la creación de normas de seguridad informática para recursos de información y en conjunto con toda la organización.

Ramiro Olmedo (2019) en su investigación titulada "*Metodología para la implementación de un sistema de gestión de seguridad de la información ISO/IEC 270001: para soporte de áreas de admisión y atención de un hospital público*" propone analizar la manera de obtener y propone una metodología que sea aplicable, desde el punto de vista práctico y de su posible adaptación local al momento de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) ISO/IEC 27001 para hospitales públicos en Ecuador, a partir de metodologías existentes en instituciones similares y otras verticales de la industria. como objetivo se planteo130.0.50.15, se revisó y ponderó la importancia que tienen las TICs en el soporte a los procesos internos que tienen los hospitales en sus diversas áreas y, por otro lado, se analizó la necesidad de políticas y procedimientos de seguridad informática y de su gestión en cada proceso para proteger los recursos financieros, la información, el cumplimiento legal y otros bienes tangibles e intangibles que permitan también salvaguardar la gestión interna de todas las áreas

Según Patiño Rosado (2018) en su estudio titulada "*Propuesta metodológica de gestión de riesgos de Tecnología de información y comunicación (TIC) para entidades públicas conforme normativa NTE INEN ISO/IEC 27005*", cuyo propósito es determinar la implementación de la norma ISO/IEC 27001:2005, en respuesta a los continuos ataques y delitos informáticos que se presentaron en la Secretaría Nacional de Administración Pública. En este trabajo se elaboró una guía metodológica práctica para la gestión de riesgo de tecnologías de información en entidades del sector público conforme la normativa NTE INEN ISO/IEC 27005 para mejorar la administración de la seguridad de la información. Se aplicó la técnica encuesta, a través de un cuestionario a 18 jefes de área de tecnología de las entidades públicas ubicadas en la ciudad de Esmeraldas, obteniendo resultados,

principalmente que, a pesar de la incorporación de la normativa internacional es todavía complejo el proceso debido en los estándares fueron creados para empresas desarrolladas en otro contexto. En respuesta, se propone la guía detallada en la cual se desarrolla cada etapa con su conjunto de actividades, y su aplicación en una entidad del sector público con la finalidad de validar cada una de las etapas previamente definidas.

Antecedentes Nacionales

García (2017) en su investigación titulada "*Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú*", cuyo objetivo es implementar un modelo de gestión de riesgos de seguridad de la información para Pymes, integrando la metodología OCTAVE-S y la norma ISO/IEC 27005. Se abarca el análisis de las metodologías y normas de gestión de riesgos, el diseño del modelo de gestión de riesgos de seguridad de la información, la validación del modelo en una Pyme en el proceso de ventas. Concluyendo en identificar los principales riesgos valorizándolos, para luego proceder a un tratamiento de acuerdo a las necesidades de la empresa. Este modelo ayuda en la gestión de riesgos de seguridad de la información dentro de las Pymes, para poder reducir el impacto de riesgos a los que pueden estar expuestas.

Cueva Paul (2017) En su tesis denominada "*Gestión de la historia clínica y la seguridad de la información del hospital II Cajamarca-ESSALUD bajo la NTP-ISO/IEC 27001:2014* ". Las Instituciones que prestan servicios de Salud cuentan con su principal activo de información la Historia Clínica que al ser un documento médico-legal y que tiene que ver con los procesos de atención de los pacientes y el Seguro Social de Salud – EsSalud cuenta con una norma a nivel nacional para cumplimiento en todos sus centros asistencial sobre Gestión de la Historia Clínica en los Centros Asistenciales del Seguro Social de Salud – ESSALUD del año 2014. La hipótesis planteada para esta investigación es que la dimensión Administrativa de la Gestión de la Historia Clínica es la más relevante en la Seguridad de la Información, es por eso que el objetivo busca aplicar una evaluación normativa a la Gestión de las Historias Clínicas y la evaluación de las cláusulas y controles necesarios para la Seguridad de la Información para analizar las características de estos dos aspectos .Se realiza unas recomendaciones para establecer los mecanismos necesarios para fortalecer la seguridad de la información y proteger los activos relacionados al proceso de la Gestión de las Historias Clínicas, que son el pilar de futuras investigaciones que complementen la Seguridad de la Información y que son el Análisis de Riesgos y la Continuidad del Negocio.

En su investigación Sotelo Bedón (2019) titulada "*Un proceso práctico de análisis de Riesgos de Activos de Información*" Con la finalidad de presentar un proceso de análisis de

riesgos de activos de información en el contexto de un Sistema de Gestión de Seguridad de Información (SGSI) alineado al estándar ISO/IEC 27001:2005 y un software (prototipo) que le brinda soporte, aunado a un portal cuyo contenido tiene por finalidad sensibilizar en gestión de riesgos y seguridad de información. Este proceso sigue los lineamientos de los principales estándares y buenas prácticas en gestión de riesgos y seguridad de la información, y viene siendo aplicado en el país en los últimos cinco años. Teniendo resultados satisfactorios, lo cual nos permite inferir que el proceso en mención es factible de aplicarse en las demás organizaciones del sector, en un contexto donde existe la necesidad cada vez mayor de implantar un SGSI.

Antecedente local

Guevara Chumán (2015) en su tesis titulada "*Aplicación de la metodología MagerIT para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruíz Gallo*" tiene como finalidad brindar un plan de mitigación de riesgos basado en las medidas de seguridad ya implementadas en el área de administración de servidores - Red Telemática aplicando la metodología MagerIT. Concluyendo en que los servidores están expuestos a un riesgo critico mediante amenazas como: Caída del sistema por agotamiento de recursos, Avería de origen físico o lógico, Corte del suministro eléctrico, Condiciones inadecuadas de temperatura o humedad, Robo de equipos, Perdida de equipos, errores del administrador del sistema/ seguridad, Desastres naturales, a pesar de las medidas ya tomadas por la administración del área de red-telemática. Lo cual sustenta la problemática expuesta y la importancia del desarrollo de la temática. Los servidores permiten la funcionalidad y generación del servicio de gestión académica.

Baca Flores (2016) en su tesis titulada "*Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local – Chiclayo*", se tuvo como objetivo diseñar un Sistema de Gestión de Seguridad de la Información para la Unidad de Gestión Educativa Local de Chiclayo, basado en las normas internacionales ISO/IEC 27001:2013 e ISO/IEC 27002:2013, y la metodología empleada para el análisis y evaluación de riesgos, se basó principalmente en MAGERIT v.3.0. Concluyendo que el Sistema de Gestión de Sistemas de Información permitió mejorar la situación actual que vive la Unidad de Gestión Educativa Local de Chiclayo en materia de seguridad de la información, ya que la utilización de estándares internacionales y buenas prácticas, repercutió directamente en una efectiva gestión de la información dentro del hospital objeto de estudio, garantizando el cumplimiento de los principios básicos de seguridad: integridad,

disponibilidad, confidencialidad, trazabilidad y autenticidad, debido a que las medidas de control implementadas, para satisfacer los requisitos mínimos de seguridad, fuero efectivas.

Alcántara Flores (2015) en su investigación titulada "*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*", cuyo propósito se enfocó en la elaboración de una guía para la implementación de la seguridad basada en la norma ISO/IEC 27001, que ayude a brindar seguridad a los sistemas de información en la institución Policial Comisaria del Norte de la ciudad de Chiclayo. Se utilizaron técnicas de recolección de datos tales como encuestas, entrevistas, fichas de observación, como medio para poder extraer la información y de esta manera medir la realidad problemática apoyado en el uso de la Norma ISO/IEC 27001. Cuyo resultado logro determinar las deficiencias para mejorar los niveles de seguridad y confiabilidad en los sistemas de información de dicha institución. Al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación se logró incrementar los procedimientos utilizados en favor de la Institución permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. Con el 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, esto manifestado en un plan adecuado para abordarlos y tomar las precauciones necesarias que minimicen sus impactos.

2.2. Bases teórico-científicas

2.2.1. Sistema de gestión de seguridad de la información

Para Miguel Pérez (2016) la seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma.

Mientras que 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.

El Sistema de Gestión de Seguridad de la Información por sus siglas SGSI es 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. Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

El Sistema de Gestión de Seguridad de la Información está conformado por Registros y evidencias, Instrucciones y técnicas de seguridad, Procesos de Seguridad, y finalmente Políticas de Seguridad.

Figura 1: Estructura de un SGSI

Fuente: ISO 27001

- Las políticas de seguridad proporcionan las líneas maestras de actuación en cada caso. Además de la Política de Seguridad de alto nivel del SGSI podemos apoyarnos en políticas específicas que desarrollan temas particulares y a los cuales podemos hacer referencia en el mismo documento de alto nivel.

- Procesos de seguridad definidos específicamente para mejorar la eficacia y la eficiencia de las tareas de la Seguridad de la información. El objetivo es gestionar responsablemente el riesgo que entraña para la seguridad de la información en relación con los tipos de tecnologías que eligen implementar, interpretando tecnología en sentido amplio de la palabra.
- Técnicas de seguridad como Instrucciones, checklists y formularios, documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.
- Registros incluye documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información.

Figura 2: Fases de un SGSI

Fuente: ISO 27001

Las fases son las siguientes:

- Fase de planificación: en ella se organiza el plan de trabajo y se establecen los objetivos de la seguridad de la información. Para elegir los controles adecuados de seguridad, se basa en un catálogo de 133 posibles controles.

- Fase de implementación: esta fase implica la realización de todo lo planificado en la fase anterior.
- Fase de revisión: el objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos "canales" y verificar si los resultados cumplen los objetivos establecidos.
- Fase de mantenimiento y mejora: el objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

2.2.2. Sistema de gestión de riesgos

De acuerdo a ISACA (2009) en los Lineamientos para la Gestión de Seguridad de Tecnologías de Información publicadas por la Organización Internacional de Estandarización (ISO) en su (ISO/IEC PDTR 13335−1), riesgo es el potencial de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y, por consiguiente, ocasione pérdida o daño a la organización.

Según Alejandro Medina (2007) riesgo se define como la probabilidad de que las amenazas exploten los puntos débiles, causando pérdidas o daños a los activos e impactos al negocio, es decir, afectando: La confidencialidad, la integridad y la disponibilidad de la información

En términos generales la gestión del riesgo se refiere a los principios y metodologías para la gestión eficaz del riesgo, mientras que gestionar el riesgo se refiere a la aplicación de estos principios y metodologías a riesgos particulares (Espinoza Aguinaga, 2013).

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 y Echeverry, 2010).

Para implementar un Sistema de Gestión de Riesgos se desarrollan las siguientes actividades:

- Planificación: En esta etapa se definirá cuáles son las áreas encargadas y quiénes son los responsables de cada rol, se hablará del plan que se busca implementar, de qué manera se realizará y cómo será su funcionamiento. Además, se creará una

guía que permitirá que todos los empleados de la compañía puedan entender cuál será el funcionamiento y cómo estarán involucrados, pues es importante saber que esto es un trabajo en equipo, esto es lo que garantizará el éxito de lo propuesto.

- Identificar los riesgos: Se reconocerá cuáles son los principales riesgos a los que está expuesta la organización, una vez estos se definan, se plantearán otros secundarios que podrían también generar ciertos desajustes dentro de la empresa y a los objetivos propuestos. Una vez estén establecidos, cada una de las áreas encargadas los asumirá como propios, para que de esta manera puedan ejecutar el plan que se va a llevar a cabo.

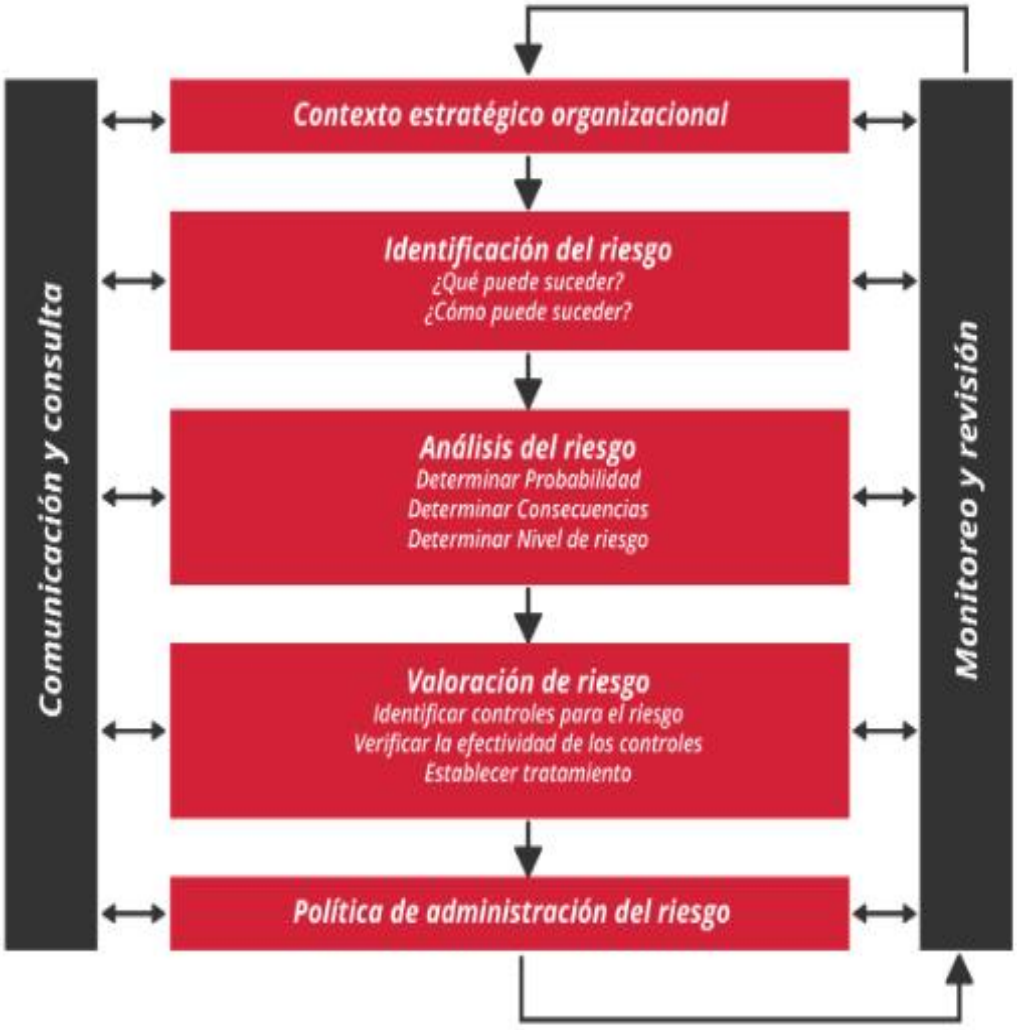


Figura 3: Pasos para implementar un Sistema de Gestión de Riesgos
Fuente: (Caso, 2019)

- Análisis: Luego de que estén definidos y consignados los riesgos se valorará en que escala se determinaran y cuáles serán las actividades de control que se ejecutarán, esto con el fin de identificar el impacto que causará. Esto permitirá

crear un mapa de riesgos el cual servirá como guía para priorizar los riesgos, clasificarlos en una escala de uno a diez, siendo diez el más alto y uno el más bajo, identificar el área encargada y cuál es el plan de acción que deben poner en práctica.

- Implementación: Después de que se hayan identificado, clasificado y elegido a los responsables de cada riesgo, se evaluarán las acciones que se van a hacer para mitigar los daños en caso de que se llegue a presentar alguno de los anteriormente identificados.
- Monitoreo: Es importante tener revisiones periódicas que harán saber y entender si los planes de acción que se han implementado en cada uno de los riesgos son los correctos, esto ayudará a entender si la tarea se está haciendo bien y trayendo resultados positivos, o si por el contrario se debe mejorar y en algunos casos cambiar.

2.2.3. Tolerancia al riesgo

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 define la tolerancia al riesgo 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.

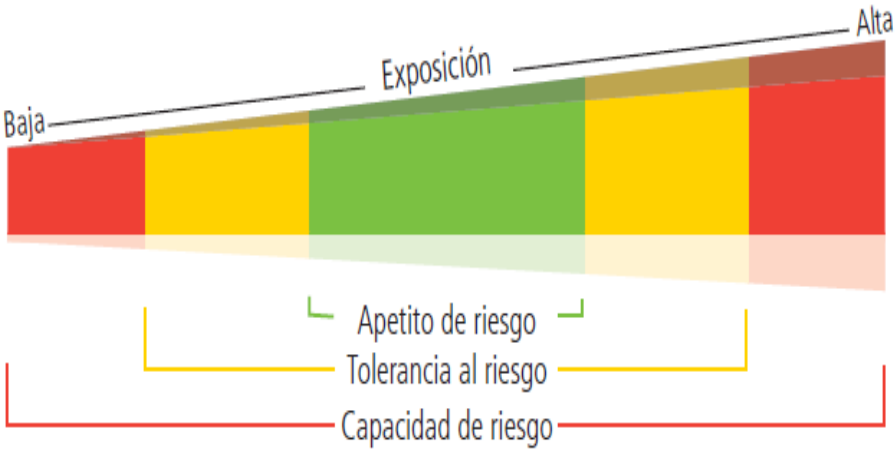


Figura 4: Relación entre apetito, tolerancia y capacidad de riesgo

Fuente: Buenas Prácticas en Gestión de Riesgo. Fábrica del Pensamiento

Las brechas de la seguridad muestran las vulnerabilidades importantes dentro de una institución, porque deja la puerta abierta 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.

2.2.4. Riesgo

Un riesgo es cualquier tipo de evento o circunstancia que de ocurrir amenazarían los objetivos de una organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad (INDECOPI, 2007).

Halvorson (2008) explica tres naturalezas del riesgo, estos son: los riesgos estratégicos, tácticos y operacionales.

- Los riesgos estratégicos son los que están vinculados a la seguridad de la información; sin embargo, se encuentran enfocados a los riesgos de las ganancias e imagen de la organización, lo cual se derivan de decisiones estratégicas que han sido realizadas por la organización.
- Los riesgos tácticos son los asociados a los sistemas que vigilan la identificación, control y monitoreo de los riesgos que afectan a la información, son aquellos que afectan indirectamente a la información.
- Los riesgos operacionales son los relacionados a aquellos activos que pueden afectar los objetivos de una empresa (tales como presupuestos, cronogramas y tecnologías).

Para Tipton, Krause y Ozier (2006) existen algunas interrogantes claves que los dueños de los activos dar respuesta a la identificación relevante del daño o pérdida producido por un riesgo, estos son:

- ¿Qué puede suceder? (¿Cuál es la amenaza?)
- Si sucede, ¿qué tan malo puede ser? (¿Cuál es el impacto?)
- ¿Qué tan seguido puede suceder? (¿Cuál es la frecuencia?)
- ¿Qué tan ciertas son las respuestas a las tres primeras preguntas? (¿Cuál es el grado de confianza?)

2.2.5. Metodologías para gestión de riesgos

Algunas de las metodologías en gestión de riesgos más destacadas internacionalmente son:

- ISO 31000: Esta una norma internacional que abarca pautas para las buenas prácticas en la gestión de riesgos. Esta guía de implementación está codificada por la International Organization for Standardization. Su proceso se caracteriza por la identificación, análisis, evaluación, tratamiento, comunicación y seguimiento de cualquier tipo de riesgo que afecte a la empresa.
- ISO 27005: Es una norma internacional con recomendaciones y directrices generales para la Gestión de Riesgos con respecto a la seguridad de la

información, siguiendo los requisitos de ISO 27001. No recomienda una metodología de gestión de riesgos concreta, pero puede ser de utilidad para elaborar una propia atendiendo a diversos factores y al Sistema de Gestión de Seguridad de la Información (SGSI).

- MAGERIT: Es una metodología desarrollada por el Consejo Superior de Administración Electrónica en España. Consta de los volúmenes de método, catálogo de elementos para aplicar la metodología y guía de técnicas a usar en las diferentes fases de la Gestión de Riesgos.
- OCTAVE. Esta metodología reconocida internacionalmente está desarrollada por el Software Engineering Institute (SEI). Octave proporciona un conjunto de criterios a partir de los cuales se pueden desarrollar distintas metodologías. Está compuesta de las fases de visión de organización, visión tecnológica y planificación de medidas y reducción de los riesgos.
- NIST 800-30. Esta metodología desarrollada por el National Institute of Standards and Technology tiene reconocimiento internacional y busca asegurar a los sistemas de información. Sus pasos básicos para la gestión de riesgos son la caracterización del sistema, identificación de amenazas y vulnerabilidades, control de análisis, determinación del riesgo, análisis de impacto, determinación del riesgo, recomendaciones de control y resultado de la implementación o documentación.
- CRAMM. Tiene reconocimiento internacional y está desarrollada por el Central Computer and Telecommunications Agency (CCTA). Su desarrollo consta de identificación y valoración de activos, valoración de amenazas y vulnerabilidades y selección de contramedidas.

2.3. Definición de términos básicos

- Activo de TI: Son los recursos tecnológicos con los que toda empresa cuenta para agilizar su gestión. Se utilizan para lograr objetivos de negocio, y se dividen en activos tangibles e intangibles. (Marquina, 2012)
- Apetito al Riesgo: Es el nivel de exposición al riesgo que una organización se encuentra dispuesta a aceptar, con los cuales opera sin problemas. (Marquina, 2012)
- Capacidad al Riesgo: Es el nivel máximo de riesgo que una empresa puede soportar. (Marquina, 2012)

- Control: Es la función que consiste en medir y corregir el desempeño individual y organizacional para asegurar que los hechos se ajusten a los planes y objetivos planteados. Implica medir el desempeño contra las metas y los planes, muestra donde existen desviaciones con los estándares y ayuda a corregirlas. (Espiñeira, 2008)
- COSO: Committee of Sponsoring Organizations of the Treadway es una Comisión voluntaria constituida por representantes de cinco organizaciones del sector privado en EEUU, para proporcionar liderazgo intelectual frente a tres temas interrelacionados: la gestión del riesgo empresarial (ERM), el control interno, y la disuasión del fraude. (Espiñeira, 2008)
- ISO: La Organización Internacional de Normalización, también llamada Organización Internacional de Estandarización es una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización. (ISO, 2011)
- NIST: El Instituto Nacional de Estándares y Tecnología tiene por objetivo promover la innovación y la competencia industrial en Estados Unidos mediante avances en metrología, normas y tecnología de forma que mejoren la estabilidad económica y la calidad de vida. (NIST, 2001)
- SEI: Instituto de Ingeniería de Software fundado por el Congreso de los Estados Unidos en el año 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software, que dieran respuesta a los problemas que generaba al ejército estadounidense la programación e integración de los sub-sistemas de software en la construcción de complejos sistemas militares. (SEI, 1984)
- Tolerancia al Riesgo: Límite 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. (Marquina, 2012).

2.4. Formulación de la hipótesis

¿Un modelo de gestión de riesgos de tecnologías de información, basada en la ISO/IEC 27005 permite mitigar los riesgos operacionales en el Hospital Privado Juan Pablo II de la ciudad de Chiclayo?

III. Materiales y métodos

3.1. Variables - operacionalización

Variables

Independiente: Modelo de gestión de riesgos de tecnologías de información basado en la ISO/IEC 27005 y MagerIT

Dependiente: Riesgos operacionales

Operacionalización

Tabla 1 - *Variable Independiente: Modelo de gestión de riesgos de tecnologías de información*

Variable	Dimensión	Indicador	Ítem	Técnica/ Instrumento
Modelo de gestión de riesgos de tecnologías de información basado en la ISO/IEC 27005 y MagerIT	Suficiencia del modelo	Nivel en que los aspectos considerados en la actividad o tarea son suficientes para obtener la medición o calificación de la metodología.	¿Cree usted que las características de las tareas del modelo son suficientes para obtener mediciones?	Encuesta / Cuestionario
	Claridad del modelo	Nivel en que los aspectos considerados en la actividad o tarea de la metodología se entienden fácilmente, es decir, su sintáctica y semántica son adecuadas.	¿Cree usted que las actividades del modelo se entienden fácilmente?	
	Coherencia del modelo	Nivel en que los aspectos considerados en la actividad o tarea de la metodología tienen una relación lógica con el objetivo o meta que se quiere lograr con la propuesta.	¿Cree usted que las actividades del modelo guardan relación lógica con el objetivo de gestión de riesgos de TI?	

	Relevancia del modelo	Nivel en que los aspectos considerados en la actividad o tarea son esenciales o importantes, para lograr los objetivos de la metodología propuesta	¿Cree usted que las actividades del modelo son importantes para lograr el objetivo de gestión de riesgos de TI?	

Fuente. Propia

Tabla 2 – *Riesgos operacionales*

Variable	**Dimensión**	**Indicador**	**Ítem**	**Técnica/ Instrum.**
Riesgos operacionales	Seguridad	Políticas. Normas.	1. ¿Existe un sistema de gestión de la seguridad de la información en el hospital? 2. ¿Cree usted que el hospital logrará una mejora significativa con la aplicación de un SGSI? 3. ¿En el hospital se ha categorizado la información de acuerdo al grado de importancia que esta tiene? 4. ¿El personal del hospital ha recibido capacitación sobre seguridad de la información de acuerdo a su función? 5. ¿El personal del hospital cuenta con una clave de acceso para ingresar a su computadora? 6. ¿Cada oficina cuenta con software antivirus actualizado?	Encuesta / Cuestionario

Riesgo	Conocimientos de seguridad. Parámetros.	7. ¿Se ha realizado una evaluación de riesgos relacionados con la información? 8. ¿Se ha realizado una evaluación de vulnerabilidades de la red? 9. ¿Se realizan copias de seguridad para proteger su información? 10. ¿Las oficinas están protegidas contra amenazas externas o ambientales que ocasionen pérdidas de información?

Fuente. Propia

3.2. Tipo de estudio, diseño de investigación o de contrastación de hipótesis

Tipo de estudio

Aplicada porque se elaborará un modelo de gestión de riesgos de tecnologías de información, aplicando los fundamentos teóricos y buenas prácticas de los marcos de referencia ISO/IEC 27005 y la metodología MagerIT, al caso específico del Hospital Privado Juan Pablo II.

El producto de la investigación aplicada es el modelo de gestión de riesgos de tecnologías de información

Diseño de contrastación

El diseño de estudio es Experimental, porque se medirá el efecto de la variable independiente, sobre la variable dependiente. El modelo de gestión de riesgos elaborado por esta investigación será validado por juicio de expertos.

3.3. Población, muestra de estudio y muestreo

Población

Según Tamayo y Tamayo (1997), ¨la población se define como la totalidad del fenómeno a estudiar donde las unidades de población poseen una característica común la cual se estudia y da origen a los datos de la investigación.

Como población se tomará a los tres (3) miembros expertos del Hospital Privado Juan Pablo II quienes toman las decisiones y además los registros de incidencias.

Muestra

Según Hernández, (2014) se afirma que la muestra es un subgrupo de la población de interés sobre el cual se recolectaran datos, y que tiene que definirse y delimitarse de antemano con precisión, además de que debe ser representativo de la población. La muestra será la misma población.

3.4. Métodos, técnicas e instrumentos de recolección de datos

Técnica:

- Análisis documental. Se revisarán los documentos estratégicos, administrativos y legales relacionados con la gestión de riesgos de TI de la entidad tomada como caso de estudio.
- Observación directa. Para obtener los datos necesarios que permitan evaluar cada uno de los factores considerados en la tabla de operacionalización de variables.
- Encuestas: Serie de preguntas que se hace a muchas personas para reunir datos o para detectar la opinión pública sobre un asunto determinado.

Instrumentos:

- Cuestionario, es el conjunto de cuestiones o preguntas que deben ser contestadas en un examen, prueba, test, encuesta, etc. Al finalizar la implementación del sistema, se realizará un cuestionario a los tres (3) miembros responsables de la toma de decisiones para corroborar el cumplimiento de los objetivos.
- Fichas de registro de datos: Es una herramienta que nos permite sistematizar y realizar un registro del contexto de la información. Es denominada ficha porque nos permite recopilar los datos importantes de la investigación. (López y Martel, 2001). En este caso se analizará registros de incidencias.
- Guía de observación: La guía de observación puede actuar como marco teórico. Al consultar esta guía, el observador accederá a información que le ayudará a saber cómo realizar su tarea y encuadrar su trabajo.

3.5. Plan de procesamiento para análisis de datos

Se obtendrá información a través de la encuesta de los expertos del área en TI para ser analizadas y de esta manera obtener el diagnóstico. Para el análisis e interpretación de tablas y figuras se utilizará la hoja de cálculo Excel y el Software estadístico SPSS V25.0 con la finalidad de procesar adecuadamente los datos.

Tabla 3 – *Propuesta de encuesta de Evaluación del Modelo*

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los aspectos considerados en la actividad o tarea son suficientes para obtener la medición o calificación de la metodología.	1. No cumple con el criterio	Los aspectos considerados en la actividad o tarea no son suficientes para medir la metodología.
	2. Bajo Nivel	Los aspectos considerados en la actividad o tarea permiten medir algún aspecto de la metodología, pero no corresponden con la totalidad de la actividad o tarea.
	3. Moderado nivel	Se deben incrementar algunos aspectos para poder evaluar la actividad o tarea de la metodología completamente.
	4. Alto nivel	Los aspectos considerados en la actividad o tarea de la metodología son suficientes.
CLARIDAD Los aspectos considerados en la	1. No cumple con el criterio	La actividad o tarea no está claramente establecida o definida.
	2. Bajo Nivel	La actividad o tarea requiere

actividad o tarea de la metodología se entienden fácilmente, es decir, su sintáctica y semántica son adecuadas.		significativas modificaciones para lograr su comprensión.
	3. Moderado nivel	Se requiere modificaciones muy específicas de algunos de los términos de la actividad o tarea para lograr la claridad total.
	4. Alto nivel	La actividad o tarea es clara, tiene semántica y sintaxis adecuada.
COHERENCIA Los aspectos considerados en la actividad o tarea de la metodología tienen una relación lógica con el objetivo o meta que se quiere lograr con la propuesta.	1. No cumple con el criterio	La actividad o tarea no tiene relación lógica con el objetivo perseguido.
	2. Bajo Nivel	La actividad o tarea tiene una relación tangencial con el objetivo perseguido.
	3. Moderado nivel	La actividad o tarea tiene una relación moderada con el objetivo que está midiendo.
	4. Alto nivel	La actividad o tarea se encuentra completamente relacionada con el objetivo que está midiendo.
RELEVANCIA Los aspectos considerados en la actividad o tarea son esenciales o importantes, para lograr los objetivos de la metodología propuesta.	1. No cumple con el criterio	La actividad o tarea puede ser eliminado sin que se vea afectada la medición del objetivo perseguido con la metodología.
	2. Bajo Nivel	La actividad o tarea tiene alguna relevancia, pero otra actividad o tarea puede estar asolapando o cumpliendo el objetivo de ésta.
	3. Moderado nivel	La actividad o tarea es relativamente importante para la adecuada aplicación de la metodología.
	4. Alto nivel	La actividad o tarea es muy relevante y debe ser considerada en la metodología.

Fuente. Propia

IV. Resultados

4.1. Realizar el diagnóstico de los niveles de exposición a los riesgos de TI de los activos de TI de los procesos del hospital.

4.1.1. Resultados de encuestas

Tabla 4 - *Resultados del Pre-Test*

Ítem	Pregunta	Experto 1		Experto 2		Experto 3		SI	NO
		SI	NO	SI	NO	SI	NO	%	%
1	¿Existe un sistema de gestión de la seguridad de la información en el hospital?		X		X		X	0.00	100.00
2	¿Cree usted que el hospital logrará una mejora significativa con la aplicación de un SGSI?	X		X		X		100.00	0.00
3	¿En el hospital se ha categorizado la información de acuerdo al grado de importancia que esta tiene?		X		X		X	0.00	100.00
4	¿El personal del hospital ha recibido capacitación sobre seguridad de la información de acuerdo a su función?		X		X		X	0.00	100.00
5	¿El personal del hospital cuenta con una clave de acceso para ingresar a su computadora?		X		X		X	0.00	100.00
6	¿Cada oficina cuenta con software antivirus actualizado?		X		X		X	0.00	100.00
7	¿Se ha realizado una evaluación de riesgos relacionados con la información?		X		X		X	0.00	100.00
8	¿Se ha realizado una evaluación de vulnerabilidades de la red?		X		X		X	0.00	100.00
9	¿Se realizan copias de seguridad para proteger su información?		X		X		X	0.00	100.00

10	¿Las oficinas están protegidas contra amenazas externas o ambientales que ocasionen pérdidas de información?	X	X	X	0.00	100.00

Fuente. Propia

Con respecto a las encuestas realizadas, la tabla 4 presenta un consolidado de los resultados obtenidos. Se indica que todos, el 100%, coinciden en que el hospital logrará una mejora significativa con la aplicación de un SGSI. Luego, en todos los casos siguientes, el 100% de encuestados indica que no existe un sistema de gestión de la seguridad de la información en el hospital y que el hospital no ha categorizado la información de acuerdo al grado de importancia que ésta tiene. Asimismo, ese mismo 100%, afirma que el personal del hospital no ha recibido capacitación sobre seguridad de la información de acuerdo a su función ni cuenta con una clave de acceso para ingresar a su computadora.

Por otro lado, el 100% indica que cada oficina no cuenta con software antivirus actualizado ni están protegidas contra amenazas externas o ambientales que ocasionen pérdidas de información.

También indican que no se ha realizado una evaluación de riesgos relacionados con la información ni de vulnerabilidades de la red.

Finalmente, todos, afirman que no se realizan copias de seguridad para proteger su información.

4.1.2. Fase 1: Identificación de los escenarios de riesgos de TI

Objetivo: identificar los diferentes escenarios de riesgos a los que está expuesto el hospital.

Para cumplir con el objetivo de esta fase, se desarrollaron las siguientes actividades generales:

4.1.2.1. Identificación y clasificación de los activos de TI

Identificar los activos de TI que dan soporte a los procesos del hospital para luego clasificarlos. Los activos se clasifican utilizando la tabla del Anexo 01.

Los principales activos de TI identificados se muestran en la tabla siguiente:

Tabla 5 – *Activos de TI identificados*

N°	Tipo de activo	Activo
1	Aplicaciones	Aplicación informática para hospitales
2	Aplicaciones	Software para desarrollo
3	Comunicaciones	Red de computadoras
4	Datos o documentos	Código fuente de los programas
5	Datos o documentos	Actas de conformidad
6	Datos o documentos	Actas de requerimientos informáticos
7	Datos o documentos	Actas de control de cambios de las aplicaciones
8	Información	Bases de datos
9	Información	Respaldo de documentos normativos y de gestión
10	Instalaciones	Centro de Procesamiento Central
11	Personal	Personal de área de tecnologías de información
12	Personal	Personal de área analistas de sistemas
13	Servicio	Servidor principal de dominio
14	Servicio	Servidor principal de base de datos y aplicaciones

Fuente. Propia

4.1.2.2. Valorización del nivel de criticidad de los activos de TI

Para cada activo se valora su importancia desde que tanto se afectaría cada una de las dimensiones de seguridad de la información (Confidencialidad, Integridad y Disponibilidad) si es que éstos son afectados por un escenario de riesgo determinado. Los valores se obtienen aplicando cuestionarios y reuniones de equipo con el personal responsable de la información en el hospital, mediante la ponderación de cada dimensión de seguridad. Se utiliza la tabla del Anexo 02

Tabla 6 – *Valoración del nivel de criticidad de los activos de TI*

N°	Activo	Dimensión de seguridad			Nivel de criticidad	Descripción de la criticidad
		C	I	D		
1	Aplicación informática para hospitales	4	5	4	4	Alto
2	Software para desarrollo	5	5	5	5	Muy Alto
3	Red de computadoras	4	2	4	3	Medio
4	Código fuente de los programas	3	2	5	3	Medio
5	Actas de conformidad	5	5	5	5	Muy Alto
6	Actas de requerimientos informáticos	5	5	5	5	Muy Alto
7	Actas de control de cambios de las aplicaciones	4	2	3	3	Medio
8	Bases de datos	5	5	5	5	Muy Alto
9	Respaldo de documentos normativos y de gestión	4	5	4	4	Alto
10	Centro de Procesamiento Central	3	2	4	3	Medio
11	Personal de área de tecnologías de información	3	2	5	3	Medio
12	Personal de área analistas de sistemas	3	2	5	3	Medio
13	Servidor principal de dominio	4	4	5	4	Alto
14	Servidor principal de base de datos y aplicaciones	4	5	4	4	Alto

Fuente. Propia

4.1.2.3. Identificación de amenazas por activo de TI

Por cada activo de TI del hospital se analiza el entorno en el cual se utilizan, así se identifican potenciales amenazas que pueden afectarlos parcial o totalmente.

Las principales amenazas por activo de TI se muestran en la siguiente tabla:

Tabla 7 – *Listado de amenazas por tipo de activo de TI*

N°	Activo	Amenaza
1	Aplicación informática para hospitales	Imposible acceder a los servicios de red del hospital, lo cual detiene la ejecución de actividades y procesos.
2	Software para desarrollo	Modificación en datos de los pacientes, generando pérdida de datos personales o historia médica
3	Red de computadoras	Se detienen los servicios de red
4	Código fuente de los programas	Daño intencionado a las instalaciones del hospital
		Se pierde los activos de tecnología de información en la sala de servidores
5	Actas de conformidad	Se pierde información de la empresa por accesos no permitidos a la base de datos
		Insuficiente espacio de almacenamiento
6	Actas de requerimientos informáticos	Se pierde información importante por falta de seguridad en los dispositivos de almacenamiento.
7	Actas de control de cambios de las aplicaciones	Fuga de talentos que genera retraso en las actividades y pérdida de información
		Cambios, divulgación y eliminación de la información
8	Bases de datos	Falla en los equipos de cómputo que dan soportan a las operaciones del negocio
9	Respaldo de documentos normativos y de gestión	Se pierde la correlación del código fuente de la versión existente en producción.
		Se pierde información de datos personales e historia médica por manipulación de código fuente para beneficio del trabajador
10	Centro de Procesamiento Central	Instituciones supervisoras realizan observaciones a los procesos de producción no sustentados.
11	Personal de área de tecnologías de información	Se pierde información lo cual no permite el cumplimiento del desarrollo de requerimientos.
12	Personal de área analistas de sistemas	El tiempo de desarrollo excede el cronograma de actividades.
		Fuga de información sensible por medio de correo electrónico
		Se pierden recursos a causa de puesta en funcionamiento no acordes a metodología y estándares de desarrollo de software del hospital
13	Servidor principal de dominio	Se pierden recursos por virus informáticos
14	Servidor principal de base de datos y aplicaciones	Imposible revertir las adecuaciones en los sistemas.

Fuente. Propia

4.1.2.4. Identificación de vulnerabilidades por activo de TI

Por cada amenaza de activo de TI se analiza las deficiencias, debilidades y carencias que tiene el hospital en los diferentes procesos de TI relacionados a los activos de TI. Finalmente se determinan cuáles son las debilidades del hospital que pueden ser aprovechadas por las amenazas para hacer fallar o atacar a los activos de TI.

Tabla 8 – *Listado de vulnerabilidades por amenaza a tipo de Activo de TI*

N°	Activo	Amenaza	Vulnerabilidad
1	Aplicación informática para hospitales	Imposible acceder a los servicios de red del hospital, lo cual detiene la ejecución de actividades y procesos.	No existe personal especialista para el mantenimiento del servidor de dominio
			Fallan los componentes físicos
			Falla el sistema operativo por falta de actualizaciones
			No existe un plan de mantenimiento de servidores
			Ataque de virus informáticos
2	Software para desarrollo	Modificación en datos de los pacientes, generando pérdida de datos personales o historia médica	El administrador puede realizar modificaciones a la base de datos
			Existen deficiencias en el diseño de la base datos
			Acceso al servidor de la base de datos de la entidad sin autorización
3	Red de computadoras	Se detienen los servicios de red	Falla en la línea principal de la red
			Falla de las comunicaciones con los servidores principales de la empresa aseguradora
			Fallas eléctricas que interrumpe los procesos y servicios
			No existe equipo firewall
4	Se detienen los servicios de red	Daño intencionado a las instalaciones del hospital	Personal no autorizado accede a la sala de servidores.
			No existe un sistema de vigilancia y de seguridad en la sala de servidores.
		Se pierde los activos de tecnología de información en la sala de servidores	No existe un registro de acceso a las áreas restringidas
			No existe de registro de acceso formales a la sala de servidores
			No existe un procedimiento para el personal responsable del mantenimiento en el hospital

			No existe revisión de maletines por parte del personal de vigilancia
5	Actas de conformidad	Se pierde información de la empresa por accesos no permitidos a la base de datos	No existe un adecuado procedimiento para asignar perfiles de acceso a la base de datos
			No existe una política de seguridad para contraseñas de usuario
			No se revisan los privilegios de los usuarios que acceden a las aplicaciones
			Es posible acceder a la base de datos desde otras aplicaciones
			Es posible la infección por virus informáticos
			Es posible crear copias de seguridad no autorizadas de la base de datos.
			Es posible modificar datos sin autorización
		Carencia de espacio para registro y guardado de la información	Incremento en operaciones
			No existe un procedimiento de mantenimiento de base de datos
			Incremento de espacio por virus.
6	Actas de requerimientos informáticos	Se pierde información importante por falta de seguridad en los dispositivos de almacenamiento.	Los dispositivos de almacenamiento fallan
			No existe un lugar adecuado para resguardo y protección de las copias de seguridad
			Existen errores en la generación de copias de seguridad
			No se lleva un registro de la generación de copias de seguridad
7	Actas de control de cambios de las aplicaciones	Fuga de talentos que genera retraso en las actividades y pérdida de información	División de funciones inadecuada
			Plan de capacitación de recurso humano inadecuado
			Indisponibilidad del personal por enfermedad o accidente que impiden al hospital realizar sus actividades
		Cambios, divulgación y eliminación de la información	Abuso de privilegios de accesos
			No existe control y seguimiento de accesos
			No existen acuerdos de confidencialidad

			El personal actúa de manera anormal en el desarrollo de sus tareas
			No existe un procedimiento de mantenimiento de usuarios
			El nivel de complejidad de las contraseñas de correo es bajo
8	Bases de datos	Falla en los equipos de cómputo que dan soportan a las operaciones del negocio	El personal no está capacitado para tareas de mantenimiento en equipos de computo
			No existe cálculo de vida útil de los equipos
			No se cumple el plan de mantenimiento de equipos.
			Existen fallas en el sistema eléctrico.
			Existen errores de configuración en los equipos
			Existe uso inadecuado del equipo por parte de los usuarios
			Inadecuada condición de los ambientes
			Los equipos críticos no se han identificado para casos de evacuación
			Los datos sensibles se guardan en cada equipo personal
9	Respaldo de documentos normativos y de gestión	Se pierde la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad
			Existen accesos no autorizados a los equipos de Software
		Se pierde información de datos personales e historia médica por manipulación de código fuente para beneficio del trabajador	Acceso sin restricción al código fuente por parte del personal de desarrollo ajenos a ello
			No existe revisión detallada de control de cambios entregado por el analista de sistema
			No existe contraseñas complejas en el respaldo de código fuente
			Existe manipulación del código fuente que altera el desarrollo normal de un proceso
10	Centro de Procesamiento Central	Instituciones supervisoras realizan observaciones a los procesos de producción no sustentados.	No existe un adecuado registro de documentación
11	Personal de área de tecnologías de información	Se pierde información lo cual no permite el cumplimiento del	No existe un adecuado registro de documentación

		desarrollo de requerimientos.	
12	Personal de área analistas de sistemas	El tiempo de desarrollo excede el cronograma de actividades.	Existe nuevo personal de desarrollo con escaso conocimiento de los procesos del hospital
			No existe personal para cumplir con la sobrecarga de requerimientos a desarrollar.
		Fuga de información sensible por medio de correo electrónico	No existe monitoreo de envío y recepción de correos
			Existe acceso total a direcciones web
		Se pierden recursos a causa de puesta en funcionamiento no acordes a metodología y estándares de desarrollo de software del hospital	Inadecuado plan de inducción
13	Servidor principal de dominio	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos	Acceso total a la Web
14	Servidor principal de base de datos y aplicaciones	Imposible revertir las adecuaciones en los sistemas.	Las copias de respaldo se guardan en los mismos equipos

Fuente. Propia

4.1.3. Fase 2: Valoración de los escenarios de riesgos de TI

Objetivo: Determinar el nivel de exposición al riesgo, mediante la valoración de los impactos y las probabilidades de ocurrencia de los mismos.

Tabla 9 – *Cálculo de los niveles de exposición a los riesgos (NR)*

N°	Activo	Amenaza	Vulnerabilidad	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Exposición al Riesgo (NR)		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
1	Aplicación informática para hospitales	Imposible acceder a los servicios de red del hospital, lo cual detiene la ejecución de actividades y procesos.	No existe personal especialista para el mantenimiento del servidor de dominio	3	Moderado	2	Improbable	R1	2	Bajo
			Fallan los componentes físicos	4	Mayor	2	Improbable	R2	2	Bajo
			Falla el sistema operativo por falta de actualizaciones	5	Catastrófico	5	Casi seguro	R3	5	Muy alto
			No existe un plan de mantenimiento de servidores	5	Catastrófico	2	Improbable	R4	3	Medio
			Ataque de virus informáticos	3	Moderado	2	Improbable	R5	2	Bajo
2	Software para desarrollo	Modificación en datos de los pacientes, generando pérdida de datos personales o historia médica	El administrador puede realizar modificaciones a la base de datos	4	Mayor	3	Posible	R6	3	Medio
			Existen deficiencias en el diseño de la base datos	3	Moderado	3	Posible	R7	3	Medio
			Acceso al servidor de la base de datos de la entidad sin autorización	4	Mayor	5	Casi seguro	R8	5	Muy alto
3	Red de computadoras	Se detienen los servicios de red	Falla en la línea principal de la red	5	Catastrófico	3	Posible	R9	4	Alto
			Falla de las comunicaciones con los servidores principales de la empresa aseguradora	4	Mayor	3	Posible	R10	3	Medio
			Fallas eléctrica que interrumpe los procesos y servicios	3	Moderado	3	Posible	R11	3	Medio
			No existe equipo firewall	3	Moderado	1	Raro	R12	1	Muy Bajo

4	Se detienen los servicios de red	Daño intencionado a las instalaciones del hospital	Personal no autorizado accede a la sala de servidores.	5	Catastrófico	3	Posible	R13	4	Alto
			No existe un sistema de vigilancia y de seguridad en la sala de servidores.	2	Mínimo	4	Probable	R14	2	Bajo
		Se pierde los activos de tecnología de información en la sala de servidores	No existe un registro de acceso a las áreas restringidas	2	Mínimo	2	Improbable	R15	2	Bajo
			No existe de registro de acceso formales a la sala de servidores	2	Mínimo	4	Probable	R16	2	Bajo
			No existe un procedimiento para el personal responsable del mantenimiento en el hospital	2	Mínimo	3	Posible	R17	2	Bajo
			No existe revisión de maletines por parte del personal de vigilancia	2	Mínimo	4	Probable	R18	2	Bajo
5	Actas de conformidad	Se pierde información de la empresa por accesos no permitidos a la base de datos	No existe un adecuado procedimiento para asignar perfiles de acceso a la base de datos	3	Moderado	4	Probable	R19	3	Medio
			No existe una política de seguridad para contraseñas de usuario	2	Mínimo	3	Posible	R20	2	Bajo
			No se revisan los privilegios de los usuarios que acceden a las aplicaciones	3	Moderado	2	Improbable	R21	2	Bajo
			Es posible acceder a la base de datos desde otras aplicaciones	3	Moderado	4	Probable	R22	3	Medio
			Es posible la infección por virus informáticos	3	Moderado	4	Probable	R23	3	Medio
			Es posible crear copias de seguridad no autorizadas de la base de datos.	4	Mayor	2	Improbable	R24	2	Bajo

			Es posible modificar datos sin autorización	5	Catastrófico	4	Probable	R25	5	Muy alto
		Carencia de espacio para registro y guardado de la información	Incremento en operaciones	3	Moderado	4	Probable	R26	3	Medio
			No existe un procedimiento de mantenimiento de base de datos	2	Mínimo	3	Probable	R27	2	Bajo
			Incremento de espacio por virus.	2	Mínimo	1	Raro	R28	1	Muy bajo
6	Actas de requerimientos informáticos	Se pierde información importante por falta de seguridad en los dispositivos de almacenamiento.	Los dispositivos de almacenamiento fallan	4	Mayor	3	Posible	R29	3	Medio
			No existe un lugar adecuado para resguardo y protección de las copias de seguridad	2	Mínimo	3	Posible	R30	2	Bajo
			Existen errores en la generación de copias de seguridad	4	Mayor	5	Casi seguro	R31	5	Muy alto
			No se lleva un registro de la generación de copias de seguridad	4	Mayor	3	Posible	R32	3	Medio
7	Actas de control de cambios de las aplicaciones	Fuga de talentos que genera retraso en las actividades y pérdida de información	División de funciones inadecuada	2	Mínimo	2	Improbable	R33	2	Bajo
			Plan de capacitación de recurso humano inadecuado	2	Mínimo	3	Posible	R34	2	Bajo
			Indisponibilidad del personal por enfermedad o accidente que impiden al hospital realizar sus actividades	2	Mínimo	4	Probable	R35	2	Bajo
		Cambios, divulgación y eliminación de la información	Abuso de privilegios de accesos	3	Moderado	3	Posible	R36	3	Medio
			No existe control y seguimiento de accesos	4	Mayor	4	Probable	R37	4	Alto
			No existen acuerdos de confidencialidad	4	Mayor	3	Posible	R38	3	Medio
			El personal actúa de manera anormal en el desarrollo de sus tareas	3	Moderado	3	Posible	R39	3	Medio

			No existe un procedimiento de mantenimiento de usuarios	3	Moderado	2	Improbable	R40	2	Bajo
8	Bases de datos	Falla en los equipos de cómputo que dan soportan a las operaciones del negocio	El personal no está capacitado para tareas de mantenimiento en equipos de computo	4	Mayor	3	Posible	R41	3	Medio
			No existe cálculo de vida útil de los equipos	2	Mínimo	2	Improbable	R42	2	Bajo
			No se cumple el plan de mantenimiento de equipos.	3	Moderado	3	Posible	R43	3	Medio
			Existen fallas en el sistema eléctrico.	3	Moderado	3	Posible	R44	3	Medio
			Existen errores de configuración en los equipos	2	Mínimo	2	Improbable	R45	2	Bajo
			Existe uso inadecuado del equipo por parte de los usuarios	3	Moderado	3	Posible	R46	3	Medio
			Inadecuada condición de los ambientes	2	Mínimo	4	Probable	R47	2	Bajo
			Los equipos críticos no se han identificado para casos de evacuación	4	Mayor	1	Raro	R48	2	Bajo
			Los datos sensibles se guardan en cada equipo personal	4	Mayor	4	Probable	R49	4	Alto
9	Respaldo de documentos normativos y de gestión	Se pierde la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad	4	Mayor	1	Raro	R50	2	Bajo
			Existen accesos no autorizados a los equipos de Software	4	Mayor	2	Improbable	R51	2	Bajo
		Se pierde información de datos personales e historia médica por manipulación de código fuente para	Acceso sin restricción al código fuente por parte del personal de desarrollo ajenos a ello	3	Moderado	3	Posible	R52	3	Medio
			No existe revisión detallada de control de cambios entregado	3	Moderado	4	Probable	R53	3	Medio

		beneficio del trabajador	por el analista de sistema							
			No existe contraseñas complejas en el respaldo de código fuente	3	Moderado	3	Posible	R54	3	Medio
			Existe manipulación del código fuente que altera el desarrollo normal de un proceso	5	Catastrófico	4	Probable	R55	5	Muy alto
10	Centro de Procesamiento Central	Instituciones supervisoras realizan observaciones a los procesos de producción no sustentados.	No existe un adecuado registro de documentación	3	Moderado	4	Probable	R56	3	Medio
11	Personal de área de tecnologías de información	Se pierde información lo cual no permite el cumplimiento del desarrollo de requerimientos.	No existe un adecuado registro de documentación	3	Moderado	3	Posible	R57	3	Medio
12	Personal de área analistas de sistemas	El tiempo de desarrollo excede el cronograma de actividades.	Existe nuevo personal de desarrollo con escaso conocimiento de los procesos del hospital	2	Mínimo	3	Posible	R58	2	Bajo
			No existe personal para cumplir con la sobrecarga de requerimientos a desarrollar.	3	Moderado	4	Probable	R59	3	Medio
		Fuga de información sensible por medio de correo electrónico	No existe monitoreo de envío y recepción de correos	3	Moderado	2	Improbable	R60	2	Bajo
			Existe acceso total a direcciones web	4	Mayor	3	Posible	R61	3	Medio
		Se pierden recursos a causa de puesta en funcionamiento no	Inadecuado plan de inducción	2	Mínimo	2	Improbable	R62	2	Bajo

		acordes a metodología y estándares de desarrollo de software del hospital								
13	Servidor principal de dominio	Retraso en las actividades, pérdida de recursos debido a Infección de Virus Informáticos	Acceso total a la Web	3	Moderado	4	Probable	R63	3	Medio
14	Servidor principal de base de datos y aplicaciones	Imposible revertir las adecuaciones en los sistemas.	Las copias de respaldo se guardan en los mismos equipos	5	Catastrófico	3	Posible	R64	4	Alto

Fuente. Propia

4.2. Elaborar el modelo de gestión de riesgos operacionales en tecnologías de información

4.2.1. Fase 3: Acciones para tratamiento de los riesgos

Objetivo: Definir un plan para tratamiento de los riesgos.

Los riesgos considerados en el plan son los valorados en niveles no aceptables y en algunos casos, para los riesgos en niveles tolerables.

En esta fase se determinó los controles necesarios para tratar cada una de las amenazas en cuya evaluación se haya obtenido niveles de riesgos no tolerantes, es decir, con el calificativo de “Alto” o “Muy Alto”.

4.2.1.1.Definir políticas de seguridad

La norma ISO/IEC 27001 establece que la implementación de controles para mitigar los niveles de exposición al riesgo no aceptable, deben ser guiados mediante políticas de seguridad. De acuerdo a la ISO/IEC 27001, un Sistema de Gestión para la Seguridad de la Información debe estar organizado

- Políticas de seguridad
- Normativas
- Procedimientos
- Controles
- Indicadores

De acuerdo al alcance de la investigación sólo propone las políticas de seguridad, pero no se contempla, las normativas y procedimientos.

4.2.1.2. Identificar controles de seguridad

Para la identificación de los controles de seguridad necesarias para la mitigación de los riesgos en niveles no aceptables, y de acuerdo a las políticas de seguridad propuestas, se utilizó el catálogo de controles propuesto por la ISO/IEC 27002.

4.2.1.3. Definir estrategia de implementación de controles

Una vez seleccionado los controles se define la estrategia de implementación del control, según la propuesta de la ISO/IEC 27005:

- Estrategia de aceptar el riesgo: cuando los niveles de exposición al riesgo están dentro de los rangos de aceptabilidad
- Estrategia de elegir el control para mitigar el riesgo: cuando los niveles de exposición al riesgo están en los rangos de tolerancia y/o No aceptabilidad; y además se cuenta con los recursos humanos, tecnológicos y económicos para su implementación.

- Estrategia de transferencia del riesgo a terceros: cuando los niveles de exposición al riesgo están en los rangos de tolerancia y/o No aceptabilidad; y además no se cuenta con los recursos humanos, tecnológicos para su implementación, pero si con la economía necesaria para contratar a un tercero especializado
- Estrategia de evitar el aumento del riesgo: cuando los niveles de exposición al riesgo están en los rangos de tolerancia y/o No aceptabilidad; pero no se cuenta con los recursos humanos, tecnológicos y económicos para su implementación.

Tabla 10 – *Estrategia de implementación de controles según el nivel de exposición al riesgo*

Nivel de Riesgo (NR)			Control		Estrategia de implementación
ID riesgo	Nivel	Categoría	ID Control	Descripción	
R1	2	Bajo	C1	Contratar con un servicio de mantenimiento correctivo por parte del fabricante	Transferencia del riesgo a terceros
R2	2	Bajo	C2	Contratar con un servicio de mantenimiento por parte del fabricante	Transferencia del riesgo a terceros
			C3	Instalar sala de servidores con controles ambientales	Evitar aumento del riesgo
R3	5	Muy alto	C4	Contratar personal capacitado en administración de servidores con sistema operativo Windows Server	Transferencia del riesgo a terceros
R4	3	Medio	C5	Incluir en el plan de mantenimiento a los servidores	Evitar aumento del riesgo
R5	2	Bajo	C6	Tener software antivirus instalado en la red de computadoras y con actualizaciones automáticas	Evitar aumento del riesgo
			C7	Tener copias de seguridad de la base de datos	Evitar aumento del riesgo
			C8	Tener un servidor para almacenar copias de seguridad	Evitar aumento del riesgo
			C9	Se ha planificado implementar un centro de cómputo alterno (CCA), el cual permite generar copias de respaldo en línea	Evitar aumento del riesgo
R6	3	Medio	C10	Monitorear frecuentemente las operaciones que realiza en la arquitectura de la base de datos	Elección de controles
R7	3	Medio	C11	Durante el desarrollo existe una fase de pruebas, donde se analizan el diseño de las tablas y las modificaciones	Evitar aumento del riesgo

			C12	Realizar un análisis de los ejecutables y códigos fuentes que pasan a desarrollo	Evitar aumento del riesgo
R8	5	Muy alto	C13	Se definen restricciones de acceso a los servidores mediante la asignación de perfiles de usuario y se deshabilitan programas que permiten acceder a la base de datos	Elección de controles
			C14	Se crean contraseñas de acceso a la base de datos con alto nivel de complejidad	Elección de controles
			C15	Se restringen los permisos de los perfiles de usuarios con acceso a la base de datos	Elección de controles
R9	4	Alto	C16	Se dispone de una línea de comunicación de contingencia	Transferencia del riesgo a terceros
			C17	Informar las averías al proveedor de servicios	Transferencia del riesgo a terceros
R10	3	Medio	C18	Informar las averías al proveedor de servicios	Transferencia del riesgo a terceros
R11	3	Medio	C19	Compra de equipo UPS y un grupo electrógeno	Elección de controles
			C20	Diagnosticar el funcionamiento de los equipos eléctricos realizando pruebas de operatividad	Elección de controles
			C21	Definir un plan de mantenimiento preventivo para el sistema eléctrico	Elección de controles
R12	1	Muy bajo	C22	Instalar firewall a nivel de software	Evitar aumento del riesgo
R13	4	Alto	C23	Definir políticas de seguridad	Evitar aumento del riesgo
			C24	Control de los accesos a la sala de servidores y al área de tecnología de información	Evitar aumento del riesgo
			C25	Los accesos por parte de personal a realizar mantenimiento, se realiza acompañado de personal del área	Evitar aumento del riesgo
			C26	Instalar una puerta con llave para restringir el acceso a la sala de servidores. La llave es responsabilidad del jefe de sistemas	Evitar aumento del riesgo
			C27	Trasladar la sala de servidores a un ambiente aislado	Evitar aumento del riesgo
			C28	Instalar una cámara de vigilancia que monitorea el ingreso de personal al área de TI	Evitar aumento del riesgo
R14	2	Bajo	C29	Instalar un equipo de aire acondicionado que evita el sobrecalentamiento de los equipos	Evitar aumento del riesgo
			C30	Instalar extintores y sensores de humo	Evitar aumento

					del riesgo
			C31	Trasladar la sala de servidores a un ambiente aislado	Evitar aumento del riesgo
			C32	Instalar luces de emergencia	Evitar aumento del riesgo
			C33	Control de los accesos a la sala de servidores y al área de tecnología de información	Evitar aumento del riesgo
			C34	Instalar una cámara de vigilancia que monitorea el ingreso de personal al área de TI	Evitar aumento del riesgo
			C35	La responsabilidad del manejo de llaves recae en el jefe de sistemas	Evitar aumento del riesgo
			C36	Instalar una sala de servidor alterno	Evitar aumento del riesgo
			C37	Realizar el mantenimiento de los equipos de seguridad	Evitar aumento del riesgo
			C38	Implementar un plan de pruebas de los equipos	Evitar aumento del riesgo
R15	2	Bajo	C39	El personal de vigilancia del hospital registra ingresos a zonas de acceso restringido	Evitar aumento del riesgo
R16	2	Bajo	C40	Implementar un libro donde registre hora de ingreso, salida y nombre del personal que ingresa a la sala de servidores	Evitar aumento del riesgo
R17	2	Bajo	C41	Implementar procedimiento para el personal que realiza mantenimiento en el hospital	Evitar aumento del riesgo
R18	2	Bajo	C42	Implementar formatos de entrada - salida para el traslado de equipos del hospital	Evitar aumento del riesgo
R19	3	Medio	C43	Reglamento de administración de usuarios en el sistema de información hospitalaria, donde se consideran opciones para asignación de perfiles de usuario	Elección de controles
R20	2	Bajo	C44	Creación de contraseñas teniendo en cuenta caracteres numéricos y alfanuméricos. cumpliendo nivel mínimo de complejidad	Evitar aumento del riesgo
R21	2	Bajo	C45	Implementar en el plan de trabajo una política de revisión de permisos al sistema	Evitar aumento del riesgo
R22	3	Medio	C46	Deshabilitar el acceso a Microsoft Excel en todas las computadoras de la red	Elección de controles
			C47	El acceso como administrador a la base de datos solo es de conocimiento del jefe de sistemas	Elección de controles
R23	3	Medio	C48	Actualización periódica del antivirus	Evitar aumento del riesgo
R24	2	Bajo	C49	El acceso como administrador a la base de datos solo es de conocimiento del jefe de sistemas	Evitar aumento del riesgo
			C50	Disponer una única carpeta compartida de la base de datos	Elección de controles

R25	5	Muy alto	C51	Se efectúa una revisión general del script que envía la sección desarrollo para el pase a producción	Elección de controles
R26	3	Medio	C52	El área de sistemas supervisa la capacidad del disco del servidor, a fin de que exista espacio suficiente para la base de datos	Evitar aumento del riesgo
R27	2	Bajo	C53	Implementar un procedimiento documentado para mantenimiento de la base de datos	Evitar aumento del riesgo
R28	1	Muy bajo	C54	Actualización periódica del antivirus	Elección de controles
			C55	Bloquear los puertos de control de acceso al servidor	Elección de controles
R29	3	Medio	C56	Implementar políticas y procedimientos de generación de copias de seguridad	Elección de controles
			C57	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno	Elección de controles
			C58	Implementar un control trimestral del estado de almacenamiento de los medios de respaldo	Elección de controles
			C59	Implementar un monitoreo del procedimiento de respaldo de las copias de seguridad	Elección de controles
			C60	Implementar un centro de cómputo de réplica de información de la base de datos de manera automática	Elección de controles
R30	2	Bajo	C61	Implementar la verificación del estado de almacenamiento y resguardo de las copias de seguridad	Evitar aumento del riesgo
R31	5	Muy alto	C62	El aplicativo que comprime la BD, permite realizar revisiones automáticas del archivo comprimido	Elección de controles
			C63	El software que graba los archivos comprimidos en los medios de almacenamiento realiza una verificación después de la grabación	Elección de controles
			C64	Periódicamente se verifican las copias generadas	Elección de controles
R32	3	Medio	C65	Se cuenta con un cuaderno de cargos en el cual se consigna el envío de las copias de respaldo por fechas de generación, responsable de envío y recepción	Evitar aumento del riesgo
R33	2	Bajo	C66	Se cuenta con manual de organización y funciones en el que se tiene establecido las responsabilidades que debe cumplir el personal en la operativa diaria	Evitar aumento del riesgo
R34	2	Bajo	C67	El jefe de sistemas aprueba un plan de capacitación del personal de TI	Evitar aumento del riesgo
R35	2	Bajo	C68	Se tiene personal de reemplazo, pero no está totalmente capacitado en las actividades	Evitar aumento del riesgo

				diarias.	
R36	3	Medio	C69	Se asignan privilegios de acuerdo al manual de funciones	Elección de controles
			C70	Implementar una bitácora de pistas de auditoria que son revisadas periódicamente	Elección de controles
R37	4	Alto	C71	Se establece procedimientos para la revisión de usuarios	Elección de controles
R38	3	Medio	C72	Definir acuerdos de confidencialidad para ser usados durante el ingreso de nuevo personal al hospital	Elección de controles
R39	3	Medio	C73	Realizar evaluaciones psicológicas durante el ingreso de nuevo personal al hospital	Evitar aumento del riesgo
			C74	Implementar políticas de seguridad y contar con reglamentos internos que establecen sanciones	Evitar aumento del riesgo
R40	2	Bajo	C75	Implementar un reglamento de altas, bajas y modificación de usuarios.	Evitar aumento del riesgo
R41	3	Medio	C76	Se cuenta con un proceso de evaluación del personal nuevo por parte de recursos humanos	Evitar aumento del riesgo
			C77	Se cuenta con una lista de técnicos que permiten realizar el mantenimiento de los equipos	Evitar aumento del riesgo
			C78	La empresa proveedora, brinda servicios de mantenimiento a los equipos arrendados	Evitar aumento del riesgo
R42	2	Bajo	C79	Implementar un contrato de leasing para los equipos de cómputo cuyo acuerdo considere niveles de servicio	Evitar aumento del riesgo
R43	3	Medio	C80	Seguimiento al cumplimiento del plan por parte del jefe de sistemas	Evitar aumento del riesgo
R44	3	Medio	C81	Implementar un plan de mantenimiento del sistema eléctrico	Evitar aumento del riesgo
			C82	Se cuenta con una red eléctrica estabilizada	Evitar aumento del riesgo
			C83	Las computadores están conectadas a UPS	Evitar aumento del riesgo
			C84	Se realizan pruebas periódicas del sistema de respaldo eléctrico donde incluyen UPS y grupo electrógeno	Evitar aumento del riesgo
			C85	Se realiza mantenimiento programado a los equipos eléctricos	Evitar aumento del riesgo
R45	2	Bajo	C86	Contratar personal capacitado para realizar la configuración de los equipos.	Evitar aumento del riesgo
R46	3	Medio	C87	Definir la responsabilidad de cada usuario sobre el uso de los activos del hospital para el cumplimiento de sus funciones.	Evitar aumento del riesgo
R47	2	Bajo	C88	Implementar un ambiente para la ubicación de los equipos	Evitar aumento del riesgo

R48	2	Bajo	C89	Identificar los equipos críticos del área de tecnología de información	Evitar aumento del riesgo
			C90	Implementar políticas para la clasificación de la información	Evitar aumento del riesgo
R49	4	Alto	C91	Implementar una política para no guardar información sensible en equipos de trabajo	Elección de controles
R50	2	Bajo	C92	Realizar copias de seguridad con frecuencia semanal	Evitar aumento del riesgo
			C93	Realizar dos copias de seguridad, guardando una en el hospital y la otra en un lugar externo	Evitar aumento del riesgo
R51	2	Bajo	C94	Implementar seguridad de acceso al local	Evitar aumento del riesgo
			C95	Separar las computadoras de integración de desarrollo de la red de producción	Evitar aumento del riesgo
			C96	Generar copias de seguridad del código fuentes	Evitar aumento del riesgo
R52	3	Medio	C97	El código fuente se considera como información restringida y controlada por el jefe de sistemas	Elección de controles
R53	3	Medio	C98	Implementar una bitácora de control de cambios, donde indique todas las modificaciones a nivel de código fuente	Elección de controles
			C99	Realizar el control de calidad de todos los puntos integrados de los analistas de sistemas	Elección de controles
			C100	Implementar el control de calidad del código antes de su pase a producción	Elección de controles
R54	3	Medio	C101	Definir contraseña con caracteres y números, la contraseña cambia en cada respaldo	Evitar aumento del riesgo
R55	5	Muy alto	C102	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	Elección de controles
			C103	Detectar cambios no programados	Elección de controles
			C104	Implementar fase de prueba en desarrollo y certificación antes del pase a producción	Elección de controles
R56	3	Medio	C105	Archivo de control de versiones para documentos como requerimientos de usuarios, manual de usuario y actas de trabajo	Evitar aumento del riesgo
R57	3	Medio	C106	Implementar un listado de inventario denominado matriz de requerimientos	Evitar aumento del riesgo
R58	2	Bajo	C107	El analista nuevo recibe curos de inducción sobre los procesos del negocio y de los procesos automatizados de negocio.	Evitar aumento del riesgo
R59	3	Medio	C108	Se priorizan los requerimientos de implementación de procesos más	Evitar aumento del riesgo

				importantes	
R60	2	Bajo	C109	Existe un reglamento específico de acceso a Internet	Evitar aumento del riesgo
R61	3	Medio	C110	Existe restricción de acceso a Internet según niveles de acceso de usuarios	Elección de controles
R62	2	Bajo	C111	Implementar un proceso de inducción del proceso del negocio y de los procesos automatizados en el sistema.	Evitar aumento del riesgo
R63	3	Medio	C112	Instalación de Antivirus en las computadoras del hospital	Evitar aumento del riesgo
R64	4	Alto	C113	Se generan dos copias de respaldo que son enviados a sitios alternos	Elección de controles
R65	3	Medio	C114	Se cuenta con licencias de uso de software de desarrollo (lenguaje de programación y manejador de BD. Se puede solicitar al proveedor copias de los instaladores	Evitar aumento del riesgo
R66	2	Bajo	C115	Cada desarrollar identifica su código fuente con comentarios con identificador del analista de sistemas, la fecha de cambio y motivo o descripción del cambio	Evitar aumento del riesgo
R67	2	Bajo	C116	Se genera una copia de seguridad de la normativa vigente, además de llevar un control de cambios en cada documento normativo.	Evitar aumento del riesgo
R68	3	Medio	C117	Una copia de respaldo se guarda en un lugar externo	Evitar aumento del riesgo

Fuente. Propia

4.3. Evaluar el cumplimiento de los indicadores de calidad para un modelo de evaluación propuesto

4.3.1. Fase 4: Seguimiento de la efectividad de los controles

Objetivo: Plantear la propuesta de seguimiento y monitoreo de los controles implementados para evaluar su efectividad en base a la reevaluación de los niveles de exposición al riesgo luego de implementado los controles.

4.3.1.1. Elaborar de plan de acción

Es necesario definir un plan de acciones que asegure la implementación de los controles y su efectividad

Tabla 11 – *Propuesta Organización de las políticas de seguridad*

Organización de las políticas de seguridad
Objetivo Desarrollar el plan director de políticas de seguridad, basándose en la normativa ISO aplicable.

Descripción

Se elabora un plan de seguridad, que deberá ser aceptado y debidamente comunicado; donde se decidirán las responsabilidades definiendo un organigrama acorde a la estructura de la organización.

Indicadores verificación

- Verificación de inicio de proyecto.
- Firma aprobación del plan de seguridad.
- Documentación de acuerdo finalización y conformidad, a fecha fin del proyecto.

Riesgos a Mitigar

La definición de las Políticas de seguridad, es paso fundamental y necesario para poder crear el SGSI en el hospital.

Se trata de mitigar los riesgos de infringir los niveles de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

Fuente. Propia

Tabla 12 – *Identificación y manejo de activos*

Identificación y manejo de activos
Objetivos
Asegurar una correcta clasificación de los activos por tipo, departamento y responsables dentro de toda la organización, tratando de detectar errores o dependencias erróneas para su más pronta resolución.
Descripción
Consiste en definir los diferentes activos según su tipo. Control efectivo y actualizado de todos los activos para su correcto uso por parte de los usuarios
Indicadores verificación
▪ Cada trimestre, registro de estado de los activos y su clasificación. ▪ Cada semestre, verificación de la correcta asignación de responsables de cada activo.
Amenazas a Mitigar
[A.11] Acceso no autorizado
[A.18] Destrucción de información
[A.6] Abuso de privilegios de acceso
[E.1] Errores de los usuarios
[E.15] Alteración accidental de la información
[E.18] Destrucción de información
[E.19] Fugas de información
[E.2] Errores del Administrador
[E.4] Errores de configuración

Fuente. Propia

Tabla 13 – *Clasificación de la Información*

Clasificación de la Información
Objetivos Asegurar la información clasificándola en base a las fuentes que la generan
Descripción Organizar la información en la forma que se utiliza y genera dentro de la organización, atendiendo a su valor económico, requisitos legales y lo crítico de su contenido. Se debe diseñar y asegurar las medidas necesarias de control y seguridad para el aseguramiento de toda la información de la organización.
Indicadores verificación ▪ Mensualmente se verificarán todas las incidencias producidas sobre los activos. ▪ Anualmente se verificará la correcta clasificación de todos los activos de la organización.
Riesgos a Mitigar [A.15] Modificación deliberada de la información [A.22] Manipulación de programas [A.4] Manipulación de la configuración [A.8] Difusión de software dañino [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas [E.21] Errores de mantenimiento / actualización de programas [E.7] Deficiencias en la organización [E.8] Difusión de software dañino

Fuente. Propia

Tabla 14 – *Cumplimiento de Requisitos Legales*

Cumplimiento de Requisitos Legales
Objetivos Asegurar el correcto cumplimiento de los requisitos legales establecidos, adaptándose a la normativa ISO aplicable en cada momento.
Descripción Adaptar todo el sistema organizativo y de producción a la normativa legal aplicable, tanto en materia de seguridad como laboral. Actualizando mediante verificaciones los sistemas a la ISO
Indicadores verificación

▪ Semestralmente se realizará una verificación de cumplimiento de los requisitos legales. ▪ Anualmente se realizará una verificación en coordinación con la auditoria programada para obtener un registro de no conformidades/y definir acciones correctivas sobre los requisitos legales establecidos.

Fuente. Propia

Tabla 15 – *Capacitación y compromiso de seguridad*

Capacitacion y compromiso de seguridad
Objetivos Definir, documentar y planificar un plan de capacitación adecuado para los empleados del hospital, según sus roles asignados.
Descripción Cada empleado de acuerdo a su categoría y puesto asignado será capacitado en las funciones y responsabilidades que tiene respecto a la seguridad de los activos de la organización.
Indicadores verificación ▪ Cada año se verificarán las acciones formativas realizadas, evaluando su funcionalidad. ▪ Cada año se revisará la actualización de los planes para definir mejoras.
Riesgos a Mitigar [A. 18] Destrucción de información [A. 19] Divulgación de información [A.3] Manipulación de los registros de actividad [A.30] Ingeniería social [A.4] Manipulación de la configuración [E.1] Errores de los usuarios [E.15] Alteración accidental de la información [E.19] Fugas de información [E.2] Errores del Administrador [E.3] Errores de monitorización [I.7] Condiciones inadecuadas de temperatura o humedad

Fuente. Propia

4.3.1.2. Calcular los niveles de riesgo residual (NRR)

Esta actividad evalúa la efectividad de los controles y sus efectos sobre la mitigación de los riesgos que están fuera de los rangos de aceptabilidad del hospital. De acuerdo al apetito de riesgo definido, sólo se evaluaron los niveles de riesgo que han obtenido valores de “Alto” y “Muy alto”.

Tabla 16 – *Valorización del NRR y brecha de seguridad*

Nivel de Riesgo Intrínseco (NRI)		Control Implantado		Valorización del Nivel de Riesgo Residual (NRR)						Brecha de seguridad
ID riesgo	Categoría	ID Control	Descripción	Nivel	Categoría	Nivel	Categoría	Nivel	Categoría	
R3	Muy alto	C4	Contratar personal capacitado en administración de servidores con sistema operativo Windows Server	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R8	Muy alto	C13	Se definen restricciones de acceso a los servidores mediante la asignación de perfiles de usuario y se deshabilitan programas que permiten acceder a la base de datos	5	Catastrófico	2	Improbable	3	Medio	Riesgo aceptable
		C14	Se crean contraseñas de acceso a la base de datos con alto nivel de complejidad							Riesgo aceptable
		C15	Se restringen los permisos de los perfiles de usuarios con acceso a la base de datos							Riesgo aceptable
R9	Alto	C16	Se dispone de una línea de comunicación de contingencia	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
		C17	Informar las averías al proveedor de servicios							Riesgo aceptable
R13	Alto	C23	Definir políticas de seguridad	4	Mayor	4	Probable	4	Alto	Riesgo NO aceptable
		C24	Control de los accesos a la sala de servidores y al área de tecnología de información							
		C25	Los accesos por parte de personal a realizar mantenimiento, se realiza acompañado de personal del área							
		C26	Instalar una puerta con llave para restringir el acceso a la sala de servidores. La llave es responsabilidad del jefe de sistemas							
		C27	Trasladar la sala de servidores a un ambiente aislado							Riesgo aceptable
		C28	Instalar una cámara de vigilancia que monitorea el ingreso de personal al área de TI							Riesgo aceptable
R25	Muy alto	C51	Se efectúa una revisión general del script que envía la sección desarrollo para el pase a producción	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R31	Muy alto	C62	La herramienta que comprime la BD, realiza una verificación	3	Moderado	3	Posible	3	Medio	Riesgo

			automática de los archivos comprimidos							aceptable
		C63	El software que graba los archivos comprimidos en los medios de almacenamiento, realiza una verificación después de la grabación							Riesgo aceptable
		C64	Periódicamente se verifican las copias generadas							Riesgo aceptable
R37	Alto	C71	Implementar un procedimiento para la revisión de usuarios del sistema de manera semestral	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
R49	Alto	C91	Implementar una política para no guardar información sensible en equipos de trabajo	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
R55	Muy alto	C102	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	4	Mayor	4	Probable	4	Alto	Riesgo NO aceptable
		C103	Detectar cambios no programados							Riesgo aceptable
		C104	Implementar fase de prueba en desarrollo y certificación antes del pase a producción							Riesgo aceptable
R64	Alto	C113	Se generan dos copias de respaldo que son enviados a sitios alternos	3	Moderado	2	Improbable	2	Bajo	Riesgo aceptable

Fuente. Propia

4.4. Validar el modelo elaborado con la opinión de experto

Tabla 17 – *Validación de expertos del modelo propuesto para la gestión de riesgos de Tecnologías de Información, aplicando los marcos de referencia ISO/IEC 27005 y la metodología MagerIT*

FASE	ACTIVIDAD	EXPERTO 1				EXPERTO 2				EXPERTO 3							
		SU	**CL**	**CO**	**RE**	**SU**	**CL**	**CO**	**RE**	**SU**	**CL**	**CO**	**RE**	**SU**	**CL**	**CO**	**RE**
Identificación de los escenarios de riesgo de TI	Identificación y clasificación de los activos de TI	4	4	3	3	4	4	4	4	5	5	5	5	**3.8**	**3.9**	**3.9**	**3.5**
	Valoración de la criticidad de los activos de TI	4	4	4	4	4	4	3	3	5	4	4	4				
	Identificación de las amenazas de por activo de TI	4	4	4	4	4	3	3	3	4	3	4	3				
	Identificación de vulnerabilidades de cada activo de TI	4	4	4	4	3	4	4	3	4	3	4	3				
Valoración de los escenarios de riesgo de TI	Estimación del impacto de los escenarios de riesgo	4	4	5	4	3	4	4	4	4	3	4	4	**3.3**	**3.9**	**3.9**	**3.9**
	Estimación de la probabilidad de ocurrencia de los escenarios de riesgo	4	4	3	4	4	4	4	4	5	4	4	4				
	Cálculo de los niveles de exposición a los riesgos	3	4	3	4	4	3	3	3	4	4	3	4				
	Determinación del apetito y tolerancia al riesgo	4	3	4	4	4	4	3	4	4	4	4	4				
Tratamiento de los riesgos	Definición de las políticas de seguridad	3	4	3	3	3	3	3	3	3	4	4	4	**3.4**	**3.4**	**3.8**	**3.4**
	Identificación de los controles/salvaguardas de seguridad	4	4	4	4	4	4	3	3	4	4	5	4				
	Definición de la estrategia de implementación de controles/salvaguardas	4	3	3	3	4	4	3	3	3	4	4	4				
Seguimiento de la efectividad de los controles	Elaboración de planes de acción	4	4	4	4	3	4	4	3	4	4	3	4	**3.5**	**4.1**	**4.1**	**3.8**
	Definición de indicadores de riesgo	4	4	4	4	3	4	4	3	3	4	4	4				
	Cálculo de los niveles de riesgo residual (NRR)	4	4	4	4	3	4	4	4	5	5	5	5				

Fuente. Propia

V. Discusión

Hipótesis

Un modelo de gestión de riesgos de tecnologías de información, basada en la ISO/IEC 27005 permite mitigar los riesgos operacionales en el Hospital Privado Juan Pablo II de la ciudad de Chiclayo.

Variables de Hipótesis

Independiente: Modelo de gestión de riesgos de tecnologías de información basado en la ISO/IEC 27005 y MagerIT

Dependiente: Riesgos operacionales

Población y muestra

Como población se tomará a los tres (3) miembros expertos del Hospital Privado Juan Pablo II quienes toman las decisiones y además los registros de incidencias.

Procesamiento de Datos

Aplicando el formato de encuesta que se muestra en el Anexo 5, se obtuvieron las valoraciones de cada uno de los expertos para cada uno de los criterios considerados para validar el modelo propuesto para la gestión de riesgos de Tecnologías de Información, cuyos resultados se muestran en la tabla 16. La valoración de los expertos para la metodología propuesta para la gestión de riesgos de TI, aplicando los marcos de referencia ISO/IEC 27005 y la metodología MagerIT, indican lo siguiente:

- Las actividades que se desarrollaron en cada etapa de la metodología propuesta son suficientes para lograr los objetivos esperados por el hospital.
- La descripción de las actividades y tareas son claras y comprensibles en su explicación para su posterior ejecución como parte de la metodología.
- Las actividades y tareas desarrolladas son coherentes y hay una lógica para su ejecución en la metodología.
- Las actividades o tareas desarrolladas son muy relevantes y debe ser incluidas en la metodología.

VI. Conclusiones

- Mediante la aplicación de los fundamentos teóricos de los marcos de referencia ISO/IEC 27005 y la metodología MagerIT se elaboró el modelo de gestión de riesgos de Tecnologías de Información, abarcando las etapas de identificación, análisis y tratamiento de los riesgos; definiendo para cada fase los componentes que deben ser considerados en la gestión de riesgos de Tecnologías de Información, de acuerdo a las buenas prácticas de los marcos de referencia utilizados.
- Se definieron los procedimientos necesarios y suficientes para cada una de las etapas del modelo de gestión de riesgos propuesto, estableciendo criterios de identificación, clasificación y valorización. De esta manera se logró integrar el modelo teórico con los procedimientos, definiendo así una metodología integrada para gestión de riesgos de Tecnologías de Información para el Hospital Privado Juan Pablo II. Se han definido procedimientos para identificar y valorar cada uno de los componentes que conforman el modelo. Así mismo, se logró definir escalas de valoración y los formatos respectivos, que sirvieron de guía.
- Mediante el uso de datos históricos del Hospital Privado Juan Pablo II, se logró determinar los niveles de exposición al riesgo de Tecnologías de Información, en base a lo cual se logró plantear una serie de mecanismos de seguridad y control que permitan mitigar los escenarios de riesgo que se encuentran en niveles no tolerables, de acuerdo a las escalas establecidas en el modelo.
- Se realizó la validación del modelo y la metodología propuesta a través de juicio de tres expertos en el tema de gestión de riesgos de Tecnologías de Información, obteniendo como resultados que la propuesta es clara, coherente, suficiente y relevancia.

VII. Recomendaciones

- Se recomienda que el modelo de gestión de riesgos de Tecnologías de Información propuesto sea implementado en un software, lo cual permitirá generar indicadores gráficos y la generación de escenarios.
- Se recomienda cumplir las acciones y directivas que se plantean en el Plan de Acción definido como parte del modelo de gestión de riesgos propuesto.
- Se recomienda que, una vez automatizado el modelo de gestión de riesgos propuesto en el hospital, sea cada dueño/responsable del proceso quien registre en el software la información necesaria de forma permanente, permitiendo de esta forma obtener rápidamente la información del nivel de criticidad de sus procesos, porcentaje de desviación de riesgo de los activos o procesos, capital necesario a invertir en la protección de un activo o proceso, entre otra información.

VIII. Referencias bibliográficas

Ahmad, A., Maynard, S., y Park, S. (2014). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 257-370.

Alberts, C., y Dorofee, A. (2001). *OCTAVE Method Implementation Guide Version 2.0.* Carnegie Mellon University.

Alcántara Flores, J. C. (Mayo de 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. Chiclayo, Lambayeque, Perú: Universidad Católica Santo Toribio de Mogrovejo.

Alexander, A. (2011). Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca Análisis y Evaluación del Riesgo de Información : Un Caso en la Banca. CENTRUM - Centro de Negocios, Pontificia Universidad Católica del Perú.

Almeida, M. S. (1999). *Getting Started with DataWarehouse and Business Intelligence*. Obtenido de http://www.redbooks.ibm.com/redbooks/pdfs/sg245415.pdf

Arciniegas Duarte, F. A. (2017). Análisis de riesgos en la empresa bilateral Call Center sede Bogotá bajo la metodología Magerit V3. Bogotá, Colombia: Universidad Católica de Colombia.

Arellano, N. (2016). *La gestión de riesgos como pilar del Gobierno Corporativo*. Obtenido de Ernst y Young Global Limited: https://www.ey.com/pe/es/newsroom/newsroom-am-gestion-riesgos-gobierno-corporativo

Arenas López, M. C. (2016). Inteligencia de negocios aplicada a los procesos de autoevaluación de la Universidad de Manizales. Manizales: Universidad de Manizales. Facultad de Ciencias e Ingeniería.

Baca Flores, V. M. (2016). Diseño de un Sistema de Gestión de la Seguridad de la Información para la Unidad de Gestión Educativa Local – Chiclayo. Pimentel, Chiclayo, Lambayeque: Universidad Señor de Sipan.

Baca, V. (2016). Diseño de un sistema de gestión de la seguridad de la información para la unidad de gestión educativa local - Chiclayo. *Tesis de pregrado*. Chiclayo, Perú: Universidad Señor de Sipán.

Bernal, C. (2010). *Metodología de la investigación.* Sabana: Pearson.

Castro Siguas, J. J. (Julio de 2018). Implementación de la NTP ISO/IEC 27001:2014 para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional, Callao - 2017. Lima, Perú: Universidad Autónoma del Perú.

Celi, E. (2016). La gestión de riesgo TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque. *Pueblo Continente, 27*(1), 73 - 84 pp.

Conesa Caralt, J. (2010). *Introducción al Business Intelligence.* Barcelona: El Ciervo 96 SA.

Conesa, J. (2015). *Cómo crear un data warehouse.* Barcelona: UOC.

Cordova Yupanqui, J. E. (Abril de 2013). Análisis, diseño e implementación de una solución de inteligencia de negocios para el área de importaciones en una empresa comercializadora/importadora. Lima, Perú: Pontificia Universidad Católica del Perú.

COSO ERM. (2004). *Enterprise Risk Management - Integrated Framework.*

Cruz, J., Jalpilla, R., y Ramírez, E. (2017). Una Metodología de Análisis y Evaluación de Riesgos en Tecnologías de las Información. *Tesis de pregrado*. Universidad Nacional Autónoma de México.

Cueva Araujo, P. O. (2017). Gestión de la Historia Clínica y la Seguridad de la Información del Hospital II Cajamarca - ESSALUD bajo la NTP-ISO/IEC 27001:2014. Cajamarca, Cajamarca, Perú: Universidad Privada del Norte.

Daniel, C. (2000). *SISTEMAS DE INFORMACIÓN PARA LOS NEGOCIOS: UN ENFOQUE DE TOMA DE DECISIONES.* México: McGraw-Hill.

Del Caño, A. (2016). Gestión de riesgos en la dirección de proyectos : el modelo del Project Management Institute. Fundación MAPFRE Estudios.

Díaz, A., y Forero, J. (2018). Diseño de un sistema de gestión del riesgo basado en la norma ISO 31000:2011 para la empresa NEGOTEC. *Tesis de pregrado*. Bogotá, Colombia: Universidad de La Salle.

Enríquez Collaguazo, A. A. (2018). Modelo de gestión de seguridad de la información para instituciones de salud, basado en las normas ISO 27799:2008, ISO/IEC 27005:2008 e ISO/IEC 27002:2013 aplicada a la clínica médica fértil. Imbabura, Ecuador: Universidad Técnica del Norte.

Espinoza, H. (2015). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *Tesis PreGrado*. Lima: Pontificia Universidad Católica del Peru.

Espinoza, H. R. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.* Tesis para optar el título de Ingeniero Informático, Pontificia Universidad Católica del Perú, Lima. Obtenido de http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957

Galan, J. (2011). *Desarrollo de una solución de Business Intelligence para la mejora en el proceso de toma de decisiones estratégica en la gestión comercial de la empresa Trucks and Motors del Perú S.A.C.* Chiclayo: USAT.

Gaona Vásquez, K. d. (Octubre de 2013). Aplicación de Metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito SA en la ciudad de Machala. Cuenca, Ecuador: Universidad Politécnica Salesiana.

García Porras, J. C. (2017). Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú. Lima, Perú: Universidad Peruana de Ciencias Aplicadas.

Gomez, R., Pérez, D., Donoso, Y., y Herrera, A. (2015). Metodología y gobierno de la gestión de riesgos de tecnologías de la información. *Revista de Ingeniería*, pp. 109-118.

Guevara Chumán, J. G. (2015). Aplicación de la metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Lambayeque, Perú: Universidad Nacional Pedro Ruiz Gallo.

Hospital José Hernan Soto Cadenillas. (2016). Plan Estrategico Institucioal 2016- 2018. Cajamarca, Perú.

Hospital José Hernan Soto Cadenillas. (2017). Plan Operativo Institucional 2017. Cajamarca, Perú.

Inmon, B. (2005). *Building the Data Warehouse* . EEUU: Wiley.

ISACA. (2014). Implementation Guideline ISO/IEC 27001:2013. ISACA Germany Chapter e.V. Information Security Expert GroupImplementation.

ISACA®. (2012). *Cobit 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Madrid: Capítulo de Madrid de ISACA®.

Jaramillo Delgado, F. R. (Diciembre de 2016). Implementación de un datawarehouse para la toma de decisiones en el área logística de la compañía PRONACA. Bogotá, Colombia: Universidad de los Andes.

Kimball, R. (1998). *The Data Warehouse Lifecycle Toolkit.* EEUU: Wiley India.

Lopez, E., y Martel, P. (2001). *La escritura en uooh.* México D.F.: mmm.

Magerit. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Ministerio de Hacienda y Administraciones Públicas de España.

Matamoros Zapata, R. (2010). Implantación en una empresa de un sistema Business Intelligence SaaS / On Demand a través de la plataforma LITEBI. Valencia, España: Universidad Politécnica de Valencia.

Miguel Pérez, J. C. (2016). *Protección de datos y seguridad de la información.* Madrid: RAMA.

MINSA. (1990). DS-005-1990-SA. *Reglamento General de Hospitales*.

MINSA. (2004). N T Nº 0021- MINSA / DGSP V.01. *Norma Técnica - Categoría de establecimientos del sector salud*.

Mogollón, A. (2016). Análisis Comparativo: Metodologías de análisis de Riesgos. *Tesis de pregrado*. Barquisimeto, Venezuela: Universidad Centroccidenta "Lisandro Alvarado".

Montesino, R., Baluja, W., y Porven, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *Revista de Ingenieria Electrónica Automática y Comunicaciones*.

NTP-ISO/IEC 27005. (2009). *EDI. Tecnología de la información. Técnicas de seguridad. Gestión del riesgo en seguridad de la información.* Lima, Perú.

Ormella M., C. (2014). Gobierno de la seguridad de la información. Integración al Gobierno Corporativo. *Gestión y Auditoría de Riesgos y Seguridad de la Información*, pp. 1-6.

Ortiz, M. (30 de 04 de 2015). *Prezi*. Recuperado el 02 de 04 de 2020, de https://prezi.com/ooatecj5_fgt/guia-de-entrevista-y-de-observacion/

Patiño Rosado, S. G. (2018). Propuesta metodológica de gestión de riesgos de Tecnología de información y comunicación (TIC) para entidades públicas conforme normativa NTE INEN ISO/IEC 27005. Ecuador: Universidad de las Fuerzas Armadas de Ecuador.

Patiño, S. (2018). Propuesta metodológica de gestión de riesgos de tecnologías de información y comunicación (TIC) para entidades públicas conforme a la normativa NTE INEN ISO/IEC 27005. *Tesis de maestría*. Pichincha, Ecuador: Universidad de las Fuerzas Armadas.

Ramirez, A., y Ortiz, Z. (2015). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *Ingeniería, Vol. 16*(No. 2), 56-66 pp.

Ribas Alejandro, J. (2018). *Gestión de Riesgos Jurídicos Derivados de las Tecnologías de la Información*. España: Thomson Aranzadi.

Rodriguez Cabanillas, K. G. (Marzo de 2011). Análisis, diseño e implementación de una solución de inteligencia de negocios para el área de compras y ventas de una empresa comercializadora de electrodomésticos. Lima, Perú : Pontificia Universidad Católica del Perú.

Rodríguez, Y. (2016). Diseño y formulación de un sistema de gestión de riesgos basado en los lineamientos establecidos por la norma NTC-ISO31000 version 2011 para la empresa SIMMA Ltda. *Tesis de pregrado*. Bucaramanga, Colombia: Universidad Industrial de Santander.

Rollano, R. (2014). *Inteligencia de Negocios y Toma de Decisiones.* EEUU: CreateSpace Independent Publishing Platform.

SAAVEDRA, D. (2019). *Modelo de Seguidad informatica.* Chiclayo, Chiclayo, Chiclayo. Obtenido de https://mail.google.com/mail/u/0/#inbox/FMfcgxwGDDlBVJVSpJrGcfpKdpkcbtMM?projector=1ymessagePartId=0.1

Salazar Tataje, J. L. (2017). Implementación de inteligencia de negocios para el área comercial de la empresa Azaleia - basado en metodología Ágil Scrum. Lima: Universidad San Ignacio de Loyola.

Sotelo Bedón, M. (2019). Un proceso práctico de análisis de Riesgos de Activos de Información. Lima, Perú: Universidad Nacional Mayor de San Marcos.

Sotelo, M., Torres, J., y Rivera, J. (2016). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. *COMTEL 2012 - IV Congreso Internacional de Computación y Telecomunicaciones*, 121 - 127 p.

Talavera, V. (2015). *Diseño de un Sistema de Gestión De Seguridad de la Información para una entidad Estatal de Salud de acuerdo a la ISO/IEC 27001:2013.* Lima-Perú: Pontificia Universidad Católica del Perú.

Trujillo, J. C. (2011). *Diseño y explotación de almacenes de datos.* Alicante: Club Universitario.

Valencia Duque, F. J. (2016). *Aseguramiento y auditoría de tecnologías de información orientado a riesgos.* Colombia: Universidad Nacional de Colombia.

Vásquez Miranda, K. (2013). Guía Metodológica para Implementar un Sistema de Gestión de Seguridad en Instituciones. Piura, Piura: Universidad de Piura.

Young, E. y. (2011). *Seguridad de la información en un mundo sin fronteras.* Mancera SC.

IX. Anexos

ANEXO 01 - Clasificación de Activos de ISO 27005

N°	ACTIVO
1	Servidor principal de dominio (DNS) Incluye: Gestión del Directorio Activo
2	Servidor principal de base de datos y aplicaciones
3	Red de comunicaciones Incluye: Firewall, gabinetes de comunicación, switch central, switchs de borde
4	Sala de servidores del Centro de Procesamiento Central
5	Bases de Datos
6	Backups de base de datos
7	Personal de área de TI Incluye: especialista en comunicaciones, especialista de base de datos, jefatura de TI
8	Aplicaciones informáticas hospitalarias
9	Correo electrónico institucional
10	Equipos de cómputo terminales
11	Código fuente de las aplicaciones Incluye: biblioteca de versiones, librerías
12	Archivos de Actas de conformidad
13	Archivo de requerimientos informáticos (físico)
14	Analistas de sistemas (responsables de la implementación de requerimientos)
15	Equipos de cómputo del Área de Desarrollo Incluye: terminales, servidor de desarrollo, laptops
16	Backups o respaldos de desarrollo y mantenimiento Incluye: código fuente, librerías
17	Herramientas de desarrollo Incluye: base de datos de desarrollo, licenciamiento de software de desarrollo
18	Registros de control de cambios de las aplicaciones Incluye: scripts, cambios en estructuras de datos, carga de datos, manuales de usuario, pruebas realizadas
19	Backups de documentos normativos y de gestión: Incluye: reglamentaciones y procedimientos operacionales de gestión, desarrollo, calidad y seguridad), planes de TI, inventarios, contratos, etc.

ANEXO 02 – Encuesta Pre-Test

INSTRUCCIONES: Marque con un aspa (X), la alternativa correcta.

1. ¿Existe un sistema de gestión de la seguridad de la información en el hospital?

a) Si b) No

2. ¿Cree usted que el hospital logrará una mejora significativa con la aplicación de un SGSI?

a) Si b) No

3. ¿En el hospital se ha categorizado la información de acuerdo al grado de importancia que esta tiene?

a) Si b) No

4. ¿El personal del hospital ha recibido capacitación sobre seguridad de la información de acuerdo a su función?

a) Si b) No

5. ¿El personal del hospital cuenta con una clave de acceso para ingresar a su computadora?

a) Si b) No

6. ¿Cada oficina cuenta con software antivirus actualizado?

a) Si b) No

7. ¿Se ha realizado una evaluación de riesgos relacionados con la información?

a) Si b) No

8. ¿Se ha realizado una evaluación de vulnerabilidades de la red?

a) Si b) No

9. ¿Se realizan copias de seguridad para proteger su información?

a) Si b) No

10. ¿Las oficinas están protegidas contra amenazas externas o ambientales que ocasionen pérdidas de información?

a) Si b) No

ANEXO 03 - Valores y criterios de referencia para la valoración de la Disponibilidad, Integridad y Confidencialidad de los activos de TI

	Valor	Criterio
Disponibilidad	**1**	No aplica/No es relevante
	2	Debe estar disponible al menos el 10% del tiempo
	3	Debe estar disponible al menos el 50% del tiempo
	4	Debe estar disponible al menos el 75% del tiempo
	5	Debe estar disponible al menos el 95% del tiempo

	Valor	Criterio
Integridad	**1**	No aplica / No es relevante
	2	No es relevante los errores que tenga o la información que falte
	3	Tiene que estar correcto y completo al menos en un 50%
	4	Tiene que estar correcto y completo al menos en un 70%
	5	Tiene que estar correcto y completo al menos en un 95%

	Valor	Criterio
Confidencialidad	**1**	No aplica / No es relevante
	2	Daños muy bajos, el incidente no trascendería del área afectada
	3	Daños bajos, el incidente no trascendería del área afectada
	4	Los daños serían relevantes, el incidente implicaría a otras áreas
	5	Los daños serían catastróficos, la reputación y la imagen del hospital se verían comprometidas

ANEXO 04 - Tabla de referencia para catalogación de activos de TI

Tipo de activo		Sub clasificación		Descripción de aclaración
[info]	Información	[adm]	datos de interés para la administración pública	
		[dv]	datos vitales (registros de la organización)	Información esencial para la supervivencia de la Organización. Su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar: Aquellos que son imprescindibles para que la Organización supere una situación de emergencia Aquellos que permiten desempeñar o reconstruir las misiones críticas Aquellas de naturaleza legal o los derechos financieros de la Organización o sus usuarios.
		[per]	datos de carácter personal	Información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.
		[clasificado]	datos clasificados	Información sometida a normativa específica de control de acceso y distribución; es decir aquellos cuya confidencialidad es

				especialmente relevante. La tipificación de qué datos deben ser clasificados y cuáles son las normas para su tratamiento, vienen determinadas por regulaciones gubernamentales, sectoriales, por acuerdos entre organizaciones o por normativa interna.
[dato]	Datos o documentos	[files]	ficheros	
		[backup]	copias de respaldo	
		[conf]	datos de configuración	Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información
		[int]	datos de gestión interna	Incluye la información referente a los niveles de acceso asignados a los distintos tipos de usuario según su función o puesto de trabajo
		[password]	credenciales	Claves de acceso a máquina asignada o a las aplicaciones
		[auth]	datos de validación de credenciales	Códigos de identificación de usuario
		[acl]	datos de control de acceso	
		[log]	registro de actividad	Los registros de actividad sustancian los requisitos de trazabilidad. Bitácoras o log.
		[source]	código fuente	
		[exe]	código ejecutable	
		[test]	datos de prueba	Generados en las pruebas de las aplicaciones o módulos antes de puesta en producción
[keys]	Claves criptográficas	[info]	protección de la información	Claves públicas o privadas de cifrado o

				descifrado de la información
		[com]	protección de las comunicaciones	Claves de cifrado del canal de comunicación, claves de autenticación
		[disk]	cifrado de soportes de información	Cifrado de soportes de información
[serv]	Servicios	[www]	acceso a Internet	
		[telnet]	acceso remoto a cuenta local	
		[email]	correo electrónico	Servidor de correo electrónico
		[file]	almacenamiento de ficheros	Servidor de datos
		[ftp]	transferencia de ficheros	
		[edi]	intercambio electrónico de datos	
		[dir]	servicio de directorio	Directorio activo. Localización de personas, permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado
		[idm]	gestión de identidades	Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización
		[ipm]	gestión de privilegios	Aplicación para definir niveles de acceso
[sw]	Aplicaciones	[prp]	desarrollo propio (in house)	
		[sub]	desarrollo a medida (subcontratado)	
		[browser]	navegador web	
		[app]	servidor de aplicaciones	
		[email_client]	cliente de correo electrónico	
		[email_server]	servidor de correo electrónico	
		[file]	servidor de	

			ficheros	
		[dbms]	sistema de gestión de bases de datos	
		[office]	ofimática	
		[av]	anti virus	
		[os]	sistema operativo	
		[mv]	gestor de máquinas virtuales	
		[backup]	sistema de backup	
[hw]	Equipos informáticos	[host]	grandes equipos	Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente altos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción
		[mid]	equipos medios	Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción
		[pc]	informática personal	Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción
		[mobile]	informática móvil	Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a otro, pudiendo estar tanto dentro del

				recinto propio de la organización como en cualquier otro lugar
		[pda]	agendas electrónicas	
		[vhost]	equipo virtual	
		[backup]	equipamiento de respaldo	Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.
		[perife]	periféricos	Impresoras y servidores de impresión, escáneres
		[bp]	dispositivo de frontera	Son los equipos que se instalan entre dos zonas de confianza
		[network]	soporte de la red	Dícese de equipamiento necesario para transmitir datos: routers, módems, etc. Módems, conmutadores, routers, bridges, firewalls, WAP (punto de acceso inalámbrico)
		[pabx]	centralita telefónica	
		[ipphone]	teléfono IP	
[com]	Comunicaciones	[PSTN]	red telefónica	
		[ISDN]	RDSI (red digital)	
		[X25]	X25 (red de datos)	
		[ADSL]	ADSL	
		[radio]	comunicaciones radio	
		[wifi]	red inalámbrica	
		[mobile]	telefonía móvil	
		[sat]	por satélite	
		[LAN]	red local	
		[MAN]	red metropolitana	
		[Internet]	Internet	
[media]	Soporte de información	[electro]	electrónicos	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo: discos, DVD, cintas, etc.
		[noelectro]	no electrónicos	Material impreso
[aux]	Equipamiento auxiliar	[power]	fuentes de alimentación	
		[ups]	sistemas de alimentación ininterrumpida	

		[gen]	generadores eléctricos	
		[ac]	equipos de climatización	
		[cabling_wire]	cable eléctrico	
		[cabling_utp]	cable de datos	
		[fiber]	fibra óptica	
		[supply]	suministros esenciales	Tóner
		[furniture]	mobiliario: armarios, etc.	
		[safe]	cajas fuertes	
[Inmueb]	Instalaciones	[building]	edificio	
		[data]	Cuarto de procesamiento de datos	
		[backup]	instalaciones de respaldo	
[pers]	Personal	[ue]	usuarios externos	
		[ui]	usuarios internos	
		[op]	Operadores	
		[adm]	administradores de sistemas	
		[com]	administradores de comunicaciones	
		[dba]	administradores de BBDD	
		[sec]	administradores de seguridad	
		[des]	desarrolladores / programadores	
		[sub]	subcontratas	
		[prov]	proveedores	

ANEXO 05 - Tabla de escala de valoración de la criticidad de los activos de TI

[pi] Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7 – 8	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5 – 6	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3 – 4	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1 – 2	pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9 - 10	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7 - 8	probablemente cause un incumplimiento grave de una ley o regulación
5 - 6	probablemente sea causa de incumplimiento de una ley o regulación
3 – 4	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1 – 2	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9 - 10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7 - 8	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5 - 6	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3 – 4	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1 – 2	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales económicos	
9 - 10	de enorme interés para la competencia de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7 - 8	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
5 - 6	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3 – 4	de bajo interés para la competencia de bajo valor comercial
1 – 2	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
[da] de interrupción del servicio	

9 - 10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7 - 8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5 - 6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3 – 4	Probablemente cause la interrupción de actividades propias de la Organización
1 – 2	Pudiera causar la interrupción de actividades propias de la Organización
[po] de orden público	
9 - 10	alteración del orden público
7 - 8	probablemente cause manifestaciones, o presiones significativas
3 - 6	causa de protestas puntuales
1 – 2	pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7 – 8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5 – 6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3 – 4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1 – 2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] administración y gestión	
9 - 10	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7 - 8	probablemente impediría la operación efectiva de la Organización
5 - 6	probablemente impediría la operación efectiva de más de una parte de la Organización
3 – 4	probablemente impediría la operación efectiva de una parte de la Organización
1 – 2	pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1 - 2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones

[pd] persecución de delitos	
6 - 10	Impida la investigación de delitos graves o facilite su comisión
1 – 5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9 –10	RTO < 4 horas
7 – 8	4 horas < RTO < 1 día
4 – 6	1 día < RTO < 5 días
1 – 3	5 días < RTO

ANEXO 06 - Formato para validación modelo propuesto por expertos

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle ayuda en la validación de nuestra propuesta de investigación denominada **MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO**. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su colaboración.

NOMBRES Y APELLIDOS	: Gilberto Martín Ampuero Pasco
PROFESIÓN	: Ingeniero de Sistemas
AREA DE EXPERIENCIA	: Desarrollo de Software
TIEMPO DE EXPERIENCIA	: 20 años
CARGO ACTUAL	: Desarrollador Externo
INSTITUCIÓN	: Hospital Juan Pablo II

Objetivo de la investigación	: Desarrollar un modelo de gestión de riesgos de Tecnologías de Información para las etapas de identificación, análisis, evaluación y tratamiento de riesgos en el Hospital Privado Juan Pablo II de la Ciudad de Chiclayo, teniendo como referencia la ISO/IEC 27005 y la metodología Magerit.
Objetivo del juicio de expertos	: Validar el modelo de gestión de riesgos de Tecnologías de Información, aplicando los marcos de referencia ISO/IEC 27005 y la metodología MagerIT en relación a la suficiencia, claridad, coherencia y relevancia.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

FASE	ACTIVIDAD	SUFICIENCIA				CLARIDAD				COHERENCIA				RELEVANCIA			
		NC	BN	MN	AN	NC	BN	MN	AN	NC	BN	MN	AN	NC	BN	MN	AN
Identificación de los escenarios de riesgo de TI	Identificación y clasificación de los activos de TI				X				X			X				X	
	Valoración de la criticidad de los activos de TI				X				X				X				X
	Identificación de las amenazas de por activo de TI				X				X				X				X
	Identificación de vulnerabilidades de cada activo de TI				X				X				X				X
Valoración de los escenarios de riesgo de TI	Estimación del impacto de los escenarios de riesgo				X				X				X				X
	Estimación de la probabilidad de ocurrencia de los escenarios de riesgo				X				X			X					X
	Cálculo de los niveles de exposición a los riesgos			X					X			X					X
	Determinación del apetito y tolerancia al riesgo				X			X					X				X
Tratamiento de los riesgos	Definición de las políticas de seguridad			X					X			X				X	
	Identificación de los controles/salvaguardas de seguridad				X				X				X				X
	Definición de la estrategia de				X			X				X				X	

	implementación de controles/salvaguardas																
Seguimiento de la efectividad de los controles	Elaboración de planes de acción				X				X				X				X
	Definición de indicadores de riesgo				X				X				X				X
	Cálculo de los niveles de riesgo residual (NRR)				X				X				X				X

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los aspectos considerados en la actividad o tarea son suficientes para obtener la medición o calificación de la metodología.	1. No cumple con el criterio	Los aspectos considerados en la actividad o tarea no son suficientes para evaluar el modelo.
	2. Bajo Nivel	Los aspectos considerados en la actividad o tarea permiten medir algún aspecto del modelo, pero no corresponden con la totalidad de la actividad o tarea.
	3. Moderado nivel	Se deben incrementar algunos aspectos para poder evaluar la actividad o tarea del modelo completamente.
	4. Alto nivel	Los aspectos considerados en la actividad o tarea del modelo son suficientes.
CLARIDAD Los aspectos considerados en la actividad o tarea de la metodología se entienden fácilmente, es decir, su sintáctica y semántica son adecuadas.	1 no cumple con el criterio	La actividad o tarea no está claramente establecida o definida.
	2. Bajo Nivel	La actividad o tarea requiere significativas modificaciones para lograr su comprensión.
	3. Moderado nivel	Se requiere modificaciones muy específicas de algunos de los términos de la actividad o tarea para lograr la claridad total.
	4. Alto nivel	La actividad o tarea es clara, tiene semántica y sintaxis adecuada.
COHERENCIA Los aspectos considerados en la actividad o tarea de la metodología tienen una relación lógica con el objetivo o meta que se quiere lograr con la propuesta.	1 no cumple con el criterio	La actividad o tarea no tiene relación lógica con el objetivo perseguido.
	2. Bajo Nivel	La actividad o tarea tiene una relación tangencial con el objetivo perseguido.
	3. Moderado nivel	La actividad o tarea tiene una relación moderada con el objetivo que está midiendo.
	4. Alto nivel	La actividad o tarea se encuentra completamente relacionada con el objetivo que está midiendo.
RELEVANCIA Los aspectos considerados en la actividad o tarea son esenciales o importantes, para lograr los objetivos de la metodología propuesta.	1 no cumple con el criterio	La actividad o tarea puede ser eliminado sin que se vea afectada la medición del objetivo perseguido con el modelo.
	2. Bajo Nivel	La actividad o tarea tiene alguna relevancia, pero otra actividad o tarea puede estar asolapando o cumpliendo el objetivo de ésta.
	3. Moderado nivel	La actividad o tarea es relativamente importante para la adecuada aplicación del modelo.
	4. Alto nivel	La actividad o tarea es muy relevante y debe ser considerada en el modelo.

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle ayuda en la validación de nuestra propuesta de investigación denominada **MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO**. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su colaboración.

NOMBRES Y APELLIDOS	: Yovane Ramos Coronado
PROFESIÓN	: Ingeniero de Informática y Sistemas
AREA DE EXPERIENCIA	: Gestión de TI
TIEMPO DE EXPERIENCIA	: 10 años
CARGO ACTUAL	: Jefe de Sistemas
INSTITUCIÓN	: Hospital Juan Pablo II

Objetivo de la investigación	: Desarrollar un modelo de gestión de riesgos de Tecnologías de Información para las etapas de identificación, análisis, evaluación y tratamiento de riesgos en el Hospital Privado Juan Pablo II de la Ciudad de Chiclayo, teniendo como referencia la ISO/IEC 27005 y la metodología Magerit.
Objetivo del juicio de expertos	: Validar el modelo de gestión de riesgos de Tecnologías de Información, aplicando los marcos de referencia ISO/IEC 27005 y la metodología MagerIT en relación a la suficiencia, claridad, coherencia y relevancia.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

FASE	ACTIVIDAD	SUFICIENCIA				CLARIDAD				COHERENCIA				RELEVANCIA			
		NC	BN	MN	AN	NC	BN	MN	AN	NC	BN	MN	AN	NC	BN	MN	AN
Identificación de los escenarios de riesgo de TI	Identificación y clasificación de los activos de TI				X				X				X				X
	Valoración de la criticidad de los activos de TI				X				X			X				X	
	Identificación de las amenazas de por activo de TI				X			X				X				X	
	Identificación de vulnerabilidades de cada activo de TI			X					X				X			X	
Valoración de los escenarios de riesgo de TI	Estimación del impacto de los escenarios de riesgo			X					X				X				X
	Estimación de la probabilidad de ocurrencia de los escenarios de riesgo				X				X				X				X
	Cálculo de los niveles de exposición a los riesgos				X			X				X				X	
	Determinación del apetito y tolerancia al riesgo				X				X			X					X
Tratamiento de los riesgos	Definición de las políticas de seguridad			X				X				X				X	
	Identificación de los controles/salvaguardas de seguridad				X				X			X				X	
	Definición de la estrategia de				X				X			X				X	

	implementación de controles/salvaguardas																
Seguimiento de la efectividad de los controles	Elaboración de planes de acción				X			X					X				X
	Definición de indicadores de riesgo				X			X					X				X
	Cálculo de los niveles de riesgo residual (NRR)				X			X					X				X

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los aspectos considerados en la actividad o tarea son suficientes para obtener la medición o calificación de la metodología.	2. No cumple con el criterio	Los aspectos considerados en la actividad o tarea no son suficientes para evaluar el modelo.
	2. Bajo Nivel	Los aspectos considerados en la actividad o tarea permiten medir algún aspecto del modelo, pero no corresponden con la totalidad de la actividad o tarea.
	3. Moderado nivel	Se deben incrementar algunos aspectos para poder evaluar la actividad o tarea del modelo completamente.
	4. Alto nivel	Los aspectos considerados en la actividad o tarea del modelo son suficientes.
CLARIDAD Los aspectos considerados en la actividad o tarea de la metodología se entienden fácilmente, es decir, su sintáctica y semántica son adecuadas.	1 no cumple con el criterio	La actividad o tarea no está claramente establecida o definida.
	2. Bajo Nivel	La actividad o tarea requiere significativas modificaciones para lograr su comprensión.
	3. Moderado nivel	Se requiere modificaciones muy específicas de algunos de los términos de la actividad o tarea para lograr la claridad total.
	4. Alto nivel	La actividad o tarea es clara, tiene semántica y sintaxis adecuada.
COHERENCIA Los aspectos considerados en la actividad o tarea de la metodología tienen una relación lógica con el objetivo o meta que se quiere lograr con la propuesta.	1 no cumple con el criterio	La actividad o tarea no tiene relación lógica con el objetivo perseguido.
	2. Bajo Nivel	La actividad o tarea tiene una relación tangencial con el objetivo perseguido.
	3. Moderado nivel	La actividad o tarea tiene una relación moderada con el objetivo que está midiendo.
	4. Alto nivel	La actividad o tarea se encuentra completamente relacionada con el objetivo que está midiendo.
RELEVANCIA Los aspectos considerados en la actividad o tarea son esenciales o importantes, para lograr los objetivos de la metodología propuesta.	1 no cumple con el criterio	La actividad o tarea puede ser eliminado sin que se vea afectada la medición del objetivo perseguido con el modelo.
	2. Bajo Nivel	La actividad o tarea tiene alguna relevancia, pero otra actividad o tarea puede estar asolapando o cumpliendo el objetivo de ésta.
	3. Moderado nivel	La actividad o tarea es relativamente importante para la adecuada aplicación del modelo.
	4. Alto nivel	La actividad o tarea es muy relevante y debe ser considerada en el modelo.

Estimado Ingeniero:

A través de la presente nos dirigimos a usted con el fin de solicitarle ayuda en la validación de nuestra propuesta de investigación denominada **MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO**. Para tal fin, se anexa el cuestionario de validación.

Agradecemos su colaboración.

NOMBRES Y APELLIDOS	: Segundo José Castillo Zumarán
PROFESIÓN	: Ingeniero de Sistemas
AREA DE EXPERIENCIA	: Inteligencia de Negocios
TIEMPO DE EXPERIENCIA	: 20 años
CARGO ACTUAL	: Consultor Externo
INSTITUCIÓN	: Hospital Juan Pablo II

Objetivo de la investigación	: Desarrollar un modelo de gestión de riesgos de Tecnologías de Información para las etapas de identificación, análisis, evaluación y tratamiento de riesgos en el Hospital Privado Juan Pablo II de la Ciudad de Chiclayo, teniendo como referencia la ISO/IEC 27005 y la metodología Magerit.
Objetivo del juicio de expertos	: Validar el modelo de gestión de riesgos de Tecnologías de Información, aplicando los marcos de referencia ISO/IEC 27005 y la metodología MagerIT en relación a la suficiencia, claridad, coherencia y relevancia.

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

FASE	ACTIVIDAD	SUFICIENCIA				CLARIDAD				COHERENCIA				RELEVANCIA			
		NC	BN	MN	AN	NC	BN	MN	AN	NC	BN	MN	AN	NC	BN	MN	AN
Identificación de los escenarios de riesgo de TI	Identificación y clasificación de los activos de TI				X				X				X				X
	Valoración de la criticidad de los activos de TI				X				X				X				X
	Identificación de las amenazas de por activo de TI				X			X					X			X	
	Identificación de vulnerabilidades de cada activo de TI				X			X					X			X	
Valoración de los escenarios de riesgo de TI	Estimación del impacto de los escenarios de riesgo				X			X					X				X
	Estimación de la probabilidad de ocurrencia de los escenarios de riesgo				X				X				X				X
	Cálculo de los niveles de exposición a los riesgos				X				X			X					X
	Determinación del apetito y tolerancia al riesgo				X				X				X				X
Tratamiento de los riesgos	Definición de las políticas de seguridad			X					X				X				X
	Identificación de los controles/salvaguardas de seguridad				X				X				X				X
	Definición de la estrategia de			X					X				X				X

	implementación de controles/salvaguardas																
Seguimiento de la efectividad de los controles	Elaboración de planes de acción				X				X			X					X
	Definición de indicadores de riesgo			X					X				X				X
	Cálculo de los niveles de riesgo residual (NRR)				X				X				X				X

CATEGORIA	CALIFICACIÓN	INDICADOR
SUFICIENCIA Los aspectos considerados en la actividad o tarea son suficientes para obtener la medición o calificación de la metodología.	3. No cumple con el criterio	Los aspectos considerados en la actividad o tarea no son suficientes para evaluar el modelo.
	2. Bajo Nivel	Los aspectos considerados en la actividad o tarea permiten medir algún aspecto del modelo, pero no corresponden con la totalidad de la actividad o tarea.
	3. Moderado nivel	Se deben incrementar algunos aspectos para poder evaluar la actividad o tarea del modelo completamente.
	4. Alto nivel	Los aspectos considerados en la actividad o tarea del modelo son suficientes.
CLARIDAD Los aspectos considerados en la actividad o tarea de la metodología se entienden fácilmente, es decir, su sintáctica y semántica son adecuadas.	1 no cumple con el criterio	La actividad o tarea no está claramente establecida o definida.
	2. Bajo Nivel	La actividad o tarea requiere significativas modificaciones para lograr su comprensión.
	3. Moderado nivel	Se requiere modificaciones muy específicas de algunos de los términos de la actividad o tarea para lograr la claridad total.
	4. Alto nivel	La actividad o tarea es clara, tiene semántica y sintaxis adecuada.
COHERENCIA Los aspectos considerados en la actividad o tarea de la metodología tienen una relación lógica con el objetivo o meta que se quiere lograr con la propuesta.	1 no cumple con el criterio	La actividad o tarea no tiene relación lógica con el objetivo perseguido.
	2. Bajo Nivel	La actividad o tarea tiene una relación tangencial con el objetivo perseguido.
	3. Moderado nivel	La actividad o tarea tiene una relación moderada con el objetivo que está midiendo.
	4. Alto nivel	La actividad o tarea se encuentra completamente relacionada con el objetivo que está midiendo.
RELEVANCIA Los aspectos considerados en la actividad o tarea son esenciales o importantes, para lograr los objetivos de la metodología propuesta.	1 no cumple con el criterio	La actividad o tarea puede ser eliminado sin que se vea afectada la medición del objetivo perseguido con el modelo.
	2. Bajo Nivel	La actividad o tarea tiene alguna relevancia, pero otra actividad o tarea puede estar asolapando o cumpliendo el objetivo de ésta.
	3. Moderado nivel	La actividad o tarea es relativamente importante para la adecuada aplicación del modelo.
	4. Alto nivel	La actividad o tarea es muy relevante y debe ser considerada en el modelo.

ANEXO 07 – Validación de cuestionario

MODELO DE GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN BASADO EN LA ISO/IEC 27005 PARA EL HOSPITAL PRIVADO JUAN PABLO II DE LA CIUDAD DE CHICLAYO

Responsable: Céspedes Vega Charles y Rivera Barboza Darwin Jair

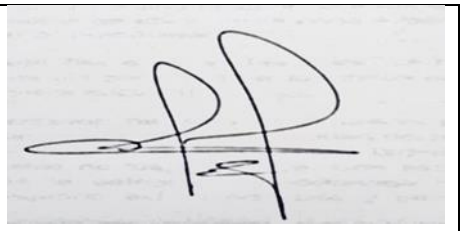
NOTA: Para cada pregunta se considera la escala de Likert:

Indicación: Señor (a) especializado (a) solicito su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta que le mostramos, marque con una (X) en el casillero que considere conveniente de acuerdo a su criterio y experiencia profesional indicando en qué nivel cuenta con los requisitos mínimos de formulación.

1. EXCELENTE (E)	2. BUENO (B)	3. REGULAR (R)	4. MALO (M)	5. PESIMO (P)

N°	ITEM	Medición				
		E	B	R	M	P
1	Identificación y clasificación de los activos de TI		X			
2	Valoración de la criticidad de los activos de TI	X				
3	Identificación de las amenazas de por activo de TI		X			
4	Identificación de vulnerabilidades de cada activo de TI	X				
5	Estimación del impacto de los escenarios de riesgo	X				
6	Estimación de la probabilidad de ocurrencia de los escenarios de riesgo	X				
7	Cálculo de los niveles de exposición a los riesgos		X			
8	Determinación del apetito y tolerancia al riesgo		X			
9	Definición de las políticas de seguridad		X			
10	Identificación de los controles/salvaguardas de seguridad	X				
11	Definición de la estrategia de implementación de controles/salvaguardas	X				
12	Elaboración de planes de acción	X				

13	Definición de indicadores de riesgo		X			
14	Cálculo de los niveles de riesgo residual (NRR)		X			

Nombre Completo	Segundo José Castillo Zumarán	
Grado académico	Ingeniero de Sistemas	