



**Universidad  
Nacional  
De Loja**



Facultad de la Energía, las Industrias y los Recursos Naturales No Renovables

---

Carrera de Ingeniería en Sistemas

# **Plan de Gestión de Riesgos de TI en el Hospital de Catacocha.**

TESIS DE GRADO PREVIA A LA  
OBTENCIÓN DEL TÍTULO DE  
INGENIERA EN SISTEMAS

***Autora:*** Rivera-Serrano, Johanna-Elizabeth

***Directora:*** Ing. Herrera Salazar, Valeria del Rosario, MSc.

**LOJA – ECUADOR  
2019**

## **Certificación**

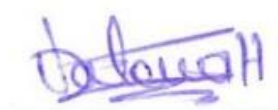
Ing. Valeria del Rosario Herrera Salazar.

**DIRECTORA DE TESIS**

Certifica:

Que la egresada **Johanna Elizabeth Rivera Serrano** autora de la tesis de grado, cuyo tema versa "**PLAN DE GESTIÓN DE RIESGOS DE TI EN EL HOSPITAL DE CATACocha**", ha sido dirigido, orientado y discutido bajo mi asesoramiento y reúne a satisfacción los requisitos exigidos en una investigación de este nivel por lo cual autorizo su presentación y sustentación.

Loja, 19 de noviembre de 2019



.....  
Ing. Valeria del Rosario Herrera Salazar MSc.

**DIRECTORA DE TESIS**

## **Autoría**

Yo, **JOHANNA ELIZABETH RIVERA SERRANO**, declaro ser autora de la presente tesis de grado y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja la publicación de la Tesis en el Repositorio Institucional-Biblioteca Virtual.



**Firma:** .....

**Cédula:** 1104935018

**Fecha:** 19 de noviembre 2019

# **Carta de Autorización de Tesis de Grado por parte de la Autora, para la consulta, reproducción parcial o total y publicación electrónica del texto completo.**

Yo, **JOHANNA ELIZABETH RIVERA SERRANO**, declaró ser autora de la Tesis de Grado titulada: **“PLAN DE GESTIÓN DE RIESGOS DE TI EN EL HOSPITAL DE CATACOCHA”**; como requisito para optar al grado de: **INGENIERA EN SISTEMAS**; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional (RDI):

Los usuarios pueden consultar el contenido de esta Tesis de Grado en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la Tesis de Grado que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los once días del mes de diciembre del dos mil diecinueve.



**Firma:** .....

**Autor:** Johanna Elizabeth Rivera Serrano

**Cédula:** 1104935018

**Dirección:** Loja, (Argelia; Calles: Einstein y Humboldt )

**Correo Electrónico:** johanna.rivera@unl.edu.ec

**Celular:** 0999641608

## **DATOS COMPLEMENTARIOS**

**Directora de Tesis:** Ing. Valeria del Rosario Herrera Salazar MSc.

**Tribunal de Grado:** Ing. Hernán Leonardo Torres Carrión, Mg. Sc.

Ing. María del Cisne Ruilova, Mg. Sc.

Ing. Francisco Javier Álvarez Pineda, Mg. Sc.

## **Dedicatoria**

Esta tesis de grado es algo muy importante para el inicio de mi vida profesional, por tal razón le dedico a mis Padres quienes me apoyaron con bienes y persona para poder sobrellevar todos los obstáculos y siempre seguir adelante, ellos me enseñaron a nunca rendirme y que siempre debo luchar por ser mejor persona y profesional día a día que con esfuerzo y sacrificio se logra todo y que no hay cosas imposibles.

A mis tres hermanos Richard, José y Jorge quienes forman parte de mi vida y me impulsan para que logre grandes cosas, a no desfallecer nunca y que crea en mí mismo para que así alcance mis objetivos.

**La autora.**

## **Agradecimiento**

Expreso mi agradecimiento al Hospital de Catacocha quien, en conjunto con la Universidad Nacional de Loja, Facultad de la Energía, las Industrias y los Recursos Naturales no Renovables de la Carrera de Ingeniería en Sistemas me apoyaron en el desarrollo de esta Tesis de grado.

Agradezco a Dios por guiar mis pasos y por darme fuerzas para salir adelante durante mi etapa estudiantil.

A mis queridos padres Gloria y Simón por todo el esfuerzo que hicieron para darme una profesión para que sea alguien en la vida.

A mis apreciados maestros que supieron guiarme día a día para poder culminar con éxito mi etapa profesional.

A mis amigos Cristian, Carlos, José, Betty quienes supieron apoyarme en todo momento cuando más lo necesitaba siempre podía contar con ellos.

Agradezco a la Ing. Valeria Herrera directora de mi Tesis de grado quien con sus conocimientos y apoyo supo guiarme para culminar con éxito.

“Gracias a todos por apoyarme para cumplir mi etapa profesional porque sin ustedes no hubiera podido lograrlo, les agradezco inmensamente por impulsarme para alcanzar mi meta”.

**La autora.**

# Índice de Contenidos

## Índice General

<b>CERTIFICACIÓN.....</b>	<b>II</b>
<b>AUTORÍA.....</b>	<b>III</b>
<b>CARTA DE AUTORIZACIÓN .....</b>	<b>IV</b>
<b>DEDICATORIA.....</b>	<b>V</b>
<b>AGRADECIMIENTO .....</b>	<b>VI</b>
<b>ÍNDICE DE CONTENIDOS.....</b>	<b>VII</b>
<b>ÍNDICE GENERAL .....</b>	<b>VII</b>
<b>ÍNDICE DE FIGURAS.....</b>	<b>X</b>
<b>ÍNDICE DE TABLAS .....</b>	<b>XI</b>
<b>1. TÍTULO .....</b>	<b>1</b>
<b>2. RESUMEN .....</b>	<b>2</b>
<b>2.1. ABSTRACT .....</b>	<b>3</b>
<b>3. INTRODUCCIÓN.....</b>	<b>4</b>
<b>4. REVISIÓN DE LITERATURA .....</b>	<b>6</b>
4.1. Definiciones relevantes para la gestión de riesgos.....	6
4.1.1. Auditoría Informática.....	6
4.1.2. Información.....	6
4.1.3. Tecnologías de Información.....	6
4.1.4. Seguridad de tecnologías de la información .....	6
4.1.5. Activo.....	7
4.1.6. Amenaza.....	7
4.1.7. Vulnerabilidad .....	7
4.1.8. Impacto.....	7
4.1.9. Análisis del Riesgo .....	7
4.1.10. Gestión de Riesgos.....	9
4.1.11. Riesgo Inherente .....	11
4.1.12. Riesgo Residual.....	11
4.2. Metodologías para la Gestión de Riesgos.....	11
4.2.1. MAGERIT.....	11
4.2.2. OCTAVE .....	12

4.2.3.	MEHARI .....	13
4.2.4.	CORAS.....	14
4.2.5.	NIST.....	14
4.2.6.	CRAMM.....	15
4.2.7.	IRAM-Information Risk Analysis Methodologies.....	16
4.3.	Hospital de Catacocha.....	16
4.3.2.	Datacenter .....	18
<b>5.</b>	<b>MATERIALES Y MÉTODOS.....</b>	<b>20</b>
5.1.	Métodos .....	20
5.2.	Técnicas.....	20
5.2.1.	Encuestas .....	20
5.2.2.	Entrevista.....	21
5.2.3.	Técnica de la investigación Bibliográfica .....	21
5.2.4.	Técnica de la Observación.....	21
5.3.	Metodología de desarrollo.....	21
5.3.1.	MAGERIT .....	21
<b>6.</b>	<b>RESULTADOS .....</b>	<b>23</b>
6.1.	FASE 1: Determinar los riesgos en las TI del Hospital de Catacocha.....	23
6.1.1.	Análisis de los riesgos y controles. ....	23
6.1.2.	Diagnóstico situacional – FODA. ....	26
6.1.3.	Lista de riesgos Encontrados.....	29
6.1.4.	Análisis de la Matriz de Riesgo Inherente .....	31
6.1.5.	Identificación del impacto y la probabilidad del escenario para el riesgo residual.....	32
6.1.6.	Identificación de riesgos no aceptables .....	33
6.1.7.	COMPARATIVA DEL ANÁLISIS INHERENTE VS. EL ANÁLISIS RESIDUAL 35	
6.2.	FASE 2: Analizar las Metodologías de Gestión de Riesgos. ....	36
6.2.1.	Búsqueda de metodologías.....	36
6.2.2.	Comparativa de las metodologías de gestión de riesgos .....	36
6.2.3.	Selección de metodologías de gestión de riesgos.....	39
6.3.	FASE 3: Elaborar el plan de gestión de riesgos de acuerdo a la metodología seleccionada.....	42
6.4.	FASE 4: Comunicar los resultados a la comunidad científica.....	51
6.4.1.	Envío del artículo .....	51
6.4.2.	Exposición del artículo en la PUCESE .....	51



6.4.3. Publicación del Artículo .....	51
<b>7. DISCUSIÓN .....</b>	<b>52</b>
7.1. Desarrollo de la Tesis de Grado .....	52
7.2. Valoración técnica económica ambiental .....	53
7.2.1. Talento Humano .....	53
7.2.2. Bienes.....	54
7.2.3. Servicios.....	54
7.2.4. Imprevistos .....	55
<b>8. CONCLUSIONES .....</b>	<b>56</b>
<b>9. RECOMENDACIONES .....</b>	<b>57</b>
<b>10. BIBLIOGRAFÍA.....</b>	<b>58</b>
<b>11. ANEXOS .....</b>	<b>60</b>
ANEXO 1: Orgánico Estructural del Hospital de Catacocha .....	60
ANEXO 2. Resumen de la Entrevista.....	62
ANEXO 3. Interpretación de Encuestas.....	65
ANEXO 4. Encuestas.....	87
ANEXO 5. Certificado de Participación en COISINT 2019.....	93
ANEXO 6. Matriz Inherente y Matriz Residual.....	95
ANEXO 7. Artículo Científico.....	107
ANEXO 8. Solicitud de Entrega y Socialización del Plan de Gestión de Riesgos .....	109
ANEXO 9. Licencia Creative Commons .....	111

## Índice de Figuras

Figura 1. Ciclo PDCA (Planificar, Hacer, Revisar y Actuar) [18].	8
Figura 2. Proceso para la Administración del Riesgo [13].	9
Figura 3. Balance de la metodología OCTAVE [11].	12
Figura 4. Hospital de Catacocha (Imagen propia).	16
Figura 5. Departamento de TIC's (Imagen Propia)	17
Figura 6. Datacenter (Imagen Propia).	18
Figura 7. Oficinas del Datacenter y el Departamento de TIC's (Imagen Propia).	23
Figura 8. Puerta de Ingreso al Datacenter (Imagen Propia).	24
Figura 9. Registro Manual de ingreso al Datacenter (Imagen Propia).	24
Figura 10. Equipos del Datacenter (Imagen Propia).	25
Figura 11. Lugar de Trabajo del Departamento Atención al Cliente (Imagen Propia).	25
Figura 12. Oficina del Departamento de TIC's (Imagen Propia).	26
Figura 13. Mapa de calor de la matriz de riesgo inherente. Elaborado de acuerdo con la aplicación proporcionada por Deloitte Consulting Ecuador.	31
Figura 14. Mapa de calor de la matriz de riesgo residual. Elaborado de acuerdo con la aplicación proporcionada por Deloitte Consulting Ecuador.	33
Figura 15. Ponencia del artículo.	51

## Índice de Tablas

TABLA I. MATRIZ FODA .....	28
TABLA II. LISTA DE RIESGOS EXISTENTES EN LA INSTITUCIÓN.....	30
TABLA III. VALORACIÓN DEL RIESGO EN CUANTO A IMPACTO. ....	31
TABLA IV. VALORACIÓN DEL RIESGO EN CUANTO A LA VULNERABILIDAD. ....	32
TABLA V. TABLA DE RIESGOS NO ACEPTABLES. ....	34
TABLA VI. COMPARATIVA DE ANÁLISIS DE RIESGO INHERENTE VS ANÁLISIS DE RIESGO RESIDUAL.....	35
TABLA VII. COMPARATIVA DE METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS. ....	37
TABLA VIII. RESULTADO DE COMPARATIVA DE METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS (ELABORACIÓN PROPIA). ....	40
TABLA IX. ACTIVOS DEL DEPARTAMENTO DE TIC'S-HOSPITAL DE CATACOCHA. ....	43
TABLA X. VALORACIÓN DE ACTIVOS. ....	43
TABLA XI. VALORACIÓN DE ACTIVOS DE ACUERDO AL IMPACTO.....	44
TABLA XII. PLAN DE GESTIÓN DE RIESGOS .....	45
TABLA XIII. TALENTO HUMANO PARA LA TESIS DE GRADO. ....	53
TABLA XIV. RECURSOS HARDWARE Y SOFTWARE.....	54
TABLA XV. PRESTACIÓN DE SERVICIOS A ADQUIRIR. ....	55
TABLA XVI. PRESUPUESTO TOTAL DEL TESIS DE GRADO.....	55
TABLA XVII. MATRIZ INHERENTE DEL DEPARTAMENTO DE TIC'S .....	96
TABLA XVIII. MATRIZ RESIDUAL DEL DEPARTAMENTO DE TIC'S .....	100

## **1. Título**

“Plan de Gestión de Riesgos de TI en el  
Hospital de Catacocha ”

## **2. Resumen**

Actualmente las organizaciones tanto públicas como privadas, al igual que las personas dependen de las tecnologías de la información como una herramienta esencial para poder desarrollar actividades y todas las operaciones administrativas u operativas de la institución. La presente Tesis de Grado(TT) plantea un plan de gestión de riesgos de TI en el Hospital de Catacocha para el Departamento de TIC's que permita identificar las vulnerabilidades que pueden atentar contra la seguridad de la información, ya que al ser una institución ligada al estado maneja grandes cantidades de información sensible y confidencial, tomando en cuenta que únicamente se realizan respaldos de información en discos externos y en lo referente a seguridad de la información no se ha tomado ninguna precaución, ya que dependen de una entidad externa que les brinda el presupuesto anual, el cual es limitado.

El proceso para el desarrollo de esta tesis de grado se lo dividió en secciones:

En la primera sección se procedió a utilizar técnicas de investigación tales como: la recolección de información para identificar los riesgos de la situación actual de la institución y la inspección física al departamento para hacer una identificación visual de los riesgos. En la segunda sección se realizó una búsqueda bibliográfica de las metodologías para la gestión de riesgos con el fin de elaborar una comparativa de estas y finalmente seleccionar la metodología MAGERIT con la que se trabajó en este TT. En la tercera sección se aplicó la metodología MAGERIT con las plantillas de la empresa Deloitte para elaborar la matriz de riesgo inherente y matriz de riesgo residual con el fin de identificar que tan expuesta al riesgo se encuentra la institución ante una eventualidad y así elaborar una comparativa que arroje el resultado de los riesgos que se pueden evaluar, aceptar, mitigar y transferir. En la cuarta sección se realizó la publicación del artículo en la revista RISTI (base de datos SCOPUS) de las II JORNADAS DE INVESTIGACIÓN CIENCIA TECNOLOGÍA Y SOCIEDAD de la Universidad PUCESE de Esmeraldas y la ponencia en la PUCESE de Ibarra.

En conclusión, el TT dejará un Plan de Gestión de Riesgos de TI al Departamento de TIC's del Hospital de Catacocha para mejorar la seguridad de la información e incentivar al personal sobre las buenas prácticas referentes a la confidencialidad, integridad y disponibilidad de la información.

## **2.1. Abstract**

Currently both public and private organizations, as well as individuals depend on information technology as an essential tool to develop activities and all administrative or operational operations of the institution. The present Degree Thesis (TT) proposes an TI risk management plan for the Catacocha Hospital for the Department of TIC's that allows the identification of vulnerabilities that may threaten the security of information, since being an institution linked to the state handles large amounts of sensitive and confidential information, taking into account that only backups of information are made on external disks and with regard to information security no precaution has been taken, since they depend on an external entity that provides them with the annual budget, which is limited.

The process for the development of this degree thesis was divided into sections:

In the first section, investigative techniques were used, such as the collection of information to identify the risks of the current situation of the institution and the physical inspection of the department to make a visual identification of the risks. In the second section, a bibliographic search of risk management methodologies was carried out in order to elaborate a comparison of these and finally select the MAGERIT methodology with which work was carried out in this TT. In the third section, the MAGERIT methodology was applied with the templates of the company Deloitte to develop the inherent risk matrix and residual risk matrix in order to identify how exposed to risk the institution is to an eventuality and thus develop a comparison that yields the result of the risks that can be evaluated, accepted, mitigated and transferred. In the fourth section, the article was published in the RISTI magazine (SCOPUS database) of the II SCIENTIFIC RESEARCH DAYS TECHNOLOGY AND SOCIETY of the University PUCESE of Esmeraldas and the paper in the PUCESE of Ibarra.

In conclusion, the TT will leave an TI Risk Management Plan to the TIC's Department of the Catacocha Hospital to improve information security and encourage staff on good practices regarding confidentiality, integrity and availability of information.

### **3. Introducción**

Actualmente el uso de Tecnologías de la Información y Comunicación (TIC's) en las instituciones públicas o privadas del Ecuador, están sujetas a varios tipos de amenazas, tales como: virus informáticos, robo de información, alteración de información, divulgación de información, espionaje, desastres naturales, etc. La seguridad de la información es parte importante dentro de una institución, ya que permite proteger y resguardar la información, para cumplir con los pilares fundamentales, que son: confidencialidad, integridad y disponibilidad.

El Hospital de Catacocha administra grandes cantidades de información, por lo que a medida que va creciendo es necesario que regulen buenas prácticas en cada uno de los procesos que se llevan a cabo, por lo tanto se planteó la siguiente hipótesis:” La falta de un adecuado Plan de Gestión de Riesgos de TI en el Hospital de Catacocha, genera vulnerabilidades en los activos del Departamento de TIC's”, con el fin de realizar el análisis de riesgos y recomendar controles que al ser implementados en la Institución mitiguen aquellos riesgos que están presentes, logrando así el aseguramiento de la información, ya que únicamente se realizan respaldos de información en discos externos y en cuanto a seguridades de información no se ha tomado ninguna medida preventiva.

Toda Institución está expuesta a cualquier tipo de riesgo, por ello se debe contar con herramientas que mitiguen el impacto y la probabilidad de ocurrencia que tienen los activos ante una amenaza.

El objetivo general de esta Tesis de grado es Desarrollar un Plan de gestión de riesgos de TI en el Hospital de Catacocha y los objetivos específicos son: Determinar los riesgos en las TI del Hospital de Catacocha, Analizar las metodologías de Gestión de Riesgos, Elaborar el plan de gestión de riesgos de acuerdo a la metodología seleccionada y Comunicar los resultados a la comunidad científica, los cuales permitieron cumplir con todas las actividades que se llevaron a cabo en el desarrollo de esta Tesis de grado.

La distribución de la presente Tesis de grado consta de la Revisión de la Literatura donde se encuentran conceptos fundamentales que permiten entender y abordar el desarrollo del TT, cuyo contenido está dividido en 3 secciones en los que se trata: Definiciones generales sobre la gestión de riesgos, metodologías para la gestión de riesgos y Descripción del Hospital de Catacocha donde se realizó la Tesis de grado.

En la sección de Materiales y Métodos se detalla los métodos/técnicas utilizados para este TT y la metodología de desarrollo en este caso MAGERIT. A continuación, en la sección de Resultados se desarrolló la Tesis de grado basada en la metodología MAGERIT. En la sección de Discusión se hace la valoración de los objetivos determinando su cumplimiento y argumentando las actividades realizadas para conseguirlos. Finalmente, en la sección de Conclusiones y Recomendaciones se describe las partes más relevantes durante el desarrollo de cada uno de los objetivos, así como también aspectos a considerar para el desarrollo de futuros Trabajos.



## **4. Revisión de Literatura**

Esta fase se clasifica en tres capítulos como son: Definiciones relevantes para la gestión de riesgos donde se encuentran conceptos que se deben tener en cuenta a la hora de realizar una gestión de riesgos; Metodologías para la gestión de Riesgos; y Descripción del Hospital de Catacocha.

### **4.1. Definiciones relevantes para la gestión de riesgos**

#### **4.1.1. Auditoría Informática**

Como expresa Martínez, Y. A., Alfonso, B. B., & Marichal, L. L. en [23] que es como el examen objetivo, crítico, sistemático y selectivo de las políticas, normas, prácticas, procedimientos y procesos para dictaminar respecto a la economía, eficiencia y eficacia de la utilización de las tecnologías de la información; la integridad, confiabilidad, oportunidad y validez de la información y la efectividad de los controles en las áreas, las aplicaciones, los sistemas de redes u otros vinculados al desarrollo de la información.

#### **4.1.2. Información**

La información es hoy en día uno de los activos más importantes de las organizaciones, y debe protegerse, es decir es un fenómeno que proporciona significado o sentido a las cosas. La información es un activo puede existir en muchas formas; puede ser de forma escrita, impresa, electrónica, transmitida por correo o usando medios electrónicos o hablado en una conversación, como afirma Sánchez en [21].

#### **4.1.3. Tecnologías de Información**

Describe C. O.-U. Val., U. T. Educ et al. en [20] que “En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e interconectadas, lo que permite conseguir nuevas realidades comunicativas”.

#### **4.1.4. Seguridad de tecnologías de la información**

Es el área de la informática que se enfoca en la protección de la infraestructura computacional especialmente, la información contenida o circulante. La seguridad de la información es evaluada por tres pilares fundamentales: Disponibilidad, Integridad y Confidencialidad, de acuerdo con A. Duros Blandos en [1].

- **Confidencialidad:** Es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

- **Integridad:** Para la Seguridad de la Información, es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.
- **Disponibilidad:** Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones, empleando las palabras de E. G. Sánchez en [22].

#### **4.1.5. Activo**

Cualquier cosa que tenga valor en la organización, sus operaciones comerciales y su continuidad, incluido los recursos de información que apoyan la misión de la organización, manifiesta María F. Molina en [2].

#### **4.1.6. Amenaza**

Vulnerabilidad de un activo que puede ser explotado por una o más causas potenciales de un incidente, que puede resultar en daño al sistema u organización, en la opinión de M. Amutio et al. en [3].

#### **4.1.7. Vulnerabilidad**

Debilidad de cualquier tipo que compromete la seguridad del sistema informático, como dice L. Ruiz et al. [5].

#### **4.1.8. Impacto**

Indicador de qué puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando se materializa sobre un activo. El impacto se estima, conociendo el valor de los activos y la degradación causada por las amenazas, según M. Amutio et al. en [3].

$$\text{Impacto} = \text{Valor} * \text{Degradación}$$

#### **4.1.9. Análisis del Riesgo**

Es conocido como el proceso sistemático para estimar la magnitud de los riesgos a lo que está expuesta una organización. Permite determinar ¿cómo es?, ¿cuánto vale? y ¿cómo de protegido? se encuentra un sistema, siguiendo los objetivos, estrategias y políticas de la organización para elaborar un plan de seguridad. Al implantar y operar este plan debe satisfacer los objetivos propuestos con el nivel de riesgo aceptado por la Dirección de la organización. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos, define M. Amutio et al. en [3].

El análisis de riesgo se realiza ya sea cuantitativa o cualitativamente.

El análisis cualitativo es recomendable hacerlo en primer lugar, utiliza una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales ya sea bajo, medio o alto; y la probabilidad de que se produzcan estas consecuencias. Un análisis cualitativo permite:

- Identificar los activos más significativos.
- Identificar el valor relativo de los activos.
- Identificar las amenazas más relevantes.
- Identificar las salvaguardas presentes en el sistema.
- Establecer claramente los activos críticos, aquellos sujetos a un riesgo máximo.

El análisis cuantitativo es más detallado y utiliza una escala con valores numéricos para las consecuencias y probabilidad, permitiendo:

- Detallar las consecuencias económicas de la materialización de una amenaza en un activo.
- Estimar la tasa anual de ocurrencia de amenazas.
- Detallar el coste de despliegue y mantenimiento de las salvaguardas.
- Permitir ser más precisos en la planificación de gastos de cara a un plan de mejora de seguridad, como plantea R. Johnson en [6].

Los sistemas de gestión de la seguridad de la información formalizan cuatro etapas cíclicas donde el análisis de riesgos es parte de las actividades de planificación, se toman decisiones de tratamiento, estas decisiones se materializan en la etapa de implantación, en el cual se despliegan elementos que permiten la monitorización de las medidas tomadas para poder evaluar la efectividad de las mismas y actuar dependiendo a éstas, dentro de un círculo de excelencia o mejora continua (ver Figura 1, pág. 8), indica R. Johnson en [6].

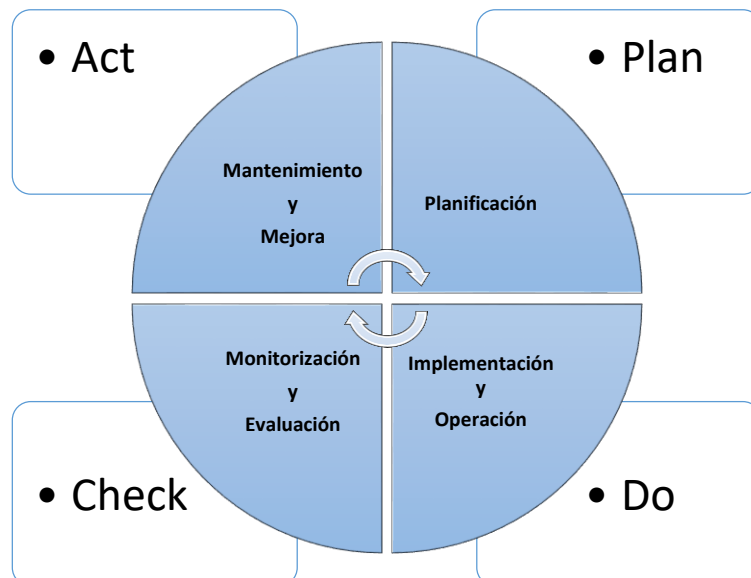


Figura 1. Ciclo PDCA (Planificar, Hacer, Revisar y Actuar) [18].

#### 4.1.10. Gestión de Riesgos

El riesgo se originó en el siglo 17 con las matemáticas asociadas con los juegos de azar, actualmente se refiere a la combinación de la probabilidad y la magnitud de pérdidas y ganancias potenciales. Durante el siglo 18, el riesgo, fue visto como un concepto neutral, considerando las pérdidas y ganancias y fue empleado en la marina. En el siglo 19, el riesgo surgió en el estudio de la economía. En el siglo 20 se hizo una connotación negativa al referirse a los peligros en la ciencia y tecnología, expresa C. Klüppelberg et al. [17].

La definición estandarizada de **riesgo** proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”, sugiere M. F. Molina en [18].

La gestión del riesgo consiste en cinco procesos: establecimiento del contexto, evaluación del riesgo, tratamiento del riesgo, comunicación/consulta de riesgos, y monitorización/revisión del riesgo (ver Figura 2).



Figura 2. Proceso para la Administración del Riesgo [13].

- **Establecimiento del Contexto:** El proceso de establecimiento de contexto recibe como entrada toda la información relevante acerca de la organización, determinando el alcance y los límites del proceso. La salida del proceso es la especificación de estos parámetros.
- **Evaluación del Riesgo:** Este proceso consta de tres subprocesos: identificación de riesgos, análisis de riesgo y evaluación de riesgos. El proceso recibe como entrada la salida del proceso de establecimiento de contexto. Identifica de forma

cuantitativa o cualitativa los riesgos y les da prioridad a los criterios de evaluación que dependen de los objetivos de la organización.

Al identificar los riesgos se busca determinar lo que podría causar una pérdida potencial y comprender cómo, dónde y por qué puede ocurrir dicha pérdida; identificando los activos, amenazas, medidas de seguridad, vulnerabilidades y sus consecuencias.

Por último, el proceso de evaluación de riesgos recibe como entrada la salida del proceso de análisis de riesgos. Se comparan los niveles de riesgo con los criterios de evaluación de riesgos y los criterios de aceptación del riesgo. El resultado del proceso es una lista de los riesgos priorizados de acuerdo a los criterios de evaluación de riesgo.

- **Tratamiento del Riesgo:** Tiene como objetivo seleccionar las medidas de seguridad para reducir o evitar los riesgos y definir un plan de tratamiento de riesgo. El proceso recibe como entrada la salida del proceso de evaluación de riesgos y produce como salida el plan de tratamiento de riesgos.

Después de que se han tomado las decisiones del tratamiento de riesgos, siempre habrá riesgo restante, llamados riesgos residuales. Estos riesgos pueden ser difíciles de evaluar, pero por lo menos se debe hacer una estimación para asegurar la suficiente protección. Si el riesgo residual es inaceptable, el proceso del tratamiento del riesgo se debe repetir. En el tratamiento del riesgo debe identificarse los factores limitantes y dependientes, prioridades, plazos, recursos, incluyendo las aprobaciones necesarias para su asignación.

- **Consulta y Comunicación del Riesgo:** Es un proceso horizontal que interactúa de forma bidireccional con todos los demás procesos de gestión de riesgos. Su propósito es establecer un entendimiento común de todos los aspectos de riesgo entre todas las partes interesadas de la organización.
- **Monitoreo y Revisión del Riesgo:** La gestión de riesgos es un proceso continuo, donde las medidas de seguridad implementadas son monitoreadas y revisadas para asegurar que funcionan correctamente de forma efectiva. El mantenimiento de las medidas de seguridad debe ser planeado y realizado sobre una base programada regularmente. Por último, se deben realizar auditorías internas de forma regular por parte de un tercero y tener una documentación completa, accesible y con procesos controlados, propone J. Vacca en [19].

#### **4.1.11. Riesgo Inherente**

Es el riesgo existente ante la ausencia de alguna acción que la dirección pueda tomar para alterar tanto la probabilidad o el impacto del mismo [14].

#### **4.1.12. Riesgo Residual**

Es el riesgo que persiste luego de la respuesta de la Dirección al Riesgo [14].

### **4.2. Metodologías para la Gestión de Riesgos**

#### **4.2.1. MAGERIT**

MAGERIT, cuyo acrónimo es “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas”, es una metodología que se orienta hacia la investigación y análisis de los riesgos que se presentan dentro de los sistemas de información, además de proporcionar medidas apropiadas, las mismas que servirán para controlar y minimizar estos riesgos, afirma M. G. Piedra et al. en [11]. Metodología española para la gestión y análisis de riesgos de los sistemas de la información que en sus tres libros “Método”, “Catálogo de elementos” y “Guía de técnicas” sirve como fuente de revisión de definiciones y lo correspondiente a la estimación de riesgos, señala A. Castro et al. en [10].

MAGERIT, tiene la posibilidad de realizar lo siguiente:

- Análisis de Riesgos.
- Gestión de Riesgos.

Los principales elementos que utiliza MAGERIT son:

- Escalas de valores cualitativos, cuantitativos y de indisponibilidad del servicio.
- Modelo de frecuencia de una amenaza como una tasa anual de ocurrencia.
- Escala alternativa de estimación del riesgo.
- Catálogos de amenazas.
- Catálogos de medidas de control.

Fases de MAGERIT

- **Fase 1.** Identificación de procesos y de sus escenarios aplicables.
- **Fase 2.** Identificación de controles claves.
- **Fase 3.** Calificación de controles.
- **Fase 4.** Identificación del impacto y la probabilidad del escenario para el riesgo residual.
- **Fase 5.** Identificación de riesgos no aceptables, revela A. Syalim et al. en [7].

#### 4.2.2. OCTAVE

Es una metodología de análisis y gestión de riesgos, donde el objetivo principal es garantizar los sistemas informáticos dentro de una organización. Cuando se aplica esta metodología, varias personas pertenecientes a los sectores operativos, de negocios y de los Departamentos de tecnología de la información (TI) trabajan juntos, enfocándose en las necesidades de seguridad y equilibrando los tres aspectos mostrados en la Figura 3: RIESGOS OPERATIVOS, PRÁCTICAS DE SEGURIDAD Y TECNOLOGÍA.

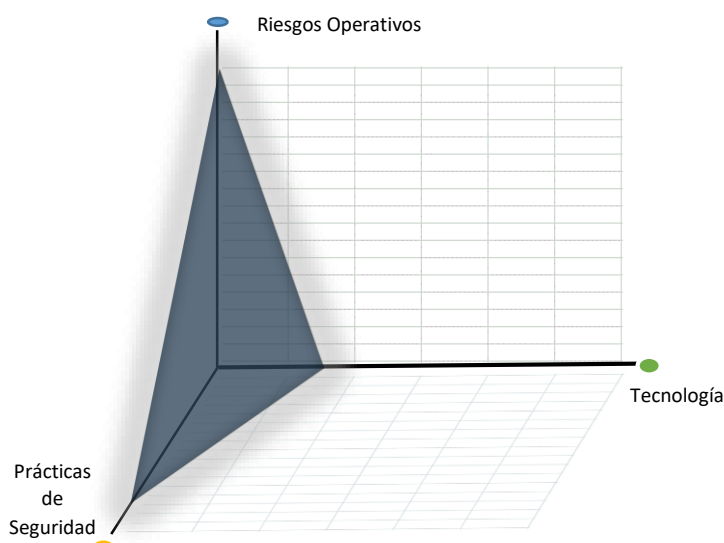


Figura 3. Balance de la metodología OCTAVE [11].

Octave realiza lo siguiente:

- Construcción de los Perfiles de Amenazas Basados en Activos.
- Identificación de la Infraestructura de Vulnerabilidades.
- Desarrollo de Planes y Estrategias de Seguridad.

Las actividades más relevantes de OCTAVE se muestran a continuación.

- Realiza medidas de probabilidad dentro de un rango de frecuencias.
- Realiza el análisis del límite entre niveles de probabilidad, tal como R. G. Montalvo Armijos en [8].

Fases de OCTAVE, en la opinión de [4]:

- **Fase 1. Construir perfiles de amenazas con base en los recursos:** se identifican los activos de información importantes, las amenazas a los activos, los requisitos de seguridad de los activos, lo que la organización está haciendo para protegerlos y las debilidades en las políticas y prácticas organizacionales.

- **Fase 2. Identificar las vulnerabilidades de la infraestructura:** los componentes operativos clave de las tecnologías de información se examinan en busca vulnerabilidades tecnológicas que puedan conducir a una acción no autorizada.
- **Fase 3. Desarrollar la estrategia y los planes de seguridad:** la información generada en las fases 1 y 2 se analiza para identificar riesgos para la empresa y evaluar los riesgos en función de su impacto en la misión de la organización. Además, se desarrolla una estrategia de protección para los planes de la organización y de mitigación que aborde los riesgos de más alta prioridad.

#### 4.2.3. MEHARI

Método Armonizado de Análisis de Riesgos, esta metodología originalmente desarrollada por la comisión Métodos de Clusif, en 1996 es una metodología utilizada para apoyar a los responsables de la seguridad informática de una empresa mediante un análisis riguroso de los principales factores de riesgos evaluando cuantitativamente de acuerdo a la situación de la organización donde se requiere el análisis, acopla los objetivos estratégicos existentes con los nuevos métodos de funcionamiento de la empresa, esto se lo realiza mediante una política de seguridad y mantenimiento de los riesgos a un nivel convenido, con base en M. G. Piedra en [11].

La metodología MEHARI comprende:

- Diagnóstico de Seguridad.
- Análisis de los Intereses Implicados por la Seguridad.
- Análisis de Riesgos.

Del estudio de esta metodología extraemos sus principales elementos:

1. Niveles de categorías de controles.
2. Niveles de calidad de los servicios de seguridad.
3. Evaluación de la calidad del servicio por medio de cuestionarios.
4. Tabla modelo de impactos.

Fases, como lo hace notar [11]:

- **Fase 1.** Preparatoria: Evaluar el contexto, establecer parámetros de riesgos principales, determinar el alcance y sus limitaciones.
- **Fase 2.** Valoración del riesgo: Clasificar activos y análisis de cuestionario, Evaluar el riesgo, la calidad de servicio de seguridad.



- **Fase 3.** Planificación del tratamiento del riesgo: Medir la planificación inmediata, planificar medidas en contextos específicos, vigilar la implantación del tratamiento del riesgo.

#### 4.2.4. CORAS

CORAS es una metodología basada en el modelo para análisis de riesgos. La meta de CORAS es desarrollar una mejor metodología para el análisis de riesgos de seguridad de sistemas de IT críticos de una manera más precisa y efectiva. Esto prevendrá que las compañías, utilicen grandes sumas en problemas de seguridad, y al utilizar esta metodología en un período más temprano, se verá qué tipos de riesgos existen, y cómo tratarlos.

La metodología CORAS puede ser dividida en las siguientes fases:

- **Fase 1.** Identificar el contexto: Caracterizar el objetivo con los análisis, cuál es el enfoque y el alcance del análisis. ¿Qué pérdidas puede tolerar el cliente, ya que siempre estará involucrado un riesgo?.
- **Fase 2.** Identificar los riesgos: Identificar las amenazas a los activos como por ejemplo lluvia de ideas, y también identificar sus vulnerabilidades.
- **Fase 3.** Estimar el nivel del riesgo, evaluar los riesgos: No todos los riesgos pueden ser eliminados, y tenemos que decidir cuál es el riesgo que necesita tratamiento. Tenemos que conocer acerca de los niveles del riesgo.
- **Fase 4.** Tratar los riesgos: identificar el tratamiento de los riesgos indeseados. Evaluar y priorizar diferentes tratamientos, como señala S. Yaqub and M. G. Piedra et al. en [9,11].

#### 4.2.5. NIST

NIST SP 800-30: Guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos. La guía provee apoyo en los procesos de valoración y mitigación dentro de la gestión de riesgos, desde la posición de A. Castro et al. [10].

La metodología NIST posee las siguientes fases, destaca H. Novoa et al. [16]:

- **Fase 1.** Caracterización del sistema: Permite establecer el alcance y los límites operacionales de la evaluación de riesgos en la empresa.
- **Fase 2.** Identificación de amenaza: Donde se definen las fuentes de motivación de las mismas.
- **Fase 3.** Identificación de vulnerabilidades: Desarrolla una lista de defectos o debilidades del sistema que podrían ser explotadas por una amenaza.
- **Fase 4.** Control de análisis: Lista de controles actuales.

- **Fase 5.** Determinación del riesgo: Ayuda a evaluar el rango de probabilidad de que una vulnerabilidad se convierta en amenaza.
- **Fase 6.** Análisis de impacto: Analizarán el impacto que pueden repercutir los riesgos.
- **Fase 7.** Determinación del riesgo: Ayuda a evaluar el riesgo en el sistema de información.
- **Fase 8.** Recomendaciones de control: Donde se proporcionan los controles que podrían mitigar el riesgo identificado disminuyéndolo hasta un nivel aceptable.
- **Fase 9.** Documentación de resultados: Genera un informe con la descripción de amenazas y vulnerabilidades, midiendo el riesgo y generando recomendaciones para la implementación de controles.

#### **4.2.6. CRAMM**

Esta metodología de análisis de riesgo fue desarrollada por el Centro de Informática y la Agencia Nacional de telecomunicaciones del Gobierno del Reino Unido en 1987. Está orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos. Puede ser aplicable en todo tipo de sistemas y redes de información en la etapa de estudio de factibilidad, donde el alto nivel de riesgo puede ser requerido para identificar los requisitos de seguridad general, la contingencia y los costos asociados de las distintas opciones. Durante el análisis detallado del negocio y de entornos técnicos donde los problemas de seguridad o contingencia asociados con la opción tomada pueden ser investigados o refinados. Antes de la ejecución, para garantizar que todos los requerimientos físicos, el personal, técnicas y contramedidas de seguridad se han identificado e implementado, deduce K. C. Torres en [12].

Fases de CRAMM, sostiene [15]:

- **Fase 1.** Establecimiento de objetivos de seguridad: Definir el alcance del estudio, el valor de la información entrevistando a los usuarios sobre los impactos potenciales, identificar y evaluar los activos físicos u activos de software que forman parte del sistema.
- **Fase 2.** Evaluación de Riesgos: Identificar y valorar el nivel de amenazas que pueden afectar el sistema, Valorar las vulnerabilidades de los sistemas ante las amenazas identificadas, combinar las valoraciones para calcular la medida de los riesgos.
- **Fase 3.** Identificación y selección de recomendaciones: Documento de inicio del proyecto, informes de análisis y gestión de riesgos.

#### 4.2.7. IRAM-Information Risk Analysis Methodologies

El ISF (Foro de Seguridad de la Información) es una organización sin ánimo de lucro de ámbito internacional que desarrolla de forma colaborativa recomendaciones y herramientas de seguridad para sus miembros. Entre las principales preocupaciones del ISF se encuentra el análisis y la gestión de riesgos y por ello se ha desarrollado y publicado diversas metodologías y modelos de análisis de riesgos a lo largo del tiempo. La metodología actual de análisis y gestión de riesgos del ISF es IRAM (Metodología de análisis de riesgo de la información) y está alineada con el resto de proyectos del ISF.

IRAM consta de tres fases principales, refiere J. M. Matalobos Veiga en [13]:

- **fase 1.** Análisis de impacto sobre el negocio (BIA): Soportada por la herramienta BIA Assistant.
- **fase 2.** Evaluación de amenazas y vulnerabilidades: Soportada por la herramienta T&VA Assistant.
- **fase 3.** Selección de controles: Soportada por la herramienta CS Assistant.

#### 4.3. Hospital de Catacocha

El Hospital de Catacocha es una institución pública, inaugurada el 2 de enero del 2013 por el presidente Ec. Rafael Correa, ubicado en la provincia de Loja, cantón Paltas, parroquia Catacocha, en la zona 7.

Esta institución brinda servicios de Medicina Interna, Pediatría, Gineco-obstetricia, Cirugía, Psicología Clínica, Endodoncia, emergencia, farmacia, laboratorio y RX las 24 horas del día.



Figura 4. Hospital de Catacocha (Imagen propia).

## **Misión**

Prestar servicios de salud con calidad y calidez en el ámbito de la asistencia especializada, a través de su cartera de servicios, cumpliendo con la responsabilidad de promoción, prevención, recuperación, rehabilitación de la salud integral, docencia e investigación, conforme a las políticas del Ministerio de Salud Pública y el trabajo en red, en el marco de la justicia y equidad social.

## **Visión**

Ser reconocidos por la ciudadanía como hospital accesible, que presta una atención de calidad que satisface las necesidades y expectativas de la población bajo los principios fundamentales de la salud pública, utilizando la tecnología y los recursos públicos de forma eficiente y transparente [20].

### **4.3.1. Departamento de TIC's**



Figura 5. Departamento de TIC's (Imagen Propia)

#### **4.3.1.1. Descripción**

Ubicado en el Cantón Paltas-Barrio el Progreso, calles Av. Panamericana s/n y la Avelina, perteneciente a la dirección Distrital de Salud, zona 7, Oficinas planta alta del Hospital de Catacocha.

#### **4.3.1.2. Servicios que brinda**

- Soporte de Telecomunicaciones.
- Mantenimiento preventivo y correctivo del parque informático.
- Restricción de acceso a usuarios no autorizados.

- Respaldo de información crítico y no crítico.
- Asistencia Técnica en todas las dependencias de la institución.
- Capacitación a los empleados en temas de manejo de Software libre.
- Manejo de Servidores de correo, proxy y nube virtual.

#### 4. 3.1.3. Personal que Labora en el Departamento de TIC's

Actualmente el Departamento de TIC's, consta de 1 profesional de TI y 1 Asistente Técnico quienes están encargados de realizar diferentes funciones en cuanto a tecnologías de información.

#### 4.3.1.4. Función del Departamento de TIC's

Garantizar que todos los servicios de Tecnologías de Información estén operativos para no desabastecer los servicios.

#### **4.3.2. Datacenter**



Figura 6. Datacenter (Imagen Propia).

Es un área de 12 metros cuadrados, el cual posee seguridad de acceso solo para personal autorizado.

##### 4.3.2.1. Ubicación

Se encuentra ubicado en la planta alta del Hospital de Catacocha, es totalmente hermético, cabe mencionar que no existen filtraciones.

#### 4.3.2.2. Componentes

Se compone de:

- 2 rack de 48UR.
- 1 rack para la transmisión de datos.
- 1 rack para la transmisión de voz.
- 1 circuito cerrado de televisión que cuenta con 2 NBR, 16 cámaras IP tipo DOMO y 4 cámaras PTZ con autonomía de grabación de 1 mes.
- 2 UPS de 16 KWA y 1KWA para el respaldo del parque informático del Hospital de Catacocha con autonomía de grabación de 1H30.
- 1 Central Telefónica híbrida que sirve para la telefonía IP y análoga.
- 3 Servidores los cuales sirven para (1 para Proxy, servidor de correo y la nube institucional).

#### 4.3.2.3. Funciones

- El Datacenter recibe mantenimiento 2 veces al año.
- Desde el Datacenter se controla y distribuye el audio del Hospital de Catacocha (existe un ecualizador de sonido).
- El internet del Datacenter llega a través de fibra óptica y se distribuye la comunicación en Switch de cascada, restringiendo el acceso a sitios no autorizados y el bloqueo de puerto TCP.

## 5. Materiales y Métodos

Para el desarrollo de la presente tesis de grado se utilizaron métodos y técnicas de recolección de información bibliográfica que ayuden a cumplir los objetivos planteados.

### 5.1. Métodos

#### 5.1.1. Método científico

Mediante este método se analizó y sintetizó los conceptos teóricos de la temática y a su vez la creación del estado del arte que fundamenta al proceso investigativo.

**Fases del método científico**, desde el punto de vista de [24] son:

- **Observación:** Se realizó una observación directa, visitando el Departamento de TIC's y el Datacenter para determinar cuáles son los riesgos existentes en el Departamento del Hospital de Catacocha.
- **Formulación de Hipótesis:** En esta sección se planteó la siguiente hipótesis: "La falta de un adecuado Plan de Gestión de Riesgos de TI en el Hospital de Catacocha, genera vulnerabilidades en los activos del Departamento de TIC's".
- **Experimentación:** El escenario donde se realizó este TT fue en el Departamento de TIC's del Hospital de Catacocha para disminuir el nivel de vulnerabilidad que tienen los activos ante una amenaza, donde se realizó una lista de riesgos, que permitió elaborar las matrices de análisis inherente y matriz de análisis residual representándolos en un mapa de calor donde indica el nivel de impacto y vulnerabilidad del riesgo.
- **Conclusiones:** Una vez realizadas las fases antes mencionadas se elaboró el plan de gestión de riesgos de TI para el Departamento de TIC's del Hospital de Catacocha cuyo fin es fortalecer la seguridad de la información en la Institución.

### 5.2. Técnicas

#### 5.2.1. Encuestas

Estuvo compuesta de preguntas abiertas, cerradas y mixtas las cuales se utilizaron para la recolección de información aplicándola al responsable de TIC's y a 7 encargados de los otros Departamentos (Técnico de mantenimiento, Bioquímico, Analista Talento Humano, Enfermera, Analista de Calidad, Médico fisiología e Imagen, Médico Ocupacional) (ver Anexo 4, pág. 68).

### **5.2.2. Entrevista**

Fue semiestructurada y se la aplicó al encargado del Departamento de TIC's (Ing. Juan Pablo Naranjo), para obtener información de dicha dependencia en cuanto a seguridades de la información (ver Anexo 2, pág. 63).

### **5.2.3. Técnica de la investigación Bibliográfica**

Esta técnica se utilizó en la Revisión de la Literatura para recopilar información relevante del problema a resolver y sustentar la parte teórica de la tesis de grado, mediante diferentes medios de consultas ya sean: fuentes bibliográficas confiables, libros, revistas indexadas, artículos científicos, base de datos científicas entre otras.

### **5.2.4. Técnica de la Observación**

Se usó esta técnica en las instalaciones del Hospital de Catacocha para visualizar aspectos que ayuden a recolectar información suficiente y así lograr entender la realidad del problema, con el fin de darnos una idea clara y concisa de los requerimientos que la Institución demanda en cuanto a seguridades de la información.

## **5.3. Metodología de desarrollo**

### **5.3.1. MAGERIT**

Es una de las metodologías más utilizadas que permite el análisis de gestión de riesgos de los Sistemas de Información; fue creada por el Consejo Superior de Administración Electrónica para minimizar los riesgos de la implantación y uso de las Tecnologías de la Información. Además, se realizaron las siguientes fases:

- **FASE 1: Identificación de procesos y de sus escenarios aplicables:** Se aplicó las 7 encuestas de los encargados de cada Departamento (Técnico de mantenimiento, Bioquímico, Analista Talento Humano, Enfermera, Analista de Calidad, Médico fisiología e Imagen, Médico Ocupacional) y la del responsable del Departamento de TIC's (Ing. Juan Pablo Naranjo) junto a la entrevista realizada, para identificar los riesgos que existen en la Institución y así elaborar la lista de los riesgos existentes.
- **FASE 2: Identificación de controles claves:** Luego de determinar los riesgos existentes en la Institución se elaboró las matrices de riesgos para el análisis de riesgo inherente y análisis de riesgo residual, empleando las plantillas facilitadas por la Empresa de Consultoría Deloitte, ubicada en Ecuador junto con la herramienta de Microsoft Excel, donde se establecieron controles para mitigar los riesgos.



- **FASE 3: Calificación de controles:** Se estableció un rango de valores entre (1-2: bajo; 3 medio y 4-5: alto) respectivamente en cuanto a la probabilidad e impacto.
- **FASE 4: Identificación del impacto y la probabilidad del escenario para el riesgo residual:** En esta fase se pudo determinar que el impacto y la probabilidad en cuanto al análisis del riesgo residual disminuyeron los riesgos de una criticidad alta a una criticidad baja con los controles sugeridos a la Institución, es decir estos riesgos se mitigaron para mejorar la seguridad de la información (ver Figura 14 pág. 33).
- **FASE 5: Identificación de riesgos no aceptables:** Luego del análisis de riesgo residual se pudo determinar que existen riesgos que la Institución debe estar consiente de asumirlos, como es el caso del riesgo (R2: Falta de presupuesto para adquirir licencias de antivirus) que se encuentra aún en una criticidad media ya que al ser una Institución del estado dependen de una entidad externa en cuanto al presupuesto anual, razón por la se debe insistir en la extensión del presupuesto para adquirir licencias y así fortalecer la seguridad de la información(ver Tabla V pág. 34).

## 6. Resultados

### 6.1. FASE 1: Determinar los riesgos en las TI<sup>1</sup> del Hospital de Catacocha.

#### 6.1.1. Análisis de los riesgos y controles.

En esta sección se identificarán los riesgos y controles existentes de la institución, para ello se realizaron encuestas al responsable del Departamento de TIC's y a los encargados de las otras dependencias, además se realizó una observación directa al Departamento de TIC's y Datacenter.

#### Observación realizada al Departamento de TIC's.

En la Institución se pudo constatar que existen riesgos que se deben mitigar inmediatamente. Para hacer uso de esta técnica realizamos un recorrido por el Datacenter y el Departamento de TIC's.



Figura 7. Oficinas del Datacenter y el Departamento de TIC's (Imagen Propia).

En el Departamento de TIC's no existe control para el ingreso, cualquiera puede acceder; Mientras que el Datacenter si existe el Lector de tarjetas, pero no se utiliza porque se ha descompuesto y el presupuesto para adquirir repuestos es limitado; (Ver Figura 7, Figura 8).

---

<sup>1</sup> TI: Tecnologías de Información



Figura 8. Puerta de Ingreso al Datacenter (Imagen Propia).

En cuanto al registro de acceso al Datacenter y para identificar quienes ingresan, se lo realiza de forma manual en una hoja de registro, (ver Figura 9).

FECHA	NOMBRE Y APELLIDO	DEPARTAMENTO	MOTIVO
11/01/2013	Juan Pablo Navarro	TICS	Mantenimiento de WIK
22/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
23/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
24/01/2013	Juan Pablo Navarro	TICS	Mantenimiento Air Conditioning
25/01/2013	Juan Pablo Navarro	TICS	Revisión
26/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
27/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
28/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
29/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
30/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
31/01/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
01/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
02/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
03/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
04/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
05/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
06/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
07/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
08/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
09/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
10/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
11/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056
12/02/2013	Juan Pablo Navarro	TICS	Revisión de Tower 1056

Figura 9. Registro Manual de ingreso al Datacenter (Imagen Propia).

Los equipos que se encuentran en el Datacenter deben ser explotados al máximo ya que en la actualidad únicamente se utiliza una pequeña parte, debido a que el presupuesto para contratar un especialista para que permanezca en esta dependencia es limitado y por ahora el responsable del Departamento de TIC's debe estar pendiente si existe algún inconveniente (Ver Figura 10).



Figura 10. Equipos del Datacenter (Imagen Propia).

El mantenimiento que se realiza a los equipos en cada Departamento (ver Figura 11.), está a cargo del Ing. Juan Pablo Naranjo responsable del Departamento de TIC's, el mismo que se lo lleva a cabo una vez al año y únicamente se guarda respaldos en discos duros en la fecha en que se lo ejecutó y se depositan en el Departamento de TIC's. Cabe mencionar que en caso de pérdida sólo se recupera la información que se encontraba hasta el momento del respaldo.

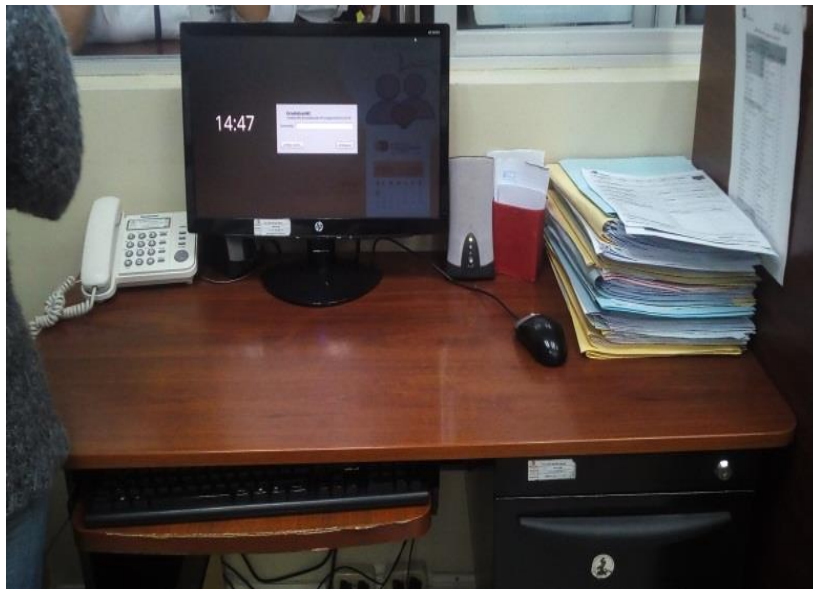


Figura 11. Lugar de Trabajo del Departamento Atención al Cliente (Imagen Propia).

El Departamento de TIC's no posee una infraestructura adecuada que le permita gestionar las seguridades de la información, por lo que se debe tener en cuenta que es una Institución que posee información altamente confidencial y que podría sufrir ataques

informáticos (virus informáticos, espionaje, etc.) que afectarían al desempeño de la Institución , es necesario que se aumente el presupuesto para este Departamento y así poder adquirir todo lo indispensable para el correcto funcionamiento, ( ver figura 12).



Figura 12. Oficina del Departamento de TIC's (Imagen Propia).

### **Encuestas realizadas**

Se puede visualizar el análisis de la interpretación de las encuestas que se realizó para identificar los riesgos existentes en la Institución, para mayor información (ver Anexo 3, pág. 66).

#### **6.1.2. Diagnóstico situacional – FODA.**

El análisis de Debilidades, Amenazas, Fortalezas y Oportunidades (FODA) se realizó sobre la situación actual del Hospital de Catacocha, en el departamento de TIC's para determinar los factores internos y externos de la institución.

#### **FORTALEZAS**

- Se mantiene operativo el Data Center y servicios de Telecomunicaciones.
- Se Lleva un control de mantenimientos realizados a cada equipo informático sean estos preventivos o correctivos.
- El personal del Departamento de TIC's posee sólidos conocimientos en soporte técnico y redes.
- Recurso Humano comprometido.
- Buen ambiente laboral.

## **DEBILIDADES**

- Deficiencia en equipamiento tecnológico para seguridad perimetral (Firewalls, UTMs).
- Ausencia de servidores Multiusos y de Archivos para respaldo y manejo de información.
- Escasez de discos duros para el CCTV (Circuito Cerrado de Televisión).
- Falta de asignación de presupuesto para adquirir equipamiento tecnológico.
- Infraestructura física deficiente en el Departamento de TIC's.

## **OPORTUNIDADES**

- Personal de TIC's dispuesto a adquirir nuevos conocimientos.
- Mejoramiento de infraestructura Tecnológica.
- Renovación de equipos informáticos.
- Manual de políticas de seguridad de la información.
- Monitorear el correcto uso de la información.

## **AMENAZAS**

- Ingreso de equipos informáticos externos a la Institución sin previa autorización.
- Colapso en el Servidor de correo Institucional, por falta de almacenamiento.
- Ataques Externos por no contar con Seguridad Perimetral.

Luego del diagnóstico situacional donde muestra con claridad cuáles son las fortalezas, oportunidades, amenazas y debilidades, que son elementos que al tenerlos claros dan una visión global de la verdadera situación, a continuación se elaboró la matriz FODA(ver Tabla I, pág. 28), que permite relacionar los factores internos y factores externos de la institución , conduciéndonos a la elaboración de estrategias que mitiguen el impacto de amenazas y reduzcan las debilidades, haciendo uso de las fortalezas y aprovechando las oportunidades.

## Matriz FODA

TABLA I. MATRIZ FODA

<p><b>FORTALEZAS-DEBILIDADES</b></p> <p><b>OPORTUNIDADES-AMENAZAS</b></p>	<p>F1: Se mantiene operativo el Data Center y servicios de Telecomunicaciones.            F2: Se Lleva un control de mantenimientos realizados a cada equipo informático sean estos preventivos o correctivos.            F3: El personal del Departamento de TIC's posee sólidos conocimientos en soporte técnico y redes.            F4: Recurso Humano comprometido.            F5: Buen Ambiente Laboral.</p>	<p>D1: Deficiencia en equipamiento tecnológico para seguridad perimetral (Firewalls, UTMs).            D2: Ausencia de servidores Multiusos y de Archivos para respaldo y manejo de información.            D3: Escasez de discos duros para el CCTV (Circuito Cerrado de Televisión).            D4: Falta de asignación de presupuesto para adquirir equipamiento tecnológico.            D5: Infraestructura física deficiente en el Departamento de TIC's.</p>
<p>O1: Personal de TIC's dispuesto a adquirir nuevos conocimientos.            O2: Mejoramiento de infraestructura Tecnológica.            O3: Renovación de equipos informáticos.            O4: Manual de políticas de seguridad de la información.            O5: Monitorear el correcto uso de la información.</p>	<p><b>ESTRATEGIAS FO</b></p> <ul style="list-style-type: none"> <li>• Capacitar al personal sobre seguridad y manejo de la información (O1, O5, F3, F4).</li> <li>• Adecuar la infraestructura de acuerdo a las necesidades (O2, F1).</li> <li>• Concientizar en la institución sobre la necesidad de establecer políticas en la seguridad de la información (O4, F5).</li> <li>• Implementar un plan de renovación de equipos informáticos (O3, F2).</li> </ul>	<p><b>ESTRATEGIAS DO</b></p> <p>Solicitar a Instituciones gubernamentales y no gubernamentales el apoyo económico para la renovación de equipos informáticos (D1, D3, D4, O3).</p> <p>Desarrollar y manejar de forma flexible una infraestructura que soporte el crecimiento de la institución (D5, O2).</p> <p>Monitorear que el responsable del Departamento de TIC's le dé la importancia a la Seguridad y manejo de información (O4, O5, D2).</p>
<p>A1: Ingreso de equipos informáticos externos a la Institución sin previa autorización.            A2: Colapso en el Servidor de correo Institucional, por falta de almacenamiento.            A3: Ataques Externos por no contar con Seguridad Perimetral.</p>	<p><b>ESTRATEGIAS FA</b></p> <p>Realizar charlas informativas sobre seguridad de la información (F3, F4, A1).            Asignación de tareas por contenidos específicos (A2, F1, F5).            Realizar pruebas de vulnerabilidades con herramientas de software libre (A3, F2).</p>	<p><b>ESTRATEGIAS DA</b></p> <p>Implementar sistemas de control de acceso en el departamento de TIC's a las personas no autorizadas (D4, D5, A1).            Adquisición de herramientas de seguridad perimetral para el uso correcto e integridad de la información (D1, A3).            Socialización de políticas de servidores (D2, D3, A2).</p>

### **6.1.3. Lista de riesgos Encontrados.**

Luego de aplicar las técnicas (ver sección 5 Materiales parte 5.2), se hizo una lista de los riesgos a los que está expuesta la Institución (ver Tabla II, pág.30) para luego de ello proceder con la elaboración de matrices de análisis inherente y análisis residual (ver Anexo 6, pág. 95).



TABLA II. LISTA DE RIESGOS EXISTENTES EN LA INSTITUCIÓN.

NRO.	RIESGOS	DESCRIPCIÓN	TÉCNICA UTILIZADA	PREGUNTA
R1	Falta de controles para el manejo de la Información.	El manejo de la información se realiza de manera física y digital.	Encuesta N°2 Entrevista	7 14
R2	Falta de presupuesto para adquirir licencias de antivirus.	Se instalan versiones FREE debido a que el presupuesto es limitado.	Encuesta N°1	2
R3	Falta de control de acceso en el ingreso de personas no autorizadas al Departamento de TIC's.	Cualquier persona puede ingresar al Departamento.	Encuesta N°1 Entrevista	10 5
R4	Falta de políticas para respaldo de Información.	Se almacena la información en discos externos y en una PC del Departamento una sola vez cuando se da mantenimiento.	Entrevista	8
R5	Falta de control de ingreso al DATACENTER.	Existen sistemas biométricos que no los utilizan de manera adecuada.	Observación Directa	Visita de las instalaciones con ayuda del Responsable del Departamento de TIC's.
R6	Uso inadecuado de Manuales de Usuario para el sistema Quipux.	Se socializan una sola vez en el mejor de los casos cuando ingresan por primera vez a la institución.	Encuesta N°2	9
R7	Falta de integridad de la información.	La información se comparte en el DRIVE	Encuesta N°2	8
R8	Falta de mecanismos de seguridad para acceder al computador.	Existen mecanismos de seguridad solo para contraseñas.	Encuesta N°2	10
R9	Uso inadecuado de contraseñas de seguridad.	Comparten las contraseñas con los otros empleados.	Encuesta N°2	11
R10	Falta de planes de contingencia.	Actualmente no existen planes de contingencia.	Entrevista	2
R11	Falta de presupuesto para adquisición de repuestos de computadores.	Presupuesto limitado para hacer la adquisición de repuestos.	Entrevista	16
R12	Deficiente infraestructura física Tecnológica.	La infraestructura no está acorde al Departamento, porque tienen que estar movilizándose de una sala a otra.	Entrevista	13

### 6.1.4. Análisis de la Matriz de Riesgo Inherente

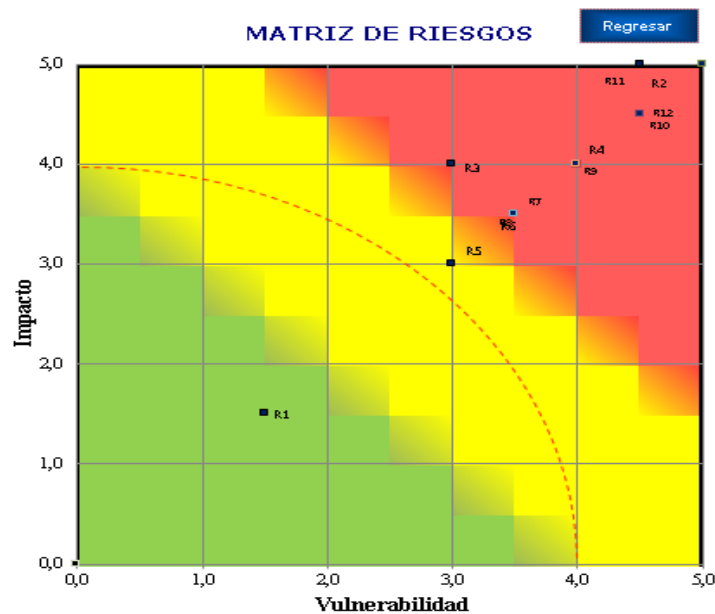


Figura 13. Mapa de calor de la matriz de riesgo inherente. Elaborado de acuerdo con la aplicación proporcionada por Deloitte Consulting Ecuador.

La empresa se encuentra actualmente en riesgo en cuanto a confidencialidad, integridad y disponibilidad de la información ya que únicamente se realizan respaldos de información y en cuanto a seguridades no se han tomado ninguna medida, es por ello que para identificar los riesgos se ha realizado una matriz de riesgos, donde podemos visualizarlos en la Figura 13, que trabaja en función del impacto y vulnerabilidad.

**Impacto:** Es un indicador de qué puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando se materializa sobre un activo. Es decir, son los efectos que puede tener en cualquier escenario, se puede realizar esta pregunta ¿Cuál es el impacto que causa? (ver Tabla III).

TABLA III. VALORACIÓN DEL RIESGO EN CUANTO A IMPACTO.

Alto	La ocurrencia del escenario tiene un impacto importante en el proceso.	5
Medio	La ocurrencia del escenario tiene un impacto significativo en el proceso.	3-4
Bajo	La ocurrencia del escenario tiene algún impacto en el proceso.	1-2

**Vulnerabilidad:** Es la debilidad de cualquier tipo que compromete la seguridad del sistema informático. Hace referencia a que tal vulnerable es el riesgo (Ver Tabla IV).

TABLA IV. VALORACIÓN DEL RIESGO EN CUANTO A LA VULNERABILIDAD.

Alto	El escenario del riesgo se presenta al menos una vez al mes.	5
Medio	El escenario del riesgo se presenta ocasionalmente o al menos una vez al año.	3-4
Bajo	El escenario del riesgo se presenta una vez en los últimos 5 años o nunca se ha presentado.	1-2

Los riesgos encontrados en la Institución son:

R1 : La falta de controles para el manejo de información posee un impacto y vulnerabilidad bajo dando como resultado una criticidad baja; R2: La Falta de presupuesto para adquirir licencias de antivirus tiene un impacto y vulnerabilidad alto es por ello que arroja una criticidad alta ;R3: La Falta de control de acceso en el ingreso de personas no autorizadas al Departamento de TIC's indica una vulnerabilidad medio y un impacto alto dando una criticidad media;R4: La Falta de políticas para respaldo de Información se encuentra en una vulnerabilidad y un impacto alto por lo tanto la criticidad es alta; R5: La Falta de control de ingreso al DATACENTER ; R6: El Uso inadecuado de Manuales de Usuario para el sistema Quipux; R7: La Falta de integridad de la información y R8: La Falta de mecanismos de seguridad para acceder al computador muestran un impacto y vulnerabilidad medio dando así una criticidad media; R9: Uso inadecuado de contraseñas de seguridad;R10: Falta de planes de contingencia ;R11: Falta de presupuesto para adquisición de repuestos de computadores;R12: Deficiente infraestructura física Tecnológica señalan un impacto y vulnerabilidad alta por lo tanto la criticidad es alta.

Del análisis realizado podemos determinar que la empresa se encuentra en su mayoría en una criticidad alta en cuanto a las seguridades en la información donde podemos ver que la curva en la Figura 13, pág. 31 muestra el nivel de exposición o pérdida que tiene la empresa.

#### **6.1.5. Identificación del impacto y la probabilidad del escenario para el riesgo residual.**

El impacto y la probabilidad en cuanto al riesgo residual permiten poder determinar qué riesgos la institución debe mitigar, evitar y transferir.

## ANÁLISIS DE LA MATRIZ DE RIESGO RESIDUAL

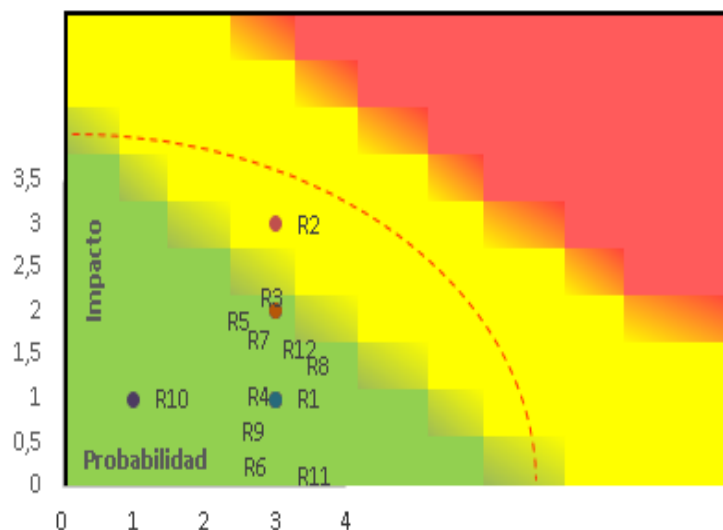


Figura 14. Mapa de calor de la matriz de riesgo residual. Elaborado de acuerdo con la aplicación proporcionada por Deloitte Consulting Ecuador.

Luego del análisis de riesgo inherente se establecen algunos controles para mejorar la criticidad en cuanto a la probabilidad de impacto, donde se obtuvo lo siguiente, (ver Figura 14). R1 : La falta de controles para el manejo de información posee un impacto bajo y vulnerabilidad media dando como resultado una criticidad baja; R2: La Falta de presupuesto para adquirir licencias de antivirus tiene un impacto y vulnerabilidad media es por ello que arroja una criticidad media ;R3: La Falta de control de acceso en el ingreso de personas no autorizadas al Departamento de TICS ;R4: La Falta de políticas para respaldo de Información; R5: La Falta de control de ingreso al DATACENTER ; R6: El Uso inadecuado de Manuales de Usuario para el sistema Quipux; R7: La Falta de integridad de la información ;R8: La Falta de mecanismos de seguridad para acceder al computador ;R9: Uso inadecuado de contraseñas de seguridad posee un impacto bajo y vulnerabilidad media lo cual da una criticidad baja ;R10: Falta de planes de contingencia muestra un impacto y vulnerabilidad baja dando así una criticidad baja ;R11: Falta de presupuesto para adquisición de repuestos de computadores ;R12: Deficiente infraestructura física Tecnológica señalan un impacto bajo y vulnerabilidad media por lo tanto la criticidad es baja.

### 6.1.6. Identificación de riesgos no aceptables

Luego de realizar el análisis de riesgo residual se pudo determinar que existen riesgos que la institución debe estar consiente de asumirlos.

## Análisis de Riesgos No Aceptables

Para determinar el análisis de riesgos no aceptables tomamos en cuenta el análisis de riesgo inherente y riesgo residual, en base a ello se puede evidenciar que 6 de los 12 riesgos evaluados poseen al menos una severidad alta en cuanto a la probabilidad de impacto, los mismos que requieren de una atención inmediata, es decir se deben evitar, transferir y mitigar con el fin de reducir los riesgos existentes en la institución.

Ya una vez tratados estos riesgos deben ubicarse en una severidad baja con el fin de fortalecer la seguridad de la información, tales como: confidencialidad, integridad y disponibilidad de la información. A continuación, se puede observar en la Tabla V.

TABLA V. TABLA DE RIESGOS NO ACEPTABLES.

RIESGOS	DESCRIPCIÓN	SEVERIDAD	
		INHERENTE	RESIDUAL
R2	Falta de presupuesto para adquirir licencias de antivirus	Alto	Media
R4	Falta de políticas para respaldo de Información	Alto	Baja
R9	Uso inadecuado de contraseñas de seguridad	Alto	Baja
R10	Falta de planes de contingencia	Alto	Baja
R11	Falta de presupuesto para adquisición de repuestos de computadores	Alto	Baja
R12	Deficiente infraestructura física Tecnológica	Alto	Baja

Para concluir el plan de gestión de riesgo se elaboró una comparativa como vemos a continuación (ver tabla VI, pág. 35):

### 6.1.7. COMPARATIVA DEL ANÁLISIS INHERENTE VS. EL ANÁLISIS RESIDUAL

TABLA VI. COMPARATIVA DE ANÁLISIS DE RIESGO INHERENTE VS ANÁLISIS DE RIESGO RESIDUAL.

RIESGOS	DESCRIPCIÓN	SEVERIDAD	
		INHERENTE	RESIDUAL
R1	Falta de controles para el manejo de la Información	Bajo	Baja
R2	Falta de presupuesto para adquirir licencias de antivirus	Alto	Media
R3	Falta de control de acceso en el ingreso de personas no autorizadas al Departamento de TIC's	Medio	Baja
R4	Falta de políticas para respaldo de Información	Alto	Baja
R5	Falta de control de ingreso al DATACENTER	Medio	Baja
R6	Uso inadecuado de Manuales de Usuario para el sistema Quipux	Medio	Baja
R7	Falta de integridad de la información	Medio	Baja
R8	Falta de mecanismos de seguridad para acceder al computador	Medio	Baja
R9	Uso inadecuado de contraseñas de seguridad	Alto	Baja
R10	Falta de planes de contingencia	Alto	Baja
R11	Falta de presupuesto para adquisición de repuestos para computadores	Alto	Baja
R12	Deficiente infraestructura física Tecnológica	Alto	Baja

En la Tabla VI se puede evidenciar que 6 de los 12 riesgos evaluados ha disminuido el grado de severidad al aplicar el análisis de riesgo residual ya que en este análisis se sugieren controles que se deben aplicar para mitigar los riesgos.

## **6.2. FASE 2: Analizar las Metodologías de Gestión de Riesgos.**

### **6.2.1. Búsqueda de metodologías**

Se procederá a la recolección de información acerca de las metodologías utilizadas para la gestión de riesgos mediante una revisión bibliográfica (ver Revisión de Literatura, parte 4.2, pág. 11).

### **6.2.2. Comparativa de las metodologías de gestión de riesgos**

Una vez obtenida la información necesaria acerca de las metodologías de gestión de riesgos, se procederá a realizar una comparativa de las metodologías (ver Tabla VII, pág. 37) para conocer cuál de ellas se adapta mejor a las necesidades de esta Tesis de Grado.

TABLA VII. COMPARATIVA DE METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS.

METODOLOGÍAS	PAÍS	HERRAMIENTA DE SOFTWARE	FASES	TIPO DE ANÁLISIS	VENTAJAS	DESVENTAJAS	REFERENCIA
<i>MAGERIT</i>	España	PILAR	<ol style="list-style-type: none"> <li>1. Identificar los activos de la empresa</li> <li>2. Determinar las amenazas</li> <li>3. Establecer respectivas salvaguardas</li> </ol>	Cuantitativo y Cualitativo	<ul style="list-style-type: none"> <li>• Posee un alcance completo en el análisis y gestión de riesgos.</li> <li>• Prepara a la institución para procesos de evaluación, auditoría y certificación.</li> </ul>	<ul style="list-style-type: none"> <li>• Posee fallas en el inventario de políticas.</li> </ul>	Novoa, H. A., & Barrera, C. R. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones e Investigación, 9, 73-86.
<i>OCTAVE</i>	España	No tiene	<ul style="list-style-type: none"> <li>• Construir perfiles de amenazas con base en los recursos</li> <li>• Identificar las vulnerabilidades de la infraestructura</li> <li>• Desarrollar la estrategia y los planes de seguridad.</li> </ul>	Cualitativo	<ul style="list-style-type: none"> <li>• Es una metodología flexible, es decir cada método se puede adaptar al entorno de riesgos</li> <li>• Involucra a todo el personal</li> <li>• Ayuda a preveer y planear distintas acciones y medidas de seguridad en caso de que se presente alguna amenaza.</li> </ul>	<ul style="list-style-type: none"> <li>• No manifiesta de forma clara la definición y determinación de los activos</li> </ul>	Bustos Lara, J. D. (2016). Análisis de las metodologías de gestión de riesgos para garantizar la continuidad del negocio en el Departamento de tecnologías de la información en la Corporación Nacional de Electricidad en Esmeraldas (Doctoral dissertation, Ecuador-PUCESE-Escuela de Sistemas y Computación).
<i>CORAS</i>	Noruego	No tiene	<ol style="list-style-type: none"> <li>1. Identificar el contexto</li> <li>2. Identificar los riesgos</li> <li>3. Estimar el nivel del riesgo</li> <li>4. Tratar los riesgos</li> </ol>	Cualitativo	<ul style="list-style-type: none"> <li>• Dispone de diferentes herramientas de apoyo para el análisis de riesgos, un editor gráfico.</li> <li>• Proporciona un repositorio de paquetes de experiencias reutilizables</li> <li>• Entrega un reporte de las vulnerabilidades encontradas.</li> </ul>	<p>Dentro de su modelo no contempla elementos como procesos y las dependencias.</p>	Novoa, H. A., & Barrera, C. R. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones e Investigación, 9, 73-86.
<i>MEHARI</i>	Francia	RISCARE	<ul style="list-style-type: none"> <li>• Fase 1. Preparatoria</li> <li>• Fase 2. Valoración del riesgo</li> <li>• Fase 3. Planificación del tratamiento del riesgo</li> </ul>	Cuantitativo y Cualitativo	<ul style="list-style-type: none"> <li>• Posee base de datos de conocimiento con manuales, guías y herramientas para el análisis de riesgos.</li> <li>• Con esta metodología se puede detectar vulnerabilidades mediante auditorías y se examinan las situaciones del riesgo</li> </ul>	<ul style="list-style-type: none"> <li>• Se centra únicamente en los principios de confidencialidad, integridad y disponibilidad.</li> </ul>	Novoa, H. A., & Barrera, C. R. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones e Investigación, 9, 73-86.



<i>NIST</i>	USA	No tiene	<ul style="list-style-type: none"> <li>• Caracterización del sistema.</li> <li>• Identificación de amenaza.</li> <li>• Identificación de vulnerabilidades.</li> <li>• Control de análisis.</li> <li>• Determinación de la probabilidad.</li> </ul>	Cualitativo	<ul style="list-style-type: none"> <li>• Consta de una guía para la evaluación de riesgos de seguridad en la infraestructura de TIC'S.</li> <li>• Su guía proporciona herramientas para la valoración y mitigación de riesgos</li> <li>• Desarrolla la administración a partir de los resultados del análisis de riesgos</li> </ul>	El modelo de esta metodología no tiene contemplados elementos como los procesos, los activos ni las dependencias.	Molina, U., & Andrés, J. (2014). Desarrollo de un plan de gestión de seguridad de la información para el centro de educación continua de la escuela politécnica nacional (Bachelor's thesis, Quito: EPN, 2015.).
<i>IRAM</i>	USA	IRAM Risk Analyst Workbench	<ol style="list-style-type: none"> <li>1. Análisis de impacto sobre el negocio(BIA)</li> <li>2. Evaluación de amenazas y vulnerabilidades</li> <li>3. Selección de controles</li> </ol>	Cuantitativo y Cualitativo	<ul style="list-style-type: none"> <li>• Participa en los procesos de Normalización internacional</li> <li>• Es reconocido como el único organismo de normalización.</li> <li>• Asesora a diferentes organismos públicos en cuestiones de Normalización.</li> <li>• Es aplicable a cualquier institución.</li> </ul>	<ul style="list-style-type: none"> <li>• No establece por si misma guías detalladas para la gestión.</li> <li>• En el modelo no se contempla elementos como los procesos y los recursos.</li> </ul>	Matalobos Veiga, J. M. (2009). Análisis de riesgos de seguridad de la información.
<i>CRAMM</i>	Reino Unido	CRAMM	<ol style="list-style-type: none"> <li>1. Establecimiento de objetivos de seguridad</li> <li>2. Análisis de Riesgos</li> <li>3. Identificación y selección de recomendaciones</li> </ol>	Cuantitativo y Cualitativo	<ul style="list-style-type: none"> <li>• Se utiliza para identificar la seguridad y requisitos de contingencia para un sistema de información.</li> <li>• Identifica y clasifica los activos</li> <li>• Combina el análisis y evaluación de riesgos</li> </ul>	Dentro de este modelo no se contempla elementos como los procesos y los recursos.	Novoa, H. A., & Barrera, C. R. (2015). Metodologías para el análisis de riesgos en los sgsi. Publicaciones e Investigación, 9, 73-86.

### **6.2.3. Selección de metodologías de gestión de riesgos**

Luego de realizar la revisión bibliográfica y el cuadro comparativo de acuerdo a las variables (ver Tabla VIII, pag.40) de la institución donde vamos a implementar el análisis de riesgos se ha seleccionado MAGERIT.

A continuación, se detallan las características:

TABLA VIII. RESULTADO DE COMPARATIVA DE METODOLOGÍAS PARA LA GESTIÓN DE RIESGOS (ELABORACIÓN PROPIA).

<b>VARIABLES/METODOLOGÍAS</b>	<b>MAGERIT</b>	<b>OCTAVE</b>	<b>CORAS</b>	<b>MEHARI</b>	<b>NIST</b>	<b>IRAM</b>	<b>CRAMM</b>
V1: Idioma Español.	X						
V2: Contempla elementos como procesos y recursos.	X	X		X			
V3: Herramienta de Software Libre.	X						
V4: Alcance completo de análisis y gestión de riesgos.	X						
V5: Procesos de Auditoría y certificación.	X					X	
V6: Análisis Cualitativo y cuantitativo.	X			X		X	X
V7: Proporciona repositorio de paquetes de experiencias reutilizables.	X		X		X		
V8: Entrega un reporte de las vulnerabilidades encontradas.	X		X		X		X
V9: Participa en procesos de Normalización Internacional.						X	
V10: Su guía proporciona herramientas para la valoración y mitigación de riesgos.	X				X		X
V11: Posee base de datos de conocimiento, con manuales, guías y herramientas para el análisis de riesgos.	X	X		X	X		
V12: Permite detectar vulnerabilidades mediante auditorías y se examinan las situaciones de riesgo.	X	X		X	X		

- Magerit presenta un plus en la V1 al encontrarse disponible en idioma español ya que fue desarrollada por el Consejo Superior de Administración Electrónica, y publicado por el Ministerio de Administraciones Públicas de España a diferencia de las demás metodologías.
- MAGERIT, OCTAVE, MEHARI en V2 contemplan elementos como procesos y recursos y las demás metodologías no toman en cuenta estos procesos.
- MAGERIT según la V3 cuenta con PILAR<sup>2</sup> que es una herramienta de software gratuito a diferencia del resto.
- MAGERIT en V4 es muy útil para las instituciones que recién empiezan con la gestión de la seguridad en la información porque permite realizar el alcance completo del análisis de los riesgos y la gestión de los mismos, cuya finalidad es tomar contramedidas, un punto a favor con relación a las otras metodologías.
- MAGERIT e IRAM en V5 prepara a la Institución para procesos de auditoría, certificación, mientras las otras metodologías trabajan de manera separada estos procesos.
- MAGERIT, MEHARI, IRAM Y CRAMM en V6 realizan el análisis cualitativo /cuantitativo, a diferencia del resto de metodologías que realizan un solo tipo de análisis.
- MAGERIT, CORAS y NIST en V7, proporcionan repositorio de paquetes de experiencias reutilizables y las demás no cuentan con este método de almacenamiento.
- MAGERIT, CORAS, NIST y CRAMM en V8, entregan reportes de las vulnerabilidades encontradas mientras las otras metodologías no cuentan con este modelo de informe.
- IRAM en V9, es la única metodología que participa en procesos de Normalización Internacional.
- MAGERIT, NIST y CRAMM en V10, poseen una guía que proporciona herramientas para la valoración y mitigación del riesgo a diferencia del resto.
- MAGERIT, OCTAVE, MEHARI y NIST en V11, poseen base de datos de conocimiento con manuales, guías y herramientas para el análisis de riesgos y las demás no poseen este paso.

---

<sup>2</sup> PILAR (Procedimiento Informático y Lógico de Análisis de Riesgos): Es una herramienta de análisis y gestión de riesgos.

- MAGERIT, OCTAVE, MEHARI y NIST en V12, permiten detectar vulnerabilidades mediante auditorías y examinan las situaciones de riesgo, mientras que las demás realizan de otra manera este procedimiento.

Por lo tanto se concluye que MAGERIT es la mejor opción ya que cumple con 11 de las 12 variables evaluadas en el resultado final de la tabla comparativa(ver Tabla 8, pág. 40) , agregando que es una metodología útil para las instituciones que recién empiezan con la gestión de la seguridad de información, ya que permite clasificar los activos de la institución en varios grupos, logrando así realizar el análisis de los riesgos y la gestión de los mismos, cuya finalidad es tomar contramedidas, un punto a favor con relación a las otras metodologías.

### **6.3. FASE 3: Elaborar el plan de gestión de riesgos de acuerdo a la metodología seleccionada.**

Considerando la situación actual del Departamento de TIC's del Hospital de Catacocha, para reducir los niveles de riesgo, es indispensable diseñar un plan de gestión de riesgos de TI para iniciar las prácticas de seguridad de información y recomendar procesos que aseguren la continuidad de los servicios. (Para más detalle ver tabla XII, pág. 45).

#### **OBJETIVO GENERAL**

Desarrollar un plan de gestión de riesgos de TI de acuerdo a la metodología seleccionada que permita minimizar los riesgos de pérdida de activos de la información en el Hospital de Catacocha.

#### **OBJETIVOS ESPECÍFICOS**

- Determinar el alcance del plan de gestión de riesgos.
- Definir los principales activos a proteger en el Departamento de TIC's.
- Identificar las principales amenazas que afectan a los activos.
- Proponer soluciones para minimizar los riesgos a los que está expuesto cada activo.

#### **ALCANCES**

- Designar funciones de liderazgo al responsable del Departamento de TIC's para apoyar y asesorar el proceso del plan de gestión.
- Capacitar al personal de la institución en el proceso de plan de gestión de riesgos.

- Se aplicará únicamente la metodología MAGERIT para la gestión de riesgos.
- Emplear las fases de la metodología MAGERIT, para el proceso de plan de gestión de riesgos de TI en el Departamento de TIC's del Hospital de Catacocha.

### LIMITACIONES

- No se utilizará ningún software para el desarrollo del plan de gestión de riesgos.
- No se hará ningún manual de la gestión de riesgos.
- No se implementará el plan de gestión de riesgos ya que al ser una institución pública depende de entes externos, únicamente se le dará a conocer y entregará el documento al encargado del Departamento de TIC's.

### CLASIFICACIÓN DE ACTIVOS DE LA INSTITUCIÓN

Se establece los activos relevantes, su interrelación y su importancia económica, (ver Tabla IX) donde se presenta la clasificación de activos de la Institución.

TABLA IX. ACTIVOS DEL DEPARTAMENTO DE TIC'S-HOSPITAL DE CATACOCHA.

Tipos de Activos	Descripción del activo
[D]Datos/Información	Reglamentos internos, procesos, formatos, código fuente, código ejecutable.
[K]Claves criptográficas	Claves de acceso a los equipos, software contable (SITAC).
[Sw]Software	Firewall, sistemas operativos (Windows, Linux), programa contable (SITAC).
[Hw]Hardware	Impresoras, teléfonos, servidores, computadores.
[M]Soportes de información	Material impreso, memorias USB, discos duros.
[I]Instalaciones	Edificio del Hospital de Catacocha (Departamento de TIC's).
[P]Personal	Personal que labora en la institución.

### VALORACIÓN DE LAS AMENAZAS

Se dimensiona la valoración a la que están siendo expuestos los activos de la institución. La metodología MAGERIT contempla el análisis cualitativo y cuantitativo, (ver tabla X) donde se describen los criterios de valoración.

TABLA X. VALORACIÓN DE ACTIVOS.

Alto	Daño grave a la institución.	5
Medio	Daño importante a la institución.	3-4
Bajo	Daño menor a la institución.	1-2

## VALORACIÓN DE ACTIVOS

Esta valoración de los activos del Departamento de TIC's, se hizo en conjunto con el responsable del Departamento de TIC's, tomando en cuenta a qué amenazas se enfrenta cada activo (ver Tabla XI, pág. 44).

TABLA XI. VALORACIÓN DE ACTIVOS DE ACUERDO AL IMPACTO

Tipos de Activos	Amenaza	Impacto
[D]Datos/Información	Falta de controles de información.	Bajo
	Falta de políticas para el manejo de información.	Alto
	Falta de integridad de la información.	Medio
	Uso inadecuado de Manuales de usuario.	Medio
[K]Claves criptográficas	Control de accesos en el ingreso de personas no autorizadas al Departamento de TIC's.	Medio
	Control de accesos en el ingreso de personas no autorizadas al DATACENTER.	Medio
	Falta de Mecanismos de seguridad para acceder al computador.	Medio
	Uso inadecuado de contraseñas de seguridad.	Alto
[Sw]Software	Falta de presupuesto para adquirir licencias de antivirus.	Alto
[Hw]Hardware	Desastres Naturales.	Alto
	Falta de presupuesto para adquirir repuestos de computadores.	Alto
[M]Soportes de información	Falta de políticas para respaldo de información.	Alto
[I]Instalaciones	Deficiente Infraestructura física tecnológica	Alto
[P]Personal	Accesos no autorizados.	Medio
	Falta de Planes de Contingencia.	Alto

A continuación, se presenta la tabla XII(pág. 45), donde se indican los riesgos encontrados, el tipo de control, plan de acción, plan de contingencia y el responsable, los mismos que fueron tomados del análisis de la matriz inherente (ver pág. 31) y análisis de matriz residual (ver pág. 33), donde se puede visualizar los mapas de calor que permitieron determinar el nivel de exposición de las amenazas encontradas y se da a conocer las posibles acciones que se pueden aplicar para disminuir el nivel de exposición de los riesgos, para más detalle (ver Anexo 6, pág. 95) con la matriz inherente y matriz residual.

TABLA XII. PLAN DE GESTIÓN DE RIESGOS

RIESGOS	DESCRIPCIÓN	TIPO DE CONTROL Técnicos y organizativos	PLAN DE ACCIÓN	PLAN DE CONTINGENCIA	RESPONSABLE
R1	Falta de controles para el manejo de la Información.	Organizativos	Establecer políticas claramente definidas para el manejo de la información. Socializar al personal temas referentes al manejo de la información.	Elaborar un manual sobre el manejo de la información.	Responsable de TIC's
R2	Falta de presupuesto para adquirir licencias de antivirus.	Técnicos	Incluir dentro del plan anual la adquisición de licencias de antivirus para los equipos que aun poseen software privativo. Que sea una regla el uso de software libre en toda la institución.	Concientizar a todo el personal de la Institución para que migren y utilicen software libre.	Responsable de TIC's
R3	Falta de control de acceso en el ingreso de personas no autorizadas al Departamento de TIC's.	Organizativos	Utilizar una credencial para el ingreso al departamento de TIC's. Implementar un programa de detección de intrusos. Revisar y actualizar cada 3 meses los derechos de accesos a las áreas restringidas.	Emitir una solicitud al responsable del departamento de TIC's para el ingreso a dicho departamento. Incluir sistemas biométricos que permitan el control de acceso al Departamento.	Responsable de TIC's
R4	Falta de políticas para respaldo de Información.	Organizativos	Coordinar una revisión periódica de copias de seguridad.	Dar a conocer a todos los que laboran en el Departamento de TIC's las políticas y ponerlas en práctica.	Responsable de TIC's



R5	Falta de control de ingreso al DATACENTER.	Organizativos	Colocar letreros indicadores para restringir el acceso a personas no autorizadas. Utilizar los sistemas biométricos que existen para explorarlos en un 100%. Monitorear y controlar continuamente el acceso al DATACENTER. El acceso al DATACENTER debe ser identificado, controlado y vigilado plenamente portando alguna identificación o autorización asignada por el encargado del departamento.	Realizar y llevar un registro manual de ingreso a áreas restringidas	Responsable de TIC's
R6	Uso inadecuado de Manuales de Usuario para el sistema Quipux.	Organizativos	Dar seguimiento mensual al personal sobre el uso de manuales. Capacitar semestralmente al personal de la institución sobre el uso de Manuales de Usuario o bajo demanda a las personas que recién ingresen.	Instruir a todo el personal para que pongan en práctica la utilización de los manuales.	Responsable de TIC's
R7	Falta de integridad de la información.	Organizativos	Asignar permisos individualmente según perfiles de usuario. Establecer mecanismos para revisar periódicamente que los	Crear políticas para mantener la información confidencial reservada y que solo tengan acceso el personal autorizado.	Responsable de TIC's

			permisos concedidos son adecuados, haciendo énfasis en los usuarios cuyos accesos han sido eliminados o modificados. Capacitar y Utilizar herramientas de cifrado de información para mantener la integridad en la información.		
R8	Falta de mecanismos de seguridad para acceder al computador.	Organizativos	Implementar mecanismos de seguridad como: antivirus, firewall, antiespias, encriptación.	Realizar charlas con personal de la Institución para hacerles conocer sobre la importancia de la utilización de mecanismos de seguridad.	Responsable de TIC's
R9	Uso inadecuado de contraseñas de seguridad.	Organizativos	Concientizar al personal respecto a su responsabilidad al frente de contraseñas. Capacitar en todas las dependencias el uso de contraseñas en cada computador.	Que sea una política institucional el uso de contraseñas de seguridad.	Responsable de TIC's
R10	Falta de planes de contingencia.	Organizativos	Planificar la elaboración del plan de contingencia para dicho Departamento. Introducir dentro del presupuesto anual un porcentaje para elaborar el plan de contingencias de acuerdo a las afectaciones correspondientes.	Pedir al Jefe Distrital mediante una solicitud personal para que se encargue de la elaboración del Plan de contingencia.	Responsable de TIC's

R11	Falta de presupuesto para adquisición de repuestos para computadores.	Técnicos	Solicitar apoyo a instituciones gubernamentales y no gubernamentales para la adquisición de repuestos para computadores. Designar del presupuesto anual un porcentaje para la adquisición de repuestos.	Trasferir un oficio al Jefe Distrital para que incremente el presupuesto en el Departamento de TIC's, y así poder adquirir repuestos para computadores.	Responsable de TIC's
R12	Deficiente infraestructura física Tecnológica.	Técnicos	Elaborar una solicitud al Director del Hospital para que se designe un lugar apropiado para el Departamento de TIC's.	Pedir al Jefe Distrital un lugar permanente y adecuado para ubicar las instalaciones del Departamento de TIC's.	Responsable de TIC's

## **POLÍTICAS DE SEGURIDAD PARA EL DEPARTAMENTO DE TIC's**

### **POLÍTICAS GENERALES**

- Cada usuario al ingresar en su computador debe tener su usuario y contraseña.
- Los funcionarios deben tener acceso solo a los servicios autorizados, mediante su usuario y contraseña.
- Se debe restringir el acceso a internet para evitar que los usuarios descarguen o naveguen en páginas no autorizadas.
- Los usuarios deben usar los equipos informáticos pertenecientes al Hospital de Catacocha para fines laborales y si alguno llegará a fallar, se debe informar de inmediato al Departamento de TIC's para tomar medidas necesarias.

### **POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN**

- Las copias de respaldo de la información se realizarán diarias, semanal y mensualmente.
- Utilizando aplicaciones de software libre se podrán realizar copias automáticas de seguridad de la información llevándolas a un disco externo.
- Se deben realizar respaldos de recuperación de la información y deben ser entregados al administrador de copias de seguridad, con su respectivo recibido.
- Deberá existir un administrador del sistema, que pueda verificar la correcta aplicación de los procedimientos de realización de las copias de seguridad y recuperación de los datos.

### **POLÍTICAS DE MANTENIMIENTO DE EQUIPOS**

- Antes de encender el equipo de cómputo asegurarse que éste cuenta con las condiciones de ambiente adecuadas para trabajar.
- Al finalizar la jornada laboral se debe apagar el equipo de cómputo, verificando que este proceso se cumpla.
- Se debe realizar mantenimiento preventivo y correctivo a los equipos de la institución, estos se realizarán cada 4 meses por personal capacitado, o de acuerdo a la necesidad.
- Toda actividad de mantenimiento realizada por el responsable del Departamento de TIC's deberá estar documentada con la finalidad de hacerle el seguimiento respectivo.
- Los mantenimientos preventivos y correctivos programados a los equipos de cómputo, se ejecutarán dentro de las instalaciones de la institución y bajo supervisión de una persona asignada por el departamento de TIC's.

## **POLÍTICAS DE USO DE SOFTWARE**

- El Departamento de TIC's debe estar revisando que los equipos contengan las últimas actualizaciones del sistema operativo (Windows, Linux) que utilizan.
- Está prohibido el uso de programas sin licencias no autorizadas por la institución.
- Solo el responsable del Departamento de TIC's puede instalar y verificar que los programas pueden ser instalados en los computadores.
- El Departamento de TIC's debe mantener catálogo de software (libre o privativo) que haya sido instalado en las diferentes áreas, con esto la finalidad de haber algún daño se vuelva a instalar las aplicaciones.
- Todo tipo de software adquirido por la institución debe ser utilizado bajo los términos de licenciamiento.
- Los usuarios que utilicen los equipos de cómputo, utilizarán programas de software solo con fines de trabajo y serán responsables por el uso correcto de éstos.
- El departamento de TIC's de la institución debe realizar revisiones periódicas por las diferentes áreas de servicio para identificar su correcto licenciamiento de software y así garantizar estabilidad y correcto funcionamiento de los equipos de cómputo.

## **6.4. FASE 4: Comunicar los resultados a la comunidad científica.**

### **6.4.1. Envió del artículo**

Se lo hizo en las II JORNADAS DE INVESTIGACIÓN CIENCIA TECNOLOGÍA Y SOCIEDAD de la Universidad PUCESE de Esmeraldas.

### **6.4.2. Exposición del artículo en la PUCESE**

Para el desarrollo de esta exposición se dio a conocer sobre la importancia de la seguridad de la información (ver Figura 15) (ver anexo 5, pág. 94).



Figura 15. Ponencia del artículo.

### **6.4.3. Publicación del Artículo**

La publicación del artículo se la hizo en una revista internacional RISTI en la edición N°20 volumen 2, dicha revista es indexada en Scopus (ver anexo 7, pág. 108).

## **7. Discusión**

### **7.1. Desarrollo de la Tesis de Grado**

Para la finalización exitosa de la tesis se cumplió con todos los objetivos específicos planteados al inicio de la investigación. Como se detallan a continuación:

#### **OBJETIVO ESPECÍFICO 1: Determinar los riesgos en las TI del Hospital de Catacocha.**

Para determinar los riesgos que se encuentran en el Departamento de TIC's del Hospital de Catacocha se utilizó la técnica de la entrevista (ver Anexo 2, pág. 63), la encuesta (ver Anexo 4, pág. 68) y la observación directa (Ver sección de Resultados 6.1.1, pág. 23) en todas las instalaciones, cuya finalidad era elaborar una lista de los riesgos (ver sección de resultados sección 6.1.3, pág. 30) que están presentes en la institución para poder realizar el análisis de riesgos.

#### **OBJETIVO ESPECÍFICO 2: Analizar las metodologías de Gestión de Riesgos.**

En este objetivo se realizó una búsqueda bibliográfica de todas las metodologías utilizadas para la gestión de riesgos, para luego de ello elaborar una tabla comparativa (ver sección de Revisión de Literatura Fase 4.2, pág. 11), y a partir de ello, seleccionar la metodología más óptima para esta investigación, donde se seleccionó Magerit (ver sección de Resultados 6.2.3, pág. 40), la misma que permite el análisis de la gestión de riesgos de los sistemas de información cuando una institución recién empieza con el proceso de gestión de riesgos.

#### **OBJETIVO ESPECÍFICO 3: Elaborar el plan de gestión de riesgos de acuerdo a la metodología seleccionada.**

Para el cumplimiento de este objetivo se tomaron los riesgos encontrados (ver sección de Resultados 6.1.3, pág. 30) y las matrices de análisis empleando el aplicativo proporcionado por la empresa de consultoría Deloitte, en donde se obtuvo los mapas de calor (ver sección de Resultados 6.1.4 pág. 31 y 6.1.5 pág. 33) y se logró determinar que se mitigaron los riesgos en la institución al sugerir los controles para mejorar la seguridad de la información en el Departamento de TIC's de Hospital de Catacocha.

## **OBJETIVO ESPECÍFICO 4: Comunicar los resultados a la comunidad científica.**

En cuanto a este objetivo se realizó el envío del artículo a las II JORNADAS DE INVESTIGACIÓN CIENCIA TECNOLOGÍA Y SOCIEDAD de la Universidad PUCESE de Esmeraldas (ver anexo 7, pág. 108) posteriormente se realizó la ponencia del artículo en la PUCESE sede de Ibarra y finalmente la publicación del mismo en la revista RISTI, indexada en la base de datos SCOPUS.

## **7.2. Valoración técnica económica ambiental**

Para la elaboración del presupuesto se han tomado en cuenta los bienes, servicios, imprevistos y talento humano necesario para lograr llevar a cabo los objetivos que demanda esta tesis de grado, los cuales son detallados a continuación.

### **7.2.1. Talento Humano**

Para el desarrollo de esta tesis de grado se necesitará contar con los siguientes recursos que se describen en la Tabla XIII, los mismos que cubrirán las actividades necesarias al desarrollo del TT en su totalidad.

TABLA XIII. TALENTO HUMANO PARA LA TESIS DE GRADO.

<b>ROL</b>	<b>Número de Horas</b>	<b>Valor por hora (\$)</b>	<b>Valor Total</b>
<b>Investigador</b>	600.00	8,00	4.800,00
<b>Tutor</b>	50.00	0,00	0,00
<b>Total (\$):</b>			<b>4.800,00</b>

Para cubrir con los gastos pertenecientes a tutorías por parte del docente encargado de la presente tesis de grado, correrán a responsabilidad netamente de la Universidad, por lo que el rubro especificado anteriormente por tutorías no se lo tomará como valor para el presupuesto.



### 7.2.2. Bienes

Los siguientes recursos hardware y software que se presentan en la Tabla XIV, representan todos bienes que serán necesarios adquirir para poder realizar sin inconvenientes el desarrollo de la presente tesis de grado.

TABLA XIV. RECURSOS HARDWARE Y SOFTWARE.

<b>BIEN</b>	<b>Cantidad</b>	<b>Valor unitario</b>	<b>Valor Total</b>
<b>HARDWARE</b>			
<b>Depreciación Laptop</b>	1	120,00	120,00
<b>Depreciación Impresora</b>	1	50,00	50,00
<b>Memoria Flash</b>	1	10,00	10,00
		<b>SubTotal (\$):</b>	180,00
<b>SOFTWARE</b>			
<b>Gantt Proyect</b>	1	00.00	00,00
<b>MAGERIT</b>	1	00.00	00,00
		<b>SubTotal (\$):</b>	00,00
		<b>Total (\$):</b>	<b>180,00</b>

### 7.2.3. Servicios

En el transcurso del desarrollo de la presente tesis de grado será necesario adquirir ciertos servicios que servirán de complemento para culminar con éxito las tareas que demanda el presente TT (ver Tabla XV).

TABLA XV. PRESTACIÓN DE SERVICIOS A ADQUIRIR.

SERVICIO	Cantidad	Valor unitario	Valor Total
Transporte	200	0,30	60,00
Copias	300	0,02	6,00
Resma de Papel	2	4,00	8,00
Anillados	6	1,00	6,00
Cartuchos	4	25,00	100,00
Internet	200 h	0,50	100,00
<b>Total (\$):</b>			<b>280,00</b>

#### 7.2.4. Imprevistos

Para imprevistos se cree conveniente tomar el 10 % del valor total del presupuesto, los cuales serán agregados al valor total de la Tesis de grado (ver Tabla XVI).

TABLA XVI. PRESUPUESTO TOTAL DEL TESIS DE GRADO.

RECURSO	SUBTOTAL
T. Humano	4.800,00
Bienes	180,00
Servicios	280,00
<b>SubTotal (\$):</b>	<b>3.260,00</b>
<b>Imprevistos 10%</b>	<b>900,00</b>
<b>Total (\$):</b>	<b>6.160,00</b>

## 8. Conclusiones

Una vez realizado el plan de gestión de riesgos de TI en el Hospital de Catacocha se concluye lo siguiente:

- En el Hospital de Catacocha, únicamente se ejecutan respaldos de información en discos externos, sin tomar en cuenta las seguridades que deben tener al manipular la información confidencial y los activos que existen en la Institución.
- De las 12 amenazas encontradas, se identificó que uno de los factores que influyen negativamente en la gestión de riesgos del Hospital de Catacocha es el presupuesto limitado asignado al Departamento de TIC's.
- Los mapas de calor son herramientas útiles para el análisis inherente y análisis residual porque permiten la identificación visual de cada uno de los riesgos y contribuyen con la toma de decisiones.
- La metodología de gestión de riesgos MAGERIT es la más adecuada para las instituciones que recién empiezan con el análisis y gestión de riesgos, ya que cumple con 11 de las 12 variables cualitativas evaluadas frente a otras metodologías, destacando que se encuentra en idioma español y posee herramienta de software libre (PILAR).
- El plan de gestión de riesgos desarrollado en el presente trabajo enfocado en el Departamento de TIC's, constituye un punto de partida para reducir los riesgos y mitigarlos, con el fin de proteger los activos.

## **9. Recomendaciones**

Una vez realizado el plan de gestión de riesgos de TI en el Hospital de Catacocha se recomienda lo siguiente:

- Capacitar continuamente al personal del Departamento de TIC's del Hospital de Catacocha sobre temas de seguridad de la información.
- Actualizar y socializar las políticas de seguridad de la información en el Departamento de TIC's del Hospital de Catacocha.
- Como trabajo futuro, aplicar el plan de gestión de riesgos de TI en el Hospital de Catacocha.

## 10. Bibliografía

- [1] A. Duros Blandos, "Seguridad en Informática," 2013.
- [2] María Fernanda Molina Miranda, "PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL," Universidad Politécnica de Madrid, 2015.
- [3] M. AMUTIO, J. Candau, and J. Mañas, "MAGERIT–versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II-Catálogo de Elementos," 2012, Pág. 27.
- [4] N. Acevedo y C. Satizábal, «Metodologías de gestión y prevención de riesgos: una comparación,» *Sistemas y Telemática*, 2016.
- [5] L. Ruiz, A. Julián, and M. M. Ortiz, "Diseño de un protocolo para la detección de vulnerabilidades en los principales servidores de la Superintendencia de Puertos y Transporte," 2017.
- [6] R. Johnson, "Security policies and implementation issues," 2010, Página 3-19.
- [7] A. Syalim, Y. Hori, K. S.- Availability, R. and, and undefined 2009, "Comparison of risk analysis methods: Mehari, magerit, NIST800-30 and microsoft's security management guide," [ieeexplore.ieee.org](http://ieeexplore.ieee.org).
- [8] R. G. Montalvo Armijos, "Generación de políticas para la gestión de riesgos de seguridad en el desarrollo de software.," 2017.
- [9] S. Yaqub, "Relating CORAS diagrams and Markov chains," 2007.
- [10] A. Castro, Z. B.- Ingeniería, and undefined 2011, "Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios," [dialnet.unirioja.es](http://dialnet.unirioja.es).
- [11] M. G. Piedra, J. Cordones, and P. Orlando, "Análisis de Riesgos Informáticos y Elaboración de un Plan de Contingencia TI para la Empresa Eléctrica Quito SA," 2011
- [12] K. C. Torres, "Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para análisis y gestión de riesgos de seguridad de la información," 2015.
- [13] J. M. Matalobos Veiga, "Análisis de riesgos de seguridad de la información," 2009.

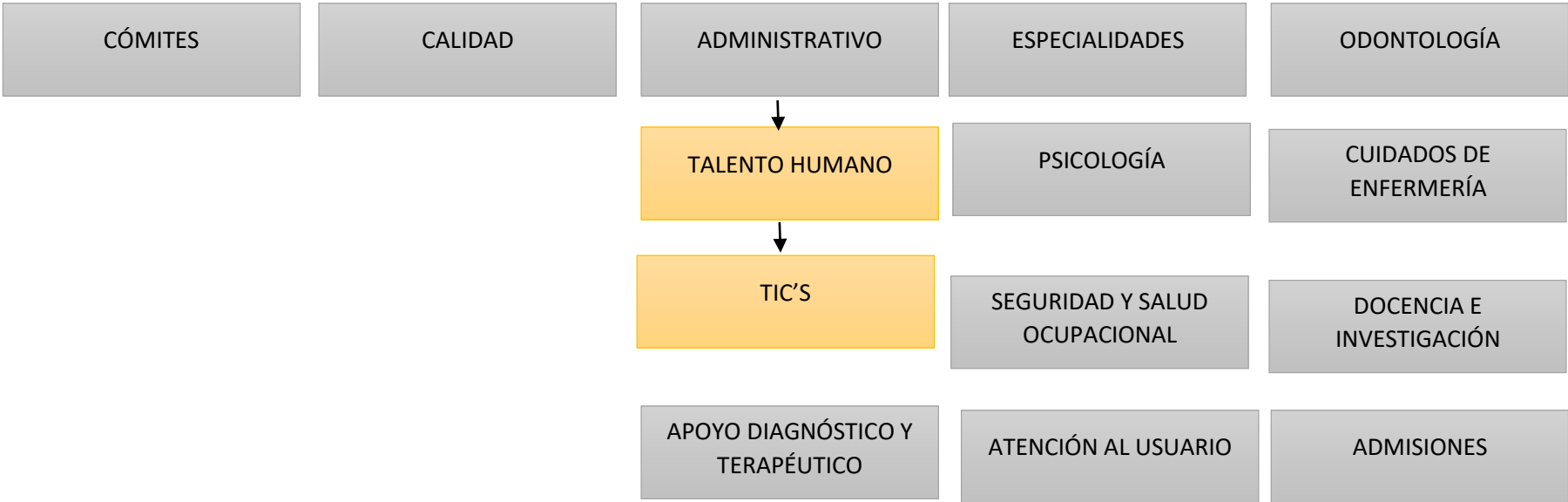
- [14] R. Abella Rubio, «COSO II y la gestión integral de riesgos del Negocio,» Estrategia Financiera, vol. 225, pp. 20-24, 2006.
- [15] J. R. Pinzón, «Metodología para identificación y valoración riesgos y salvaguardas en una mesa de ayuda tecnológica,» 2013.
- [16] H. Novoa, C. B.-P. e Investigación, and undefined 2015, «Metodologías para el análisis de riesgos en los sgsi,» hemeroteca.unad.edu.co.
- [17] C. Klüppelberg, D. Straub, and I. M. Welpé, Eds., Risk - A Multidisciplinary Introduction. Cham: Springer International Publishing, 2014.mx.
- [18] M. F. Molina-Miranda, Espirales: Revista Multidisciplinaria de Investigación, vol. 1, no. 11. [s.n.], 2017.
- [19] J. Vacca, «Computer and information security handbook,» 2012.
- [20] D. E. Sánchez Díaz y D. Eduardo, «Propuesta de seguridad alimentaria para mejorar el área operativa de la cocina en el Hospital de Catacocha,» 2017
- [20] Consuelo Belloch Ortí, «LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN (T.I.C.),» España/Valencia.
- [21] J. Sánchez and M. Ignoto, «La seguridad informática,» 1991.
- [22] E. G. Sánchez, «Calidad y seguridad de la información y auditoría informática,» 2009.
- [23] Y. Martínez, B. A.-... A. e Ingeniería, and undefined 2012, «Auditoría con informática a sistemas contables,» dialnet.unirioja.es.
- [24] R. Ruiz, El Método Científico y sus Etapas. Biblioteca Lascasas, 2007; 3(3), Available: <http://www.index-f.com/lascasas/documentos/lc0256.php>

## **11. Anexos**

### **ANEXO 1: Orgánico Estructural del Hospital de Catacocha**

DIRECCIÓN DISTRITAL  
11D03 Paltas-Salud

DIRECCIÓN HOSPITAL DE  
CATACOA





## **ANEXO 2. Resumen de la Entrevista**

## ENTREVISTA

**Fecha:** 13 de junio de 2018

**Nombre:** Ing. Juan Pablo Naranjo

**Departamento:** TIC's

**Objetivo:** Identificar los riesgos de TI en el Hospital de Catacocha.

### 1. La empresa cuenta con manuales:

Si existen manuales de:

- Manuales de usuario para QUIPUX
- Manuales para sistemas de comunicación
- Manuales de inducción (es para lo que ingresan por primera vez sobre la documentación que deben presentar)
- Manuales de Funciones (establecidos por el Ministerio mediante decreto 8520)
- Manual de manejo de correo institucional
- Manuales de Software Libre
- Manuales de sistemas que se manejan en el establecimiento que vienen directamente del Ministerio

### 2. Poseen planes de contingencia

No existen planes de contingencia

### 3. Que planes poseen en la institución

Lo que existe es:

- Planes de actualización de Equipo Informático
- Planes de mantenimiento preventivo y correctivo
- Planes de trabajo de todo el año

### 4. Realizan ustedes capacitaciones

Si se coordina con Talento Humano para capacitar

### 5. Poseen control en el Departamento de TICS

No existe control de acceso al Departamento ya que el presupuesto es limitado.

### 6. Hay antivirus en todas las computadoras

En los computadores nuevos si existe, algunos utilizan software libre y otros no tienen debido a que no existe presupuesto para adquirir licencias de antivirus.

### 7. Poseen algún software privativo

Si tenemos el SITAC para toda la parte contable

### 8. Realizan respaldos de información

Si se realiza respaldos de información en discos externos, pero solo se almacena la información de la fecha con que se realizó el mantenimiento

**9. A los equipos nuevos ustedes dan mantenimiento**

No a esos da la empresa donde se los adquirió mientras cubra la garantía

**10. La información que se maneja en el Departamento donde se almacena**

La información se encuentra en la nube y si se pierde se puede sincronizar en otro lado.

**11. Quien nomas tiene acceso a esa información**

A esa información tenemos acceso los que trabajamos en este Departamento y la dirección zonal cuando lo requiera.

**12. Realizan respaldo al servidor de correo**

Si se realiza el respaldo en disco duro externo y en la computadora de forma trimestral

**13. Cree que deben mejorar la infraestructura tecnológica**

Pues sería bueno, pero por el momento hay que conformarse con lo que hay

**14. Utilizan algún estándar para manipulación de información**

No existe por el momento

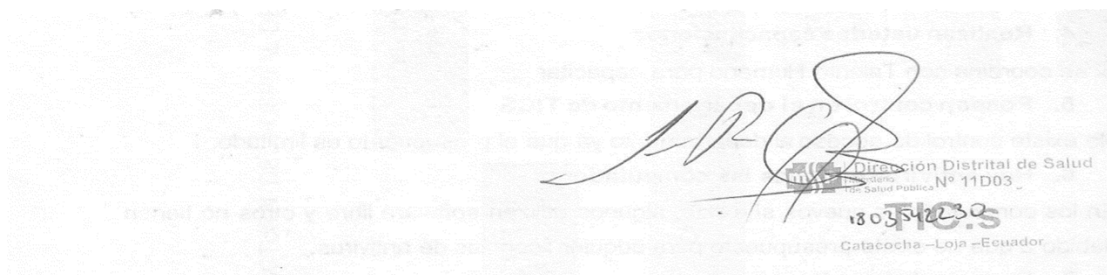
**15. Utilizan alguna norma**

Si solo se utiliza la norma para cableado estructurado

**16. Algún otro inconveniente que exista en el Departamento**

Los inconvenientes que tenemos son:

- No hay presupuesto para adquirir repuestos de computadores
- No hay seguridad perimetral

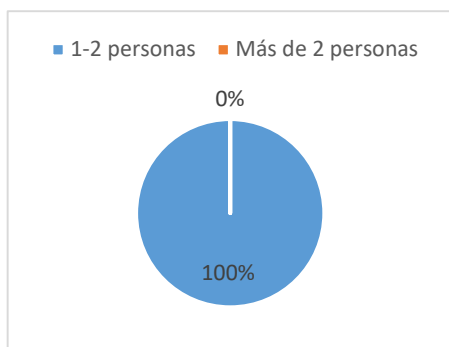


## **ANEXO 3. Interpretación de Encuestas**

### Interpretación de Encuesta realizada al Responsable del Departamento de Tic's

En la encuesta que se le realizo al encargado del Departamento de TIC'S del Hospital de Catacocha, se obtuvo lo siguiente:

#### Pregunta 1: ¿Cuántas personas trabajan en este Departamento?

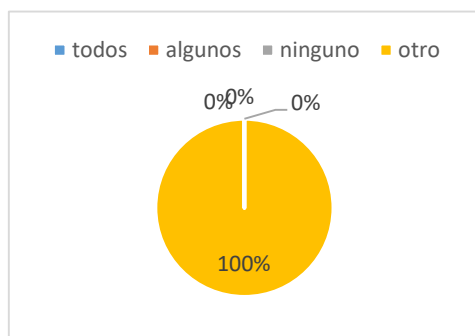


ÍTEMS	%
1-2 personas	100%
Más de 2 personas	0%

**Interpretación:** De los datos encuestados manifiesta que el 100% está entre 1-2 personas y un 0% de más de 2 personas trabajan en este Departamento.

**Análisis:** Del total de datos obtenidos manifiesta que trabajan 2 personas en su Departamento, por lo que puede ser vulnerable ya que la información que se maneja es confidencial.

#### Pregunta 2: ¿Sabe Ud. Si los programas (Ej: ¿antivirus), instalados en los equipos informáticos del Hospital de Catacocha poseen licencia?

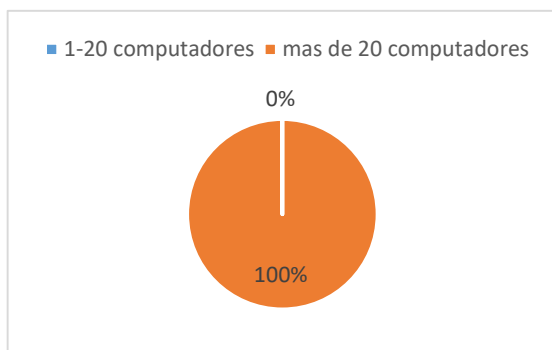


ÍTEMS	%
Todos	0%
Algunos	0%
Ninguno	0%
Otro	100%

**Interpretación:** De la encuesta realizada un 100% manifiesta que existe otra opción y un 0% menciona que todos, algunos y ninguno de los programas poseen licencias.

**Análisis:** Del total de datos se puede decir que existe una mayoría que plantea otra opción denominada "se utilizan versiones free" para los programas, ya que existe presupuesto limitado por tal razón podrían ser vulnerados y se debería implementar mecanismos de seguridad.

**Pregunta 3: ¿Cuántos computadores existen en el Hospital de Catacocha?**

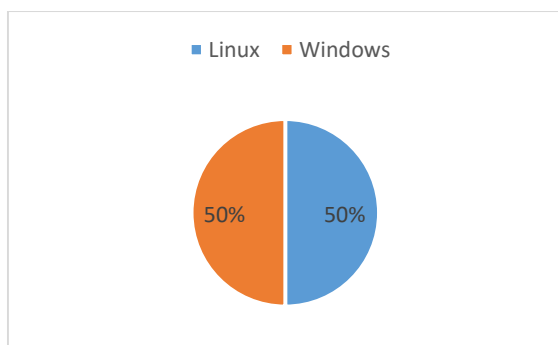


ÍTEMS	%
1-20 computadores	100%
Más de 20 computadores	0%

**Interpretación:** De la encuesta realizada un 100% manifiesta que existen más de 20 computadores y un 0% tiene de 1-20 computadores.

**Análisis:** De total de la encuesta realizada se puede decir que existen 45 computadores en el Hospital de Catacocha.

**Pregunta 4: ¿Esta Ud. Enterado que sistema Operativo se encuentra instalado en los computadores?**

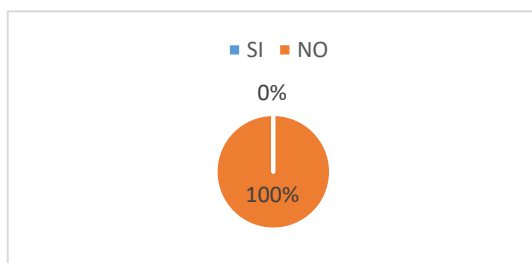


ÍTEMS	%
Linux	50%
Windows	50%

**Interpretación:** De la encuesta realizada se puede obtener un 50% utiliza Linux y otro 50% Windows para sus computadores.

**Análisis:** Del total de la encuesta se puede decir que utilizan los 2 sistemas operativos.

**Pregunta 5: ¿Se han registrado ataques informáticos (Ej: ¿virus, etc) dentro del Departamento?**

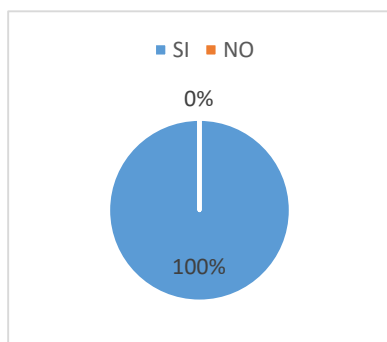


ÍTEMS	%
SI	0%
NO	100%

**Interpretación:** De la encuesta realizada un 100% manifestó que no se han registrado ataques informáticos y un 0% no menciona nada.

**Análisis:** Del total de la encuesta en su mayoría dicen que no ha sufrido ataques informáticos esto se debe también por el desconocimiento del factor humano.

**Pregunta 6: ¿Cree usted que la tecnología y los equipos que existen dentro del Departamento son suficientemente seguros y no sufrirán un ataque informático (Ej: ¿virus, etc)?**

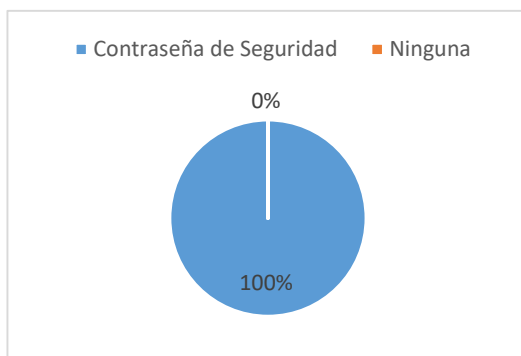


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** De la encuesta realizada un 100% menciona que, si son seguros los equipos y la tecnología, pero un 0% no dice nada.

**Análisis:** Del total de la encuesta en su mayoría dicen que si son seguros los equipos contra ataques informáticos.

**Pregunta 7: ¿Para acceder al computador destinada a sus labores diarias que tipo de seguridad utiliza usted?**

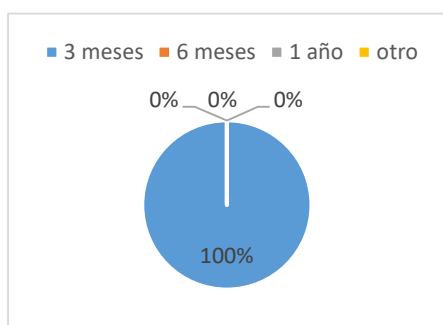


ÍTEMS	%
CONTRASEÑA DE SEGURIDAD	100%
NINGUNO	0%

**Interpretación:** De la encuesta realizada, el 100 % utiliza contraseñas de seguridad en su computador y un 0% no utiliza ningún mecanismo de seguridad.

**Análisis:** Del total de la encuesta la mayoría manifiesta que si tiene contraseñas de seguridad en el computador destinado a sus labores diarias y una minoría supo manifestar que no utiliza ningún mecanismo de seguridad, por lo que se hace falta implementar políticas de seguridad.

**Pregunta 8: ¿Cada que tiempo cambia la contraseña en su computador?**

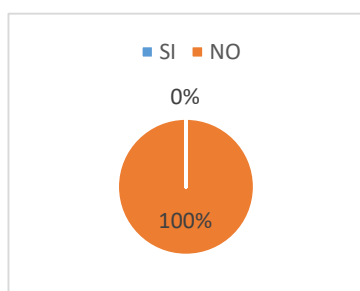


Tiempo	%
3 meses	100%
6 meses	0%
1 año	0%
Otro	0%

**Interpretación:** De la encuesta realizada manifiesta que un 100% cambia la contraseña cada 3 meses y un 0% en 6 meses, un año, otro.

**Análisis:** Del total de la encuesta se puede decir que en su mayoría se cambia cada 3 meses y eso es beneficioso para que no sean vulnerados.

**Pregunta 9: ¿Utiliza usted una misma contraseña de seguridad para acceder a todas sus cuentas personales?**

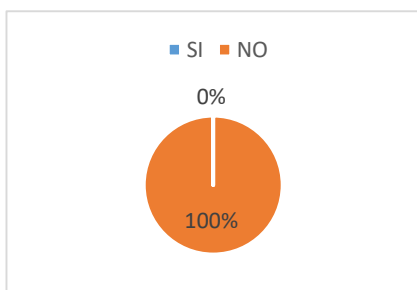


ÍTEM	%
SI	0%
NO	100%

**Interpretación:** De las personas encuestadas, el 100% de las personas asegura que no utiliza una misma contraseña de seguridad para el acceso a sus cuentas personales.

**Análisis:** El responsable del Departamento de TIC'S posee precauciones en cuanto a la utilización de claves.

**Pregunta 10: ¿Conoce Ud. ¿Si al momento de ingreso al Departamento se utiliza algún tipo de control para los visitantes?**



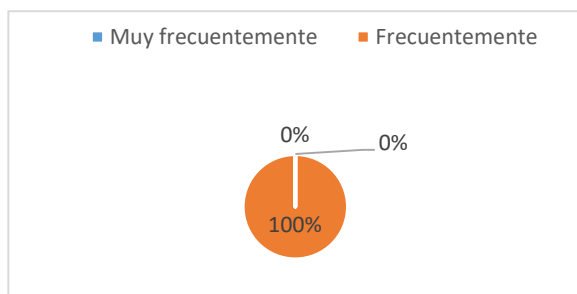
ÍTEM	%
SI	0%
NO	100%

**Interpretación:** De la encuesta realizada, el 100% afirma que no existe ningún tipo de seguridad física para los visitantes.



**Análisis:** Del total de los datos obtenidos afirman la existencia de una vulnerabilidad en cualquier tipo de ataque informático que requiera el acceso físico hacia un equipo.

**Pregunta 11: ¿Con qué frecuencia ingresan personas diferentes al Departamento?**

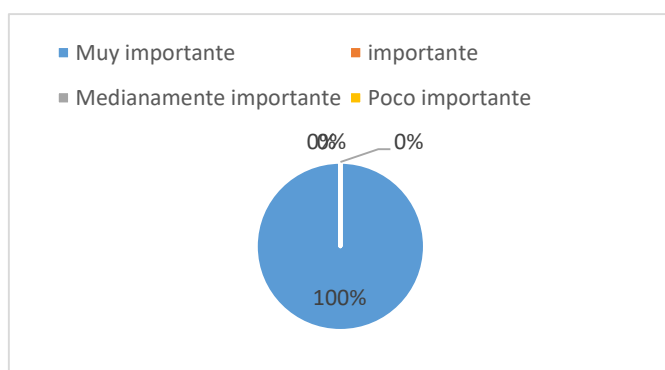


ÍTEMS	%
Muy frecuentemente	0%
Frecuentemente	100%
Poco frecuentemente	0%

**Interpretación:** De la encuesta realizada, el 100% afirma que se recibe a las personas de manera Frecuente dentro del Departamento y el 0% afirma que las personas ingresan muy frecuentemente y poco frecuentemente.

**Análisis:** Debido a la afluencia de gente es necesario establecer procesos para controlar esta afluencia.

**Pregunta 12: ¿Cómo clasifica usted la importancia de la información que maneja en el Departamento?**

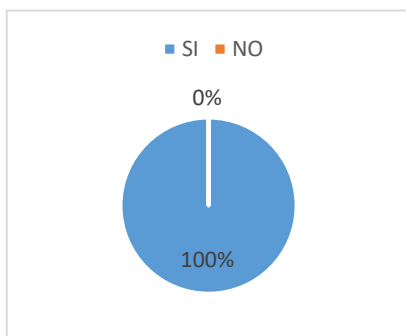


ÍTEMS	%
Muy importante	100%
importante	0%
Medianamente importante	0%
Poco importante	0%

**Interpretación:** De la encuestada realizada, el 100% considera que su información es Muy importante para el Departamento y el 0% considera que la información que maneja es Importante; Medianamente Importante, Poco Importante.

**Análisis:** Los datos obtenidos revelan la importancia de la información manejada dentro del Departamento.

**Pregunta 13: ¿Se realizan respaldos de la información?**

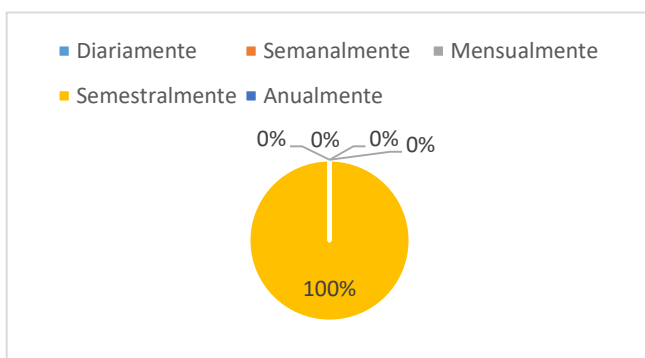


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** De la encuesta realizada se conoce que la información es respaldada.

**Análisis:** Del total de la encuesta se puede analizar que esta información es respaldada y se puede deducir que la información que es respaldada es almacenada de manera física.

**Pregunta 14: ¿Con qué frecuencia se realizan los respaldos?**

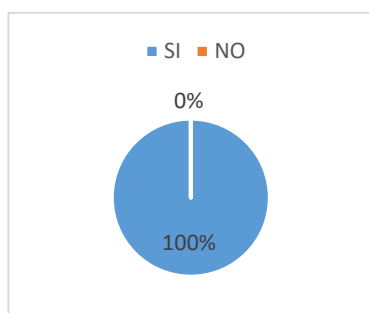


ÍTEMS	%
Diariamente	0%
Semanalmente	0%
Mensualmente	0%
Semestralmente	100%
Anualmente	0%

**Interpretación:** Según los datos obtenidos de la encuesta se obtiene que se realizan respaldos semestralmente.

**Análisis:** Del total de la encuesta se puede analizar que los períodos de respaldo de la información no liberan a la misma de un ataque informático.

**Pregunta 15: ¿Conoce usted cuáles son los procedimientos de seguridad que debe seguir en caso de que exista un ataque informático (Ej:virus, etc) dentro del Departamento?**

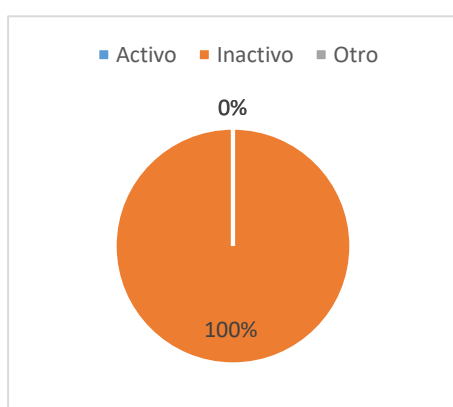


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** De la encuesta realizada, el 100% conoce sobre los procedimientos que se debe seguir en caso de que exista algún tipo de ataque informático y el 0% desconoce los procedimientos que se debe seguir en caso de que exista algún tipo de ataque informático.

**Análisis:** Del total de la encuesta podemos deducir que el Departamento de TIC'S posee un alto nivel de vulnerabilidad por la falta de procedimientos de prevención de ataques informáticos.

**Pregunta 16: ¿Cuándo un empleado deja de trabajar en la institución? ¿En qué estado se encuentran sus cuentas de usuario?**

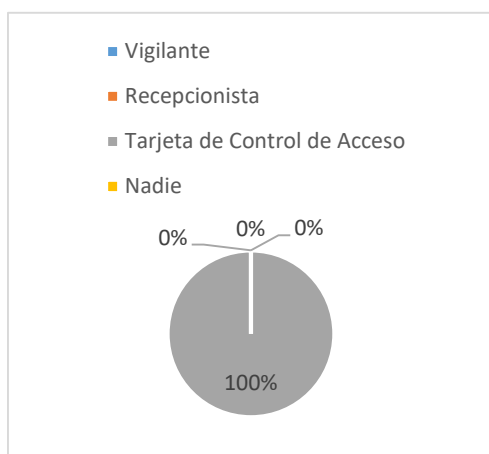


ÍTEMS	%
Activo	0%
Inactivo	100%
Otro	0%

**Interpretación:** De la encuesta realizada, el 100% pertenece a que el empleado se encuentra en estado Inactivo y el 0% se refiere al estado activo y otro estado.

**Análisis:** Del total de la encuesta se puede determinar que el responsable del Departamento inactiva al empleado cuando deja de trabajar.

**Pregunta 17: ¿Existe vigilancia en el DATACENTER las 24horas?**

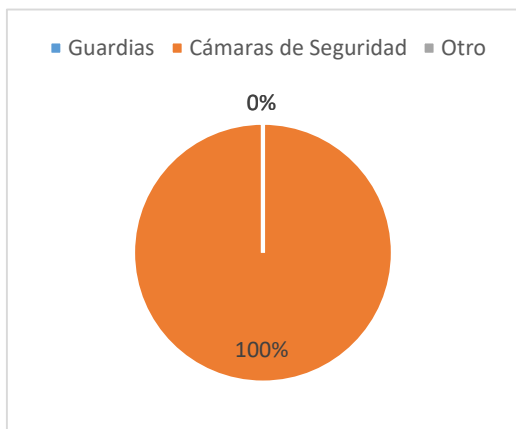


ÍTEMS	%
Vigilante	0%
Recepcionista	0%
Tarjeta de Control de Acceso	100%
Nadie	0%

**Interpretación:** De la encuesta realizada, el 100% menciona que se utiliza Tarjetas de control de acceso y el 0% se refiere a vigilante, recepcionista, nadie.

**Análisis:** Del total de la encuesta manifiestan que la vigilancia en el DATACENTER se la realiza con Tarjetas de control de acceso, pero para ello es importante realizar controles de acceso y políticas de seguridad.

**Pregunta 18: ¿Qué tipo de vigilancia existe en su Departamento?**

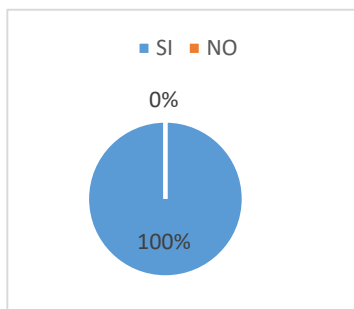


ÍTEM	%
Guardias	0%
Cámaras de Seguridad	100%
Otro	0%

**Interpretación:** De la encuesta realizada, el 100% dice que se utiliza cámaras de seguridad para la vigilancia del DATACENTER y el 0% hace referencia a guardias y otro recurso.

**Análisis:** Del total de la encuesta en su mayoría mencionan que utilizan cámaras de seguridad, pero se debe mejorar los mecanismos de seguridad para evitar ataques informáticos.

**Pregunta 19: ¿El DATACENTER se encuentra en un sitio seguro?**

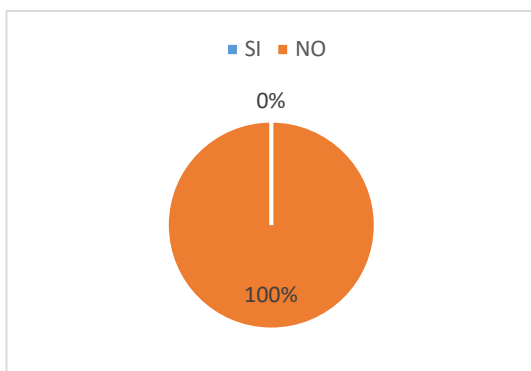


ÍTEM	%
SI	100%
NO	0%

**Interpretación:** De la encuesta realizada, el 100% dice que el Datacenter está en un lugar seguro y el 0% no dice nada.

**Análisis:** Del total de la encuesta realizada en su mayoría menciona que está en un sitio seguro, pero se debe implementar planes de contingencia que ayuden a mitigar los riesgos.

**Pregunta 20: ¿Tiene capacitaciones sobre planes de contingencia?**

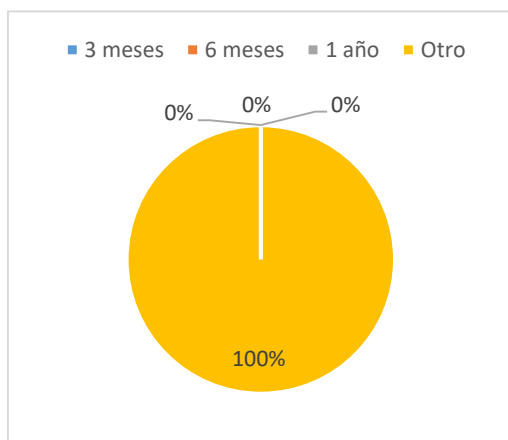


ÍTEM	%
SI	0%
NO	100%

**Interpretación:** De la encuesta realizada, el 100% dice que no tienen capacitaciones y el 0% manifiesta que si tienen.

**Análisis:** Del total de la encuesta realizada en su mayoría menciona que no tienen capacitaciones por lo que se debe implementar planes de contingencia que ayuden a mitigar los riesgos.

**Pregunta 21: ¿Cada que tiempo tienen capacitaciones sobre seguridad y planes de contingencia?**

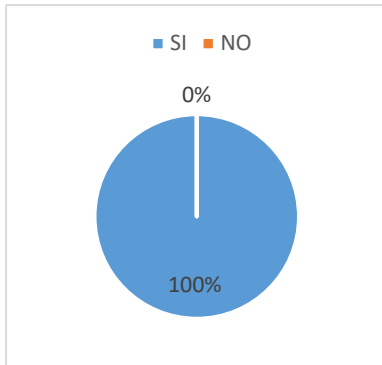


Tiempo	%
3 meses	0%
6 meses	0%
1 año	0%
Otro	100%

**Interpretación:** De la encuesta realizada, el 100% dice que las capacitaciones únicamente es autoeducación sobre este tema y el 0% manifiesta que se realizan en 3 meses, 6 meses, 1 año.

**Análisis:** Del total de la encuesta realizada en su mayoría menciona que no tienen capacitaciones sobre este tema por lo que se debe implementar planes de contingencia que ayuden a mitigar los riesgos y políticas de seguridad.

**Pregunta 22: ¿Ud. Sabe si existe sistema de aire acondicionado en el DATACENTER?**

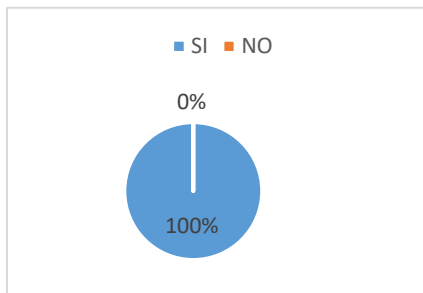


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** Según la entrevista realizada, el 100% manifiesta que si existe sistema de aire acondicionado en el DATACENTER.

**Análisis:** Del total de la encuesta realizada podemos decir que el DATACENTER si posee sistema de ventilación.

**Pregunta 23: ¿La capacidad de memoria y de almacenamiento del servidor es suficiente para atender los procesos que se llevan a cargo en el Hospital?**

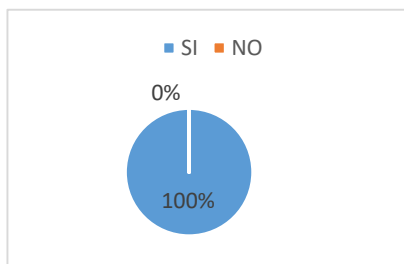


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** Según la entrevista realizada, el 100% manifiesta que si existe capacidad de memoria y de almacenamiento en el servidor para atender los procesos.

**Análisis:** Del total de la encuesta realizada podemos decir que el servidor es suficiente para atender los procesos que se llevan a cabo en el Hospital, ya que actualmente no se tiene mucha información, pero es necesario realizar planes de seguridad.

**Pregunta 24: ¿Conoce usted si existe generador en caso de que el suministro de energía sea interrumpido?**



ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** Según la entrevista realizada, el 100% dice que si existe generador de energía y un 0% no manifiesta nada.

**Análisis:** Del total de la encuesta realizada podemos decir que gracias al generador los procesos que se llevan en la institución no se pierden porque esta tecnología le permite al regulador emitir una corriente eléctrica estable que neutraliza la vulnerabilidad de tus aparatos eléctricos

**Pregunta 25: ¿Cómo registran la asistencia?**

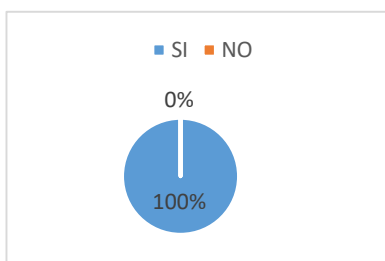


ÍTEMS	%
Reloj Biométrico	100%
Reconocimiento Facial	0%
Otro	0%

**Interpretación:** De la entrevista realizada, el 100% se refiere a que utilizan Reloj biométricos para registrar la asistencia y un 0% dice que registran con reconocimiento facial y otra opción.

**Análisis:** Del total de la encuesta realizada podemos decir que en su mayoría utilizan el Reloj Biométrico, pero es necesario implementar mecanismos de seguridad y control que ayuden a mitigar riesgos.

**Pregunta 26: ¿Poseen en el Hospital de Catacocha políticas de seguridad informática?**

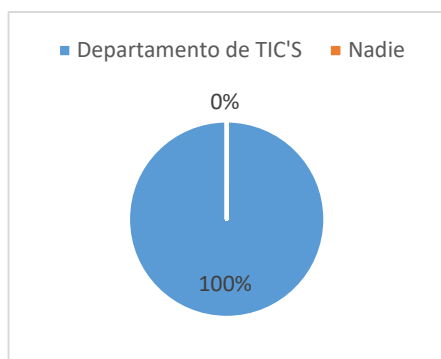


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** De la encuesta realizada, el 100% menciona que si poseen políticas de seguridad y el 0% no pronuncia nada.

**Análisis:** Del total de la encuesta realizada menciona que, si poseen políticas de seguridad informática, pero estas pueden mejorarse incluyendo más mecanismos de seguridad y control.

**Pregunta 27: ¿Quién es el responsable de la administración de cuentas de usuario y cuando se crean las cuentas a los empleados?**



ÍTEMS	%
Departamento de TIC'S	100%
Nadie	0%

**Interpretación:** De la encuesta realizada, el 100% menciona que el Departamento de TICS se encarga de respaldar información y bloquear cuentas de usuarios y el 0% nadie realiza este proceso.

**Análisis:** Del total de la encuesta realizada menciona que es su mayoría el Departamento de TIC'S se encarga de eso procesos ya que no existen mecanismos de control y seguridad en la información.

**Interpretación de encuesta realizada a los encargados de los otros Departamentos**

En la encuesta que se aplicó a 7 encargados de los Departamentos del Hospital de Catacocha, se obtuvo lo siguiente:

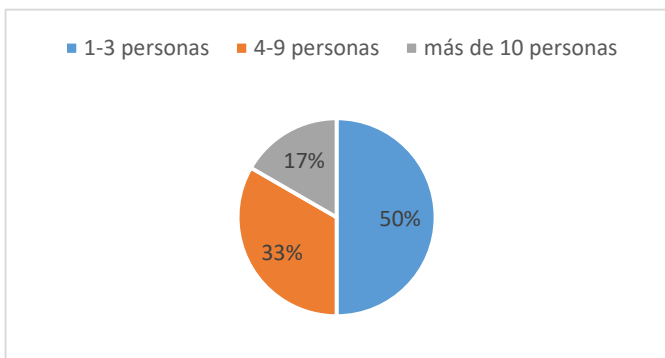
**Pregunta 1: ¿Cuál es el cargo que desempeña en la institución?**

**Interpretación:** Del total de encuestados mencionan que los cargo que desempeñan es de Técnico de Mantenimiento, Médico Ocupacional, Enfermera, Analista de Talento Humano, Analista de Calidad, Tecnóloga en Fisiología e Imagen, Bioquímica.

**Análisis:** Del total de datos obtenidos podemos determinar que cada responsable desempeña su función en dicho Departamento.



**Pregunta 2: Cuántas personas trabajan en su Departamento?**

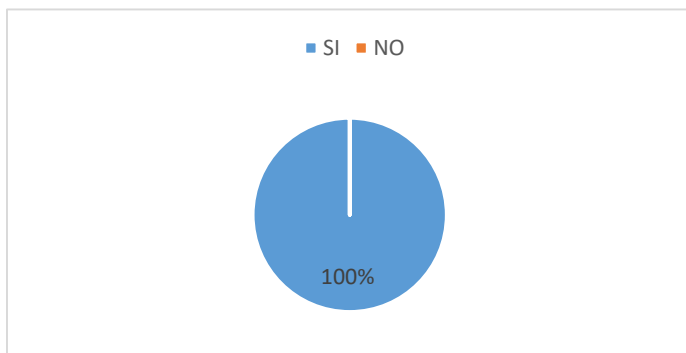


ÍTEMS	%
1-3 personas	50%
4-9 personas	33%
Más de 10	17%

**Interpretación:** De las personas encuestadas, el 50% menciona que trabajan de 1-3 personas, el 33% pertenece a que el número de personas es de 4-9 y el 17% posee un número mayor a 10 de personas que laboran en su Departamento.

**Análisis:** De total de datos obtenidos podemos determinar que existen mínimo 2 personas trabajando en cada Departamento y que esto podría ser factor de riesgo ya que podrían ser una amenaza que evidencie vulnerabilidades.

**Pregunta 3: Considera usted que el Departamento de TIC'S brinda los resultados esperados?**

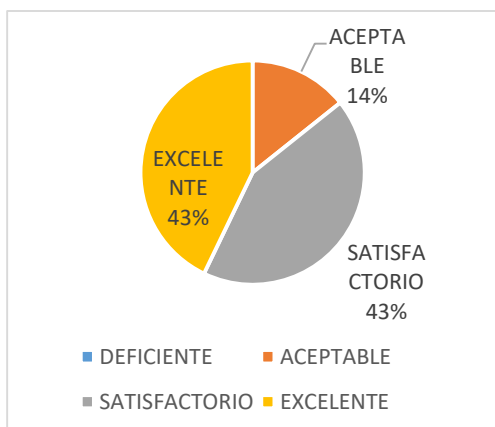


ÍTEMS	%
SI	100%
NO	0%

**Interpretación:** De las personas encuestadas, el 100% menciona que el Departamento de TIC'S brinda los resultados esperados y un 0% no brinda los resultados esperados.

**Análisis:** Del Total de datos obtenidos podemos determinar que los encargados de dichos Departamentos están agradecidos con los resultados que presentan los del Departamento de Tics.

**Pregunta 4: ¿Cómo considera usted al servicio proporcionado por el Departamento de TICs?**

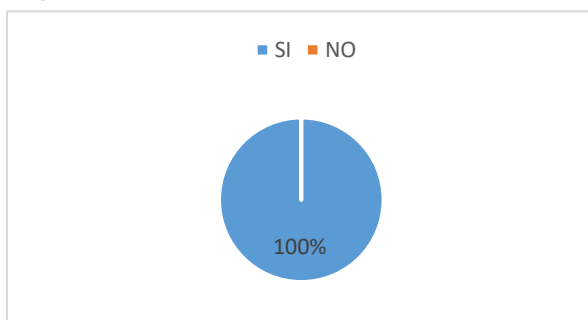


ÍTEM	%
DEFICIENTE	0%
ACEPTABLE	14%
SATISFACTORIO	43%
EXCELENTE	43%

**Interpretación:** De las personas encuestadas, el 43% menciona que los servicios proporcionados por el Departamento de TIC'S son excelentes y el 43% expresa que son satisfactorios y un 14% dice que son Aceptable y un 0% el servicio es deficiente.

**Análisis:** Del total de datos obtenidos el 43 % manifiesta que el servicio proporcionado por el Departamento es excelente o satisfactorio, pero existe una % menor que menciona que se puede mejorar.

**Pregunta 5: Hay disponibilidad en el Departamento de TIC's para sus requerimientos?**

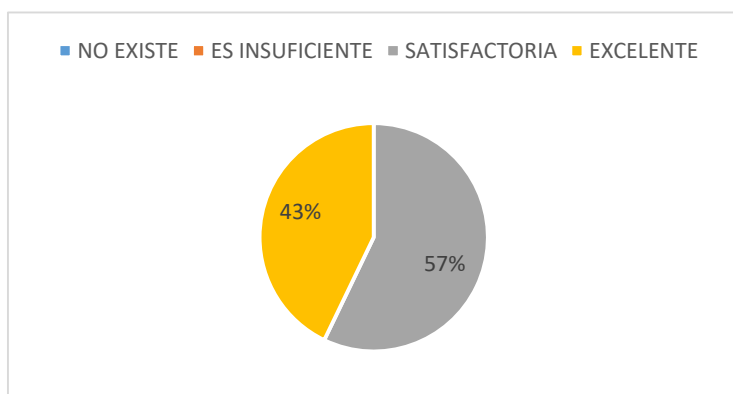


ÍTEM	%
SI	100%
NO	0%

**Interpretación:** De las personas encuestadas, el 100% menciona hay disponibilidad Departamento de TIC'S en cuanto a sus requerimientos y un 0% no manifiesta nada.

**Análisis:** De los datos obtenidos podemos determinar que los encargados de dichos Departamentos mencionan que si existe disponibilidad por parte del Departamento de TIC'S.

**Pregunta 6: Qué opina usted de la asesoría que imparte el Departamento de TIC's?**

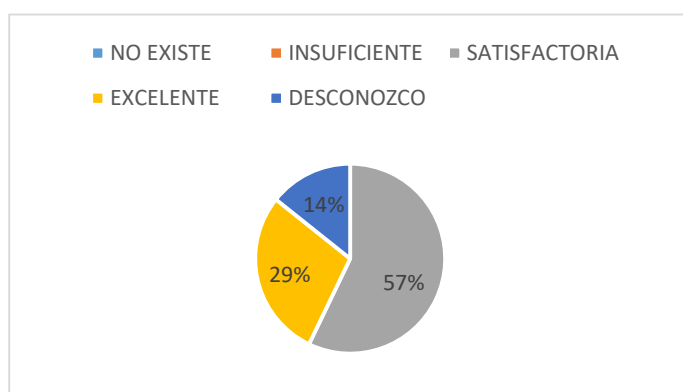


ÍTEMS	%
NO EXISTE	0%
ES INSUFICIENTE	0%
SATISFACTORIO	57%
EXCELENTE	43%

**Interpretación:** De las personas encuestadas, el 57 % menciona que la asesoría del Departamento de TIC'S es Satisfactoria, un 43 % dice que es excelente y un 0% manifiesta que no existe o que es insuficiente.

**Análisis:** La mayoría de los datos obtenidos determina que la asesoría brindada en el Departamento de TIC'S es excelente.

**Pregunta 7: Qué opina usted de la seguridad en el manejo de información proporcionada por el sistema que utiliza?**

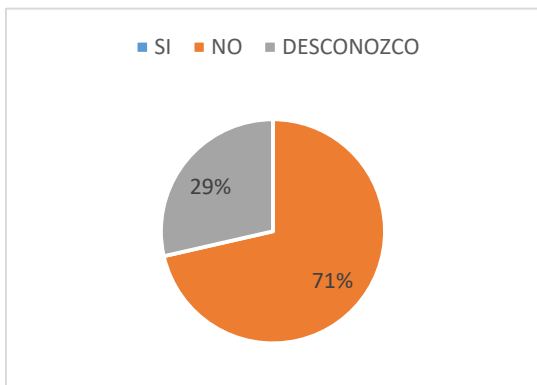


ÍTEMS	%
NO EXISTE	0%
INSUFICIENTE	0%
SATISFACTORIA	57%
EXCELENTE	29%
DESCONOZCO	14%

**Interpretación:** De las personas encuestadas, el 57 % opina que la seguridad en el manejo de información es satisfactoria, el 14% Desconoce, el 29% menciona que es excelente en cuanto a la seguridad en el manejo de información y un 0% dice que es Insuficiente o que no existe seguridad en el manejo de información proporcionada por el sistema.

**Análisis:** La mayoría de los encuestados determina que la seguridad en el manejo de información proporcionada por el sistema que utiliza es Satisfactoria, pero existe un % menor que se puede mejorar.

**Pregunta 8: ¿Conoce usted si la información que está bajo su responsabilidad ha sido alterada?**

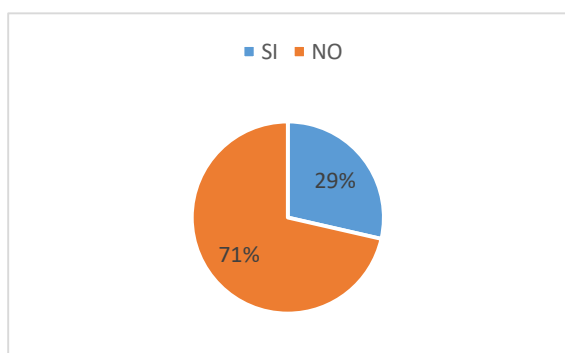


ÍTEM	%
SI	0%
NO	71%
DESCONOZCO	29%

**Interpretación:** Del total de los encuestados, el 71 % menciona que no saben si su información está siendo alterada y un 29% desconoce este tema.

**Análisis:** De los datos obtenidos podemos determinar que la mayoría de los encuestados no conocen si su información que está bajo su responsabilidad ha sido alterada por lo que pueden existir ataques informáticos y que estas personas lo estén desconociendo.

**Pregunta 9: Conoce usted si existen Manuales de Usuario del sistema?**

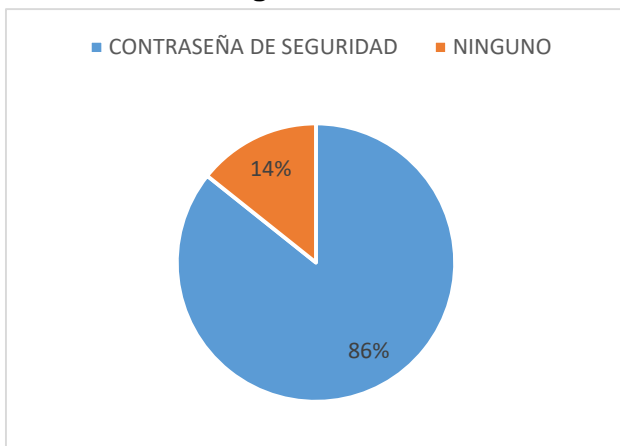


ÍTEM	%
SI	29%
NO	71%

**Interpretación:** Del total de los encuestados, el 71 % menciona que no conoce si existen manuales de usuario y un 29 % restante si tiene conocimiento.

**Análisis:** Del total de los encuestados podemos determinar que en su mayoría desconocen los manuales de usuario y existe una minoría los cuales manifestaron que si tienen conocimiento de que existen manuales, razón por la cual hace falta manuales de políticas y procedimientos.

**Pregunta 10: Para el acceso al computador asignado a sus labores diarias que mecanismo de seguridad, utiliza:**

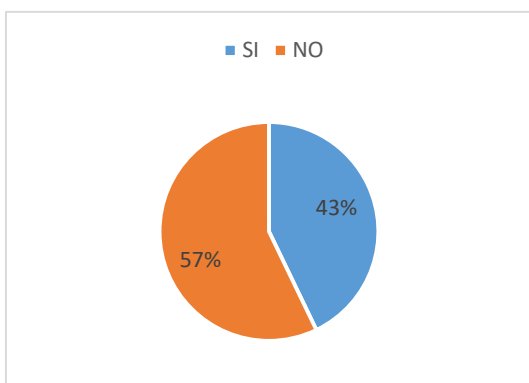


ÍTEMS	%
CONTRASEÑA DE SEGURIDAD	86%
NINGUNO	14%

**Interpretación:** De las personas encuestadas, el 86 % utiliza contraseñas de seguridad en sus computadores y un 14% no utiliza ningún mecanismo de seguridad.

**Análisis:** Del total de los encuestados la mayoría manifiestan que si tienen contraseñas de seguridad en los computadores que realizan sus labores diarias y una minoría supo manifestar que no utiliza ningún mecanismo de seguridad, por lo que se hace falta implementar políticas de seguridad.

**Pregunta 11: ¿Ha compartido alguna vez su contraseña de seguridad con alguna persona de su confianza?**

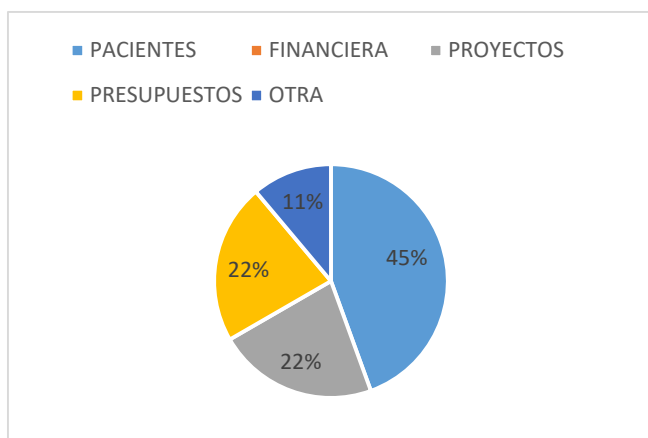


ÍTEMS	%
SI	43%
NO	57%

**Interpretación:** De las personas encuestadas, el 57 % no comparte su contraseña de seguridad con nadie y un 43% si comparte la contraseña.

**Análisis:** Del total datos obtenidos, un poco más de la mitad de los encuestados manifiesta que no comparte su contraseña de seguridad y existe % que se acerca a la mitad de los encuestados que, si comparte su contraseña, razón por la cual corren el riesgo de ser atacados por hackers.

**Pregunta 12: Qué tipo de información maneja en su Departamento?**

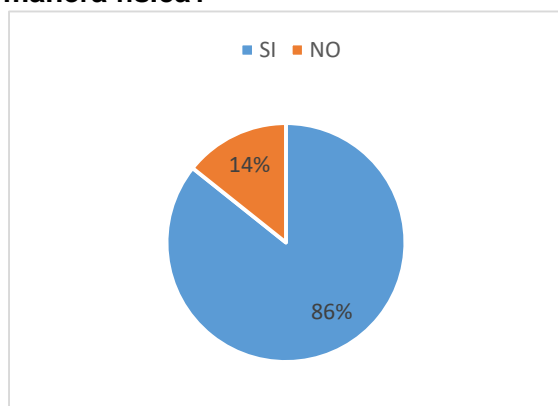


ÍTEM	%
PACIENTES	45%
FINANCIERA	0%
PROYECTOS	22%
PRESUPUESTOS	22%
OTRA	11%

**Interpretación:** De las personas encuestadas, el 45 % maneja información de Pacientes, 0% Financiera; 22% Proyectos y Presupuestos y un 11% Otro tipo de información.

**Análisis:** Del total de datos obtenidos podemos determinar que los encargados de dichos Departamentos manejan información confidencial referentes a Pacientes que pueden ser vulneradas por entes externos, para prevenir esto se debe aplicar mecanismos de seguridad informática.

**Pregunta 13: ¿La información que maneja en su Departamento es guardada de manera física?**

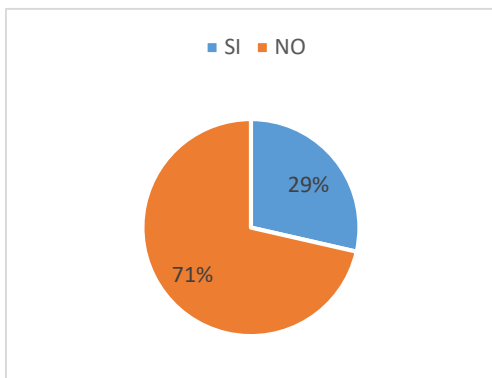


ÍTEM	%
SI	86%
NO	14%

**Interpretación:** De las personas encuestadas, el 86 % menciona que la información la guardan de manera física y un 14% manifiesta que no lo hacen.

**Análisis:** Del total de datos obtenidos podemos determinar que en su mayoría los encargados de dichos Departamentos mantienen almacenada la información de manera física en caso de existir algún tipo de ataque informático, pero cabe mencionar que aún existe una minoría que no lo hace, por lo cual pueden ser vulnerados ya que no cuentan con políticas de seguridad u mecanismos de protección de la información.

**Pregunta 14: Conoce usted si existen licencias en los programas de sus computadores?**

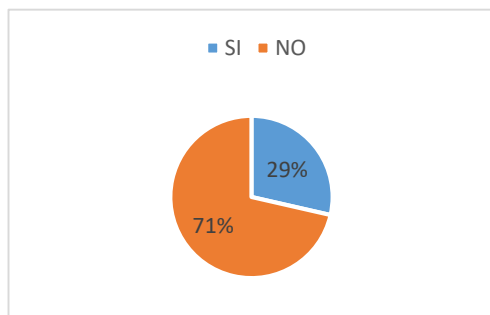


ÍTEM	%
SI	0%
NO	100%

**Interpretación:** De las personas encuestadas, el 100 % desconoce si existen licencias en los programas de sus computadores.

**Análisis:** De total de datos obtenidos podemos determinar que los encargados de dichos Departamentos pueden ser vulnerados diariamente ya que no cuentan con procedimientos y herramientas de seguridad y privacidad de la organización.

**Pregunta 15: ¿Conoce Ud. ¿Si existen programas que sean espías que puedan capturar todas las acciones que realiza en su computador y la información que se transmiten por la red?**

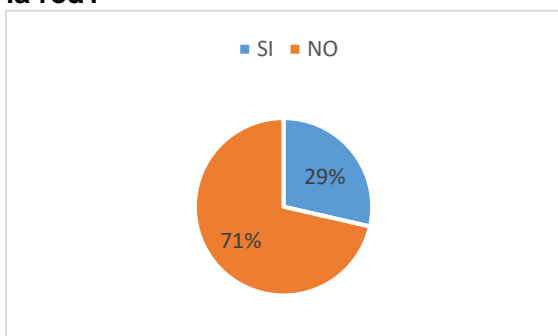


ÍTEM	%
SI	14%
NO	86%

**Interpretación:** Del total de las personas encuestadas, el 86 % desconoce Si existen programas que pueden espías que puedan capturar todas las acciones que realiza en su computador y la información que se transmiten por la red y un 14% si conoce sobre esta temática.

**Análisis:** De total de datos obtenidos podemos determinar que la mayoría desconoce, pero existe un % menor que se debe concientizar ya que con esto pueden poseer un alto nivel de vulnerabilidad debido a que no poseen procesos que les ayuden a prevenir estos ataques informáticos.

**Pregunta 16: ¿Conoce Ud. ¿Si sus correos electrónicos o cuentas personales están protegidos contra robo, pérdida y espionaje de la información cuando usa la red?**

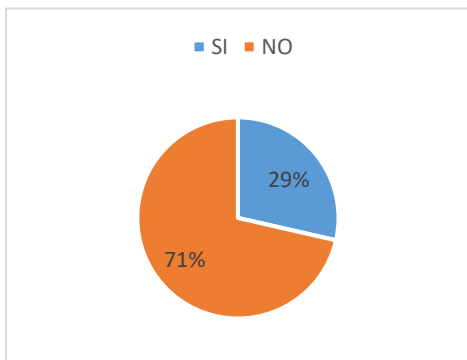


ÍTEM	%
SI	14%
NO	86%

**Interpretación:** De las personas encuestadas, el 86 % desconoce si sus correos electrónicos o cuentas personales están protegidos contra robo, pérdida y espionaje de la información cuando usa la red y un 14% si tiene conocimiento sobre el tema.

**Análisis:** De total de datos obtenidos podemos determinar que en su mayoría desconocen sobre el tema, pero existe una minoría que se debe orientar para que no sean víctimas de ataques informáticos ya que no cuentan con procedimientos de prevención de ataques informáticos.

**Pregunta 17: Conoce Ud. las políticas de seguridad de la información y de la red?**



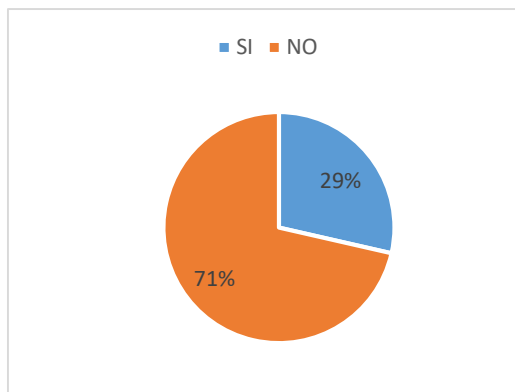
ÍTEM	%
SI	29%
NO	71%

**Interpretación:** De las personas encuestadas, el 71 % no conoce las políticas de seguridad de la información y de la red y un 29% si tiene conocimiento sobre el tema abordado.

**Análisis:** Del total de datos obtenidos podemos determinar que existe una mayoría que desconoce las políticas de seguridad de la información, pero cabe mencionar que hay una minoría que, si tiene conocimiento, por lo tanto, están inmersos a ser vulnerados porque no existen políticas de seguridad en cuanto a la información y a la seguridad de la red.



**Pregunta 18: ¿Conoce Ud. la existencia de sitios web seguros (https) que evitan que la información y claves utilizadas puedan ser plagiadas?**



ÍTEMS	%
SI	29%
NO	71%

**Interpretación:** De las personas encuestadas, el 71 % no conoce la existencia de sitios web seguros y un 29% si tiene conocimiento de este tema.

**Análisis:** Del total de los datos obtenidos podemos determinar que existe una mayoría que desconoce la existencia de sitios web seguros, pero cabe destacar que existe una minoría que, si conoce, por lo que pueden ser vulnerados debido a que no existen procedimientos para prevención de ataques informáticos.

## **ANEXO 4. Encuestas**



**UNIVERSIDAD  
NACIONAL  
DE LOJA**

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO  
RENOVABLES



CARRERA DE INGENIERÍA EN SISTEMAS

ENCUESTA N°1

"PLAN DE GESTIÓN DE RIESGOS DE TI EN EL HOSPITAL DE CATACOCCHA"

Fecha: 23 de Mayo de 2018

Nombre: Ing. Juan Pablo Narango

Departamento: ...T.I.C.S. ....

Objetivo: Identificar los riesgos de TI en el Hospital de Catacocha.

Como estudiante de la Universidad Nacional de Loja perteneciente a la Carrera de Ingeniería en Sistemas, cuyo proyecto titulado "PLAN DE GESTION DE RIESGOS DE TI EN EL HOSPITAL DE CATACCHA", solicito a su Usted me colabore con la presente encuesta.

1. Cuántas personas trabajan en este departamento?

... Dos .....

2. Sabe Ud. Si los programas (Ej: antivirus) instalados en los equipos informáticos del Hospital de Catacocha poseen licencia?

Todos ( )

Algunos ( )

Ninguno ( )

Otro... Se utilizan versiones free / Presupuesto limitado .....

3. Cuántos computadores existen en el hospital de Catacocha?

... 45 .....

4. Esta Ud. enterado que sistema Operativo se encuentra instalado en los computadores?

Linux (✓)

Windows (✓)

Otro.....

5. ¿Se han registrado ataques informáticos (Ej:virus,etc) dentro del departamento?

SI ( )

NO (✓)

6. ¿Cree usted que la tecnología y los equipos que existen dentro del departamento son suficientemente seguros y no sufrirán un ataque informático (Ej:virus, etc)?

SI (✓)

NO ( )

Porque.....

7. Para acceder al computador destinada a sus labores diarias que tipo de seguridad utiliza usted?

Contraseña de Seguridad (✓)

Ninguna ( )

Otros.....

8. ¿Cada que tiempo cambia la contraseña en su computador?

3 meses (✓)

6 meses ( )

1 año ( )

Otros.....



**UNIVERSIDAD  
NACIONAL  
DE LOJA**

*FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO  
RENOVABLES*



*CARRERA DE INGENIERÍA EN SISTEMAS*

9. ¿Utiliza usted una misma contraseña de seguridad para acceder a todas sus cuentas personales?

SI ( )  
NO (✓)

10. ¿Conoce Ud. Si al momento de ingreso al Departamento se utiliza algún tipo de control para los visitantes?

SI ( )  
NO (✓)

11. ¿Con qué frecuencia ingresan personas diferentes al Departamento?

Muy Frecuente ( )  
Frecuente (✓)  
Poco Frecuente ( )

12. ¿Cómo clasifica usted la importancia de la información que maneja en el Departamento?

Muy Importante (✓)  
Importante ( )  
Medianamente Importante ( )  
Poco Importante ( )

13. ¿Se realizan respaldos de la información?

SI (✓)  
NO ( )

14. ¿Con qué frecuencia se realizan los respaldos?

Diariamente ( )  
Semanalmente ( )  
Mensualmente ( )  
Semestralmente (✓)  
Anualmente ( )

15. Conoce usted cuáles son los procedimientos de seguridad que debe seguir en caso de que exista un ataque informático (Ej:virus, etc) dentro del departamento?

SI (✓)  
NO ( )

16. ¿Cuándo un empleado deja de trabajar en la institución . En que estado se encuentran sus cuentas de usuario?

Activo ( )  
Inactivo (✓)  
Otros.....

17. Existe vigilancia en el DATACENTER las 24horas?

Vigilante ( )  
Recepcionista ( )  
Tarjeta de control de acceso (✓)  
Nadie ( )



**UNIVERSIDAD  
NACIONAL  
DE LOJA**

FACULTAD DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO  
RENOVABLES



CARRERA DE INGENIERÍA EN SISTEMAS

18. Qué tipo de vigilancia existe en su Departamento?

- Guardias   
Cámaras de seguridad   
Otros.....

19. El DATACENTER se encuentra en un sitio seguro?

- SI   
NO

20. Tiene capacitaciones sobre planes de contingencia?

- SI   
NO

21. Cada que tiempo tienen capacitaciones sobre seguridad y planes de contingencia?

- 3 meses   
6 meses   
1 año   
Otro. Únicamente autoeducación sobre este tema.....

22. Ud. Sabe si existe sistema de aire acondicionado en el DATACENTER?

- SI   
No

23. La capacidad de memoria y de almacenamiento del servidor es suficiente para atender los procesos que se llevan a cargo en el Hospital?

- SI   
NO

24. Conoce usted si existe generador en caso de que el suministro de energía sea interrumpido?

- SI   
NO

25. Como registran la asistencia?

- Reloj Biométrico   
Reconocimiento Facial   
Otros.....

26. Poseen en el Hospital de Catacocha políticas de seguridad informática?

- SI   
NO

27. Quién es el responsable de la administración de cuentas de usuario y cuando se crean las cuentas a los empleados?

La Unidad de TICS, quien se encarga de respaldar información y bloquear cuentas.....

Gracias por su colaboración

18/05/2023

## ENCUESTA N°2

Fecha: .....

Nombre: .....

Departamento: .....

**Objetivo:** Identificar los riesgos de TI en el Hospital de Catacocha.

Como estudiante de la Universidad Nacional de Loja perteneciente al X Ciclo de la Carrera de Ingeniería en Sistemas, cuyo proyecto titulado "PLAN DE GESTION DE RIESGOS DE TI EN EL HOSPITAL DE CATACOCHA", solicito a usted me colabore con la presente encuesta.

1. **Cuál es el cargo que desempeña en la institución?**  
.....
2. **Cuántas personas trabajan en su Departamento?**  
.....
3. **Considera usted que el Departamento de TIC'S brinda los resultados esperados?**  
SI ( )  
NO ( )  
Porqué? .....
4. **Cómo considera usted al servicio proporcionado por el Departamento de TIC's?**  
Deficiente ( )  
Aceptable ( )  
Satisfactorio ( )  
Excelente ( )  
Porqué? .....
5. **Hay disponibilidad en el Departamento de TIC's para sus requerimientos?**  
SI ( )  
NO ( )  
Ocasionalmente ( )
6. **Qué opina usted de la asesoría que imparte el Departamento de TIC's?**  
No existe ( )  
Es insuficiente ( )  
Satisfactoria ( )  
Excelente ( )  
Porqué? .....
7. **Qué opina usted de la seguridad en el manejo de información proporcionada por el sistema que utiliza?**  
No existe ( )  
Insuficiente ( )  
Satisfactoria ( )  
Excelente ( )  
Desconozco ( )  
Porqué? .....
8. **¿Conoce usted si la información que está bajo su responsabilidad ha sido alterada?**  
SI ( )  
NO ( )  
Desconozco ( )  
Cómo ha sido alterada?.....

9. **Conoce usted si existen Manuales de Usuario del sistema?**  
 SI ( )  
 NO ( )
10. **Para el acceso al computador asignado a sus labores diarias que mecanismo de seguridad, utiliza:**  
 Contraseña de Seguridad ( )  
 Ninguno ( )
11. **¿Ha compartido alguna vez su contraseña de seguridad con alguna persona de su confianza?**  
 SI ( )  
 NO ( )
12. **Qué tipo de información maneja en su Departamento?**  
 Pacientes ( )  
 Financiera ( )  
 Proyectos ( )  
 Presupuestos ( )  
 Otra.....
13. **¿La información que maneja en su Departamento es guardada de manera física?**  
 SI ( )  
 NO ( )  
 Desconozco ( )
14. **Conoce usted si existen licencias en los programas de sus computadores?**  
 SI ( )  
 NO ( )  
 Desconozco ( )
15. **¿Conoce Ud. Si existen programas que pueden espías que puedan capturar todas las acciones que realiza en su computador y la información que se transmiten por la red?**  
 SI ( )  
 NO ( )  
 Desconozco ( )
16. **¿Conoce Ud. Si sus correos electrónicos o cuentas personales están protegidos contra robo, pérdida y espionaje de la información cuando usa la red?**  
 SI ( )  
 NO ( )  
 Desconozco ( )
17. **Conoce Ud. las políticas de seguridad de la información y de la red?**  
 SI ( )  
 NO ( )  
 Desconozco ( )
18. **¿Conoce Ud. la existencia de sitios web seguros (https) que evitan que la información y claves utilizadas puedan ser plagiadas?**  
 SI ( )  
 NO ( )  
 Desconozco ( )

Gracias por su colaboración (Firma.....)

## **ANEXO 5. Certificado de Participación en COISINT 2019**





Pontificia Universidad  
Católica del Ecuador  
Sede Ibarra



UNIVERSIDAD TÉCNICA  
FEDERICO SANTA MARÍA



Otorgan el Presente

# Certificado

A: JOHANNA ELIZABETH RIVERA SERRANO

Por haber asistido en calidad de participante en el "II Congreso Internacional de Sistemas Inteligentes y Nuevas Tecnologías: Tendencias Interdisciplinarias en Comunicación", realizado del 8 al 10 de mayo de 2019, con una duración de 24 horas académicas.

Ibarra, mayo de 2019

Ph. D. María José Rubio Gómez  
PRORRECTORA DE LA PUCE-SI

Ph. D. Franklin Rivas Echeverría  
PRESIDENTE DEL COISINT II 2019



## **ANEXO 6. Matriz Inherente y Matriz Residual**

TABLA XVII. MATRIZ INHERENTE DEL DEPARTAMENTO DE TIC's

	PROCESO	LIDER PROCESO	TIPIFICACIÓN RIESGO	RIESGO EVALUADO	OBSERVACIÓN	CRITICIDAD	VULNERABILIDAD	IMPACTO	VOTO / CARGOS	Calificación Funcionario Nro. 1 (Cargo)	Calificación Funcionario Nro. 2 (Cargo)	Calificación Funcionario Nro. 3 (Cargo)	Controles Existentes	Control Sugerido
R1	Gestión de TI	Responsable de Departamento de TIC's	R1	Falta de controles para el manejo de la Información	Trabajan 2 personas en dicho Departamento o manejando información confidencial	Bajo	1,5	1,5	VOTO IMPACTO	2,0	1,0	1,5	Se lleva un control de manera física y digital de la información que es confidencial	Implementar la norma ISO/IEC 27001 para manejo de información
									VOTO VULNERABILIDAD	2,0	1,0	1,5		
R2	Gestión de TI	Responsable de Departamento de TICS	R2	Falta de presupuesto para adquirir licencias de antivirus	No existe presupuesto para adquisición de licencias de antivirus	Alto	4,5	5,0	VOTO IMPACTO	5,0	5,0	5,0	Se instalan versiones FREE ya que el presupuesto es limitado	Implementar el estándar ISO/IEC 27002 de Políticas de uso y asignación de licencias de software para que sea una regla establecida la adquisición de licencias.
									VOTO VULNERABILIDAD	4,0	5,0	4,5		
R3	Gestión de TI	Responsable de Departamento de TICS	R3	Falta de control de acceso en el ingreso de	Cualquier persona no autorizada puede	Medio	3,0	4,0	VOTO IMPACTO	5,0	3,0	4,0	No se lleva ningún control	Implementar el estándar ISO/IEC 27002 de

R4			personas no autorizadas al Departamento de TIC's	ingresar al Departamento										mecanismos de seguridad para el ingreso de personas autorizadas como: biométricos,..
								VOTO VULNERABILIDAD	3,0	3,0	3,0			
R4	Gestión de TI	Responsable de Departamento de TICS	R4	Falta de políticas para respaldo de Información	se utilizan discos duros para realizar respaldos de información	Alto	4,0	4,0	VOTO IMPACTO	5,0	3,0	4,0	Se almacenan en discos duros externos y una pc del Departamento	Implementar el estándar ISO/IEC 27002 de políticas de copias de seguridad
									VOTO VULNERABILIDAD	5,0	3,0	4,0		
R5	Gestión de TI	Responsable de Departamento de TICS	R5	Falta de control de ingreso al DATACENTER	Cualquiera puede ingresar porque los equipos que existen están dañados y se ingresa con llaves	Medio	3,0	3,0	VOTO IMPACTO	3,0	3,0	3,0	Existen tarjetas de acceso y cámaras de seguridad que no se utilizan de manera adecuada	Implementar el estándar ISO/IEC 27002 y capacitar al personal para el manejo adecuado del control de acceso al Datacenter
									VOTO VULNERABILIDAD	3,0	3,0	3,0		
R6	Gestión de TI	Responsable de Departamento de TICS	R6	Uso inadecuado de Manuales de Usuario para el sistema Quipux	No existe personal designado para capacitar a los empleados del buen uso de estas tecnologías	Medio	3,5	3,5	VOTO IMPACTO	4,0	3,0	3,5	Se realizan capacitaciones al empleado cuando se integran por primera vez o el número es mayor de 4 personas	Implementar la norma ISO/IEC 27001 de manuales de políticas y procedimientos para el manejo adecuado de la información
									VOTO VULNERABILIDAD	4,0	3,0	3,5		

R7	Gestión de TI	Responsable de Departamento de TICS	R7	Falta de integridad de la información	La información se comparte en el drive	Medio	3,5	3,5	VOTO IMPACTO	5,0	2,0	3,5	No existe control	Implementar la norma ISO / IEC 27001 de políticas de cumplimiento inmediato de manejo adecuado de la información
									VOTO VULNERABILIDAD	5,0	2,0	3,5		
R8	Gestión de TI	Responsable de Departamento de TICS	R8	Falta de mecanismos de seguridad para acceder al computador	Solo cuentan con mecanismos de contraseñas	Medio	3,5	3,5	VOTO IMPACTO	5,0	2,0	3,5	No existe control	Implementar la norma ISO/IEC 27001 de mecanismos de seguridad como: antivirus, firewall, antiespías, encriptación
									VOTO VULNERABILIDAD	5,0	2,0	3,5		
R9	Gestión de TI	Responsable de Departamento de TICS	R9	Uso inadecuado de contraseñas de seguridad	Comparten contraseñas de seguridad	Alto	4,0	4,0	VOTO IMPACTO	5,0	3,0	4,0	No existe control	Implementar la norma ISO / IEC 27001 de políticas de cumplimiento inmediato para el uso de contraseñas seguras en todos los Departamentos
									VOTO VULNERABILIDAD	5,0	3,0	4,0		
R10	Gestión de TI	Responsable de Departamento de TICS	R10	Falta de planes de contingencia	No hay personal dedicado para realizar esta actividad	Alto	4,5	4,5	VOTO IMPACTO	5,0	4,0	4,5	No existen planes de contingencia	Implementar la norma ISO/IEC 27001 de planes de contingencia para dicho

R1 1	Contratación y adquisición de bienes y servicios	Responsable de Departamento de TICS	R11	Falta de presupuesto para repuestos de computadores	Presupuesto limitado para adquirir repuestos de computadores	Alto	5,0	5,0	VOTO VULNERABILIDAD	5,0	4,0	4,5		Departamento y capacitar a todo el personal
									VOTO IMPACTO	5,0	5,0	5,0	No existe un presupuesto para la adquisición de repuestos de computadores	Implementar la norma ISO 9001 en el presupuesto anual para la adquisición de repuestos de equipos informáticos
R1 2	Administración de recursos físicos	Responsable de Departamento de TICS	R12	Deficiente infraestructura física Tecnológica	Presupuesto limitado para mejorar la infraestructura tecnológica	Alto	4,5	4,5	VOTO IMPACTO	5,0	4,0	4,5	No existe presupuesto para mejorar la infraestructura tecnológica	Implementar la norma ISO 9001 de políticas donde se establezca un lugar apropiado para el Departamento de TICS
									VOTO VULNERABILIDAD	5,0	4,0	4,5		

TABLA XVIII. MATRIZ RESIDUAL DEL DEPARTAMENTO DE TIC's

Información del proceso		Escenarios de riesgo	Análisis de controles				Calificación del riesgo residual			
Área	Proceso	Escenario	Controles	Descripción de la implementación del control	Tipo de control	Efectividad del control	Efectividad conjunta de controles	Probabilidad	Impacto	Severidad
Departamento de TIC'S	Gestión de TI	E01. Departamento de TIC's-Manejo de información	Las instalaciones donde se almacena la documentación física cuentan con controles ambientales y de seguridad adecuados	Existe un cuarto especializado para la gestión de datos de la empresa donde se encuentra el servidor principal.	Correctivo	No efectivo	Insuficiente	media	bajo	Baja
			Se cuenta con almacenamiento externo especializado, con las debidas medidas físicas y ambientales para resguardar apropiadamente la información.	No existe almacenamiento externos especializados	Preventivo	No efectivo				
			Solo el personal autorizado tiene acceso a la documentación física	Cualquier persona puede cruzar la puerta del cuarto de servidor.	Preventivo	No efectivo				
			Existen políticas y procedimientos documentadas y actualizadas sobre los mecanismos vigentes de	Existe un pequeño manual de configuración de respaldos de	Preventivo	No efectivo				

			protección de la información física	cada computadora.							
			Existe copia de la información física crítica en otras localidades u otros medios de respaldo.	La información del servidor principal esta replicada en el segundo servidor que se encuentra a 50 mts.	Preventivo	Efectivo con oportunidad de mejora					
		E02.Hospital de Catacocha- Adquisición de licencias de antivirus	Adquirir licencias de antivirus para las computadoras de la institución	Del presupuesto Anual , designar un capital para la adquisición de licencias de antivirus	Correctivo	Efectivo con oportunidad de mejora	No confiable	Media	MEDIO	Media	
			Implementar políticas de adquisición de licenciamiento de software	Culturalizar a los usuarios de la red como deben manejar la información que están grabando en cada equipo	Preventivo	No efectivo					
			Instalar Software libre a todas las computadoras	Tratar de que todas las computadoras de la institución utilicen software libre para no tener que instalar antivirus	Correctivo	Efectivo con oportunidad de mejora					



		E03. Departamento de TICS- Control de acceso en el ingreso de personas no autorizadas	Implementar en las instalaciones del Departamento controles de acceso para el ingreso.	Cualquier persona puede ingresar al Departamento	Preventivo	No efectivo	No confiable	Media	bajo	Baja
			Implementar políticas de seguridad y Control de acceso físico de personas y equipos	El responsable del Departamento de TICS será el responsable de autorizar los permisos correspondientes	Preventivo	No efectivo				
		E04. Departamento de TICS-Políticas de respaldo de información	Se hacen respaldos periódicos de la información relevante de los computadores del personal	Los backups de las computadoras se ejecutan cuatrimestralmente	Preventivo	Efectivo con oportunidad de mejora	Confiable	Media	Bajo	Baja
			Se hace configuración y mantenimiento adecuado de equipos personales	A los equipos personales se les realiza mantenimiento físico y lógico una vez al año	Preventivo	Efectivo con oportunidad de mejora				
			Implementación de un buen procedimiento para la realización de respaldos de información	Utilizar las normas ISO/IEC 27002	Preventivo	No efectivo				

		E05.DATACENTER- Control de acceso al Datacenter	Implementar mecanismos y procedimientos de control de acceso al data center	Cualquiera puede ingresar al Departamento ya que actualmente el registro se lo realiza manualmente.	Preventivo	Efectivo con oportunidad de mejora	Confiable	Media	bajo	Baja
			Implementar las normas ISO/IEC 27002	Capacitar al personal para el manejo adecuado del control de acceso al DATACENTER	Preventivo	No efectivo				
		E06. Departamento de TICS- Uso inadecuado de Manuales de Usuario	Implementar Manuales de políticas y procedimientos de Usuario	Capacitar periódicamente al personal sobre la utilización de los manuales de usuario que existen en la institución	Preventivo	Efectivo con oportunidad de mejora	Confiable	Media	Bajo	Baja
			Implementar estándares ISO/ IEC 27001	Estos estándares permiten un manejo adecuado de los manuales de usuario	Preventivo	No efectivo				
		E07. Departamento de TICS- Integridad de la información	Implementar políticas de integridad de la información	Capacitar al personal sobre el uso de estas políticas	Preventivo	No efectivo	Confiable	Media	bajo	Baja

			Implementar estándares ISO/ IEC 27001	Estos estándares permiten un manejo adecuado de la información	Preventivo	No efectivo				
		E08. Departamento de TICS- Mecanismos de seguridad para acceder al computador	Existen métodos para autenticación de usuarios desde conexiones externas al computador personal	El usuario puede acceder a su computador previa solicitud del responsable de TIC's	Preventivo	Efectivo	Adecuado	Media	Bajo	Baja
			Implementar mecanismos de seguridad para acceso al computador	Estos mecanismos servirán para impedir la conexión a redes inalámbricas externas que se encuentren al alcance de los dispositivos electrónicos institucionales.	Preventivo	No efectivo	Confiable			
		E09. Departamento de TICS-Uso inadecuado de contraseñas de seguridad	Implementar políticas de seguridad de contraseñas	Capacitar al personal sobre el buen uso de políticas de contraseñas	Preventivo	No efectivo	Confiable	Media	bajo	Baja
			Control de los accesos y consolidación de las cuentas privilegiadas de la institución	Todas estas cuentas deben ser registradas y categorizadas. Aquellas que no resulten	Preventivo	No efectivo				

				necesarias, sean redundantes o estén en desuso deberían ser eliminadas.						
		E10. Departamento de TICS-Planes de contingencia	Implementar un plan de contingencia para el Departamento de TICS	Dar a conocer a todo el personal sobre el plan de emergencia y que sepan cómo actuar en caso de un incidente suscitado dentro y fuera de las instalaciones para evitar que la emergencia se agrave.	Preventivo	No efectivo	No confiable	Media	bajo	Baja
			Utilizar estándares ISO para el uso de Planes de contingencia	Utilizar las normas ISO/IEC 27001	Preventivo	No efectivo				
	<b>Contratación y adquisición de bienes y servicios</b>	E11. Departamento de TICS-Repuestos de computadores	Adquirir repuestos de computadores	Del presupuesto Anual , designar un capital para la adquisición repuestos de computadores	Preventivo	No efectivo	Insuficiente	Media	bajo	Baja
				Implementar la norma ISO 9001	Esta norma sirve para la adquisición de equipos informáticos	Preventivo				

	<b>Administración de recursos físicos</b>	E12. Departamento de TICS- Infraestructura física Tecnológica	Las instalaciones donde se desarrolla el proceso, tienen una infraestructura sismorresistente.	Revisión no frecuente de las instalaciones	Preventivo	No efectivo	Insuficiente	Media	bajo	Baja
Existen sistemas contra incendios			Existen extintores cada 50 metros por norma	Preventivo	Efectivo					
Mecanismos de seguridad física para acceder a las instalaciones			No existe seguridad física	Correctivo	No efectivo					

## **ANEXO 7. Artículo Científico**

## Gestión de Riesgos de TIC en hospitales públicos

Johanna Elizabeth Rivera Serrano<sup>1</sup>, Valeria Herrera Salazar<sup>2</sup>, Ximena Naranjo Ruiz<sup>3</sup>, Cristian Narváez Guillén<sup>4</sup>

joanna.rivera@unl.edu.ec, vherrera@unl.edu.ec, ximena.naranjo@unl.edu.ec, cristian.narvaez@unl.edu.ec

<sup>1,2,3,4</sup> Universidad Nacional de Loja, 110111, Loja, Ecuador.

Pages: 280–291

**Resumen:** Este documento presenta el análisis de riesgos realizado en un hospital público del Ecuador, que al ser una institución ligada al Estado, manejan información altamente sensible y confidencial. Tomando en cuenta todo esto, se realizó un análisis e identificación de los riesgos a los que está expuesto el Hospital Básico de Catacocha, a través de su Departamento de Tecnologías de la Información y Comunicación (TIC), para, de esta manera, identificar las vulnerabilidades que pueden atentar contra la seguridad de la información, y elaborar una comparativa que arroje el resultado de los riesgos que se pueden evaluar, logrando así el plan de gestión que permita mitigar los riesgos, obtener conclusiones y recomendaciones que deben ser implementados en las instituciones, cumpliendo así con los pilares fundamentales de la seguridad de la información.

**Palabras-clave:** Gestión de Riesgos; Riesgo Inherente; Riesgo Residual; Magerit; Seguridad de la Información.

### *ICT Risk Management in public hospitals*

**Abstract:** This document presents the risk analysis carried out in a public hospital in Ecuador, which, being an institution linked to the State, handles highly sensitive and confidential information. Taking into account all this, an analysis and identification of the risks to which the Basic Hospital of Catacocha is exposed, through its Department of Information and Communication Technologies (ICT), was carried out, in order to identify the vulnerabilities that can threaten the security of information, and develop a comparison that yields the result of the risks that can be evaluated, thus achieving the management plan to mitigate the risks, obtain conclusions and recommendations that must be implemented in the institutions, thus fulfilling the fundamental pillars of information security.

**Keywords:** risk management; inherent risk; residual risk; Magerit; information security.

## **ANEXO 8. Solicitud de Entrega y Socialización del Plan de Gestión de Riesgos**



Catacocha, 5 de Noviembre de 2019

Ing. Juan Pablo Naranjo  
**RESPONSABLE DE DEPARTAMENTO DE TIC's**

En su despacho.-

De mis consideraciones:

Yo, **JOHANNA ELIZABETH RIVERA SERRANO**, portadora de cédula de identidad Nro.1104935018, estudiante de la carrera de Ingeniería en Sistemas de la Universidad Nacional de Loja, me dirijo a usted con la finalidad de hacerle la entrega y socialización del trabajo de titulación denominado **“Plan de gestión de riesgos de TI en el Hospital de Catacocha”**.

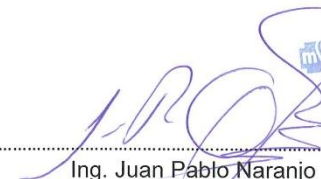
Por la atención favorable se designe dar al presente, le anticipo mis agradecimientos.

Atentamente



Johanna Elizabeth Rivera serrano  
**1104935018**

Aceptación:



Dirección Distrital de Salud  
MSP - Ministerio de Salud Pública, N° 11D03  
**TIC.s**  
Catacocha -Loja -Ecuador

Ing. Juan Pablo Naranjo  
**RESPONSABLE DE DEPARTAMENTO DE TIC's**

## **ANEXO 9. Licencia Creative Commons**



Plan de Gestion de Riesgos de TI en el Hospital de Catacocha by Johanna Rivera is licensed under a [Creative Commons Reconocimiento-NoComercial-CompartirIgual 4.0 Internacional License](https://creativecommons.org/licenses/by-nc-sa/4.0/).