



**UNA UNIVERSIDAD CON ALMA DE GUERRERO**

# **IMPLEMENTACIÓN DE GESTIÓN DE RIESGOS DE TI PARA OBTENER LA CERTIFICACIÓN ISO 27001 EN EL HOSPITAL REGIONAL LAMBAYEQUE**

Tesis para optar por el Título de Ingeniero  
de Sistemas, que presenta la Bachiller.

**AUTORA**

**HILDA MILAGROS SANTA CRUZ QUIROZ**

**ASESOR**

**ING. HERMES MARINO QUINTEROS GONZALES**

**CHICLAYO - PERÚ 2016**



**IMPLEMENTACIÓN DE GESTIÓN DE RIESGOS DE TI PARA  
OBTENER LA CERTIFICACIÓN ISO 27001 EN EL HOSPITAL  
REGIONAL LAMBAYEQUE**

**Aprobación de la tesis:**

---

**Bach. Hilda Milagros Santa Cruz Quiroz  
Autora**

---

**Ing. Heber Iván Mejía Cabrera  
Asesor Metodológico**

---

**Ing. Hermes Marino Quinteros Gonzales  
Asesor Especialista**

---

**Ing. Jaime Arturo Bravo Ruiz  
Presidente de Jurado**

---

**Ing. Rosa América Cobeñas Sánchez  
Secretaria de Jurado**

---

**Ing. Hermes Marino Quinteros Gonzales  
Vocal de Jurado**

## DEDICATORIA

Posiblemente en este momento no entiendas mis palabras, pero para cuando seas capaz, quiero que te des cuenta de lo mucho que significas para mí.

Eres la razón de que me levante cada día, esforzarme por el presente y el mañana, eres mi principal motivación.

Gracias infinitas Matteo.



## AGRADECIMIENTO

Parece como si nunca hubiéramos estado en paz,  
siempre batallando por cualquier cosa; sin embargo,  
siempre llegaron los momentos en los que nuestra lucha  
cesó e hicimos una tregua para lograr metas conjuntas.

Les agradezco no solo por estar presentes aportando  
buenas cosas a mi vida, sino por los grandes momentos  
de felicidad y diversas emociones que siempre me han  
causado.

Gracias Familia.

## ÍNDICE

DEDICATORIA.....	i
AGRADECIMIENTO.....	ii
ÍNDICE.....	iii
RESUMEN.....	v
ABSTRACT.....	vi
INTRODUCCIÓN .....	vii
<b>CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN.....</b>	<b>10</b>
1.1. Problematización .....	10
1.2. Formulación del Problema .....	16
1.3. Justificación e importancia .....	16
1.4. Objetivos .....	18
<b>CAPÍTULO II: MARCO TEÓRICO .....</b>	<b>19</b>
2.1. Antecedentes de Estudios.....	19
2.2. Estado del Arte .....	22
2.3. Sistemas teórico conceptuales .....	23
<b>CAPÍTULO III: MARCO METODOLÓGICO .....</b>	<b>38</b>
3.1. Trayectoria Cualitativa.....	38
3.2. Enfoque Seleccionado.....	39
3.3. Objeto de Estudio .....	39
3.4. Sujetos Participantes.....	46
3.5. Métodos, técnicas e instrumentos de recolección de datos.....	46
3.6. Procedimiento para la recolección de datos .....	46
3.7. Procedimiento de análisis de datos.....	47
3.8. Criterios éticos .....	47
3.9. Criterios de rigor científico.....	48
<b>CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS .....</b>	<b>50</b>
4.1. Análisis y discusión de los resultados .....	50
4.2. Consideraciones finales.....	70
<b>CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN.....</b>	<b>73</b>



<b>CAPÍTULO VI: CONSIDERACIONES FINALES Y RECOMENDACIONES</b> .....	142
<b>6. 1. Consideraciones finales</b> .....	142
<b>6. 2. Recomendaciones</b> .....	143
<b>REFERENCIAS</b> .....	144
<b>ANEXOS</b> .....	146

## RESUMEN

Uno de los principales problemas que afrontan las instituciones hoy en día es la inadecuada gestión de riesgos, considerando la percepción y realidad de los riesgos que podrán afectarlas, dañando así su integridad.

Es por ello, que se ha creído conveniente realizar el análisis de los riesgos de TI del Hospital Regional Lambayeque, y así poder establecer una adecuada gestión de riesgos que nos ayude a asegurar la continuidad del Negocio, para tal motivo se creyó conveniente utilizar la metodología MagerIT, la cual según un análisis realizado teniendo en cuenta las principales características de las diversas metodologías que existen para tratar gestión de riesgos, es la más indicada para este tipo de Institución Pública.

Esta metodología nos permitirá el correcto análisis de los riesgos para luego plantear la mejor respuesta a cada uno de ellos, asegurando así la confidencialidad y resguardo de la información en el Hospital Regional Lambayeque.

## ABSTRACT

One of the main problems facing the institutions Today is inadequate risk management, considering the perception and reality of the risks which may affect them, damaging So Do Integrity.

It is for wave, which is thought proper to Perform Risk Analysis IT Regional Hospital of Lambayeque, and so to establish adequate risk management help us one Ensuring Business Continuity paragraph that reason m is wanted As use the Magerit methodology, whatever the according to an analysis taking into account the main characteristics of the various methodologies EXIST para TREAT Risk Management, is the most suitable paragraph This type of public institution.

This methodology will allow us to correct Risk Analysis then raise the best answer to each of them, thus ensuring privacy and safeguarding Use the information in the regional hospital of Lambayeque.





## INTRODUCCIÓN

Una buena gestión de Tecnologías de Información es de gran relevancia en el mercado, un punto de crítica importancia al respecto es la gestión de riesgos tecnológicos, que en una gran medida pueden ser desencadenantes de riesgos operacionales para la empresa (Romeral & Torres Gallego, 2008).

La mayoría de los empresarios y/o dirigentes de las instituciones creen que los riesgos están creciendo cada día más, lo cual hace que las compañías e instituciones sientan que hay más riesgos para invertir en los cambios tecnológicos. La gestión de riesgos debe ser considerada como un proceso cíclico que incluye el análisis y la priorización de riesgos. Estas actividades permiten a la organización tener una visión detallada y exacta de los riesgos, y constituyen una buena herramienta de decisión acerca de qué riesgos pueden ser gestionados en un entorno de recursos limitados (Romeral & Torres Gallego, 2008).

En el entorno y dinámica competitiva actuales, la posesión de tecnología no supone por sí misma una ventaja competitiva para las organizaciones, es la gestión de esa tecnología la que puede darle una ventaja competitiva o un factor diferencial con especial énfasis en la gestión de los riesgos derivados del uso de Tecnología de la Información (Marulanda Echeverry, López Trujillo, & Cuesta Iglesias, 2009).

## CAPÍTULO I: PROBLEMA DE INVESTIGACIÓN

### 1.1. Problematización

Los problemas o los fallos de los sistemas informáticos ocasionan graves crisis empresariales, daños en la reputación causados por suplantaciones de identidad, pérdidas de negocios por fallos en sistemas, así como restricciones normativas que surgen por temas derivados del cumplimiento de las políticas establecidas.

Hemos podido ver algunas noticias sobre historias relacionadas con los riesgos en las tecnologías de la información, incluyendo ataques de phishing, robo de datos confidenciales, suplantaciones de identidad, robo de cintas con copias de seguridad, pleitos derivados de un deficiente mantenimiento y backup de registros electrónicos, problemas derivados de la propiedad intelectual, entre otros. (Fuertes, 2007)

Debido a esto, los ejecutivos de diversas corporaciones, se ven en la necesidad de reducir de manera significativa el riesgo, y mejorar los rendimientos de las inversiones realizadas en sistemas informáticos. Los riesgos de TI necesitan ser identificados, medidos y gestionados como parte de un único entorno que incorpora todos los riesgos corporativos. Asimismo, dichos riesgos informáticos deben estar supervisados por el equipo de gestión de mayor nivel para conocer y ofrecer pautas

que permitan establecer las combinaciones apropiadas de riesgos/recompensas, y con ello conseguir un mayor rendimiento de las inversiones en TI. (Fuertes, 2007)

Todas estas acciones para gestionar y equilibrar los riesgos y recompensas en bienes informáticos es Gestión de Riesgos en TI; el cual, no puede verse como un proceso aislado, sino todo lo contrario, es parte integral para la creación de valor, y por lo tanto tiene influencia directa en los otros componentes de la empresa.

Las tecnologías y los sistemas de información (TSI) se han convertido en los elementos más esenciales para la supervivencia de las organizaciones, ya que de las TSI dependen el buen funcionamiento y la evolución de sus procesos de negocio, así como la información que necesitan para tomar todas sus decisiones operacionales, tácticas y estratégicas. (Fernández Sánchez & Piattini Velthuis, 2012)

Esto significa que el diseño de nuevos productos y servicios, la eficiencia de las operaciones y la capacidad de reaccionar ante cambios en el entorno competitivo depende, en gran medida, de la capacidad de adquirir, procesar y analizar información, lo que permite a su vez brindar a la alta dirección información de forma continua, oportuna y condensada para un adecuado proceso de toma de decisiones respecto a riesgos y controles.

Con el entorno y dinámicas competitivas de la actualidad, contar con tecnología de información y comunicaciones no supone por sí misma una ventaja competitiva para las organizaciones. Es la gestión de esa tecnología la que puede dar una ventaja o marcar factor diferencial para el éxito de éstas. De acuerdo a esto, apropiarse de un modelo de gobierno de TI, para esta gestión, es un elemento clave para el cumplimiento de los objetivos de la empresa (Marulanda Echeverry, López Trujillo, & Cuesta Iglesias, 2009).

Por ello, cobran cada día más interés el gobierno y la gestión de las TSI, temas en los cuales el director de TI es llamado a desempeñar un papel crucial. El director de TI deberá implementar un conjunto de buenas prácticas de gobierno y de gestión en las diferentes áreas relacionadas con la prestación de servicios, desarrollo de software, seguridad, gestión de activos, etc. (Fernández Sánchez & Piattini Velthuis, 2012).

Según (Westerman, 2006) con la tecnología de la información convirtiéndose en una parte cada vez más importante en toda empresa, la gestión de riesgos de TI se ha convertido en vital importancia para las oficialías de seguridad de la información y sus contrapartes comerciales. Cada empresa se enfrenta a un gran número de riesgos como parte de hacer negocios. Algunos



riesgos, como la pérdida de un ejecutivo clave, no están relacionados con TI. Otros, como el riesgo de crédito global, tienen un importante componente de TI.

Toda empresa desarrolla un “Perfil de Riesgo Empresarial”. Todavía, pocas organizaciones, al considerar una nueva iniciativa (producto o servicio), van más allá del retorno de la inversión y no consideran su efecto sobre el perfil de riesgo de la empresa. Se debe tener en cuenta que un cambio en TI afecta múltiples dimensiones dentro de la empresa. Muchas empresas caen en patrones de análisis de un solo tipo de riesgo, comúnmente disponibilidad, dándosele prioridad sobre los demás. O, peor aún, no tienen la capacidad para analizar y examinar más de una dimensión de riesgo. Con el tiempo, esta forma de gestión del riesgo se convierte en una práctica habitual de la empresa, dando lugar a un perfil de riesgo en la que algunos riesgos están bien controlados, mientras que otros tienen enormes, a menudo desconocidos, exposiciones (Westerman, 2006).

La pregunta es ¿cómo hacer que la gestión de TI desarrolle un modelo de perfil de riesgo de TI empresarial, concordante con su Sistema de Gestión de Sistemas de Información (SGSI) y capacidad instalada de TI; y a su vez que satisfaga todas las





perspectivas funcionales de los responsables de la gobernanza y de la gestión de las TI internos y externos?

En los últimos años, la gestión de los riesgos del negocio, incluidos los derivados de las inversiones tecnológicas, se ha ubicado en el puesto número cuatro de la lista de prioridades de las empresas, cuando hasta hace poco se encontraba en una posición que ni siquiera se acercaba al top ten, según un estudio de la consultora Gartner, que analizó las opiniones de unos 880 Ejecutivos de Tecnologías de Información (CIOs), mostrado en la revista *Perspectivas Microsoft*.

Los riesgos de las inversiones tecnológicas son hoy contingencias de nivel empresarial, y por lo tanto, no podemos hablar de ningún elemento de riesgo de negocio sin haber contemplado antes estos mismos peligros para la TI. (Richard Hunter, vicepresidente de la firma de investigación Stamford).

Los riesgos de seguridad de información deben ser considerados en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, etcétera y los clientes deben ser identificados para lograr una imagen global y completa de estos riesgos.

Cada organización tiene una misión, en esta era digital, las organizaciones que utilizan sistemas tecnológicos para automatizar sus procesos o información deben de estar conscientes que la administración del riesgo informático juega un rol crítico. La meta principal de la administración del riesgo informático debería ser “proteger a la organización y su habilidad de manejar su misión” no solamente la protección de los elementos informáticos. Además, el proceso no solo debe de ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización (Stoneburner, Goguen, & Feringa, 2002).

Es importante recordar que el riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia. Por lo que podemos decir a grandes rasgos, la administración de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable.

El análisis de riesgo informático es un elemento que forma parte del programa de gestión de continuidad de negocio (Business Continuity Management), donde es necesario identificar si existen controles que ayudan a minimizar la probabilidad de ocurrencia



de la vulnerabilidad (riesgo controlado), de no existir, la vulnerabilidad será de riesgo no controlado.

Dentro de la evaluación del riesgo es necesario realizar acciones como calcular el impacto en caso que la amenaza se presente, tanto a nivel de riesgo no controlado como el riesgo controlado; así como evaluar el riesgo de tal forma que se pueda priorizar. Esta evaluación se puede realizar de dos formas, cuantitativa asignando pesos o cualitativa mediante una matriz de riesgos

El Hospital Regional Lambayeque, siendo una de las instituciones de mayor importancia y complejidad de la Región Lambayeque, tanto que se constituye como un Hospital con nivel III-1, es decir un nosocomio de Alta Complejidad; genera la necesidad de gestionar riesgos para optimizar sus recursos y aumentar su productividad llevando así a brindar servicios integrales de salud que contribuyen a mejorar la calidad de vida de las personas.

## **1.2. Formulación del Problema**

¿Cómo mejorar la Gestión de Riesgos de TI en el Hospital Regional Lambayeque?

## **1.3. Justificación e importancia**

La gestión de riesgos de TI es importante porque tiene como principal objetivo asegurar la continuidad del negocio; y para conseguirlo, es necesario es necesario establecer un Proceso de

Continuidad de los Sistemas, que nos proporcione métricas relevantes. Estas métricas deben servir de base para obtener informes y un Cuadro de Mando ejecutivo, los cuales facilitarán la toma de buenas decisiones de gestión (Romeral & Torres Gallego, 2008).

Los temas relativos a la gestión de las Tecnologías de Seguridad de la Información (TSI) son cada vez más importantes para las empresas, ya que el gasto e inversión en TSI no se controlan como se debiera, y en demasiadas ocasiones no se consigue un uso eficaz, eficiente y económico de las TIC. En los últimos años han surgido numerosos marcos y normas ISO para la gestión de las TSI, que consideramos como una valiosísima ayuda en la consecución de este objetivo, aun teniendo en cuenta que siempre deberemos evaluar los riesgos que suponen las TIC valorando su importancia respecto a los controles y costes que pueden conllevar.

En un futuro cercano, todos los departamentos de informática deberán tener implantadas buenas prácticas que cubran las diferentes áreas de gestión, para lo cual centrarán sus esfuerzos en definir, medir y analizar los procesos relacionados con las TSI y en su mejora continua; los CIO's estarán alineados e integrados con los objetivos de sus empresas u organizaciones para lograr la

excelencia en el servicio de las TIC, innovando y desarrollando nuevos productos. Y ello no es el fruto de una moda: es un síntoma de la madurez que está alcanzando la gestión de las TSI (Fernández Sánchez & Piattini Velthuis, 2012).

## **1.4. Objetivos**

### **1.4.1. Objetivo General**

Implementar una adecuada gestión de riesgos de TI para reducir los riesgos de los activos existentes en el Hospital Regional Lambayeque a fin de obtener la certificación ISO 27001.

### **1.4.2. Objetivos Específicos:**

- a. Seleccionar la metodología adecuada para la gestión de riesgos en el Hospital Regional Lambayeque.
- b. Planificar la Administración de Riesgos.
- c. Identificar los Riesgos de los principales activos de la institución.
- d. Realizar un Análisis de Cualitativo y Cuantitativo de Riesgos.
- e. Planificar los mecanismos de protección de darán respuesta a los Riesgos.



## CAPÍTULO II: MARCO TEÓRICO

### 2.1. Antecedentes de Estudios

(Celi Arévalo E. , 2013), en su trabajo de investigación denominado “Un modelo para la gestión de riesgos de TI en las empresas microfinancieras: Caso Lambayeque, Perú”; en el cual propuso un modelo de gestión de riesgos operativos relacionadas con las tecnologías de información como parte de un sistema de gestión de la seguridad de la información, desde una perspectiva que integra técnicas cuantitativas y cualitativas, teniendo como base a ISO/IEC 27001, ISO/IEC 27002, la metodología MagerIT, y el marco normativa de la SBS, que es el ente que rige a las empresas financieras. Se logró implementar un modelo de gestión de riesgos de TI, que identifica, evalúa y trata nítidamente los activos de TI, sus amenazas, debilidades y niveles de riesgo relacionadas con las categorías: disponibilidad, integridad y confidencialidad de la información, que exige la SBS para este tipo de organizaciones en sus planes de seguridad; quedando así demostrado que el producto tangible de la metodología de gestión de riesgos es la matriz de riesgos, la cual sirve de información para la toma de decisiones en relación a la inversión para la implementación de los controles que sirvan de salvaguardas en la protección del proceso contra posibles amenazas y vulnerabilidad, permitiendo una adecuada sinergia con los



procedimientos de continuidad del negocio. La metodología MagerIT, sirve como marco de referencia para poder implementar gestión de riesgos de ti, puesto que nos muestra paso a paso lo que debemos hacer para lograrlo.

(López Vargas, Salmerón Silvera, & Mena Nieto, 2009), en su trabajo de investigación denominado “Análisis de los riesgos en proyectos SI/TI basado en el enfoque IPA”, plantearon una matriz denominada IP (Importancia – Rendimiento), basada en dos variables impacto y probabilidad; donde un riesgo será más o menos importante en función del grado en el que impacta negativamente sobre el éxito del proyecto; por tanto, el nivel de impacto de cada riesgo indica la importancia del mismo; y la existencia o producción del riesgo depende del grado de probabilidad de ocurrencia en el proyecto. Dicha matriz, está basada en IPA, una herramienta que da soporte a la priorización y toma de decisiones, permitiendo identificar, analizar los riesgos en proyectos SI/TI y definir qué estrategias deben seguir los profesionales para tratarlos de forma eficaz. Compañías de todo el mundo realizan importantes esfuerzos desarrollando proyectos SI/TI, pero resultan fallidos en demasiadas ocasiones; para evitar que esto se produzca se elaboró una taxonomía compuesta por 46 riesgos clasificados en 6 categorías en función de sus características, los profesionales pueden utilizarla como lista de



control para identificar las amenazas existente en sus proyectos, que no debe ser cerrada, permitiendo así que los profesionales la actualicen cada vez que identifiquen nuevos riesgos en sus proyectos. Luego se planteó la matriz IP, la cual en función del área en que se sitúa cada riesgo, indica qué estrategias deben seguir para minimizar eficientemente los riesgos existentes en sus proyectos; de esta manera, pueden planificar y ejecutar el proyecto, y a la vez gestionar los riesgos clave que lo amenazan.

(Celi Arévalo E. K., 2015), en su trabajo de investigación denominado “Aplicación de Dashboards y Scorecards para el Aprendizaje - Modelos de Gestión de Riesgos de TI: Una Experiencia de Usuario” nos presenta el proceso de formación de los estudiantes, y la formación profesional en temas como Gestión de Riesgos, lo cual implica el uso de marcos de referencia como MagerIT u Octave. La comprensión de estos marcos se convierte en difíciles sesiones de aprendizaje cuando son cortos, incluso si utilizamos un software específico, debido al gran número de elementos para identificar, comprender, relacionar y aplicar. El uso de cuadros de mando y scorecards preparados de herramientas como Excel ayuda a mejorar este aprendizaje. El propósito de este estudio fue medir la utilidad y la eficacia en el logro de los resultados esperados, la evaluación de la experiencia de los usuarios a través de cuestionarios tipo de sistema



Usabilidad Escala Usabilidad (SUS); y examinar las necesidades y expectativas de los usuarios. Los resultados muestran que participantes aprenden más rápido la aplicación práctica de los marcos estudiados, debido a que los cuadros de mando permiten que sean más fáciles de identificar sus elementos y su aplicación práctica.

## **2.2. Estado del Arte**

Desde 1901, y como primera entidad de normalización a nivel mundial, British Standards Institution (BSI), es responsable de la publicación de importantes normas como: 1979 Publicación BS 5750 - ahora ISO 9001, 1992 Publicación BS 7750 - ahora ISO 14001, 1996 Publicación BS 8800 - ahora OHSAS 18001.

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa un conjunto de buenas prácticas para la gestión de la seguridad de su información (Marulanda Echeverry, López Trujillo, & Cuesta Iglesias, 2009).

BS 7799, el estándar para la gestión de seguridad de la información que cubre el uso apropiado y eficaz de los controles de seguridad tras un análisis de riesgo que identifica los activos correspondientes y las amenazas a la seguridad de ellos (Kenning, 2001).

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de julio de 2007 manteniendo el contenido así como el año de publicación formal de la revisión (Marulanda Echevrry, López Trujillo, & Cuesta Iglesias, 2009).

### **2.3. Sistemas teórico conceptuales**

#### **2.3.1. Definición de Riesgo:**

En términos generales, podemos definir el riesgo como la posibilidad de que los eventos, los impactos resultantes, las acciones asociadas, y las interacciones dinámicas entre los tres, pueden ser distintas de lo previsto.

Según la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información en versión 2 (MagerIT v2), riesgo es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios al a Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir,



analizar el sistema. (Ministerio de Administraciones Públicas de España, 2006)

Hay un gran debate sobre si el riesgo es una característica objetiva o refleja las percepciones subjetivas que impulsan a la toma de decisiones, toda vez que para la psicología, los individuos anclan su percepción de riesgo en relación con algún nivel de aspiración (Shapira & Berndt, 1997); (Tversky & Kahneman, 1986).

El riesgo es simplemente la posibilidad de complicaciones y problemas con respecto a la finalización de una tarea y la consecución de una anotación. El riesgo es inherente a todas las empresas, incluidos los proyectos de ingeniería y construcción. Como tal, nunca puede eliminarse por completo, pero se puede manejar de manera efectiva para mitigar los impactos a la consecución de los objetivos de un proyecto. Proyectos diseñados y construidos suelen definir los objetivos en términos de tiempo, coste y rendimiento.

En cualquier proyecto para cumplir con estos objetivos definidos, el riesgo debe ser gestionado, y por lo tanto debe integrarse en el enfoque de gestión de los componentes del proyecto general del proyecto. Esta integración sólo puede lograrse mediante la identificación primera de las principales fuentes de riesgo y

cuando se producen durante la vida de un proyecto diseñado y construido.

Ejemplos específicos ofrecen información a los contratistas, gerentes de construcción y propietarios involucrados con proyectos internacionales diseñados y construidos para ayudar en la identificación y evaluación de los principales recursos de los riesgos adecuadamente. Tras la identificación de las fuentes y el calendario de riesgo, es necesaria una comprensión de los diversos tipos de impactos que resultan rutinariamente de los riesgos para facilitar el desarrollo / utilización del potencial de mitigación y gestión de mecanismos / procesos.

Además, para facilitar este entendimiento, es necesario analizar el ciclo de vida de un proyecto típico diseñado y construido, concentrándose específicamente en los procesos que se están implementando, así como del momento de relativo. Este conocimiento del ciclo de vida del proyecto permite una comprensión global de los principales factores de riesgo identificados, incluyendo el tiempo y el impacto del riesgo. Es sólo a través de esta comprensión fundamental de que los posibles mecanismos y procesos para la mitigación de los impactos resultantes de las principales fuentes de riesgo pueden ser implementadas de manera efectiva. (Cohen, PE, & Palmer, 2004)

En base a lo antes mencionado, European Network and Information Security Agency (ENISA) nos dice que la Gestión de Riesgos es el proceso distinto de la evaluación de riesgos, que considera las normativas en consulta con las partes interesadas, teniendo en cuenta la evaluación de riesgos y otros factores pertinentes, y la selección de las opciones de prevención y control apropiadas. Así mismo, se considera como el conjunto de cinco procesos principales: Definición de Alcance, la Evaluación de Riesgos, Tratamiento de Riesgos, Comunicación de Riesgos, y Supervisar y Examinar (ENISA, 2006).

**Definición de Alcance:** Proceso para el establecimiento de parámetros globales para el rendimiento de Gestión de Riesgos dentro de una organización. Dentro de la definición del ámbito de aplicación de Gestión de Riesgos, han de ser adoptadas tanto factores internos como externos en cuenta (ENISA, 2006).

**Evaluación de riesgos:** Proceso científico y tecnológicos que comprende tres etapas: la identificación de riesgos, análisis de riesgos y evaluación de riesgos (ENISA, 2006).

**El tratamiento del riesgo:** Proceso de selección e implementación de medidas para modificar el riesgo. Medidas de tratamiento del riesgo pueden incluir evitar, la optimización, la transferencia o retención de riesgo (ISO/IEC Guide 73, 2008).



**La comunicación de riesgos:** Proceso para intercambiar o compartir información acerca de los riesgos entre el tomador de decisiones y otras partes interesadas dentro y fuera de una organización (por ejemplo, departamentos y empresas externas, respectivamente).

La información puede relacionarse con la existencia, naturaleza, forma, la probabilidad, la gravedad, la aceptabilidad, el tratamiento u otros aspectos de riesgo (ISO/IEC Guide 73, 2008).

**Supervisar y revisar:** Un procedimiento para medir la eficiencia y eficacia de los procesos de gestión de riesgos de la organización es el establecimiento de un proceso de seguimiento y examen en curso. Este proceso se asegura de que los planes de acción de gestión especificados siguen siendo relevante y actualizada. Este proceso también lleva a cabo actividades de control incluyendo la re-evaluación del alcance y cumplimiento con las decisiones (ENISA, 2006).

### 2.3.2. Introducción al análisis y gestión de riesgos

Seguridad es la capacidad de las redes o de los sistemas de información para resistir con un determinado nivel de confianza a los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y

confidencialidad de los datos almacenados o transmitidos, y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Para (Ministerio de Administraciones Públicas de España, 2006), el objetivo a proteger es la misión de la Organización, teniendo en cuenta las diferentes dimensiones de la seguridad:

**Disponibilidad:** Es la disposición de los servicios a ser usados cuando sea necesario, su carencia supone una interrupción del servicio, la cual afecta directamente en la productividad de las organizaciones.

**Integridad:** Mantenimiento de las características de completitud y corrección de los datos. La integridad afecta directamente al correcto desempeño de las funciones de una organización, cuando la información puede aparecer manipulada, corrupta o incompleta.

**Confidencialidad:** Es una propiedad de difícil recuperación porque pueden darse fugas o filtraciones de información, así como accesos no autorizados; suponiendo así, el incumplimiento de leyes y compromisos relativos a la custodia de los datos.

### **2.3.3. Fases para la Metodologías para el Análisis de**

#### **Riesgos:**

- Caracterización del sistema

- Identificación de amenazas
- Identificación de vulnerabilidades
- Análisis de controles
- Determinación del riesgo
- Recomendaciones de control
- Documentación de resultados
- Establecimiento de parámetros
- Necesidades de Seguridad

### **2.3.4. Metodologías**

#### **2.3.4.1. MagerIT**

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MagerIT) ha sido elaborada y promovida por el Consejo Superior de Administración Electrónica (CSAE) como respuesta a la percepción de que la Administración, y en general toda la sociedad, depende de forma creciente de las tecnologías de información para la consecución de sus objetivos de servicio.

Su razón de ser, está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios.



Es imprescindible conocer el riesgo al que están sometidos los elementos de trabajo para poder gestionarlos, para ello han aparecido multitud de guías informales, aproximaciones metódicas y herramientas de soporte, que buscan objetivar el análisis para saber cuán seguros o inseguros están. El reto aquí es la complejidad del problema al que se enfrentan, es por ello que se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

El temor a lo desconocido es el principal origen de la desconfianza; lo ideal es que los sistemas no fallen, pero se acepta convivir con sistemas que fallan; el asunto no es tanto la ausencia de incidentes sino la confianza de que estén bajo control, saber qué pasa y cuándo puede pasar. Por todo ello, se busca conocer los riesgos para poder afrontarlos y controlarlos, y así cumplir con los objetivos de las organizaciones.

**Objetivos:**

**a. Directos:**

Concientizar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.

Ofrecer un método sistemático para analizar tales riesgos.



Ayudar a descubrir y planificar las medidas oportuna para mantener los riesgos bajo control.

**b. Indirectos:**

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

**2.3.4.2. Mehari**

La metodología MEHARI se diseñó inicialmente y se actualiza continuamente, para ayudar a los Chief Information Security Officers (CISO) en la gestión de actividades de la seguridad de información, también está concebida para auditores, CIO's o gestores de riesgos que comparten ampliamente los mismos o similares retos.

Tiene como objetivo proporcionar un método para la evaluación y gestión de riesgos, concretamente en el dominio de la seguridad de la información, conforme a los requerimientos de la ISO/IEC 27005:2008, proporcionando el conjunto de herramientas y elementos necesarios para su implementación; además que, permite un análisis directo e individual de situaciones de riesgos descritas en los escenarios, y proporciona un completo conjunto de herramientas específicamente diseñadas para la gestión de la seguridad a corto, mediano y largo plazo, adaptables a diferentes

niveles de madurez y tipos de acciones consideradas (CLUSIF, 2010).

#### **2.3.4.3. Octave**

La metodología OCTAVE (Operationally Critical Threats Assets and Vulnerability Evaluation), desarrollada por el Equipo de Respuesta ante Emergencias Informáticas (CERT, por sus siglas en inglés), evalúa los riesgos de seguridad de la información y propone un plan de mitigación de los mismos dentro de una empresa. Por tanto, se tienen en cuenta las necesidades de la empresa donde se está implementando, permitiendo reducir los riesgos de seguridad de información, para lograr una mayor protección a estos elementos dentro del sistema. OCTAVE equilibra aspectos de riesgos operativos, prácticas de seguridad y tecnología para que a partir de éstos, los entes empresariales puedan tomar decisiones de protección de información basado en los principios de la seguridad de la información. Esta metodología persigue dos objetivos específicos que son: concientizar a la organización que la seguridad informática no es un asunto solamente técnico y presentar los estándares internacionales que guían la implementación de seguridad de aquellos aspectos no técnicos. Con una metodología de análisis de riesgos como OCTAVE la empresa puede obtener beneficios como: dirigir y



gestionar adecuadamente sus evaluaciones de riesgos, tomar decisiones basándose en los mismos, proteger los activos de información y, por último, comunicar de forma efectiva la información clave de seguridad, los cuales se derivan de las siguientes características: en primera medida, se establecen equipos auto dirigidos dentro de la organización con la finalidad de dar solución a las necesidades de seguridad que esta puede tener. Y por otro lado, se dice que este método es FLEXIBLE ya que es adaptable a todo tipo de organización independientemente de la capacidad de recuperación y la experiencia que se tenga en este tema. Finalmente, es importante mencionar que OCTAVE busca asegurar la continuidad del negocio, identificar y medir riesgos, establecer controles para mitigarlos, conservar la información (activo más importante) e intervenir en todas las dependencias de la organización, ya que de esta manera puede aprovechar al máximo el conocimiento de los distintos niveles de la empresa (Abril, Pulido, & Bohada, 2013).

Al utilizar el método OCTAVE, una organización toma decisiones de protección de la información en base a los riesgos para la confidencialidad, integridad y disponibilidad de los activos críticos relacionados con la información. Todos los aspectos de riesgo (activos, las amenazas, las vulnerabilidades y el impacto de la organización) se tienen en cuenta en la toma de decisiones, lo que



permite a la organización tener una estrategia de protección basada en la práctica de sus riesgos de seguridad (Carnegie Mellon Software Engineering Institute)

### **2.3.5. Certificación**

La gestión de las actividades de las organizaciones se realiza, cada vez con más frecuencia, según sistemas de gestión basados en estándares internacionales: se gestiona la calidad según ISO 9001, el impacto medio ambiental según ISO 14001 o la prevención de riesgos laborales según OHSAS 18001. Ahora, se añade ISO 27001 como estándar de gestión de seguridad de la información.

#### **ISO 27001**

Publicada el 15 de octubre de 2005, es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de julio de 2007), para que sean

seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados (El Portal de ISO 27001 en Español, 2012).

Es el estándar internacional para la gestión de seguridad de la información. En él se esbozan cómo poner en marcha un sistema de gestión de seguridad de la información evaluado y certificado de forma independiente. Esto permite asegurar más eficazmente todos los datos financieros y confidenciales, por lo que minimiza la probabilidad de que sea accesible de manera ilegal o sin permiso.

Con esta norma se puede demostrar el compromiso y el cumplimiento de las mejores prácticas globales, demostrando a los clientes, los proveedores y los grupos de interés que la seguridad es de suma importancia para la forma en que operan.

ISO/IEC 27001 es un marco de mejores prácticas reconocidas internacionalmente para un sistema de gestión de seguridad de la información. Ayuda a identificar los riesgos de información importantes y poner en marcha los controles adecuados para ayudar a reducir el riesgo. (The British Standards Institution, 2016)



Beneficios de la norma ISO/IEC 270001 de Gestión de Seguridad de la Información:

- a. Identificar los riesgos y poner controles para gestionar o reducirlos.
- b. Flexibilidad para adaptarse a todos los controles o determinadas zonas de su empresa.
- c. Ganar la confianza del cliente y las partes interesadas de que sus datos están protegidos.
- d. Demostrar el cumplimiento y el estado de ganancia como proveedor preferente.
- e. Satisfacer las expectativas más tiernas por el cumplimiento demostrado.

El SGSI-ISO 27001 es un sistema activo, integrado en la organización, orientado a los objetivos empresariales y con una proyección de futuro. Es importante resaltar que cada vez que se incorpora una nueva herramienta o negocio de TIC a la empresa se debe actualizar el análisis de riesgos para poder mitigar de forma responsable los riesgos y, por supuesto, considerando la regla básica de Riesgo de TI vs. Control Vs. Coste, es decir, minimizar los riesgos con medidas de control ajustadas y considerando los costes del control. Los certificados respaldan el cumplimiento de las normas, como en el caso de la ISO 27001.



En una economía cada vez más globalizada, en la que productores de bienes y servicios deben competir, los certificados de conformidad son pasaportes de calidad que abren mercados y una garantía de confianza entre empresas y consumidores de todo el mundo (Fernández, 2012).

El principal objetivo de la ISO/TEC 27001 es proporcionar un modelo para implementar y administrar un sistema de gestión de la seguridad de la información (SGSI) y para ser utilizado internamente o por terceras partes, incluyendo las entidades de certificación. Asimismo, determina que se debe utilizar una metodología de análisis de riesgos, pero ésta no forma parte del estándar, y tampoco se propone ningún método específico, aparte de su integración en el Plan, Do, Check, Act (PDCA), proceso recursivo del modelo de creación del SGSI (CLUSIF, 2010).



## CAPÍTULO III: MARCO METODOLÓGICO

### 3.1. Trayectoria Cualitativa

#### 3.1.1. Tipo de investigación:

El presente trabajo corresponde a una investigación descriptiva debido a que se describirá situaciones eventos como resultado del impacto de las personas, procesos y tecnología, no experimental porque se buscara en forma empírica y sistemática, no se posee control directo de las variables independientes, debido a que su manifestaciones ya han ocurrido o que son inherentemente no manipulables debido que solo se tiene autorización para estudiarlas y proponer cambios, mas no para realizar dicho cambios en los procesos, personas tecnología del caso de estudio. Se harán inferencias sobre las relacione entre las variables, sin intervención directa sobre la variación simultanea de las variables independiente y dependiente (Kerlinger & Lee, 2002).

#### 3.1.2. Diseño de Investigación:

De acuerdo al tipo de investigación el diseño utilizado es transeccional descriptivo, debido a que ubicara, categorizara y proporcionara una visión general del caso de estudio.

Las causas y los efectos serán inferenciados a partir del análisis, siguiendo el siguiente esquema:



$$M = XY$$

**Fuente:** (módulo de metodología de la investigación científica)

Dónde:

X: Causa

Y: Efecto

M: Muestra

### 3.2. Enfoque Seleccionado

Caso de Estudio: Hospital Regional Lambayeque, puesto que es un Hospital nuevo de alta complejidad, con tecnología de primera acorde con los servicios que brinda, y que aún no cuenta con un Sistema de Gestión de Sistema de Información, por lo cual no está preparado para asumir riesgos. Por lo cual, se ve la necesidad de Implementar ISO 27001.

### 3.3. Objeto de Estudio

#### HOSPITAL REGIONAL LAMBAYEQUE

El Hospital Regional Lambayeque, Órgano desconcentrado de la Gerencia Regional de Salud, es el responsable de la Implementación de las políticas Regionales de Salud, en concordancia con la política Nacional y Planes Sectoriales. Ésta



importante asunción de funciones, requiere de decididas acciones planificadas que garanticen la continuidad y sostenibilidad de las políticas y acciones de Salud antes indicadas.

### **3.3.1. Misión**

Somos el Hospital Regional Lambayeque de alta complejidad que brinda servicios integrales de salud, con calidad, equidad y eficiencia, con personal calificado, competente y comprometido, desarrollando investigación y Docencia, contribuyendo a mejorar la calidad de vida de las personas.

### **3.3.2. Visión**

Ser al 2018 un Hospital docente y de investigación, líder, competitivo y reconocido a nivel nacional e internacional, que satisface las necesidades de salud de las personas.

### **3.3.3. Objetivos Estratégicos**

En el Hospital Regional Lambayeque definimos y asumimos que un objeto estratégico es la formulación, específica y medible, de lo que se quiere lograr en el mediano plazo.

Los objetivos estratégicos generales orientarán, tanto las acciones fundamentales para dirigir y promover servicios integrales de salud, desarrollando investigación y docencia,

contribuyendo a mejorar la calidad de vida de las personas. Estos objetivos estratégicos generales son los siguientes:

### **Objetivos Generales:**

**OEG1:** Fortalecer las capacidades organizacionales para contribuir al desarrollo del Sistema Regional de Salud, administrando de manera eficiente y eficaz los recursos financieros, materiales y de información en el marco de la gestión por resultados, con la participación activa de las personas.

**OEG2:** Lograr el acceso de las personas a los servicios de salud con atención integral de calidad, con enfoque de derechos, interculturabilidad, equidad y género, disminuyendo la morbimortalidad de los daños priorizados.

**OEG3:** Fortalecer la capacidad resolutive con personal capacitado, infraestructura, equipamiento de alta complejidad y un eficiente Sistema de Gestión de Pacientes, promoviendo acciones en Servicios de Salud, investigación y docencia con énfasis en las prioridades Regionales.

### **Objetivos Estratégicos Específicos:**

## **OBJETIVOS ESTRATÉGICOS POR LOS PROBLEMAS SANITARIOS**

**OEE1:** Disminuir la morbilidad y mortalidad materno neonatal.



**OEE2:** Reducir la mortalidad en población de niños y adultos mayores.

**OEE3:** Disminuir la morbimortalidad de Enfermedades no Transmisibles.

(Enfermedades hipertensivas, diabetes, salud ocular, salud mental, salud bucal).

**OEE4:** Reducir la morbimortalidad de casos de TBC.

**OEE5:** Reducir la morbimortalidad de pacientes con ITS y VIH.

**OEE6:** Disminuir la morbimortalidad por cáncer.

#### **OBJETIVOS ESTRATÉGICOS POR EL SISTEMA DE SALUD:**

**OEE1:** Fortalecer el desarrollo del recurso humano a través de la gestión por competencias e impulso de la capacidad docente e investigadora.

**OEE2:** Incrementar el acceso a los Servicios de Salud (Cobertura SIS, débil Sistema de Referencia y Contrareferencia).

**OEE3:** Mejorar la calidad del servicio.

#### **3.3.4. Servicios**

El Hospital cuenta con los servicios de:

Medicina Física y Rehabilitación.

Hemodiálisis

Apoyo al Diagnóstico por Imágenes

Laboratorio Clínico

Banco de Sangre

Farmacia

Emergencia y Áreas Críticas

Unidad de Cuidados Intensivos (Adultos, Intermedios y Neonatos).

Centro Quirúrgico

Centro Obstétrico

Central de Esterilización

Hospitalización

Consulta Externa

Oncología

Oftalmología Especializada

Investigación Clínica

### **3.3.5. Especialidades**

El Hospital Regional Lambayeque cuenta con más de 30 especialidades, tales como:

Anestesiología

Cardiología

Cirugía de Tórax y Cardiovascular

Cirugía Pediátrica

Cirugía Plástica

Cirugía Oftalmológica

Cirugía Oncológica

Dermatología

Endocrinología

Gastroenterología

Gastropediatría

Geriatría

Ginecología

Ginecología Materno

Ginecología Oncológica

Neonatal

Hematología

Infectología

Medicina Física

Medicina Interna

Medicina Ocupacional

Nefrología

Neumología

Neurocirugía

Neurología

Neurología Pediátrica

Nutrición

Odontología

Oftalmología

Oncología

Otorrinolaringología

Pediatría

Psicología

Psiquiatría

Reumatología

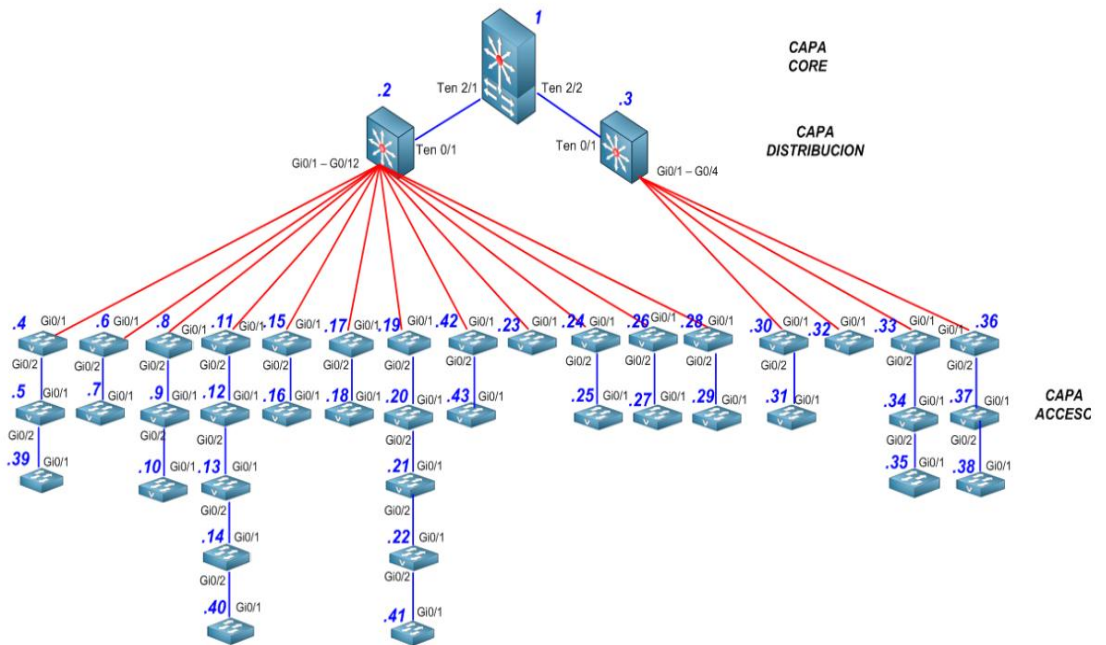
Tópico

Traumatología

Urología

### 3.3.6. Topología

Topología de Switching del Hospital Regional de Lambayeque



### 3.4. Sujetos Participantes

Los sujetos participantes en esta investigación serían tanto los directivos como los encargados de la División de Tecnologías de la Información.

### 3.5. Métodos, técnicas e instrumentos de recolección de datos

El método de investigación que se ha empleado responde a la técnica e instrumentos de recolección de datos desde la perspectiva metodológica cualitativa (observación participativa).

### 3.6. Procedimiento para la recolección de datos



**Análisis de documentos:** Es el conjunto de documentos de gestión estratégica y operativa del caso de estudio, estos documentos contienen la planificación y orientación de la organización en cuanto a la definición de su misión, visión, objetivos estratégicos, análisis situacional, estrategias. También corresponde los documentos normativos, Manual de Procedimientos y Funciones (MOF), Reglamento de Organización y Funciones (ROF), Plan estratégico de tecnologías de Información, documentos de gestión de TI, inventario de Tecnologías de Información.

### **3.7. Procedimiento de análisis de datos**

Para esta investigación en primer lugar se realizó un estudio de la situación actual del Hospital Regional Lambayeque, viendo sus principales características, y siguiendo la matriz de evaluación se procedió a elegir una metodología acorde que nos ayudó para definir las principales amenazas a las que está expuesto el Hospital y qué hacer con cada una de ellas para que produzcan el menor daño a nuestra Institución.

### **3.8. Criterios éticos**

Los criterios éticos que se respetan en el presente proyecto de investigación es el Código Deontológico del Colegio de Ingenieros





de Perú en su Capítulo II “De la Relación con el Público” en su artículo 106 expresa:

Los ingenieros, al explicar su trabajo, méritos o emitir opiniones sobre temas de ingeniería, actuarán con seriedad y convicción, cuidando de no crear conflictos de intereses, esforzándose por ampliar el conocimiento del público a cerca de la ingeniería y de los servicios que presta a la sociedad.

Por ello se considera:

**Confidencialidad:** Debido a que se asegurará la protección de la información de la institución y las personas que participan como informantes de la investigación, de acuerdo al acuerdo de confidencialidad de datos con la empresa.

**Objetividad:** El análisis de la situación encontrada se basará en criterios técnicos e imparciales

**Veracidad:** La información mostrada será verdadera, cuidando la confidencialidad de ésta.

### 3.9. Criterios de rigor científico

La presente propuesta de investigación se realizará siguiendo los juicios científicos establecidos y definidos como un conjunto de buenas prácticas de la industria llamados frameworks, estos permiten garantizar la calidad de la propuesta de investigación.

Así, seguimos la coherencia metodológica durante el desarrollo de la propuesta de la investigación, según el sujeto de

investigación elegido por los criterios de inclusión y exclusión, por ello se considera:

**Validación:** Se validarán los instrumentos de recolección de datos y la propuesta de solución a través de Juicio de Expertos.

## CAPÍTULO IV: ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

### 4.1. Análisis y discusión de los resultados

Para la presente investigación se hizo uso de unas encuestas a modo de entrevista al personal de la División de Tecnologías de la Información, así como algunos trabajadores del Hospital Regional Lambayeque.

Teniendo en cuenta la dimensión de la Institución y de los diversos departamentos y área con las que cuenta, se creyó conveniente encuestar solo al personal administrativo, teniendo así a los jefes, secretarias, administradores, estadísticos, asistente, entre otros, generando así una muestra total de 78 personas según detalle:

ÁREA	PERSONAL
Dirección Ejecutiva (2)	- Director - Secretaria
Dirección de Servicios de Salud (3)	- Sub Director - Secretaria - Asistente
Administración (3)	- Administradora - Secretaria



	- Asistente
Unidad de Logística (6)	<ul style="list-style-type: none"> <li>- Jefe de Logística</li> <li>- Secretaria</li> <li>- Adquisiciones</li> <li>- Procesos</li> <li>- Patrimonio</li> <li>- Almacén</li> </ul>
Unidad de Economía (5)	<ul style="list-style-type: none"> <li>- Jefa de Economía</li> <li>- Secretaria</li> <li>- Tesorería</li> <li>- Control Previo</li> <li>- Integración Contable</li> </ul>
Unidad de Desarrollo Humano (7)	<ul style="list-style-type: none"> <li>- Jefe de DD. HH.</li> <li>- Secretaria</li> <li>- Remuneraciones</li> <li>- Control de Asistencia</li> <li>- Legajos</li> <li>- Asesoría Legal</li> </ul>



	- Bienestar Social
Unidad de Mantenimiento (5)	- Jefe de Mantenimiento - Secretaria - Ing. Biomédica - Ing. Electrónica - Arquitectura
Departamento de Área Clínica (4)	- Jefatura - Secretaria - Administradora - Estadística
Departamento de Área Quirúrgica (4)	- Jefatura - Secretaria - Administradora - Estadística
Departamento de Apoyo al Tratamiento (4)	- Jefatura - Secretaria - Administradora - Encargada de Farmacia



<p>Departamento de Apoyo al Diagnóstico (5)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> <li>- Administradora</li> <li>- Encargada de Laboratorio</li> <li>- Encargada de Banco de Sangre</li> </ul>
<p>Departamento de Emergencia y Áreas Críticas (5)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> <li>- Administradora</li> <li>- Encargado del Servicio de Emergencia.</li> <li>- Encargado de Áreas Críticas</li> </ul>
<p>Departamento de Enfermería (3)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> <li>- Asistente</li> </ul>
<p>Dirección de Investigación (4)</p>	<ul style="list-style-type: none"> <li>- Director</li> <li>- Secretaria</li> <li>- Estadística</li> <li>- Encargado de Laboratorio</li> </ul>





<p>Oficina de Gestión de la Calidad (5)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> <li>- Estadística</li> <li>- Epidemiología</li> <li>- Calidad</li> </ul>
<p>Oficina de Planeamiento Estratégico (5)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> <li>- Encargada de Presupuesto</li> <li>- Encargada de Planificación</li> <li>- Asistente</li> </ul>
<p>Unidad de Gestión de Pacientes (5)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> <li>- Encargado de Admisión</li> <li>- Encargada de Seguros y Referencias.</li> <li>- Encargado de Archivo.</li> </ul>
<p>Unidad de Salud Ocupacional (3)</p>	<ul style="list-style-type: none"> <li>- Jefatura</li> <li>- Secretaria</li> </ul>



	- Enfermera Asistente
--	-----------------------

En base a la aplicación de la encuesta, se obtuvieron resultados que muestran la realidad de la Institución, teniendo en cuenta que por la naturaleza del mismo, se cuenta con personal no solo de salud o asistencial, sino también con personal administrativo, que es el encargado de mantener los servicios del Hospital.

Para la obtención de los siguientes gráficos se hizo uso del Microsoft Excel, en el cual a través de tablas dinámicas llegamos a los siguientes gráficos:

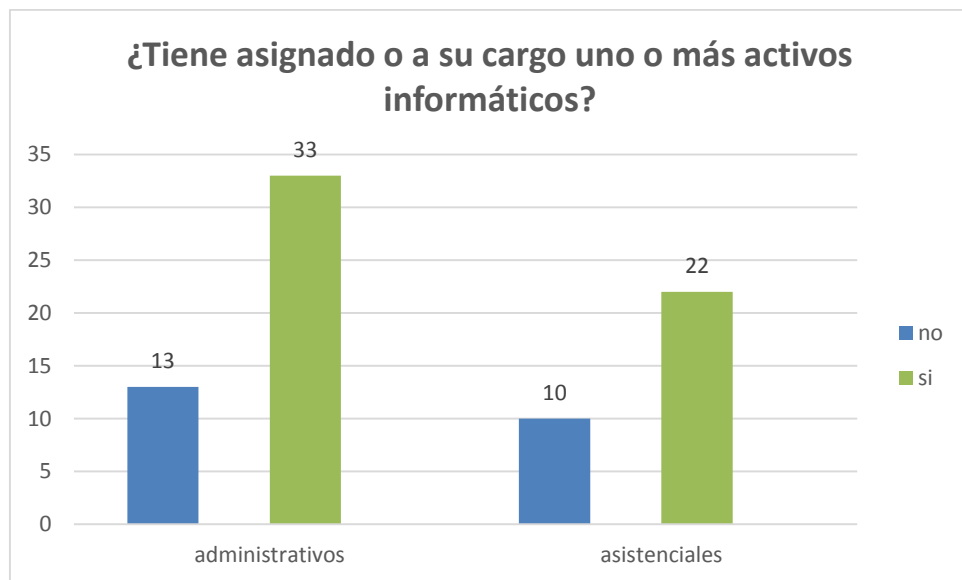


Figura N° 1. Resultados de la Pregunta N° 1

Fuente: Elaboración Propia



En la Figura N° 1, se aprecia que de un total de 78 personas encuestadas entre personal administrativo y asistencial, 55 de ellos tienen asignados uno o más activos informáticos, representando así el 58.97% del total; de los cuáles según las encuestas, serían los jefes de cada área. Del mismo modo, se encontró que es menor la cantidad de asistenciales que tienen equipos informáticos a su cargo en relación a los administrativos.

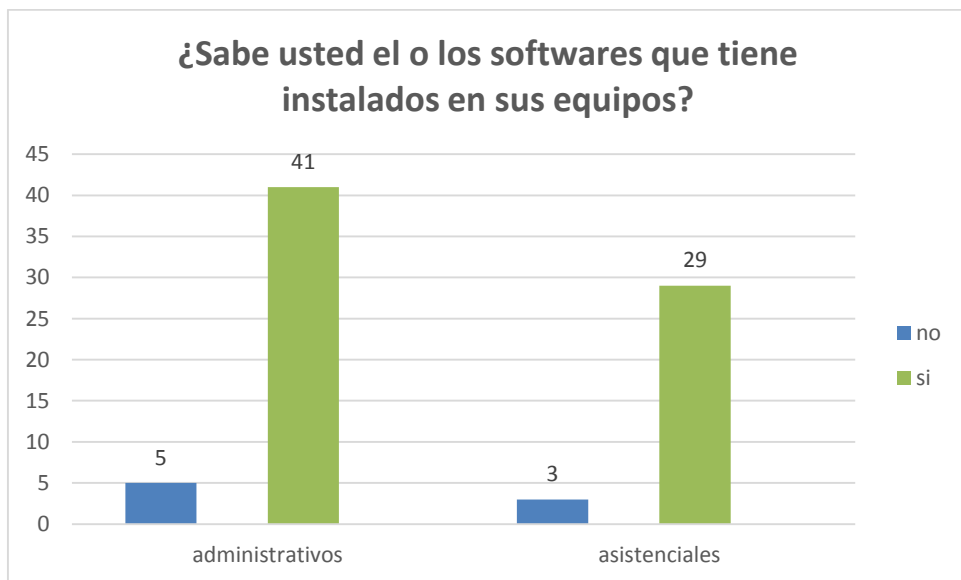


Figura N° 2. Resultados de la Pregunta N° 2

Fuente: Elaboración Propia

En la Figura N° 2 se aprecia que la mayoría, tanto de administrativos como asistenciales, tienen conocimiento de los softwares que tienen instalados en sus equipos, de un total de 78 personas encuestadas, solo 8 de ellos, 5 administrativos y 3 asistenciales no saben que software tienen instalados; por lo



general, las secretarías que son quienes usan sus equipos para redactar y derivar documentos a través del Sistema de Gestión Documentaria (SIGGEDO).

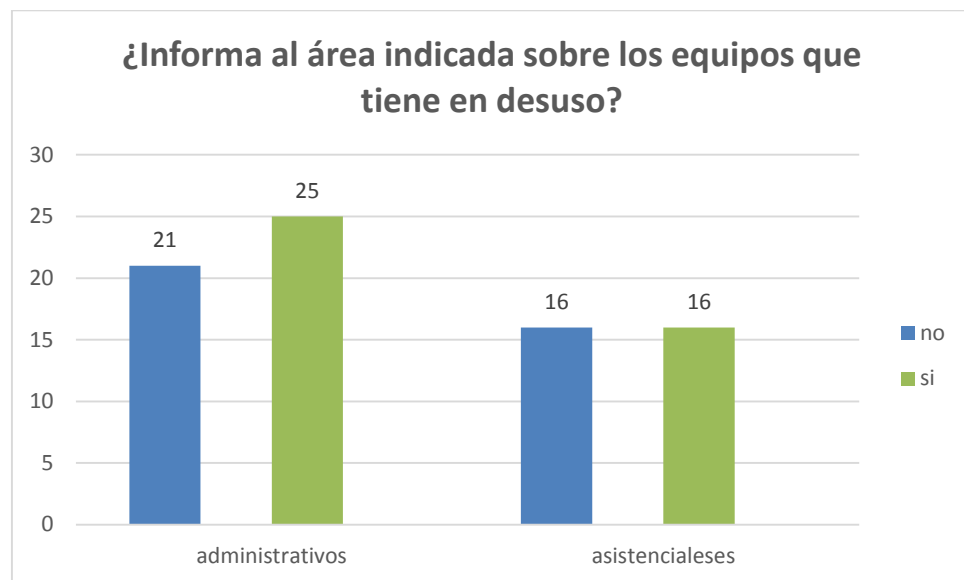


Figura N° 3. Resultados de la Pregunta N° 3

Fuente: Elaboración Propia

En la Figura N° 3 indica que hay una cantidad similar tanto en administrativos como asistenciales, que avisan y no sobre los equipos que tienen en desuso, puesto que no saben el correcto procedimiento para el mismo, o en todo caso desconocen el área indicado para dicho proceso.



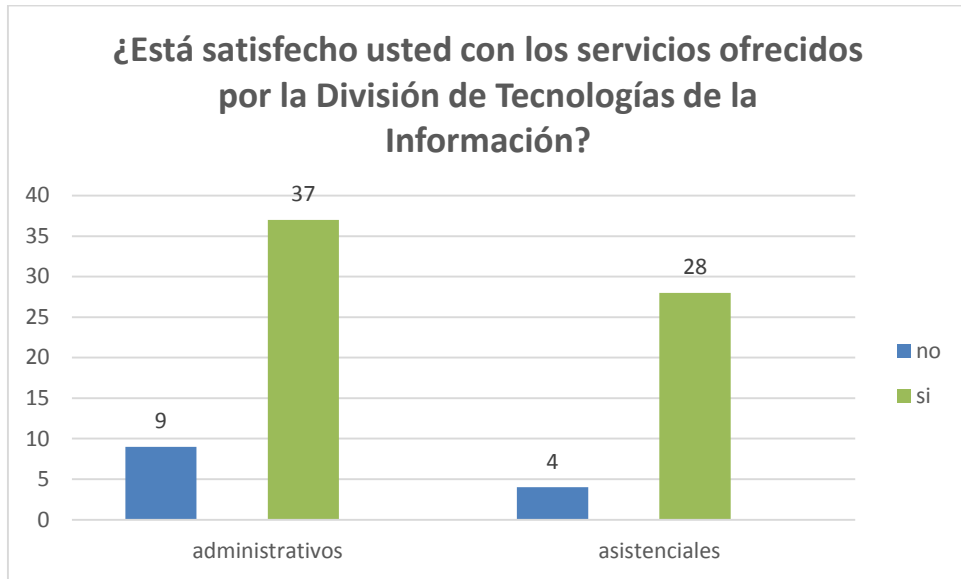
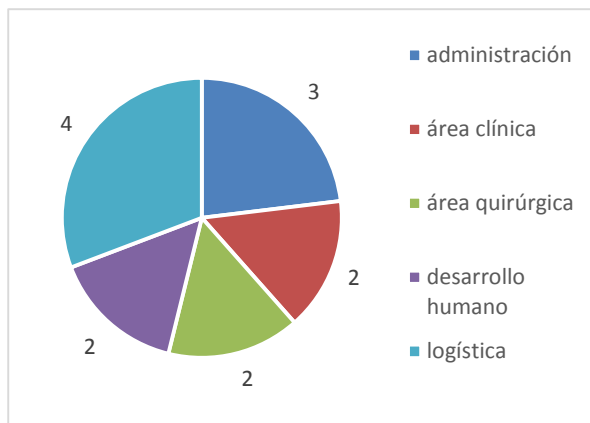


Figura N° 4. Resultados de la Pregunta N° 4

Fuente: Elaboración Propia

En la Figura N° 4 se muestra que la mayoría del personal están satisfechos con los servicios que brinda la División de Tecnologías de la Información, salvo algunas áreas, en donde



usan programas como el SIGA y el SIAF, que no están muy conforme, por los continuas fallas, tal como muestra el

Gráfico adjunto.

Gráfico N° 1



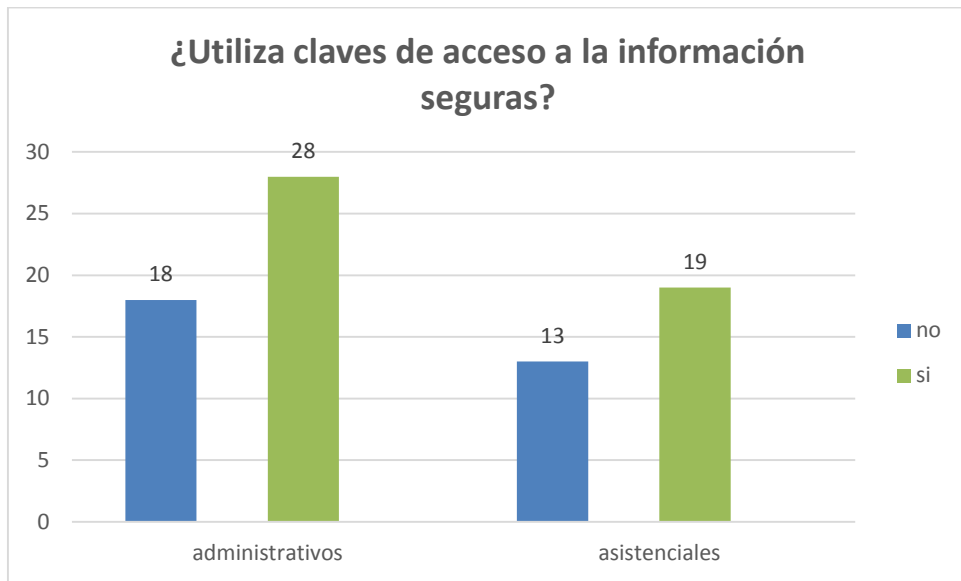


Figura N° 5. Resultados de la Pregunta N° 5

Fuente: Elaboración Propia

En la Figura N° 5 se aprecia que no hay mucha desigualdad entre los que utilizan claves de acceso a la información segura y los que no, tanto en personal de áreas administrativas y de áreas asistenciales. La gran cantidad de información importante está guardada en un servidor principal al que todos tienen acceso.





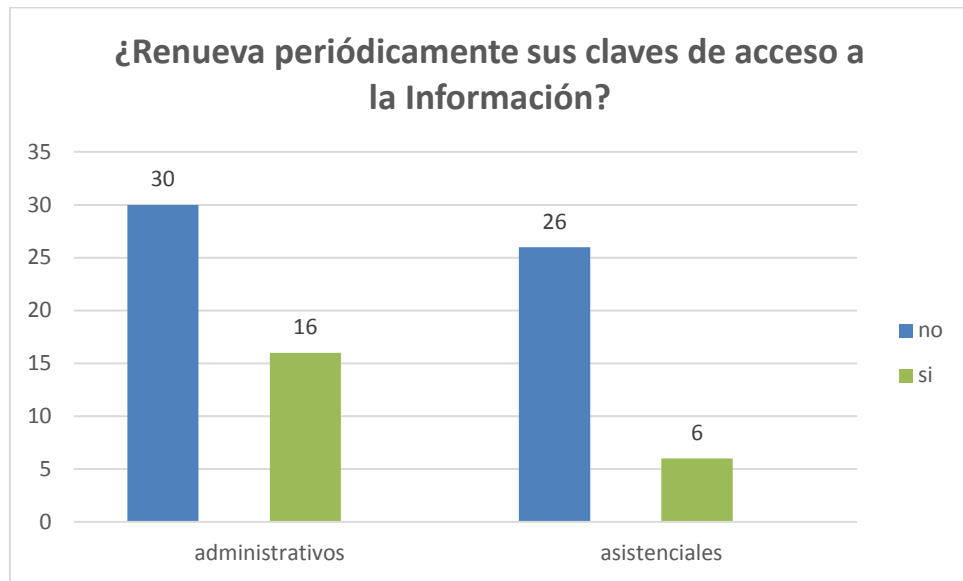


Figura N° 6. Resultados de la Pregunta N° 6

Fuente: Elaboración Propia

En la Figura N° 6 se muestra que la mayoría de usuarios no renuevan sus claves, puesto que son precisamente estos usuarios los que usan el Sistema Operativo Ubuntu, el cual no te pide renovar contraseñas, son usuarios del SISGEDO, el cual tampoco está configurado para eso, y por la poca cultura informática el personal no lo hace. En cambio, el personal que si lo hace, los 16 administrativos son porque usan programas más complejos, que requieren por seguridad estar cambiando continuamente de claves, para así proteger la información.





Figura N° 7. Resultados de la Pregunta N° 7

Fuente: Elaboración Propia

En la Figura N° 7, se muestra claramente que el 100% de personas encuestadas tiene conocimiento de a quién tienen que reportar en caso les suceda algún incidente informático. La División de Tecnologías de la Información tiene un área de Soporte Técnico que atiende a todas las unidades del Hospital, así como el área de Data Center por cualquier problema que suscite.



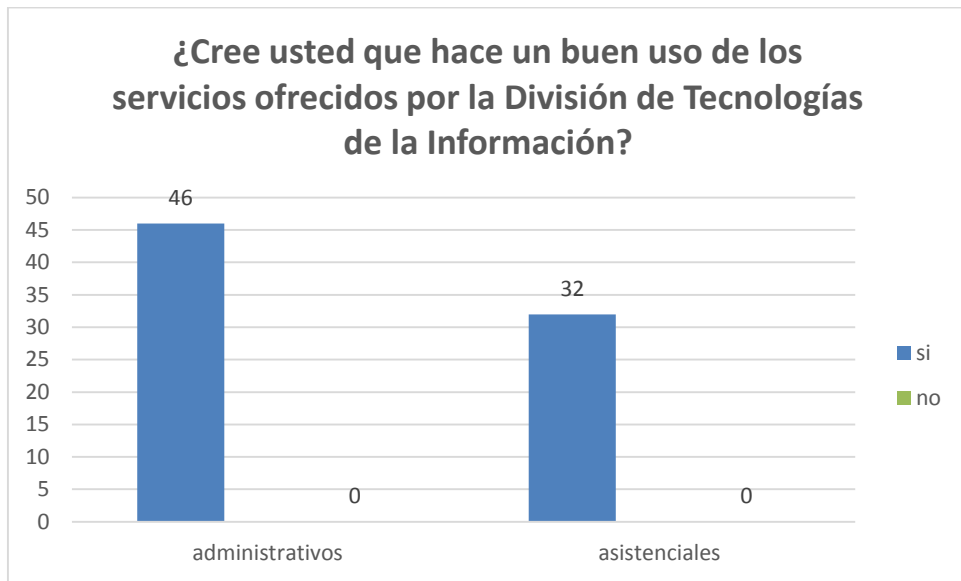


Figura N° 8. Resultados de la Pregunta N° 8

Fuente: Elaboración Propia

En la Figura N° 8 se puede apreciar que los 78 encuestados afirman que hacen un buen uso de los servicios que ofrece la División de Tecnologías de la Información, puesto que son los encargados de configurar los sistemas acordes para el correcto desempeño de sus labores.



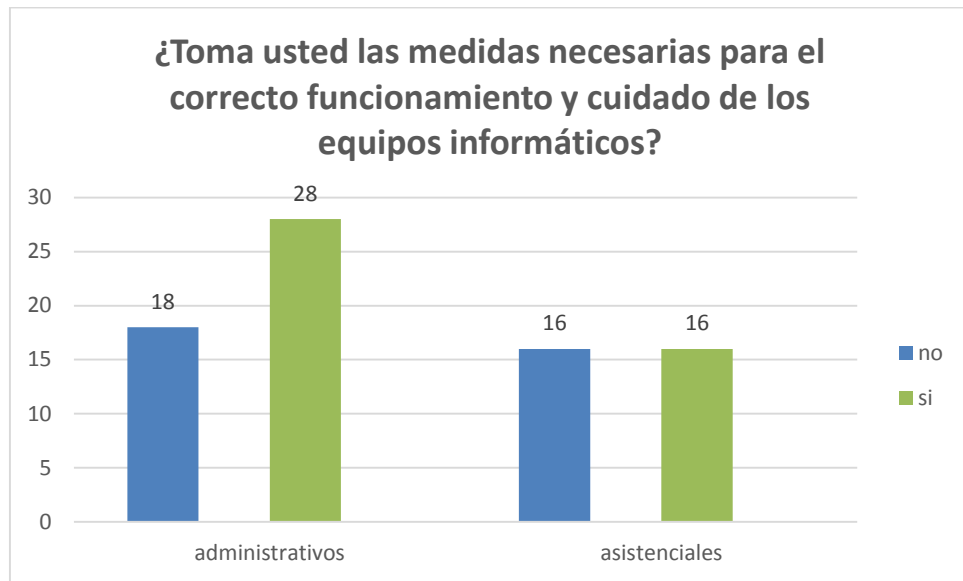


Figura N° 9. Resultados de la Pregunta N° 9

Fuente: Elaboración Propia

En la Figura N° 9, se aprecia que existe casi igualdad de porcentajes entre los que toman las medidas necesarias para el correcto funcionamiento y cuidado de los equipos informáticos y los que no; esto ya pasaría por un tema de cultura de cada personal, sin importar si son de áreas administrativas o asistenciales.



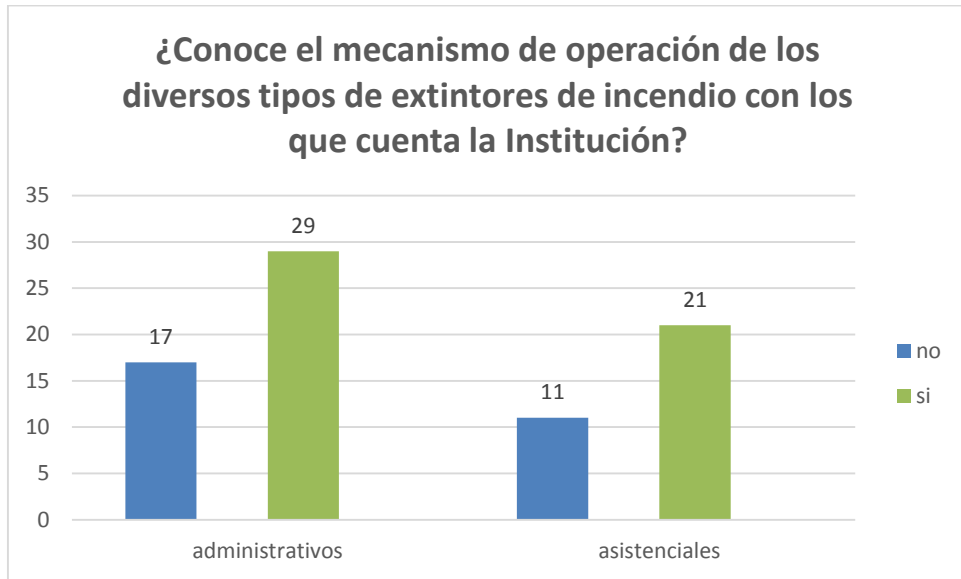


Figura N° 10. Resultados de la Pregunta N° 10

Fuente: Elaboración Propia

La Figura N° 10 denota claramente que el 64.10% si conocen el mecanismo de operación de los diversos tipos de extintores de incendio con los que cuenta el Hospital, dentro de los cuales son 21 asistenciales y 29 administrativos.



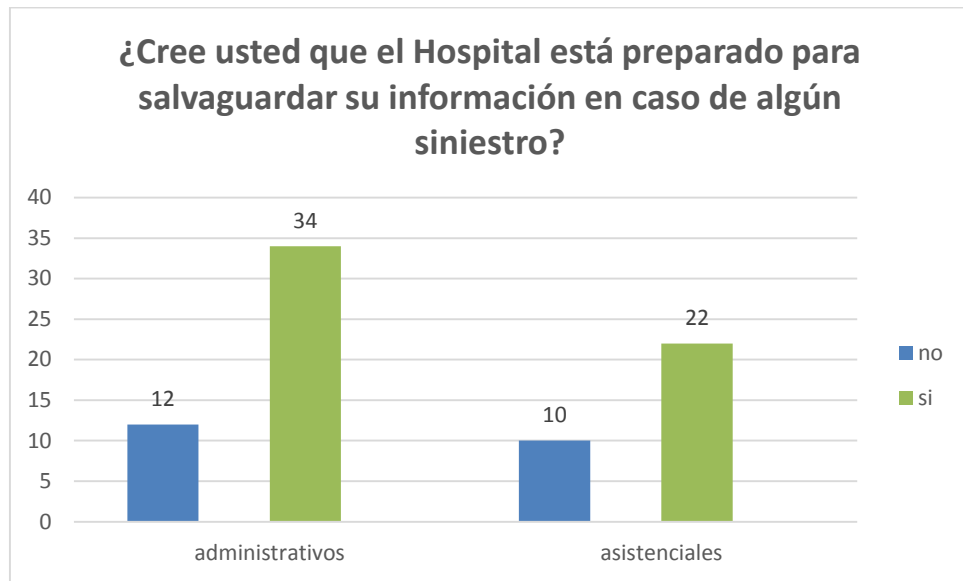


Figura N° 11. Resultados de la Pregunta N° 11

Fuente: Elaboración Propia

Según los resultados obtenidos en la Figura N° 11, el 71.79% de los encuestados consideran que el Hospital está preparado para salvaguardar su información en caso de algún siniestro, sin embargo, existen incidencias que dan lugar a ese 28.21%.

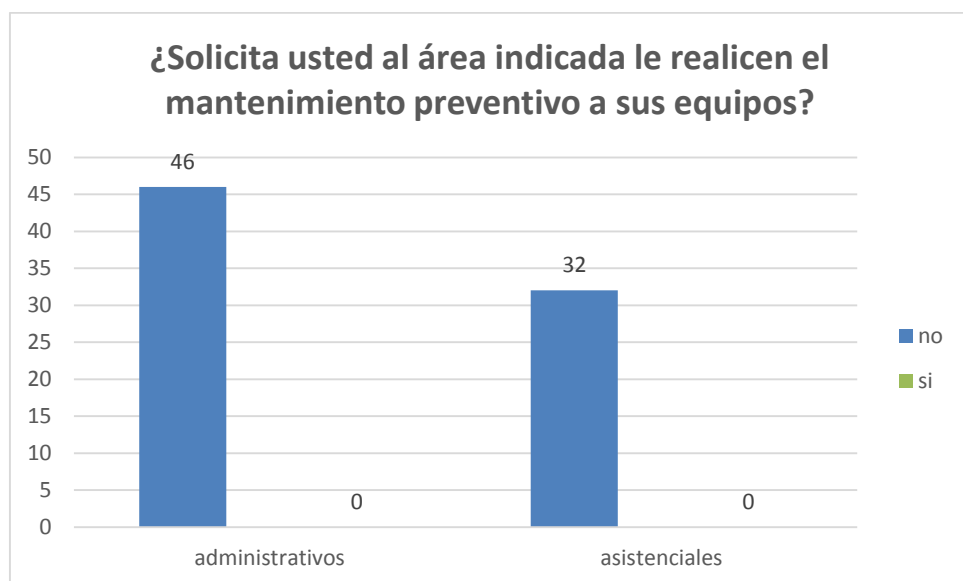




Figura N° 12. Resultados de la Pregunta N° 12

Fuente: Elaboración Propia

Lamentablemente la Figura N° 12 muestra que el 100% de los encuestados manifiestan que no son ellos los que solicitan al área indicada que realicen un mantenimiento preventivo a sus equipos, por no creerlo importante para el desarrollo de sus funciones.

Del mismo modo, se realizó una serie de preguntas a los encargados de la División de Tecnologías de la Información, a modo de entrevista, puesto que son pocos y lo que más se necesitaba era conocer experiencias.

Actualmente, la División de Tecnologías de la Información (DTI) cuenta con un plan anual de trabajo, el cual se ve en la necesidad de modificarse de acuerdo a las necesidades del Hospital, las cuales tienen que ser priorizadas y resueltas al momento para asegurar la continuidad del mismo.

Si bien es cierto, no se realiza un informe mensual de las acciones realizadas en el área, es en la evaluación trimestral cuando solicitan el reporte de las acciones tomadas para beneficio de la Institución.

Cada año, el Hospital Regional Lambayeque como Institución Pública tiene que realizar un inventario de los bienes con los que



cuenta, dentro de los cuales se encuentran los activos informáticos; y es ahí, donde un equipo encargado realiza el control del registro de bienes, además que en base a ello, se puede establecer el estado actual de cada equipo, y así poder solucionar algunas deficiencias presentadas.

Lamentablemente, la adquisición de nuevos equipos se ve limitado por el presupuesto asignado al Hospital para este tipo de bienes; así como, para los licenciamientos y licencias de software especializado. Es por esto que, el Hospital actualmente cuenta con Sistema Operativo Ubuntu, salvo algunos usuarios que por los sistemas que usan como son el Sistema Integrado de Gestión Administrativa (SIGA) y el Sistema Integrado de Administración Financiera (SIAF), se ven en la necesidad de tener instalado el Sistema Operativo Windows.

Los encargados de DTI son conscientes de los riesgos a los que la Institución, a lo que Tecnologías de Información concierne, está expuesto. Se han implementado políticas de control de acceso a la Información, usuarios en dominio que periódicamente se ven en la necesidad de renovar sus claves, se cuenta con un servidor en el cual los usuarios según los permisos establecidos pueden guardar su información.

Existe una política de creación de usuarios, de acuerdo a los roles que desempeña cada uno en su área, pero es el jefe de cada dependencia el que solicita la creación de los mismos a través de un correo institucional.

Se cuenta con un plan de mantenimiento preventivo de los equipos anual, pero este se ve limitado por la cantidad de trabajadores, ya que son los practicantes quienes lo realizan.

En cuanto a los extintores, los encargados de la verificación del correcto estado de los mismos, es la Unidad de Mantenimiento, a través de su área de Arquitectura; y a su vez, los miembros la brigada de Defensa Civil son los encargados de la manipulación de los extintores. Por ese lado, el Hospital está preparado, pero como área no todos cuentan con la debida capacitación, en caso el suceso ocurra dentro de las oficinas; además, que se cuenta con un detector contra incendios.

### **Metodología de Evaluación y de Tratamiento de Riesgos**

La evaluación y tratamiento de riesgos se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los activos que se utilizan dentro de la organización o que pueden tener un impacto sobre la seguridad de la información en el ámbito del SGSI.

El primer paso en la evaluación de riesgos es la identificación de todos los activos dentro del alcance del SGSI; es decir, todos los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en la organización. Asimismo, se debe identificar a sus propietarios: la persona o unidad organizativa responsable de cada activo.

De igual forma, se debe identificar todas las amenazas y vulnerabilidades relacionadas con cada activo; a su vez, cada activo puede estar relacionado a varias amenazas, y cada amenaza puede estar vinculada a varias vulnerabilidades.

#### Funciones y Obligaciones del Personal.

Las funciones que los trabajadores del Hospital Regional Lambayeque desarrollen en relación a los sistemas de información, serán aquellas para las que hayan sido expresamente autorizados, independientemente de las limitaciones, que se establecen para controlar su acceso.

Todo el personal está obligado a respetar las normas, tanto las de carácter general y la de carácter específico.

Independientemente de las funciones y responsabilidades específicas asignadas a los usuarios, a cualquier trabajador del Hospital se le exige con carácter general:



1. Confidencialidad, con respecto a la documentación e información que reciben o usan perteneciente a la institución o de su responsabilidad.
2. No incorporar a la institución información o datos sin ninguna autorización previa y antes coordinada con su jefe inmediato.
3. Comunicar al responsable de seguridad cualquier incidencia respecto a la seguridad de la información.

#### **4.2. Consideraciones finales**

Del análisis de las encuestas, y según la entrevista realizada al personal de la División de Tecnologías de la Información, podemos precisar cuáles son los puntos críticos en cuanto a Tecnologías de la Información se refiere, tiene el Hospital Regional Lambayeque.

Si bien es cierto, cuentan con un plan de trabajo anual en el cual plasman las principales actividades que van a realizar en mejora del Hospital, no siempre se llevan a cabo, ya sea por un tema de tiempo, personal o presupuesto.

Por tratarse de una entidad pública, el Hospital depende económicamente del presupuesto anual que asigna el Ministerio de Economía y Finanzas (MEF), el cual por la naturaleza del sector salud, está mayormente destinado a la adquisición de



insumos y material médico, así como de medicamentos y pago al personal.

Existen servidores especializados para el mantenimiento y funcionamiento de programas como SIGA y SIAF para áreas administrativas, Sistemas para citas, sistema de colas y programaciones de atenciones, sistema para programar los roles de los médicos, etc.; pero que, no están preparados para soportar tanta información.

Una mala cultura informática por parte de los usuarios, lo cual limita el correcto funcionamiento del Hospital, y obstaculiza el adecuado cumplimiento de las políticas de seguridad establecidas por la División de Tecnologías de la Información.

Desinterés por parte de los directivos hacia la inversión en Tecnologías de la Información, así como en la implantación de mejores políticas informáticas.

Al implementar gestión de riesgos de TI en el Hospital Regional Lambayeque estamos reduciendo el nivel de impacto de las amenazas a las que están expuestos los activos; asegurando así, la confidencialidad de la información, la continuidad de los servicios que se brindan y apoyando al desarrollo socio económico de la región.





Existen dos tipos de certificados ISO 27001: (a) para las organizaciones y (b) para las personas. Las organizaciones pueden obtener la certificación para demostrar que cumplen con todos los puntos obligatorios de la norma; las personas pueden hacer el curso y aprobar el examen para obtener el certificado.

Para obtener la certificación como organización, se debe implementar la norma y luego se debe aprobar la auditoría que realiza la entidad de certificación.

La primera auditoría que se realiza es para revisar toda la documentación referente a los procesos que se siguen en la Institución; es por eso, que la implementación de gestión de riesgos de TI que hemos detallado en el desarrollo de la propuesta, es un punto clave que va ayudar al Hospital Regional Lambayeque a obtener la Certificación ISO 27001.



## CAPÍTULO V: PROPUESTA DE INVESTIGACIÓN

La gestión de riesgos, es un proceso enmarcado dentro del proceso de mejora continua, y cumple un ciclo de vida, que se ve operativizado en las metodologías de gestión de riesgos que proponen los diversos autores y la industria.

En el sujeto de estudio Hospital Regional Lambayeque, se enfrentó el dilema: ¿Qué metodología de gestión de riesgos utilizar como guía?, para ello fue necesario seleccionar una metodología de gestión de riesgos que apoye el proceso en una organización de servicio de salud pública como es el Hospital Regional Lambayeque.

Basándonos en un estudio realizado por (Carrillo Sánchez, 2013), quién propone un modelo para elegir qué metodología de gestión de riesgos es la adecuada según los requisitos que reúne para utilizar en una Institución Pública como nuestro objeto de estudio. Entre las principales metodologías de gestión de riesgos que existen tenemos: CMMI, SPICE, PMBOK, PRINCE2, COBIT 4.1<sup>3</sup>, RISK IT, OCTAVE, NIST 800-30 y MAGERIT; para tal análisis, se ha creído conveniente presentar una tabla con sus principales características, tales como: la descripción de sus siglas, el nombre de la Institución de las creo, así como el país de origen donde se dio cada metodología.



METODOLOGÍA	DESCRIPCIÓN	ORGANIZACIÓN	PAÍS
CMMI	Capability Maturity Model Integration	SEI (Software Engineering Institute)	EE.UU.
SPICE	Software Process Improvement and Capability Determinarion	ISO (International Organization for Standarization)	Suiza
PMBOK	Project Management Body of Knowledge	PMI (Project Management Institute)	EE.UU.
PRINCE2	Projects IN Controlled Environments	OGC (Office of Government Commerce)	Reino Unido
COBIT	Control Objectives for Information and realated Technology	ISACA (Information Systems Audit and Control Association) & ITGI (IT Governance Institute)	EE.UU:



RISK IT	Risk IT Model	ISACA (Information Systems Audit and Control Association)	EE.UU.
OCTAVE	Operationally Critical Threat, Asset and Vulnerability Evaluation	Carnegie Mellon SEI (Software Engineering Institute) y CERT (Computer Emergency Response Team)	EE.UU.
NIST 800-30	Risk Management Guide for Information Technology Systems	NIST (National Institute of Standards and Technology)	EE.UU.
MAGERIT	Metodología de Análisis y Gestión de Riesgos de IT	MAP (Ministerio de Administraciones Públicas)	España

Los criterios que se tomarán en cuenta para poder identificar las fortalezas de cada metodología son los **Elementos de Tecnologías de**



**Información**, las cuales son áreas de especialidad en la ejecución de proyectos: HARDWARE, SOFTWARE, BASE DE DATOS, REDES Y TELECOMUNICACIONES, RECURSO HUMANO, LEGAL, FINANCIERO, SERVICIOS. Para ello se detalla las principales características de cada uno en la tabla siguiente:

ELEMENTOS DE TI	DESCRIPCIÓN
HARDWARE (HW)	Equipos informáticos. Bienes materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos. También se incluyen dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo. Pueden ser o no portátiles. Equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.



<p>SOFTWARE (SW)</p>	<p>Con varias denominaciones (programas, aplicativos, desarrollos, etc.) se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.</p> <p>NOTA: El denominado “código fuente” o programas que serán datos de interés comercial a valorar y proteger como tales, serán considerado como datos.</p>
<p>BASES DE DATOS (BD)</p>	<p>Elementos de datos, información que, de forma singular o agrupada representan el conocimiento que se tiene de algo. Almacenados en equipos o soportes de información. Pueden ser transferidos de un lugar a otro por los medios de transmisión de datos. Informes, líneas de texto denominados código fuente (Source code, code base) escrito en un lenguaje de programación específico.</p>





<p>REDES Y COMUNICACIONES (COM)</p>	<p>Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.</p>
<p>RECURSO HUMANO (RH)</p>	<p>Personas relacionadas con los sistemas de información. Equipo de TI. Usuarios Internos y externos. Operadores, Administradores.</p>
<p>LEGAL (L)</p>	<p>Contratos, Licenciamiento, Derechos de Autor. Ley de Trabajo (Contratación de Personal), Ley de Servicio de Rentas Internas (Impuestos). Seguridad de la información. Normativa de la Información.</p>
<p>FINANCIERO (F)</p>	<p>Procesos involucrados en estimar, presupuestar y controlar los costos de modo que se complete el proyecto dentro del presupuesto aprobado. También involucra procesos de estimación y control en cuanto a entrega y recepción de productos (bienes y servicios).</p>



SERVICIOS (S)	<p>Función que satisface una necesidad de los usuarios. Servicios de información, servicios de comunicaciones, servicios de seguridad, servicios de capacitación. Servicios requeridos para el eficaz desempeño de la misión del proyecto/ organización.</p>
---------------	--

Teniendo el detalla de las metodologías, y después de haber analizado las principales características de las mismas, se realizó una Matriz de evaluación según los elementos de TI, en la cual según una escala iremos considerando valores para poder elegir la adecuada para la Institución.

METODOLOGÍAS	ELEMENTOS DE TI								TOTAL
	HW	SW	BD	COM	RH	L	F	S	
<b>CMMI</b>	3	4	4	3	3	1	2	3	23
<b>SPICE</b>	3	4	4	3	3	2	4	4	27
<b>PMBOK</b>	3	3	3	3	4	1	4	3	24
<b>PRINCE2</b>	3	3	3	3	3	2	2	4	23
<b>COBIT</b>	4	4	4	4	4	4	3	4	31
<b>RISK IT</b>	4	4	4	4	4	3	3	4	30
<b>OCTAVE</b>	4	4	4	4	4	2	2	3	27



<b>NIST 800-30</b>	4	4	4	4	4	3	3	4	30
<b>MAGERIT</b>	4	4	4	4	4	4	4	4	<b>32</b>

VALOR	ESCALA LIKER
1	NO CUMPLE
2	CUMPLE DEFICIENTEMENTE
3	CUMPLE PARCIALMENTE
4	CUMPLE ADECUADAMENTE
5	CUMPLE COMPLETAMENTE

MAGERIT es una metodología que alcanza niveles satisfactorios al momento de Gestionar el Riesgo con respecto a Hardware, Software, Bases de Datos, Redes y Telecomunicaciones; destaca al momento de Administrar el Recurso Humano, matizando su acción definiendo un equipo de trabajo con perfiles y competencias para los proyectos, con su respectiva asignación de funciones y responsabilidades apoyadas en una matriz RACI (Responsable, Aprobador, Consultado, Informado). En cuanto al tema legal, la alineación de las leyes y normativas se basan según requerimientos gubernamentales cubriendo temas que no tratan otras metodologías como: Contratos, Licenciamiento, Derechos de Autor, Contratación de Personal, Impuestos, Protección de datos de carácter personal, entre otros, los cuales pueden servir como referencia según el área de aplicabilidad y ejercicio.



Una vez elegida la metodología adecuada para nuestra Institución, procedemos con el **análisis de riesgos** que nos va permitir determinar qué tiene la Institución y estimar lo que podría pasar.

El análisis de riesgo es el inicio de una gestión planificada y ordenada de los riesgos operacionales y de TI, para lo cual el desafío más importante es entender la interrelación que tiene el proceso de negocio con los riesgos de TI que son necesarios para que los mismos funcionen correctamente; en este caso, para el correcto funcionamiento de los diversos servicios del Hospital Regional Lambayeque.

Dicho análisis se realiza en el marco de la gestión integral del riesgo institucional, donde un conjunto de activos de información asisten a los procesos institucionales y constituyen el alcance del Sistema de Gestión de Seguridad de la Información (SGSI). En este proceso, se determina el riesgo en forma cualitativa, a partir de la probabilidad de que materialice o no una amenaza y el impacto que ocasione en la Institución.

En primer lugar tenemos que definir y clasificar las posibles **amenazas** que pueden atacar al Hospital, así como las inundaciones, lluvias, robos, ataques cibernéticos, etc. Estas amenazas se pueden clasificar teniendo en cuenta su origen:

Clasificación	Riesgos
Desastres Naturales	<ul style="list-style-type: none"> <li>- Inundaciones</li> <li>- Lluvias</li> <li>- Terremotos</li> <li>- Fuego</li> </ul>
Incidentes de origen no natural	<ul style="list-style-type: none"> <li>- Terrorismo</li> <li>- Fuego</li> </ul>
Eventos o hechos no intencionados	<ul style="list-style-type: none"> <li>- Configuraciones erróneas</li> <li>- Pérdida de equipamiento</li> <li>- Errores en la administración</li> </ul>
Acciones o hechos intencionados	<ul style="list-style-type: none"> <li>- Robo de información</li> <li>- Accesos no autorizados</li> <li>- Destrucción de equipos</li> </ul>

Asimismo, debemos tener una clasificación de los **activos**, que no son más que componentes o funcionalidades susceptibles a ser atacados deliberada o accidentalmente causando daños a la Institución. Éstos a su vez, según (Ministerio de Administraciones Públicas de España, 2006) tienen dimensiones que para poder ubicarlos responden a ciertas preguntas:



**Disponibilidad:** ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo?

**Confidencialidad:** ¿Qué daño causaría que lo conociera quien no debe?

**Integridad:** ¿Qué perjuicio causaría que estuviera dañado o corrupto?

Teniendo como base estas preguntas podemos valorar cada activo de la siguiente manera:

Activos de TI	Dimensiones		
	Disponibilidad	Confidencialidad	Integridad
Aplicaciones	X		X
Datos / información	X	X	X
Equipos	X		
Infraestructura	X		
Comunicaciones		X	
Personal de TI			X
Servicios	X	X	

Para un adecuado análisis de los riesgos, es importante conocerlos, para lo cual debemos determinar ciertos parámetros que nos serán de mucha ayuda. La Probabilidad de que un riesgo ocurra es difícil de determinar pero para este caso tomaremos valores teniendo como referencia un





año, para que luego para cualquier valor estadístico se pueda tomar como tasa anual de ocurrencia.

SIGLAS	DENOMINACIÓN	VALOR	OCURRENCIA
MF	Muy frecuente	5	A diario
F	Frecuente	4	Mensualmente
N	Normal	3	Una vez al año
PF	Poco Frecuente	2	Cada varios años
MP	Muy poco frecuente	1	Siglos

De igual manera debemos poder determinar el impacto que causaría un riesgo en caso ocurriera, para lo cual se ha creído conveniente establecer ciertos valores.

IMPACTO DE RIESGO	DESCRIPCIÓN DEL RIESGO	VALOR EL IMPACTO	INTERPRETACIÓN DEL VALOR DEL IMPACTO
Insignificante	Puede ser fácilmente mitigado	1	Este riesgo retrasa el progreso de una tarea individual dentro del grupo.



Menor	Afecta de forma menor el presupuesto del proyecto y puede tomar unos pocos días para resolver	2	Este riesgo retrasa el progreso del proyecto de forma mínima
Moderado	Afecta de forma moderada el presupuesto del proyecto y puede requerir una replanificación en el plan del proyecto.	3	Este riesgo afecta de alguna manera el progreso del proyecto y al equipo de trabajo.
Serio	Afecta la credibilidad e integridad del proyecto. Puede requerir solicitar nuevo financiamiento y adición de	4	Este riesgo afecta el progreso de todo el equipo de trabajo y demanda la atención del gerente del proyecto.



	recursos. Se debe considerar un importante cambio en la planificación del proyecto.		
Crítico	Puede representar el fracaso total o abandono del proyecto.	5	Este riesgo afecta a todo el equipo de trabajo y requiere de la atención inmediata del gerente del proyecto.

Otro parámetro importante es la **Exposición**, que no es más que la relación existe entre la ocurrencia y el impacto de que cada riesgo ocurra, que podemos caracterizarlo como una exposición baja, media o alta, teniendo así la siguiente tabla:

Probabilidad de Ocurrencia		Impacto del Riesgo				
		Insignificante	Menor	Moderado	Serio	Crítico
Muy frecuente	5	Bajo	Bajo	Bajo	Medio	Medio



Frecuente	4	Bajo	Bajo	Medio	Medio	Alto
Normal	3	Bajo	Medio	Medio	Medio	Alto
Poco Frecuente	2	Medio	Medio	Alto	Medio	Alto
Muy poco frecuente	1	Medio	Alto	Alto	Alto	Alto

Una vez identificados los riesgos y sus características, existen estrategias para poder dar respuesta a los mismos:

**Reducción del Riesgo (R):** Se deben implementar controles apropiados para poder reducir los riesgos a un nivel aceptable.

**Aceptar el Riesgo (A):** Muchas veces se presentan situaciones en la cual la organización no encuentra controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias, la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada.

**Transferencia del Riesgo (T):** Es una opción cuando para la Institución es difícil reducir o controlar el riesgo a un nivel aceptable. La alternativa de transferencia a una tercera parte es más económica ante estas circunstancias.



**Evitar el Riesgo (E):** Cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad en particular, y así evitar la presencia del riesgo.

En base a esto se ha creído conveniente establecer una lista de los principales activos de la Institución, así como las amenazas a las que están expuestos.

**ANÁLISIS Y EVALUACIÓN DE RIESGOS**

N°	ACTIVO	AMENAZA	Confidencialidad	Integridad	Disponibilidad	Valoración	VULNERABILIDADES	MECANISMOS DE PROTECCIÓN EXISTENTES	Probabilidad	Impacto	Riesgo
1	Documentación sobre Gestión de Pacientes	Fuga o divulgación de información por parte del personal interno	3	3	3	9	No existe políticas, cartas u otros documentos que evidencien confidencialidad de información	Efectuar el respaldo de la información. Respaldar los back up en un lugar adecuado.	2	4	8
		Acceso no autorizados					No se cuenta con el control adecuado de	2	4	8	





						acceso configurado por usuario.	Control de acceso a la información.			
		Robo de documentación				Los documentos son fácilmente extraíbles	Restaurar información.	2	4	8
		Información desactualizada				No se cuenta con un procedimiento para actualización de información		2	4	8
		Modificación de información accidental o intencional.				No se cuenta con un control adecuado sobre el acceso a los documentos		3	4	12



2	Documentación de Proyectos de Investigación sobre Tecnología	Fuga o divulgación por parte del personal interno.	1	2	3	6	No existen políticas de confidencialidad para el personal interno.	Control de acceso a la información Restaurar información	1	2	2
		Modificación de información					No se cuenta con un ambiente independiente para pruebas de investigación		2	2	4
		Desastres (fuego, inundación, sismo, explosión, disturbios y demás)							2	2	4



		Pérdida parcial o completa de información							2	2	4
3	Herramientas y entornos de desarrollo (.net, visual basic)	Mala instalación, configuración, actualización de software	1	3	4	8	No existen manuales de soporte para la solución de problemas (configuraciones, instalaciones y actualizaciones)	Todos los usuarios deben de contar con la misma versión de software	2	3	12
		Herramientas desactualizadas					No se cuenta con el soporte adecuado		2	3	6



						para actualizar las herramientas			
		Cambio de versión de las herramientas y entornos				No se cuenta con un soporte para revisar el cambio de versión	2	4	8
		Instalación de software no licenciado.				No se cuenta con un control para la instalación de software no licenciado.	2	5	10



		Falta de renovación de licencias.				El amarre de los desarrollos a las versiones del software.		2	5	10
		Falta de Licencias para el software				Número limitado de licencias para el software.		2	3	6
		Eliminación de archivos propios del lenguaje.				Desconocimiento del personal de soporte para la solución de problemas como configuraciones y actualizaciones.		2	3	6



4	Motores de Base de Datos	Mala instalación, configuración y/o actualización de software.	3	4	4	11	No existen manuales de soporte para la solución de problemas como configuraciones, instalaciones y actualizaciones.	Obtener backup de la información. Registro de incidentes según los errores que se van presentando.	2	5	10
		Infección por código malicioso, virus, troyanos, gusanos					No se cuenta con un antivirus actualizado.		1	5	5
		Caída de los motores de Base					No existe un ambiente en donde poder		2	5	10





		de Datos y su impacto en Aplicativos				realizar pruebas por actualización de versión.  Impacto en los sistemas por actualización de versión.			
		Falta de soporte técnico apropiado para los software				Desconocimiento del personal de soporte para la solución de problemas.	2	5	10



		Accesos al software para usuarios no autorizados.				No se cuenta con un control para el control de accesos		2	5	10
		Herramientas desactualizadas.				No se cuenta con el soporte para actualizar herramientas.		2	3	6
		Cambio de versión de las herramientas y entornos.				No se cuenta con un soporte para revisar el cambio de versión.		2	4	8



		Instalación de software no licenciado.				No se cuenta con un control para la instalación de software no licenciado.		2	3	6
		Falta de renovación de licencias				El amarre de los desarrollos a las versiones del software		2	3	6
		Falta de licencias para el software.				Número limitado de licencias para los softwares.		2	3	6



5	Personal de la División de Tecnologías de la Información	Indisponibilidad del personal.	3	3	3	9	Desconocimiento de las funciones y responsabilidad inherentes al cargo.	.Políticas y procedimiento s de selección de nuevo persona.	2	4	8
		Poco interés del personal en seguridad de información					No existe una cultura de seguridad de información		2	4	8
		Robo de información					Nivel de compromiso del trabajador con la Institución		2	4	8



		Extorsión					No existe un seguro de protección contra Extorsión.		1	1	1
6	Reportes contables	Daño o deterioro del papel, ya sea por agua, polvo, etc.	1	1	1	3	No contar con la aclimatización para el papel.	Control de acceso físico a las áreas.	2	2	4
		Accesos no autorizados.					Ausencia de personal.	Control de visitantes del Hospital como	2	2	4
		Desperfecto en impresión de documentos					Ausencia de personal	proveedores.	2	2	4



		Mala impresión de documentos					Ausencia de transferencia de conocimientos		2	2	4
		Pérdida de documentos.					Ausencia y falta de compromiso del personal.		2	3	6
7	Información Logística	Accesos no autorizados	1	1	1	3	No se cuenta con control de acceso.	Control de acceso físico a las áreas. Control de visitantes del Hospital como proveedores.	3	2	6
		Daño o deterioro por polvo, agua, etc.					No se cuenta con control de accesos físicos.		3	2	6
		Mala distribución de reportes.					Ausencia de control de reportes.		3	2	6



8	PC - Laptops	Deterioro de equipos debido a contaminación	2	3	3	8	Ausencia de programa de mantenimiento preventivo.	Acceso restringido.	2	3	6
		Mala manipulación de equipos					Ausencia de política de uso de equipos.		3	2	6
		Trabajos de mantenimientos en oficinas					Ausencia de repuestos en stock Ausencia de programa de mantenimiento preventivo.		3	2	6





		Falla de equipos				Ausencia de repuestos en stock.		2	3	6
		Equipos descontinuados				Ausencia de garantías.				
		Infeción por código malicioso, virus, troyano, gusanos.				Ausencia de repuestos en stock.		2	3	6
						Ausencia de garantías.				
						Ausencia de monitoreo del estado del antivirus.		2	3	6



		Desinstalación de aplicativos y sistemas				No se cuenta con un control para la desinstalación de aplicativos.		3	3	9
		Desastres (incendios, explosiones, etc.)				No se cuenta con muchos extintores. Los detectores de incendios no se encuentran en buen funcionamiento.		1	5	5
		Acceso no autorizado				Mala configuración del protector de pantalla.		5	2	10



		Existencia de usuarios genéricos					No se cuenta con una definición clara de las funciones por usuario.		5	3	15
		Pérdida de información por baja de equipos.					Ausencia de políticas.		3	1	3
		Robo de equipos					Ausencia de controles de seguridad de información. Ausencia de controles físicos.		5	3	15
9	Servidores	Falla de equipos	2	3	5	10	Ausencia de repuestos en stock.		2	5	10



						Ausencia de garantía.			
						Ausencia de contingencia de servidores	de	Monitoreo de espacio en disco.	
						Ausencia de programa de mantenimiento preventivo.	de	UPS Grupo electrógeno Control de	
		Falla de espacio en disco				Ausencia de alertas.		acceso físico.	
						Ausencia de soluciones automatizadas.	de	Control de visitantes.	3
									5
									15



		Falla de energía y otras interrupciones eléctricas				UPS soporta carga de equipos de Data Center.		2	5	10
		Virus, troyanos, gusanos especializados que afecten específicamente servidores				Ausencia del monitoreo del estado del antivirus.		3	5	15
		Mala manipulación de equipos.				Ausencia de manuales de soporte		3	4	12



		Falla en firewall				Ausencia de dispositivos de respaldo de alta complejidad.		2	5	10
		Equipo descontinuado				No se cuenta con soporte ni presupuesto para renovación de equipos.		2	3	6
		Saturación de Rack de servidores						1	5	5



		Sobrecarga de tráfico en red LAN.						2	5	10
		Mala configuración				No se cuenta con personal correctamente capacitado para las configuraciones.		2	4	8
		Accesos no autorizados.				Mal funcionamiento		2	5	10
		Deterioro de equipos debido a contaminación				Fallas en el air acondicionado y		3	4	12





							control de temperatura.				
		Desastres (fuego, inundaciones, sismos, etc.)					Fallas en el detector de incendios.	1	5	5	
		Robo de equipos.					Ausencia de control estricto de personal.	2	5	10	
10	Cámaras de Vigilancia	Manipulación por personal no calificado.	2	2	2	6	Equipos sin protección física.	Control de acceso físico.	1	3	3
		Falla de equipos					Equipos descontinuados.	Control de visitantes.	2	2	4



		Deterioro de equipos por causa de la contaminación					Ausencia de programa de mantenimiento preventivo				2	2	4
--	--	--	--	--	--	--	--	--	--	--	---	---	---

Una vez detallados las principales amenazas a las que están expuestos los activos de la Institución, se plantea una serie de mecanismos de protección según la estrategia escogida; para este caso, escogeremos REDUCIR, debido a que lo se busca es minimizar el daño que pueden causar estas amenazas.

Según el valor del RIESGO obtenido de la multiplicación de la probabilidad por el impacto de cada amenaza de los activos, seleccionamos los de mayor valor, a los cuales les aplicaremos la estrategia con sus respectivos mecanismos de protección.



**GESTIÓN DE RIESGOS**

N°	ACTIVO	AMENAZA	MECANISMOS DE PROTECCIÓN	ESTRATEGIA
1	Documentación sobre Gestión de Pacientes	Fuga o divulgación de información por parte del personal interno	Implementar una política de confidencialidad. Implementar un compromiso de confidencialidad firmado.	Reducir
		Acceso no autorizados	Configurar accesos a carpetas por perfiles.	Reducir
		Robo de documentación	Implementar controles para protección de documentos.	Reducir
		Información desactualizada	Revisiones periódicas del Jefe de DITI.	Reducir



		Modificación de información accidental o intencional.	Implementar un sistema de control de versiones	Reducir
2	Documentación de Proyectos de Investigación	Fuga o divulgación por parte del personal interno.	Implementar una política de confidencialidad. Implementar un compromiso de confidencialidad firmado.	Reducir
		Modificación de información	Revisiones periódicas del Jefe de DITI.	Reducir
	Tecnología	Desastres (fuego, inundación, sismo, explosión, disturbios y demás)	Implementar un plan de mantenimiento preventivo de extintores y detectores de incendio.	Reducir



		Pérdida parcial o completa de información	Implementar controles para protección de documentos.	Reducir
3	Herramientas y entornos de desarrollo (.net, visual basic)	Mala instalación, configuración, actualización de software	Implementar manuales, video tutoriales para los softwares.	Reducir
		Herramientas desactualizadas	Revisiones periódicas de nuevas actualizaciones.	Reducir
		Cambio de versión de las herramientas y entornos	Planificación del cambio de versiones.	Reducir
		Instalación de software no licenciado.	Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir



		Falta de renovación de licencias.	Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir
		Falta de Licencias para el software	Elaborar un plan de dimensionamiento de licencias según demandas presentes y futuras.	Reducir
		Eliminación de archivos propios del lenguaje.	Implementar manuales, video tutoriales para los softwares.	Reducir
4	Motores de Base de Datos	Mala instalación, configuración y/o actualización de software.	Implementar manuales, video tutoriales para los softwares.	Reducir
		Infección por código malicioso, virus, troyanos, gusanos	Mantener actualizados los antivirus.	Reducir



	Caída de los motores de Base de Datos y su impacto en Aplicativos	Implementar un laboratorio para las pruebas de cambio de versiones.	Reducir
	Falta de soporte técnico apropiado para los software	Implementar manuales, video tutoriales para los softwares. Implementar monitoreos de performance de las BD	Reducir
	Accesos al software para usuarios no autorizados.	Configurar acceso a carpetas por perfiles.	Reducir
	Herramientas desactualizadas.	Revisiones periódicas de nuevas actualizaciones.	Reducir
	Cambio de versión de las herramientas y entornos.	Planificación del cambio de versiones.	Reducir





		Instalación de software no licenciado.	Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir
		Falta de renovación de licencias	Implementar controles y revisiones mensuales para las renovaciones de licencias.	Reducir
		Falta de licencias para el software.	Elaborar un plan de dimensionamiento de licencias según las demandas presentes y futuras.  Administración de licencias.	Reducir
5	Personal de la División	Indisponibilidad del personal.	Difundir el MOF para cada puesto.	Reducir



	de Tecnologías de la Información	Poco interés del personal en seguridad de información	Concientizar al personal sobre la Seguridad de la Información	Reducir
		Robo de información	Implementar compromiso de confidencialidad.	Reducir
		Extorsión		Reducir
6	Reportes contables	Daño o deterioro del papel, ya sea por agua, polvo, etc.	Digitalizar documentos.	Reducir
		Accesos no autorizados.	Configurar acceso a carpetas por perfiles.	Reducir
		Desperfecto en impresión de documentos	Implementar mantenimientos correctivos de equipos.	Reducir
		Mala impresión de documentos	Capacitación en uso de equipos y seguridad a todo el personal.	Reducir



		Pérdida de documentos.	Implementar controles para visitas externas. Implementar controles para prevenir el acceso físico del personal a lugares restringidos.	Reducir
7	Información Logística	Accesos no autorizados	Configurar acceso a carpetas por perfiles.	Reducir
		Daño o deterioro por polvo, agua, etc.	Digitalizar documentos.	Reducir
		Mala distribución de reportes.	Concientizar al personal sobre la importancia de la documentación existente.	Reducir



8	PC - Laptops	Deterioro de equipos debido a contaminación	Implementar un programa de mantenimiento preventivo de equipos.	Reducir
		Mala manipulación de equipos	Capacitación en uso de equipos y seguridad a todo el personal.	Reducir
		Trabajos de mantenimientos en oficinas	Capacitación al personal en cuidado de equipos. Coordinaciones previas a los trabajos de mantenimiento.	Reducir
		Falla de equipos	Contar con un stock mínimo de repuestos y laptops.	Reducir



			<p>Implementar un programa de mantenimiento preventivo de los equipos.</p> <p>Realizar mantenimiento a las instalaciones eléctricas.</p> <p>Hacer seguimiento a las garantías.</p> <p>Mantener relaciones comerciales con proveedores estratégicos.</p>	
		Equipos descontinuados	<p>Establecer un inventario actualizado de equipo según su vida útil.</p>	Reducir



		Infección por código malicioso, virus, troyano, gusanos.	Implementar entrega de informes mensuales sobre el estado del antivirus.	Reducir
		Desinstalación de aplicativos y sistemas	Elaborar política de protección de equipos. Habilitar restricciones en el dominio para prohibir desinstalación de programas. Capacitar al personal sobre seguridad en la información.	Reducir
		Desastres (incendios, explosiones, etc.)	Implementar extintores apropiados.	Reducir



			<p>Capacitar al personal en el uso de extintores.</p> <p>Realiza mantenimientos preventivos y correctivos a los detectores de incendio.</p>	
		Acceso no autorizado	<p>Habilitar el protector de pantalla automático según usuario.</p> <p>Capacitar al personal en seguridad de la información.</p>	Reducir
		Existencia de usuarios genéricos	<p>Eliminar a los usuarios genéricos.</p>	Reducir
		Pérdida de información por baja de equipos.	<p>Implementar protocolos de baja de equipos.</p>	Reducir





		Robo de equipos	<p>Implementar documentos para el retiro de equipos fuera de las instalaciones.</p> <p>Implementar controles de encriptación de equipos.</p> <p>Implementar controles físicos de seguridad.</p> <p>Implementar controles para visitas externas.</p> <p>Implementar controles para prevenir el acceso físico del personal a lugares restringidos.</p>	Reducir
--	--	-----------------	--	---------



9	Servidores	Falla de equipos	<p>Implementar programas de mantenimiento preventivo de equipos.</p> <p>Implementar mecanismos de control a los contratos de mantenimientos de terceros.</p> <p>Implementar contingencia de servidores.</p> <p>Independizar UPS para protección exclusiva de servidores.</p> <p>Seguimiento a las garantías.</p>	Reducir
---	------------	------------------	--	---------



			Mantener buenas relaciones comerciales con proveedores estratégicos.	
		Falla de espacio en disco	Implementar alertas sobre espacio en disco. Implementar soluciones automatizadas para monitoreo de servidores.	Reducir
		Falla de energía y otras interrupciones eléctricas	Independizar UPS para protección exclusiva de servidores.	Reducir



		Virus, troyanos, gusanos especializados que afecten específicamente servidores	Implementar entrega de informes mensuales sobre el estado del antivirus.	Reducir
		Mala manipulación de equipos.	<p>Capacitación a operadores.</p> <p>Actualizar el MOF de la Institución detallando responsabilidades.</p> <p>Elaborar instructivos técnicos sobre la función de cada servidor.</p> <p>Asignar personal capacitado para Data Center.</p>	Reducir
		Falla en firewall	Implementar un firewall alternativo.	Reducir



		Equipo descontinuado	Establecer un inventario actualizado de los equipos según su vida útil.  Elaborar un plan de renovación y adquisición de equipos.	Reducir
		Saturación de Rack de servidores	Implementar nuevos racks.	Reducir
		Sobrecarga de tráfico en red LAN.	Implementar herramientas de monitoreo de tráfico.	Reducir
		Mala configuración	Implementar protocolos de cambios de configuración.	Reducir
		Accesos no autorizados.	Implementar control de claves a los servidores.	Reducir



			<p>Implementar control dual de clave maestra.</p> <p>Renovar el sistema de control de accesos.</p> <p>Implementar procedimientos o protocolos para cambios de configuración.</p>	
		Deterioro de equipos debido a contaminación	<p>Implementar un programa de mantenimiento preventivo de equipos.</p> <p>Implementar detectores para el control de temperatura.</p>	Reducir



			<p>Implementar aire acondicionado de precisión.</p> <p>Implementar deshumecedor.</p>	
		Desastres (fuego, inundaciones, sismos, etc.)	<p>Implementar extintores apropiados.</p> <p>Capacitar al personal en el uso de extintores.</p> <p>Realiza mantenimientos preventivos y correctivos a los detectores de incendio.</p>	Reducir
		Robo de equipos.	<p>Implementar documentos para el retiro de equipos fuera de las instalaciones.</p>	Reducir





			<p>Implementar controles de encriptación de equipos.</p> <p>Implementar controles físicos de seguridad.</p> <p>Implementar controles para visitas externas.</p> <p>Implementar controles para prevenir el acceso físico del personal a lugares restringidos.</p>	
10	Cámaras de Vigilancia	Manipulación por personal no calificado.	Implementar control de acceso a personal externo.	Reducir



	Falla de equipos	Implementar un programa de mantenimiento preventivo de equipos.	Reducir
	Deterioro de equipos por causa de la contaminación	Implementar un programa de mantenimiento preventivo de equipos.	Reducir

Asimismo, cada mecanismo propuesto conlleva a una serie de actividades para poder cumplir con la estrategia escogida; para este caso, escogeremos algunos debido a que por ser una Institución del estado, y teniendo que cumplir con ciertos parámetros burocráticos, se ha creído conveniente detallar las actividades más factibles de cumplir, las cuales están relacionadas con el equipo de trabajo de la División de Tecnologías de la Información.



N°	MECANISMOS DE PROTECCIÓN	ACTIVIDADES	RESPONSABLES
1	Concientizar al personal sobre la Seguridad de Información.	Elaborar un plan de concientización en seguridad de la información.	Jefe de Desarrollo de Sistemas
		Elaborar material de concientización para su difusión.	
		Ejecutar la primera capacitación en concientización en Seguridad de la Información	
2	Administración de licencias	Elaborar lineamientos para la gestión de licencias.	Jefe de Desarrollo de Sistemas
		Ejecutar la primera revisión del inventario de licencias.	



		Definir criterios de dimensionamiento de licencias	
		Realizar dimensionamiento anual de licencias	
3	Elaborar y difundir el MOF	Actualizar el MOF de personal de la Institución.	Oficina de Desarrollo Humano – Jefe de la División de Tecnologías de la Información
		Difundir el MOF a todo el personal de la Institución.	
4	Implementar políticas de seguridad	Definir con la oficina de asesoría legal los tipos de documentos para establecer confidencialidad del personal.	Jefe de Data Center



		Aprobación de los documentos mediante Resolución emitida por el Director de la Institución.	
5	Implementar manuales o video tutoriales para la instalación y configuración de software.	Identificar los softwares que necesitan los manuales.	Jefe de Soporte Técnico
		Implementar los manuales de configuración y/o instalación.	
6	Revisiones periódicas de nuevas actualizaciones	Elaborar lineamientos de nuevas actualizaciones	Jefe de Soporte Técnico
		Ejecutar la primera revisión de nuevas versiones de los aplicativos	



7	Implementar procedimientos para configurar ambientes de pruebas	Elaborar procedimientos e instructivos para la configuración de ambientes adecuados para pruebas.	Jefe de Desarrollo de Sistemas
		Revisar y aprobar los procedimientos mediante resolución firmado por el Director de la Institución	
8	Capacitación al personal en cuidado y uso de equipos	Elaborar un plan de capacitación en equipos de cómputo.	Jefa de la División de Tecnologías de la Información
		Capacitar al personal en cuidado y uso de equipos de cómputo.	



9	Asignar personal capacitado para el Centro de Cómputo de contingencia	<p>Evaluar al personal para el Data Center de Contingencia</p> <p>Asignar personal adecuado para el data center de contingencia</p>	<p>Jefa de la División de Tecnologías de la Información</p>
10	Contar con un stock mínimo de repuestos	<p>Evaluar stock mínimo de Routers, Switch y Patch Panel</p> <p>Adquisición del stock mínimo de Routers, Switch y Patch Panel</p> <p>Inventariar equipos de comunicación</p>	<p>Jefe de Soporte Técnico</p>
11	Contar con un stock mínimo de repuestos y laptops	<p>Evaluar stock mínimo de repuestos de PC's y laptops</p> <p>Adquisición de repuestos de PC's y laptops.</p>	<p>Jefe de Soporte Técnico</p>





		Inventariar repuestos de PC's y laptops.	
12	Implementar programa de mantenimiento preventivo de equipos	Seleccionar equipos para el mantenimiento preventivo interno.	Jefe de Soporte Técnico
		Elaborar el procedimiento para el Mantenimiento preventivo de equipos.	
		Elaborar el programa de mantenimiento preventivo	
13	Seguimiento a las garantías	Elaborar lineamientos para el seguimiento y control de garantía	Jefe de Soporte Técnico
14	Implementar procedimientos para la baja de equipos	Elaborar procedimientos de baja de equipos y eliminación de datos	Jefe de Soporte Técnico



		Difundir procedimientos de baja de equipos	
15	Implementar detectores para el control de temperatura, aire acondicionado de precisión y deshumecedor para el Data Center	Evaluación de tipos de detectores, aire acondicionado y deshumecedor de primera.	Jefe de Data Center – Jefa de la División de Tecnologías de la Información.
		Presentación y sustentación al director de la Institución.	
		Adquirir el detector, aire acondicionado y deshumecedor.	
		Implementación del material adquirido.	
16		Cotizar trabajo de circuito eléctrico independiente	Jefe de Data Center



	Independizar UPS para protección exclusiva de los equipos de Data Center	Ejecutar trabajo de circuito eléctrico. Elaborar plan de pruebas de UPS Realizar pruebas de independización.	
17	Implementar pruebas periódicas de restauración	Elaborar cronograma de programación de pruebas de restauración Elaborar instructivos técnicos de pruebas Aperturar un archivo físico de cronograma de programación	Jefe de Data Center
18	Implementar informes mensuales sobre el estado del antivirus	Definir procedimientos de trabajo Elaborar política y procedimiento de antivirus	Jefe Soporte Técnico



19	Implementar un plan de actualización de versiones	Elaborar un inventario de software	Jefe de Desarrollo de Sistemas
		Programar reuniones de coordinación para actualización de versiones de Software.	
		Definir un plan de actualización de versiones anual.	
20	Renovación tecnológica	Programación anual de renovación tecnológica	Jefa de la División de Tecnologías de la Información



## **CAPÍTULO VI:      CONSIDERACIONES FINALES Y RECOMENDACIONES**

### **6. 1. Consideraciones finales**

Podemos afirmar que se cumple con los objetivos del proyecto, ya que se obtiene una herramienta capaz de manejar los riesgos y hacerles un seguimiento, cumpliendo la estructura de la metodología aplicada y la aceptación de los directivos de la Institución. Podemos decir que el análisis de riesgos nos permitió determinar qué tiene la Institución, en este caso el Hospital Regional Lambayeque, y estimar lo que podrá suceder. El análisis de riesgos también permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y obtener resultados positivos que aseguren la continuidad del negocio.

Esta nueva gestión de riesgos, permitirá al Hospital Regional Lambayeque organizar la defensa concienzuda y prudente, previniendo sucesos perjudiciales y al mismo tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones. Se dice que el riesgo se reduce a un nivel residual que la dirección lo asume, y de este modo el Hospital estaría en condiciones para poder obtener la Certificación ISO 27001, y así obtener más prestigio del q ya tiene.

Con esta gestión de riesgos se buscó asegurar la confidencialidad, integridad y disponibilidad de los activos de información del Hospital Regional Lambayeque, minimizando así las amenazas de seguridad de la información.

## 6. 2. Recomendaciones

Podemos recomendar que el Hospital Regional Lambayeque, cree un área de seguridad informática, capaz de gestionar técnicas y metodologías, para aplicar la solución más efectiva posible contra las amenazas de sus activos.

El Hospital Regional Lambayeque deberá definir una estructura del estándar ISO 27001, definiciones, descripciones e indicaciones de seguridad de la información; así como, también deberá realizar el cumplimiento de los requisitos legales y normas de seguridad, consideraciones sobre las auditorías de la seguridad de la información.

Se plantea además que el análisis y gestión de riesgos de tecnologías de la información se realice de manera trimestral, debido al tipo de evaluaciones que se realizan en el sector público en cuanto a logro de objetivos y avance de ejecución presupuestal; lo cual va permitir tener una mejor visión de lo que se necesita alcanzar para poder minimizar el impacto del riesgo.



## REFERENCIAS

- Abril, A., Pulido, J., & Bohada, J. A. (2013). Análisis de Riesgos en Seguridad de la Información. *Ciencia, Innovación y Tecnología*, 40-53.
- Carnegie Mellon Software Engineering Institute. (s.f.). Introduction to the OCTAVE Approach. Pittsburgh: Networked Systems Survivability Program.
- Carrillo Sánchez, J. (2013). Gestión del riesgo en las metodologías de proyectos de tecnologías de información y comunicaciones. *Enfoque UTE*, 77-94.
- Celi Arévalo, E. (2013). Un modelo para la gestión de riesgos de TI en las empresas microfinancieras: caso Lambayeque, Perú. *Universidad Pedro Ruiz Gallo*.
- Celi Arévalo, E. K. (2015). Aplicación de Dashboards y Scorecards para el Aprendizaje - Modelos de Gestión de Riesgos de TI: Una experiencia de Usuario. *aaa*.
- CLUSIF, C. d. (2010). MEHARI. *MEHARI 2010*. Paris: Comisión de Métodos.
- Cohen, M. W., PE, & Palmer, G. R. (2004). Project Risk Identification and Management. *AACE International Transactions*.
- El Portal de ISO 27001 en Español*. (2012). Obtenido de El Portal de ISO 27001 en Español: [www.iso27001.es](http://www.iso27001.es)
- ENISA, (. N. (Junio de 2006). Risk Management. *Risk Management: Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools*. Europa: [www.enisa.europa.eu](http://www.enisa.europa.eu).
- Fernández Sánchez, C. M., & Piattini Velthuis, M. (2012). *Modelo para el gobierno de las TIC basado en las normas ISO*. Madrid: AENOR (Asociación Española de Normalización y Certificación).
- Fernández, C. M. (Setiembre de 2012). La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información. *Calidad*, 40-44.
- Fuertes, L. (2007). *Gestión de Riesgos TI. Cómo implementar las mejores prácticas*. Madrid, España: Asociación de Proveedores de Sistemas de Red, Internet y Telecomunicaciones .
- ISO/IEC Guide 73. (01 de 04 de 2008). ISO/TMB WG on Risk Management. *Risk Management - Vocabulary*. ISO.
- Kenning, M. J. (2001). Security Management Standard - ISO 17799/BS 7799. *BT Technol J*, 132-136.





- Kerlinger, F., & Lee, H. (2002). *Investgaciones del comportamiento. Metodos de invetigacion en ciencia sociales (4ª ed.)*. Mexico: McGraw-Hill.
- López Vargas, C., Salmerón Silvera, J. L., & Mena Nieto, Á. (2009). *Análisis de los Riesgos en Proyectos SI/TI basado en el Enfoque IPA*. España: Universidad Pablo de Olavide - Universidad de Huelva.
- Marulanda Echeverry, C. E., López Trujillo, M., & Cuesta Iglesias, C. A. (2009). Modelos de Desarrollo para Gobierno TI. *Scientia et Technica Año XV, No 41*, 185 - 190.
- Ministerio de Administraciones Públicas de España. (20 de 06 de 2006). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT versión 2. *MAGERIT versión 2*. Madrid, España: Catálogo general de publicaciones oficiales.
- Romeral, L. M., & Torres Gallego, Á. (2008). Gestión de los Riesgos Tecnológicos. *RPM-AEMES*, 14-22.
- Shapira, Z., & Berndt, D. (1997). Managing Grand-Scale Construction Projects: A Risk-Taking Perspective. *Research in Organizational Behavior*, 19: 303-360.
- Stoneburner, G., Goguen, A. Y., & Feringa, A. (2002). *Risk Management Guide for Information Technology Systems*. Gaithersburg: National Institute of Standards & Technology.
- The British Standards Institution. (2016). *BSI... making excellence a habit*. Obtenido de BSI... making excellence a habit: [www.bsigroup.com](http://www.bsigroup.com)
- Tversky, A., & Kahneman, D. (1986). Rational Choice and the Framing of Decisions. *Journal of Business*, 59(4): S251-79.
- Westerman, G. (2006). IT Risk Management: From IT Necessity to Strategic Business Value. *Center for Information Systems Research and Massachusetts Institute of Technology*.



## ANEXOS

### ENCUESTA A TRABAJADORES DE LA DIVISIÓN DE TECNOLOGÍAS DE LAS INFORMACIÓN (ENTREVISTA)

Pregunta	Sí	No	NA	Comentarios
1. ¿Se establece un plan de trabajo anual de las actividades de TI?				
2. ¿Se realiza una exposición del plan de trabajo a la Administración y/o Dirección del Hospital?				
3. ¿Se deja evidencia formal del plan de trabajo, los cambios realizados y la supervisión ejercida?				
4. ¿Se realiza un informe periódico de labores realizadas: oral y escrito?				
5. ¿Se ha definido un proceso de planificación para la obtención de los recursos requeridos?				
6. ¿Se lleva un registro detallados de los activos de la Institución?				



7. ¿Existe un inventario de las configuraciones de los equipos, así como de los componentes y software instalado?				
8. ¿Se lleva control de licencias de software y costos de licenciamiento?				
9. ¿Se lleva un control de la vida útil de los activos de información?				
10. ¿Se sigue algún procedimiento para borrar la información de los discos duros u otras unidades de almacenamiento, antes su desecho?				
11. ¿Se tiene identificados y priorizados los servicios de TI para asegurar su entrega oportuna?				
12. ¿Se tiene alguna estadística de la utilización de los diferentes servicios ofrecidos?				



<p>13. ¿Se han identificado los riesgos de TI asociados a la gestión y operación de la plataforma informática de la Institución?</p>				
<p>14. ¿Se han identificado los activos o servicios más críticos para el cumplimiento de los objetivos de la Institución?</p>				
<p>15. ¿Se han establecido los riesgos asociados a los recursos más críticos?</p>				
<p>16. ¿Se han establecido controles para mitigar los riesgos de los recursos de información más críticos?</p>				
<p>17. ¿Se informa periódicamente a la administración respecto a las amenazas y riesgos asociados a los recursos de TI y los requerimientos para mitigar esos riesgos?</p>				

18. ¿Se renuevan periódicamente las claves de acceso a la información?				
19. ¿Se eliminan los derechos de acceso a funcionarios inactivos o que han dejado de laborar para la Institución?				
20. ¿La carga de los extintores de incendio se encuentra vigente?				
21. ¿Se conoce el mecanismo de operación de los diversos tipos de extintores de incendio?				
22. ¿Se han establecido controles para resguardar la información ante la salida de activos por parte de terceros, personal de la Institución o por motivos de reparación?				
23. ¿Se tiene una clasificación de la información de la Institución por nivel de sensibilidad o privacidad?				



<p>24. ¿Se revisan con frecuencia los medios de almacenamiento para asegurar la integridad de la información contenida en ellos?</p>				
<p>25. ¿Se realizan revisiones periódicas para verificar la integridad física de los activos de información?</p>				

**ENCUESTA A TRABAJADORES DE LAS DIVERSAS ÁREAS DEL  
HOSPITAL REGIONAL LAMBAYEQUE**

<b>Pregunta</b>	<b>Sí</b>	<b>No</b>	<b>NA</b>	<b>Comentarios</b>
1. ¿Tiene asignado a su cargo uno o más activos informáticos?				
2. ¿Sabe usted el o los softwares que tiene instalados en sus equipos?				
3. ¿Informa al área indicada sobre los equipos que tiene en desuso?				
4. ¿Está satisfecho usted con los servicios ofrecidos por la División de Tecnologías de la Información?				
5. ¿Utiliza claves de acceso a la información seguras?				
6. ¿Renueva periódicamente sus claves de acceso a la Información?				
7. ¿Sabe usted a quién reportar en caso le suceda algún incidente informático?				





<p>8. ¿Cree usted que hace un buen uso de los servicios ofrecidos por la División de Tecnologías de la Información?</p>				
<p>9. ¿Toma usted las medidas necesarias para el correcto funcionamiento y cuidado de los equipos informáticos?</p>				
<p>10. ¿Conoce el mecanismo de operación de los diversos tipos de extintores de incendio con los que cuenta la Institución?</p>				
<p>11. ¿Cree usted que el Hospital está preparado para salvaguardar su información en caso de algún siniestro?</p>				
<p>12. ¿Solicita usted al área indicada le realicen el mantenimiento preventivo a sus equipos?</p>				

