INSTITUTO DE TECNOLOGIAS SUDAMERICANO®

CARRERA DE ANÁLISIS DE SISTEMAS

TEMA:

"ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN PARA LA INFRAESTRUCTURA DE LA EMPRESA FOUR POINTS BY SHERATON CUENCA"

AUTORA:
ERIKA BELÉN ÁVILA CAGUANA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE:
TECNÓLOGO EN ANÁLISIS DE SISTEMAS

TUTOR:
• MGS. GALO HURTADO CRESPO

CUENCA – ECUADOR, 2019

CARRERA DE ANÁLISIS DE SISTEMAS

COMITÉ TÉCNICO MULTIDISCIPLINARIO

Certificación de Aprobación del Trabajo de Titulación

Damos fe que el trabajo desarrollado por la estudiante: **ÁVILA CAGUANA ERIKA BELÉN** con el título: **"ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFOMACIÓN PARA LA INFRAESTRUCTURA DE LA EMPRESA FOUR POINTS BY SHERATON CUENCA"** cumple con las exigencias metodológicas y técnicas.

Por lo antes mencionado, los TUTORES asignados del COMITÉ TÉCNICO MULTIDISCIPLINARIO resuelve **APROBAR** el Trabajo de Titulación.

Atentamente,

Mgs. Galo Hurtado Crespo.

Ing. Max Zuñiga López

Ing. Juan Pérez Perez.

Mgs. Juan Hurtado Ortiz.

INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO
COORDINADOR DE CARRERA
DESARROLLO DE SOFTWARE

DECLARACIÓN DE AUTORÍA DEL TRABAJO

Yo, **ÁVILA CAGUANA ERIKA BELÉN**, estudiante del **Instituto Tecnológico Superior Particular Sudamericano** de la ciudad de Cuenca - Ecuador, que cursó la Tecnología en **ANÁLISIS DE SISTEMAS,** declaro en forma libre y voluntaria que la presente investigación que versa sobre **"ANÁLISIS DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN PARA LA INFRAESTRUCTURA DE LA EMPRESA FOUR POINTS BY SHERATON CUENCA"** así como las expresiones vertidas en la misma, son autoría de la compareciente, quien ha realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la misma y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

ÁVILA CAGUANA ERIKA BELÉN

Cédula: 010519523-4

DERECHOS DE AUTOR

RESUMEN

Este trabajo tiene como objetivo desarrollar un análisis de riesgo para la Empresa Four Points by Sheraton Cuenca en base a la metodología MAGERIT permitiendo dar una adecuada solución de seguridad para los activos de mayor importancia, se enfoca en crear medidas preventivas para reducir la probabilidad de incidentes y aportando con la educación de los empleados que manejan información sensible.

El proyecto se encuentra conformado por seis capítulos, con el siguiente contenido:

En el primer capítulo se presenta la problemática a resolver mediante el planteamiento de preguntas para establecer un inicio en el desarrollo del proyecto, se definen los alcances y las limitaciones.

En el segundo capítulo se encuentra la elaboración del marco teórico-conceptual para definir la fundamentación teórica del proyecto e instituir las bases de su desarrollo precisando los conceptos más relevantes.

En el capítulo tercero se presenta las metodologías elegidas para el desarrollo del análisis de riesgos y la justificación de la elección basada en los requerimientos de la organización

En el cuarto capítulo se encuentra el análisis e interpretación de los resultados que se dieron a conocer a través del desarrollo del proyecto, el análisis de los resultados de la encuesta y las falencias de seguridad encontradas en el análisis de riesgo además se ofrece medidas que se recomiendan seguir para dar un tratamiento adecuado a las vulnerabilidades encontradas

En el último capítulo se da a conocer en detalle las etapas y fases empleadas para el desarrollo de la propuesta, proponiendo la solución de la mitigación del riesgo y la creación de un manual de buenas prácticas dirigido a los empleados que manejen información confidencial de la empresa.

Por último, el cronograma de actividades, las conclusiones, recomendaciones, bibliografía y anexos se encuentra que muestran los resultados de la aplicación del proyecto.

PALABRAS CLAVE: SGSI, Análisis de Riesgo, MAGERIT, Normas ISO 270001, Análisis GAP, Salvaguardas, Activos de información, SI.

ABSTRACT

This work aims to develop a risk analysis for the Four Points by Sheraton Cuenca Company based on the MAGERIT methodology allowing to provide an adequate security solution for the most important assets, focusing on creating preventive measures to reduce the probability of incidents and contributing with the education of the employees that handle sensitive information in the company.

The project is made up of six chapters, with the following content:

The first chapter presents the problem to be solved by asking questions to establish a start in the development of the project, the scope and limitations are defined.

In the second chapter there is the elaboration of the theoretical-conceptual framework to define the theoretical foundation of the project and to establish the bases of its development specifying the most relevant concepts.

The third chapter presents the methodologies chosen for the development of the risk analysis and the justification of the choice based on the requirements of the organization

In the fourth chapter there is the analysis and interpretation of the results that were made known through the development of the project, the analysis of the results of the survey and the safety shortcomings found in the risk analysis.

In the last chapter, the stages and phases used for the development of the proposal are presented in detail, proposing the solution of risk mitigation and the creation of a manual of good practices aimed at employees who handle confidential company information.

Finally, the schedule of activities, conclusions, recommendations, bibliography and annexes are found that show the results of the project application.

KEY WORDS: ISMS, Risk Analysis, MAGERIT, ISO 270001 Standards, GAP Analysis, Safeguards, Information assets, Information System.

AGRADECIMIENTO

Quiero agradecer a Dios por nuca haberme dejado sola en los momentos más difíciles de mi vida y brindarme la dicha de cumplir mis metas.

Agradezco al Instituto Superior de Tecnologías Sudamericano, a las autoridades y los profesores que impartieron sus conocimientos y me ayudaron a formarme como una profesional entregaron todo su apoyo y comprensión.

Al Hotel Four Points by Sheraton Cuenca en especial a los que conforman la Dirección de Tecnología por darme la oportunidad de desarrollar mi tesis en sus instalaciones, muchas gracias.

A mi familia y amigos que siempre estuvieron alentándome a cumplir mis sueños.

DEDICATORIA

Dedico esta tesis en primer lugar a mi Madre por siempre apoyarme en cada proyecto de mi vida porque sin ella yo no sería quien soy ahora, a mi padre, mis hermanos, mis tíos, tías y abuelitos que siempre estuvieran conmigo. A mi gran amigo Sebastián que descansa en paz, a mi mejor amigo Leonel que siempre me apoyo incondicionalmente desde el colegio, a mis dos grandes mejores amigas Verónica y Nicole, gracias por formar parte de este gran sueño y por ultimo a todas aquellas personas que de una manera u otra influyeron para que yo estuviera hoy aquí. Gracias de todo corazón.

- Erika Ávila.

ÍNDICE

Índice de Figuras

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el presente proyecto de titulación se realizó un análisis de riesgos de seguridad de la información para la Empresa Four Points by Sheraton Cuenca, con el objetivo de generar un informe de evaluación que permita descubrir las amenazas y vulnerabilidades presentes en los activos que conforman el departamento de TI. Se encuentra basado en el reconocimiento del volumen real de datos y las políticas previamente establecidas por la organización que permitieron tener una idea de la situación actual en la que se mantenía la empresa antes de detectar los riegos tanto de afuera, como dentro de la infraestructura informática. Con el objetivo de minimizar el riesgo se proponen controles de respuesta formales que se encuentran basados en las normas ISO 27001 y un conjunto de buenas prácticas de seguridad.

Para realizar la evaluación correspondiente se utilizó las herramientas dispuestas por la metodología “MAGERIT”, en la que se definen las tareas principales para el análisis de riesgo, gracias a la cual se identificó los activos que guardan relación con el departamento de TI, se seleccionaron las amenazas correspondientes a cada activo mediante un enfoque práctico y por ultimo permitió cuantificar los riesgos.

El enumerar las amenazas fue un proceso de entender el ambiente de operaciones que permitieron poner las vulnerabilidades al descubierto en contexto con la realidad, además se usó la información existente de los informes de anomalías en los activos de información y las amenazas que afectan a las empresas de hoy. Todo los controles y buenas prácticas de seguridad definidos en este informe serán tomados en consideración por el departamento de seguridad informática en la empresa (quedando a decisión de los responsables de seguridad) su respectiva implementación con el fin de minimizar el impacto que pueden producir los incidentes.

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General

- Realizar un análisis de SGSI aplicando la metodología MAGERIT, que permita identificar las vulnerabilidades y amenazas cuantificando su impacto hacia los activos de información de la red interna en la empresa Four Points by Sheraton Cuenca.

Objetivos Específicos

- Revisar las políticas actuales de seguridad de la información establecidas por la empresa para verificar su aplicabilidad.
- Identificar, clasificar y valorar los activos de información que conforman el departamento de TI en la empresa.
- Enumerar las amenazas a los que están expuestos cada activo manteniendo un enfoque aplicado, basado en el catálogo dispuesto por metodología “Magerit”.
- Cuantificar los riesgos de seguridad.
- Mitigar los riesgos generando controles para reducir el impacto de su materialización.
- Generar un manual de buenas prácticas para reducir la probabilidad de su materialización.

Preguntas de Investigación

- ¿Cuáles son las consecuencias operativas de perder el acceso a los activos de información?
- ¿De qué manera el análisis de gestión de riesgos informáticos puede apoyar al departamento de TI de la empresa Four Points by Sheraton?
- ¿De qué manera se puede educar a los empleados de la empresa para que comprender el papel importante que desenvuelven en la seguridad de la información?
- ¿Con que frecuencia es necesario realizar una reevaluación del análisis de riesgo?

JUSTIFICACIÓN

En la actualidad los desafíos por mantener un nivel más que aceptable de seguridad en las redes empresariales son una de las principales preocupaciones entre los líderes de TI y de telecomunicaciones, debido a la dependencia que las empresas han generado con ayuda de la tecnología para seguir realizando sus actividades operacionales. Por los cual surge la importancia de conocer lo que se quiere proteger dentro de la empresa. Lo cual permitirá que las empresas puedan identificar los riesgos con mayor impacto negativo para la continuidad del negocio.

"Cuando hablamos de seguridad informática nos referimos a las amenazas y vulnerabilidades que existen en los actuales sistemas de cómputo. En la actualidad debido al diseño de las redes informáticas la información está al alcance de todos, por lo cual debemos tener mucha precaución al momento de manejar información confidencial o sensible." (Goez, 2014). Es necesario que las empresas mantengan actualizadas sus políticas, controles y procedimientos con el fin de ser capaces de responder de manera rápida y eficiente a la posible materialización de las amenazas. Four Points by Sheraton Cuenca es una empresa con una infraestructura bastante modernizada en cuanto a tecnología se refiere, preocupada por el cumplimiento de los lineamientos que continuamente se requieren con respecto a la seguridad de la información.

El proyecto a desarrollar tiene como objetivo apoyar al departamento de TI a implementar el análisis de las vulnerabilidades y la protección de sus activos más importantes mediante la mitigación de los riesgos de mayor impacto con la creación de controles y buenas prácticas, todo esto basado en Magerit. Es una metodología para el desarrollo de SGSI, la cual ofrece un método sistematizado que facilita el análisis de riesgos, ya que aporta con herramientas para la identificación de amenazas y ayuda a planificar las medidas necesarias para su respectiva mitigación. Todo el análisis que se desarrolle en este proyecto queda a disposición de la empresa para ser analizado y aplicado según lo disponga la gerencia y las partes implicadas que correspondan.

1. CAPÍTULO I

PROBLEMÁTICA

1.1. Antecedentes del Problema

La Empresa Four Points by Sheraton cuenta con una estructura física ubicada en la ciudad de Cuenca en la provincia del Azuay y ha prestado sus servicios de hotelería desde el año 2017, está conformada por once plantas, en el piso de administración se ubican los departamentos de contabilidad, gerencia, sistemas, etc. En el tercer piso se encuentra el Lobby donde se encuentran los departamentos de recepción al cliente, en la planta baja se ubican las oficinas operacionales y los ocho pisos restantes están los cuartos para los huéspedes todos con servicio de cable, telefonía y acceso a internet.

En la organización el uso de tecnologías de la información ha ido aumentando rápidamente a pesar de que sean pocos los años que lleve establecido en el mercado, todos los departamentos se encuentran interconectados por medio de una red LAN lo que permite la comunicación entre las estaciones de trabajo, esta misma red se encuentra segmentada por subredes interconectadas con la estructura informática permitiendo hacer más manipulable a la red, Por otro lado esto también conlleva a que exista una variedad de vulnerabilidades de seguridad que pueden llegar a afectar la confidencialidad, integridad y disponibilidad de la información. Las brechas son aprovechadas por los atacantes que tratan de pasar sobre los mecanismos de protección del sistema para entrar a las áreas restringidas y tomar el control de información que es valiosa para la continuidad de las actividades de la empresa y todo esto debido a la falta de medidas preventivas y análisis de riesgos que deberían realizarse cada cierto periodo de tiempo con los que no cuenta la empresa.

1.2. Definición de Problema

Las vulnerabilidades crecen día tras día mientras la sociedad se vuelve más digital y existen nuevas brechas que ponen en riego los datos empresariales, la reevaluación de las estrategias de seguridad es algo que debe importar a las empresas para que puedan seguir operando. Por otro lado, esta brindar la confianza necesaria para los clientes que exigen garantías de seguridad para su información.

Para la empresa Four Points by Sheraton Cuenca es de suma importancia gestionar y mitigar las amenazas presentes en su sistema de información pero la falta de asesoría y seguimiento de los procesos actuales provoca que se desconozca el nivel de madurez del sistema de gestión de seguridad de la información (SGSI) y por tanto no exista un catálogo actualizado de las amenazas que pueden poner en peligro al activo de mayor importancia para la empresa, la información, una organización no puede esperar a que se susciten incidentes de seguridad para tomar medidas de protección.

1.3. Pregunta General

¿De qué manera se puede reforzar la seguridad de la información en la empresa Four Points by Sheraton Cuenca mediante un análisis de riesgos de seguridad para sus activos más importantes?

1.4. Preguntas Específicas

- ¿Cómo prevenir la ocurrencia de ataques exitosos que permitan aumentar la seguridad, sin aumentar los costos?
- ¿De qué manera se puede clasificar los activos de información con mayor relevancia en el desarrollo de actividades de la empresa?
- ¿Cuáles son los servicios y aplicaciones de negocio y de misión crítica?
- ¿Qué otro tipo de controles se pueden aplicar para la protección correcta de la red que no sea solamente soluciones tecnológicas?
- ¿Qué ocurriría si una amenaza llegase a materializarse?
- ¿Cuáles son los procesos que requieren una mayor prioridad para la empresa?

1.4.1. Alcances y Limitaciones

Este proyecto procura en primer lugar realizar un analizar de la disposición actual de todos los controles y políticas de seguridad para medir el nivel de madurez del SGSI para posteriormente poder desarrollar un análisis de riesgo para la organización, lo cual se compone principalmente de la clasificación y valoración de los activos de información con mayor impacto, el desarrollo de un catálogo de amenazas a los que se encuentran expuestos cada uno de los grupos de activos con la respectiva mitigación de riesgos y para finalizar la creación de un manual de buenas prácticas que recoge un conjunto de recomendaciones para educar a todos los empleados de la empresa a cerca de la seguridad de la información.

La información que se genere en el transcurso de desarrollo de este análisis de riesgo serán:

- Informe del nivel de madurez actual del SGSI.
- Catálogo de los activos de información y su clasificación.
- Informe de hallazgos de amenazas, vulnerabilidades y su valoración.
- Documento del tratamiento del riesgo y su mitigación
- Manual de buenas prácticas.

El proyecto está orientado en su mayoría al proceso de gestión de riesgos ya que por falta de tiempo no se puedo enfocar en la aplicación de los controles ni medir el nivel de eficacia del manual de buenas prácticas, no fue posible aplicar procesos de pentesting para el análisis de vulnerabilidades por la falta de tiempo y disposición de recursos por parte de la empresa.

2. CAPÍTULO II

MARCO REFERENCIAL

2.1. Marco Teórico

Se presentan a continuación los conocimientos en los que está basado el desarrollo de este proyecto que servirán como la base fundamentada para alcanzar los objetivos expuestos anteriormente desde un punto de vista conceptual y dar paso a la aplicación del análisis re riesgo de la seguridad de la información.

2.1.1. Aspectos Relevantes de la Seguridad de Información con los Años

La seguridad de la información no siempre fue uno de las inquietudes principales de las organizaciones, después de la llegada de las nuevas tecnologías que automatizó las actividades diarias en la empresa comenzó a percibirse la necesidad de proteger la información. Los principales retos de los años noventa eran garantizar la seguridad de la información mediante sus tres principios que son: Confidencialidad, integridad y disponibilidad. Para el año 2001 cambio la situación ya que la ciberseguridad tuvo mayor importancia para la sociedad y las empresas principalmente (Santos, 2009).

A medida que la economía global crece, también crece la adopción de las nuevas tecnologías para poder cubrir todas las facetas de un negocio moderno. Por lo cual el trabajo de proteger los activos críticos del negocio se ha tornado desafiante debido al aumento de la probabilidad de un ataque, a esto se añade el aumento de las probabilidades de un ataque que tiene como consecuencia obstaculizar la continuidad del negocio, aumento en los costos de las actividades, errores y fallas en la arquitectura de seguridad.

Sin embargo, el problema de planificar estrategias que permitan detectar el riesgo una vez hayan ocurrido el incidente se encuentra en el enfoque de hace décadas atrás,

por lo que no está diseñado para acaparar la seguridad de todas las áreas que integran la infraestructura TI, ni tampoco para poder mantenerse en evaluación continua. Las empresas que mantienen este enfoque desactualizado pueden correr el riesgo de una deficiencia en el cumplimiento de las operaciones, con impactos graves de reputación y costos de recuperación.

Según la encuesta de realizada por las Compañías (MARSH & McLennan, 2019), denominada "Percepción del Riesgo Cibernético en Latinoamérica 2019", las empresas asumen el riesgo cibernético como una prioridad, además de existir una mayor confianza en su capacidad de resiliencia con respecto a los resultados obtenidos en 2017. Se puede comprender que debido al aumento de las dependencias digitales por parte de las empresas ha traído consigo nuevos riesgos cibernéticos.

Es claro que las empresas que forman parte de esta encuesta la mayoría han ido desarrollado un nivel considerable de mejoras en el transcurso de los años, comienzan a adaptarse al cambio con ayuda de análisis de seguridad con el propósito de encontrar las amenazas más críticas y poder tomar decisiones sobre cómo evaluar y mitigar antes de que se materialicen.

2.1.2. Tipos de Ataques y su Clasificación

"Son acciones deliberadas, llevadas adelante por ciberdelincuente organizados o personas que no necesariamente se dedican al cibercriminal pero tienen la intención de provocar daños en sistemas, redes y/o dispositivos informáticos de terceros, con múltiples propósitos" (BACSCIRT, 2018).

Los ataques informáticos son provocados por la presencia de vulnerabilidades en la red de información de las empresas, pueden provocar todo tipo de riesgos que afectan las actividades y operaciones de los empleados. Que una amenaza llegue a ocurrir conlleva la pérdida de tiempo, dinero y la reputación frente a los clientes, por lo tanto que una empresa entienda la importancia de protegerse de los varios ataques informáticos que hoy en día se han ido generando y la responsabilidad de cuidar la información privada que no solo perjudica de las maneras anteriormente mencionadas.

A continuación se presentan los ataques que en las últimas décadas ha cambiado su modalidad de ataque pero persiguen el mismo beneficio:

Tabla 1
Tipos de ataques informáticos

Descripción	Motivaciones	Clasificación
Actividades para el reconocimiento de los sistemas-	Escaneo de puertos para determinar qué servicios se encuentran activos o bien un reconocimiento de versiones de aplicaciones.	Intercepción.
Modificación de los contenidos de datos.	Modificación de la información y actividades por parte de los atacantes que persiguen un beneficio.	Intercepción
Conexiones no autorizadas hacia los equipos y servidores.	Explotación de "agujeros de seguridad", Utilización de "puertas traseras" con el uso de programas similares a los troyanos.	Intercepción Eliminación.
Análisis del tráfico.	Transferencias desde sus propias cuentas corrientes si en ese momento se encuentra conectado al servidor de una entidad financiera.	Modificación
Introducción en el sistema de "malware".	Estarían incluidos los virus, troyanos, gusanos, bombas lógicas, etcétera.	modificación
Modificaciones del tráfico y de las tablas de enrutamiento.	Atraviesen otras redes o equipos intermedios antes de llegar a su destino legítimo, para facilitar de este modo las actividades de interceptación de datos.	Interrupción Modificación
DNS Spoofing provocar un direccionamiento	La redirección de los usuarios de los sistemas afectados hacia páginas Web falsas o bien la interceptación de sus mensajes de correo electrónico.	Intercepción.

erróneo en los equipos.		
Ataques generados por "Cross-Site Scripting" (XSS)	Contra los usuarios y no contra el servidor Web. Mediante "Cross-Site Scripting", un atacante pueda realizar operaciones o acceder a información en un servidor Web.	Interrupción

Los ataques y su clasificación según su impacto (Elaboración propia)

2.1.3. Metodologías de Análisis de Riesgos de la Información

Existen muchas metodologías para construir un SGSI para una empresa, las cuales se componen por herramientas que facilitan realizar este tipo de tareas y generar un análisis con mayor precisión para garantizar que la aplicación de los sistemas cumpla con los requerimientos de la organización. Que hoy en día exista una variedad de metodologías no significa que todas puedan ser válidas para aplicarse en cualquier negocio, al contrario, para poder hacerlo hay que analizar los requerimientos y la disponibilidad que tenga la empresa para realizarlo y también el factor económico que se requiere invertir para este tipo de proyectos.

A continuación, se presenta una tabla comparativa entre metodologías que sirven para el análisis de riego, con la finalidad de aplicar la que sea más adecuada dependiendo de las necesidades de la organización.

Tabla 2
Comparación entre metodologías de análisis de riesgo.

	ISO 27005	MAGERIT 3.0	COBIT 5
Características	Identifica las necesidades del negocio para protegerla de las amenazas, Es la base de otras metodologías porque contiene controles y requiere de una alta participación de las personas que forman parte del entorno.	Ña última versión se compone de tres libros que son: metodología, catálogo de elementos y guías prácticas para el análisis de resultados, basado en las normas ISO 27001 pero adaptable para las circunstancias que se presenten.	Todos los procesos están basados en la gestión de ITIL que recoge procesos y buenas prácticas usados en la gestión de servicios de TI, que requieren de un profundo análisis para obtener resultados más precisos
Ámbito de aplicación.	Tiene una aceptación a nivel mundial por lo que puede ser aplicada en cualquier empresa se cual sean los servicios que tengan relación con el uso de TI.	Puede ser utilizada por cualquier entidad sin importan su naturaleza o tamaño, tienen una aceptación grande por parte de Latinoamérica y Europa con muchos casos de éxito.	Puede ser aplicado en una empresa que no cuente con procesos de TI y no contengan ningún tipo de bases para sus procesos, es decir crea los servicios que dan valor a la empresa.
Fases	- Necesidades/ contexto del negocio. - Identificar las amenazas - Valorar el riesgo. - Tratar el riesgo. - Aceptar el riesgo. - Informar de riesgos. - Revisar y reevaluar.	- Identificar de activos. - Valorar y la clasificar los activos. - Identificar y valorar las amenazas. - Valorar el riesgo. - Tratar el riesgo. - Informar sobre los hallazgos. - Revisar y reevaluar.	- Identificar el caso de negocio. - Proveer la solución. - Planificar la solución. - Implementar la solución. - construir sostenibilidad.

Ventajas	Para la fase de valoración de las amenazas cuenta con varias técnicas para obtener valores cuantitativos, presenta ejemplos y es más práctica si la empresa está buscando su certificación en base a estas normas.	Tienen un catálogo de las amenazas más comunes presentes en un negocio, se adapta a las necesidades, permite valorar de forma cualitativa y cuantitativa, cuenta con herramientas para automatizar el análisis de riesgo.	Aplica criterios para la evaluación de sus procesos, para así obtener ventajas a nivel competitivos por lo que trabaja con la asignación de roles y entregar las responsabilidades necesarias a los ejecutivos de la organización.
Desventajas	El personal que interviene en estos procesos deberá dedicar una gran parte de tiempo lo que reduciría sus responsabilidades laborales con la empresa y por otra parte sus normas están pensadas en estándares internacionales lo que no garantiza que países con menores políticas se beneficien completamente.	Puede resultar realmente costosa por el hecho de que se necesite traducirse toda su valoración hacia valores económicos.	Lleva tiempo ver las reducciones de costos y la mejora en la entrega de los servicios y tienen muy poca compatibilidad con los demás estándares internacionales.

Comparación entre metodologías (Elaboración propia).

2.1.4. Normas ISO/IEC 27001

"Es un estándar que especifica los requerimientos para establecer, implementar, operar, monitorear, revisar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la información (SGSI). Se busca que los aspectos trabajados dentro del SGSI se ajunten con las necesidades de la organización" (Giraldo, 2014).

Se trata de una norma internacional emitida por la Organización Internacional de Normalización (ISO), su principal función es gestionar la seguridad de la información que puede ser implementada en cualquier organización. También permite a las empresas alcanzar una certificación; de manera que una entidad encargada confirma que la organización evaluada ha implementado satisfactoriamente la seguridad de la información en base a la norma. La primera revisión de esta norma se publicó en el año del 2005 y fue en base a la norma británica BS7799-2 (Segovia, 2013).

2.1.5. Métodos de Análisis de riesgos de la Información (MAGERIT 3.0)

MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

MAGERIT interesa a todos aquellos que trabajan con información digital y sistemas informáticos para tratarla. Si dicha información, o los servicios que se prestan gracias a ella, son valiosos, MAGERIT les permitirá saber cuánto valor está en juego y les ayudará a protegerlo. Conocer el riesgo a los que se someten los elementos de trabajo es, simplemente, imprescindible para su gestión. Con MAGERIT se persigue una aproximación metódica que no deje lugar a la impremeditación, ni dependa de la arbitrariedad del analista (Ministerio de Administraciones Públicas, 2011).

2.1.6. Libros de MAGERIT versión 3.0

Está dividida en tres libros, El primer libro de MAGERIT: método, es una guía detallada para el análisis de gestión. En sus contenidos se describe: método de análisis de riesgos, los cuales poseen tres tipologías de métodos: métodos cualitativos, métodos

cuantitativos y métodos semi cuantitativos, procesos de gestión de riesgos, estos procesos actúan mediante dos pasos: la evaluación y el tratamiento de los riesgos; proyectos de análisis de riesgos, se realizan mediante tareas como: el estudio de oportunidad, la elaboración del análisis de riesgos y la comunicación de resultados; planes de seguridad, que se planifican en tres niveles de detalle: plan director, plan anual y plan de proyecto; desarrollo de SI (como se sita en Alvarado, Pacheco, & Martillo, 2018).

El segundo libro de MAGERIT: catálogo de elementos, es una especie de inventario que las empresas pueden usar para enfocar el análisis de los riesgos. En sus contenidos propone un catálogo referente a: tipos de activos; una dimensión de valoración de los activos, que incluyen: disponibilidad, integridad, confidencialidad, autenticidad y la trazabilidad; Criterios de valoración de los activos, amenazas típicas sobre los SI y las salvaguardias a considerar para proteger SI (como se sita en Alvarado, Pacheco, & Martillo, 2018).

El tercer libro de MAGERIT: guías técnicas tanto específicas como generales para realizar proyectos de análisis y gestión de los riesgos. Dentro de las guías técnicas están: el análisis mediante tablas, que tienen como objetivo especificar las valoraciones; análisis algorítmico, existen dos enfoques algorítmicos: el modelo cualitativo, que busca una valoración relativa del riesgo que corren los activos y el modelo cuantitativo que ambiciona responder a la pregunta de cuánto más y cuánto menos; arboles de ataque, constan de: nodos con atributos, riesgo residual y la construcción del árbol. Mientras que las guías técnicas generales contienen: técnicas gráficas, existen diferentes tipos de graficas: técnicas graficas por puntos y líneas, técnicas gráficas por barras, técnicas graficas por área y técnicas gráficas por radar; secciones de trabajo, estas sesiones pueden ser de varios tipos: entrevistas, reuniones y presentaciones en función de las personas que participen en ellas, el objetivo que se persiga y el modo de llevarlas a cabo (como se sita en Alvarado, Pacheco, & Martillo, 2018).

2.1.7. Proyectos de Referencia

Gestión de riesgos con MAGERIT elaborado por tiTHINK:

Esta publicación fue desarrollada con el objetivo de abordar las implicaciones prácticas que tiene la implementación de la metodología MAGERIT en los proyectos, por lo que presentan en este documento los aspectos fundamentales del análisis de la gestión de riesgos con las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así poder reducir al mínimo su potencialidad o sus posibles perjuicios para la organización ya que un análisis de riesgos no es una tarea de importancia menor que realiza cualquiera en sus ratos libres. Es una tarea mayor que requiere esfuerzo y coordinación, su correcta planificación y justificación podrá garantizar que una organización pueda depender de los sistemas de información para el cumplimiento de su misión. (Rodríguez & Peralta, 2013).

Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de seguridad de la información aplicada a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala

Este proyecto fue presentado por la Universidad Politécnica Salesiana con sede en Cuenca y desarrollado por (Goana, 2013), con el objetivo de conocer como está constituida la empresa mediante el análisis de sus procesos e identificar las carencias de seguridad que posee y mediante los pasos que propone la metodología realizar un análisis de riesgos de seguridad donde se obtuvieron resultados realistas del riesgo que posee la empresa seguido de la gestión en la que se diseña un plan de seguridad para llevar los riesgos a niveles aceptables. Los resultados fueron que la empresa no contaba con medidas de seguridad guiados y documentados por lo que el desarrollo de este proyecto ayudara para minimizar los riesgos con la ayuda de un documento que está encaminado hacia la seguridad para crear sus propias normativas.

Diseño de un sistema de gestión de seguridad (SGSI) para la empresa manufacturera persianas y enrollables SAFRA SAS basado en los estándares de la norma ISO 27001

Este proyecto fue presentado por la Universidad Distrital Francisco José De Caldas en la ciudad de Bogotá Colombia y desarrollado por (Perdomo & Frankye, 2018) en

este documento se puede evidencian los riesgos, amenazas, vulnerabilidades y nivel de criticidad de los mismos a los cuales está expuesta la organización, el cual se encuentra definido en diferentes segmentos para su mejor comprensión, donde se brinda una estimación de costos para una futura implementación, un módulo web interno con el que se podrá obtener información sobre los actuales riesgos activos de la organización, permitiendo notificar si existe o se evidencia algún riesgo o amenaza que no se contemplaron en el presente documento.

2.2. Marco Conceptual

2.2.1. Seguridad Informática

Está orientada a proteger la infraestructura de la información y de comunicación, mediante los tres pilares fundamentales que respaldan la ciberseguridad, los cuales son: Confidencialidad, integridad y disponibilidad. Por lo que permiten dar un soporte sólido al negocio junto con el apoyo de estándares que permiten identificar y responder eficazmente los posibles riesgos tanto de afuera con de adentro de la infraestructura. Por lo tanto, la seguridad informática comprende una serie de controles de seguridad que ayudan a proteger el sistema informático de amenazas que ponen en peligro la continuidad del negocio.

2.2.2. Seguridad de la Información

Es asegurar un nivel considerable de seguridad que tiene como objetivo resguardar y encargarse de los activos de información, mediante la aplicación de medidas preventivas, detectivas y correctivas para mantener a salvo toda la información que es relevante para la empresa.

“La información va mucho más allá de la netamente procesada por equipos informáticos y sistemas, es decir, también abarca aquello que pensamos, que está escrito en un papel, que decimos, etcétera…” (Daniel Benchimol, 2011).

2.2.3. Sistema de Gestión de Seguridad de la Información

Un sistema de gestión de seguridad busca proteger a los activos de información en una empresa de los posibles ataques que pueda recibir y crear un ambiente seguro en la empresa, para (Mendoza, 2015). Consiste en gestionar los riesgos de seguridad de la información de una forma documentada, tiene como propósito reducir el impacto que producen las amenazas cuando no se encuentra bajo los controles necesarios, teniendo como consecuencia su materialización.

2.2.4. Análisis de Brechas GAP

"El objetivo principal de este análisis es conocer el diferencial en el desempeño de una organización respecto a las mejores prácticas, estándares, regulaciones legales; evaluar la desviación y establecer los planes para dirigir la organización hacia el cumplimiento de las mismas. Esta diferencia entre el estándar y la realidad del cliente es lo que conocemos como Gap Análisis o brecha. El análisis responde dos interrogantes: ¿dónde estamos? y ¿dónde deberíamos estar?" (Nilo & Salinas, 2017).

2.2.5. Pilares de Seguridad de la Información según MAGERIT

Confidencialidad: Se refiere a la privacidad, la información deberá solamente estar disponible por personal autorizado, en el ámbito empresarial la divulgación de información confidencial es un factor importante para mantener la confianza de los clientes por lo que es aconsejable que adopten todas las medidas posibles para proteger su carácter reservado. (INCIBE, 2017).

Disponibilidad: Es otro factor importante ya que la disponibilidad de la información y los servicios deben mantenerse en continuidad para que pueda ser utilizado por el personal que la requiera.

Integridad: Hace referencia a que la información de un negocio se mantenga libre de cualquier tipo de alteración o corrupción y que solo pueda ser manejada por personal autorizadas.

Autenticidad: Esta valoración es típica de servicios (autenticidad del usuario) y de los datos (autenticidad de quien accede a los datos para escribir o, simplemente, consultar).

Tranzabilidad: "Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad." (Ministerio de Administraciones Públicas, 2011).

2.2.6. Gestión de Riesgos TI

Según (Rodríguez & Peralta, 2013), la gestión de riesgos permite tomar las decisiones de poder asignar recursos con perspectiva de negocio, sean tecnológicos, humanos o financieros. Para cumplir con la tarea de identificar los activos de información, identificar sus vulnerabilidades y amenazas, realizar la gestión de los riesgos y asignar los controles y salvaguardias necesarios para reducir su ocurrencia dentro de la empresa se necesitan dos factores importantes que son:

Análisis de riesgo: el análisis de riesgo es una herramienta propia de la gestión de activos de información que permite comprender lo que se encuentra en juego y estimar cada incidente que podría pasarle al sistema de información, todo esto a través de un análisis de los activos de información y la identificación de sus vulnerabilidades.

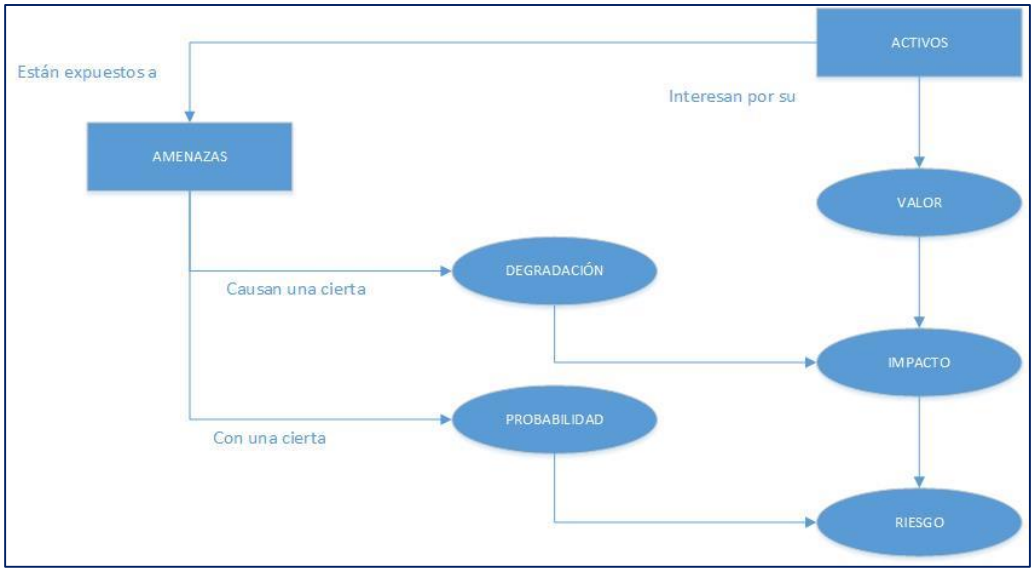

Figura 1: *Análisis de riesgo.*
Fuente: *(Autor, 2019).*

Tratamiento de los riesgos: son los métodos que permiten resguardar la información de la materialización de las amenazas, permite desarrollar planes de contingencia para sobrellevar un incidente, para el tratamiento de los riesgos existen las siguientes estrategias:

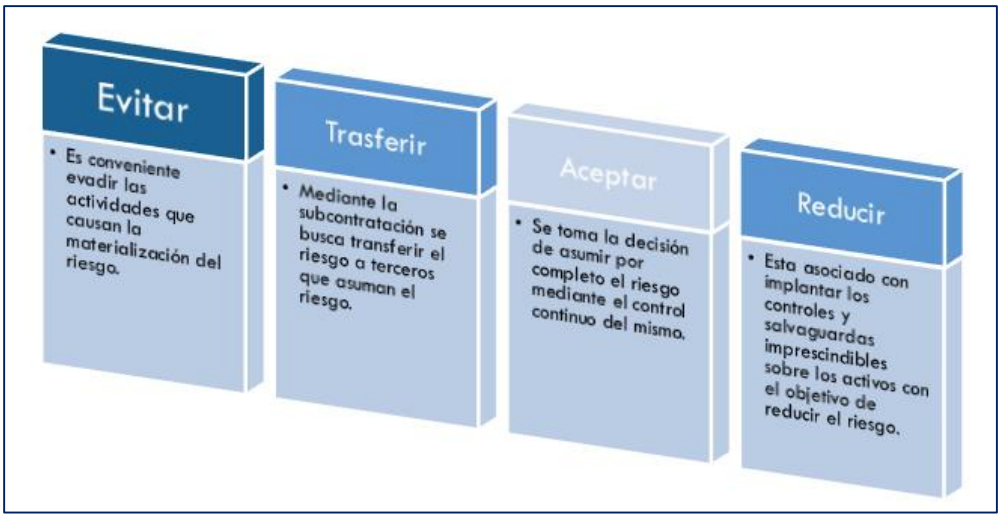

Figura 2: *Tratamiento del riesgo.*
Fuente: *(Autor, 2019).*

2.2.7. Componentes del Análisis de Riesgo

El riesgo de la información se compone de ciertos componentes importantes que ponen en peligro los activos de información, los cuales son:

Activos de Información: Son todos los elementos que forman parte del sistema de información de la empresa y su ayuda para realizar las actividades de la empresa es esencial.

Agente de amenaza: Es el responsable de la explotación de la vulnerabilidad que está conformado por una entidad humana o no humana con el objetivo de obtener algún beneficio.

Vulnerabilidad: Son las amenazas presentes en los activos de información, el atacante aprovecha las brechas de información que no han sido mitigadas correctamente.

Riesgo: es la probabilidad de que una amenaza se materialice y cause un impacto a las actividades del negocio.

Resultados: Es el beneficio que obtiene un intruso al momento de realizar la explotación de seguridad gracias a las vulnerabilidades antes mencionadas.

Impacto: Son todas las consecuencias que deja la explotación de vulnerabilidades. En la mayoría de los casos resulta perjudicial para la continuidad del negocio y para la imagen empresarial.

Políticas de seguridad: específicamente es considerado como un plan de acción para mantener un cierto nivel de seguridad frente a los riesgos.

Controles: también conocidos como mecanismos de control ayudan a controlar los activos mediante la aplicación de recursos necesarios.

Salvaguardias: son todas las medidas de precaución para reducir la probabilidad de que una amenaza se produzca.

2.2.8. Ciclo de Vida de la Seguridad

"Como cualquier otro proceso de TI, la seguridad puede seguir un modelo de ciclo de vida. El modelo presentado aquí sigue los pasos básicos de Identificar - Evaluar - Proteger - Monitorear. Este ciclo de vida proporciona una buena base para cualquier programa de seguridad. El uso de este modelo de ciclo de vida le proporciona una guía para garantizar que la seguridad sea continuamente siendo mejorado." (GIAC Certifications, 2013).

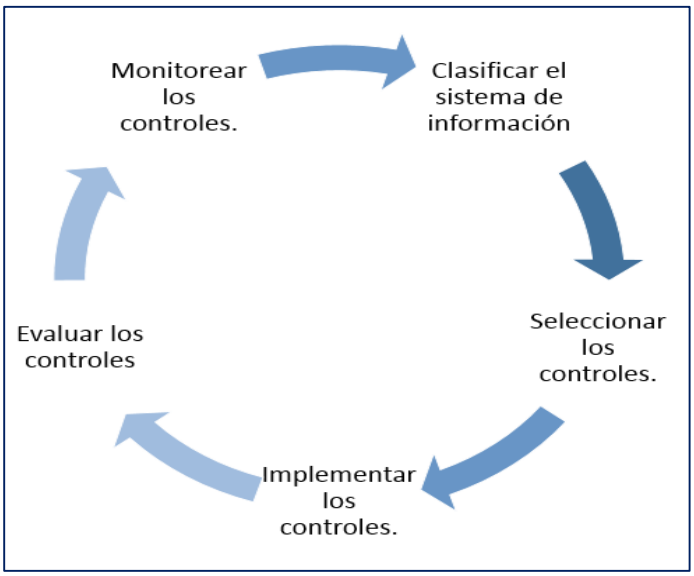

Figura 3: Ciclo de vida de la seguridad.
Fuente: (Autor, 2019)

3. CAPÍTULO III

METODOLOGÍA DEL ANÁLISIS DE RIESGO

3.1. Tipo de Estudio

Para el presente trabajo se emplea el método de investigación cuantitativo, con la intención de obtener resultados basados mediante el análisis de datos detallados y principios teóricos. El objeto de estudio engloba toda la infraestructura de la empresa y los recursos humanos que trabajan en ella, para el análisis de riesgo se utilizan la metodología "Magerit" la cual se adapta a las necesidades y objetivos de la empresa frente a la gestión de la información.

3.2. Métodos de Recolección de Datos

El método de recolección de datos es cualitativo y cuantitativo, debido a que no se dispone de ningún dato histórico que facilite en análisis, pero si la posibilidad de evaluar las diferentes áreas administrativas de la empresa y los activos de información mediante ciertas técnicas definidas a continuación:

Entrevistas

Este método de recolección de datos solo se aplica para cierto número de encuestados, por lo que se tomó en consideración en personal que trabajaba con mayor cantidad de información del negocio. Estas entrevistas se realizaron de manera presencial con los siguientes jefes de área:

Tabla 3: *Lista de personal entrevistado.*

Área	Descripción
Jefe de contraloría	Encargado de la vigilancia y control de los gastos de la administración de la empresa.

Auditor de interno	Encargado de la iniciativa organizacional para monitorear y analizar sus propias operaciones de negocios.
Talento humano	la planeación, organización, desarrollo y coordinación y el control establecido para promover el desempeño eficiente del personal
Gerente general	Tiene la responsabilidad general de administrar los elementos de ingresos y costos de la empresa además es responsable de liderar y coordinar las funciones de la planificación estratégica

Empleados entrevistados para realizar el análisis de riesgos (Elaboración propia).

Fuentes internas de datos secundarios

Se obtiene cierto tipo de datos, que no comprometan la confidencialidad de la empresa, que tengan que relación con la investigación, como: políticas de seguridad, plan de contingencia, informes sobre la infraestructura de la red, etc.

3.3. Magerit Versión 3.0 como Metodología para Desarrollo del Proyecto

"MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza" (Ministerio de Administraciones Públicas, 2011).

"Cabe mencionar que a pesar de que pueda haber un sin número de metodologías que den solución a determinada problemática, cada una de ellas fueron creadas para

resolver una matriz específica, con un enfoque específico y con nivel de granularidad distinto" (Alvarado, Pacheco y Martillo, 2018).

Tomando en consideración la disponibilidad de la información que es facilitada por la empresa y el nivel de detalle de lo que se quiere alcanzar, la mejor metodología que se adapta para el desarrollo del presente proyecto es MAGERIT versión 3.0 porque muestra ser una herramienta valiosa que permite sistematizar el análisis de riesgos gracias a que las decisiones para identificar y planificar mediadas de seguridad se encuentran bien fundamentadas y son fáciles de defender. Además, es la metodología que más se adapta a los estándares del SGSI utilizado por empresas que pertenecen a la misma cadena hotelera por lo que los casos de éxito por su aplicación son notorios; por tanto, efectuar este análisis no será una pérdida de tiempo.

Además según (Alvarado, Pacheco, & Martillo, 2018) Magerit persigue objetivos directos e indirectos. En los objetivos directos están: concienciar a los responsables y jefes en la empresa de la existencia de riesgos, dando a conocer la necesidad de poder gestionarlos y planear un tratamiento oportuno en caso de que los riesgos ataquen los activos de información, mientras que en los indirectos están: preparar a la organización para procesos de evaluación, auditoría, certificación y acreditación.

3.4. Etapa 1: Análisis GAP para diagnóstico del nivel de cumplimiento normativo en la empresa.

El desarrollo de esta etapa es primordial para comenzar con el análisis de riesgo porque es necesario determinar el nivel actual que posee la empresa sobre su aplicación y cumplimiento de los controles precisando el nivel de los requisitos para que un SGSI, lo que permitirá obtener las brechas de seguridad de mayor impacto para la organización. Para el desarrollo de esta etapa se realizarán entrevistas con los departamentos definidos anteriormente con el ánimo de determinar los procesos que desarrollan cotidianamente y los controles que se relacionan con sus actividades.

El análisis GAP está basado en las normas ISO 9001 2015 y las normativas son del listado de los requisitos de la ISO27001 que son obligatorios para tener un SGSI estable, el catalogo desarrollado fue adaptado de un documento proporcionado por (ISO27k, 2013).

3.4.1. Fase 1: Revisión de los Controles Existentes.

En esta fase se desarrolla a través de múltiples entrevistas dirigidas hacia el personal clave del proyecto para saber el nivel de aplicación de las normativas establecidas en las actividades que desarrollan diariamente. Se realiza una calificación cualitativa y cuantitativa según en nivel de aplicabilidad que tienen cada norma.

Para conocer cuáles son las brechas que restan al nivel de madures de un SGSI se procede a valorar la aplicación de los requerimientos necesarios que componen al sistema de gestión de seguridad ayudando a establecer la distancia que existe entre los practicas actuales que aplica la empresa sobre las que espera la normativa establecida, una vez definida esa distancia e identificado las brechas se procede a su respectivo análisis.

3.5. Etapa 2: Análisis de Riesgos Basadas en la Metodología MAGERIT

Para determinar el riesgo es necesario realizar unos procesos sistemáticos que permita desarrollar el análisis pertinente de los activos lógicos de la empresa, la cual se encuentra compuesta por fases detalladas a continuación:

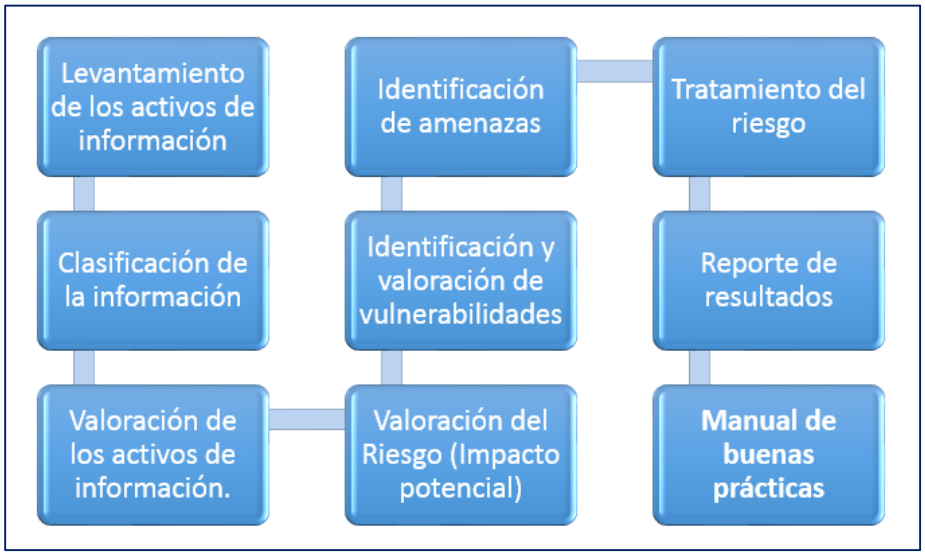

Figura 4: *Etapas para el análisis de riesgo.*
Fuente: (Autor, 2019)

3.5.1. Fase 1: Levantamiento de activos de información.

En esta fase se busca determinar los activos de mayor relevancia para el sistema de seguridad de la información y para sus operaciones organizacionales, mediante una clasificación que brinda Magerit en donde los divide por categorías, de la siguiente manera:

- **Arquitectura del sistema:** Se trata de elementos que forman parte de la estructurar del sistema de información.
- **Datos / Información:** Los datos son el pilar fundamental de la empresa, sin ella no tendría ningún valor, la cual se encuentra almacenado en equipos o soportes de información.
- **Claves criptográficas:** La criptografía ayuda a proteger el secreto y autenticar a las partes que tienen accesos a la información.
- **Software:** Hace referencia al software de sistema y aplicación y herramientas de desarrollo.
- **Equipamiento informático (hardware):** Son los medios materiales, físicos, destinados a soportar los servicios que presta la empresa.
- **Redes de Comunicación:** Incluyendo tantas instalaciones dedicadas y los servicios de comunicaciones prestados de terceros.
- **Soportes de Información:** Son los dispositivos físicos que permiten almacenar información de forma permanente o, durante periodos largos.
- **Equipamiento Auxiliar:** Se consideran los equipos que sirven de soporte al sistema de información.
- **Instalaciones:** Son los lugares donde se ubican los sistemas de información y comunicaciones.
- **Personal:** Las personas relacionadas estrechamente con el manejo sistemas de información.

El método para realizar el levantamiento de los activos en la empresa es por medio de las diferentes revisiones técnicas en las instalaciones que forman parte del sistema de información, con la finalidad de comprender su interrelación. Los activos de información permiten el desarrollo de las actividades empresariales y son el principal elemento a defender, se puede encontrar de manera tanto física como intangible los cuales se registrarán de manera digital.

3.5.2. Fase 2: Clasificación de la Información

Para realizar un análisis de gestión es necesario realizar esta fase para relacionar los activos informáticos y de información, es decir conocer cuáles son los medios o canales de mayor importancia en la empresa para en tratamiento de la información. Gracias a esta clasificación es más fácil conocer que activo necesita mayores políticas o controles para poder fortalecer su confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad, entonces la información se puede clasificar en:

- **Pública:** La información que puede considerarse como publica es aquella que está conformada por datos de esta naturaleza, es decir, puede ser compartida, comunicada sin requerir algún tipo de autorización previa y que sea definida por la ley ecuatoriana considerando que la información es de uso público.
- **Semiprivada:** La información es considerada como semiprivada cuando los datos que la conforman son particulares, pero no reservadas, además de interesarle a su titular también es de interés por parte de las organizaciones, por lo que antes de ser requerida se necesita algún tipo de autorización, se debe tener en cuenta que si no se procede con lo anterior podría causar un tipo de violación a la confidencialidad y perjudicar a su titular.
- **Privada:** La información es netamente privada es aquella que los datos que la componen son de esa naturaleza, es decir, solo pueden ser de uso único por el titular de la información, para el uso de terceros es importante que el titular lo autorice, si se llegase a manejar sin esta autorización puede provocar ciertas acciones negativas para los terceros.

3.5.3. Fase 3: Valoración de Activos.

La valoración de activos se realiza en base a los seis pilares de la seguridad que funcionan como dimensiones para la evaluación cualitativa y cuantitativa de manera que permita conocer las consecuencias de la materialización de las amenazas de cada activo, su valor está basado en su interrelación. De manera que su nivel de importancia está ligada a las propiedades que posee además del tipo de información que maneja.

3.5.4. Fase 4: Identificación de Amenazas

Una vez identificado los principales activos de información, el siguiente paso consiste en identificar las amenazas a las que estos están expuestos. “Tal y como imaginamos, el conjunto de amenazas es amplio y diverso por lo que debemos hacer un esfuerzo en mantener un enfoque práctico y aplicado” (INCIBE, 2017). Para realizar esta tarea se emplearon las amenazas sugeridas por MAGERIT que conforman el catalogo principal en el que se base el análisis de riesgo.

3.5.5. Fase 5: Identificación y Valoración de las Vulnerabilidades.

La siguiente fase se enfoca en descubrir las debilidades que se encuentran asociadas a cada grupo de activos de información y por estas brechas puede suscitar las amenazas, este paso es esencial para conocer cuáles son los puntos débiles que tiene el sistema de información. El catálogo de las vulnerabilidades es el resultado de revisiones a los equipos finales, análisis de las políticas de seguridad establecidas en la empresa, reportes de vulnerabilidades por parte de los auditores y los proveedores de tecnología, sediciones de la cada área de trabajo, la aplicación de controles manejados por en jefe de TI/Sistemas de la empresa.

Típicamente suelen realizarse pruebas de pentesting dirigidas hacia la red de comunicación de la empresa para descubrir las vulnerabilidades en los equipos que lo conforman, en este caso, no se realizaran este tipo de análisis por falta de las medidas necesarias de seguridad para desarrollar pruebas de este tipo. Para la valoración de vulnerabilidades se toma en consideración dos características importantes que son la severidad y la exposición.

3.5.6. Fase 6: Valoración del Riesgo

El catálogo de riesgo se realiza en base a las vulnerabilidades que tuvieron mayor valoración en criterio de que la explotación de las misma aumenta la probabilidad de explotar vulnerabilidades adicionales, es decir, esta lista de riesgos está conformada por las vulnerabilidades que tienen mayor nivel de exportación dentro de la empresa y la valoración se estima la probabilidad en cada activo, en el peor de los casos, de que se materialice la vulnerabilidad mediante parámetros cualitativos y cuantitativos se ubican los riesgos después de su evaluación en un mapa de calor, para determinar los riesgos que tienen un nivel de criticidad alto.

3.5.7. Fase 7: Tratamiento el Riesgo Potencial.

Una vez que se hayan identificados los riesgos la última fase consiste en responder mediante medidas de seguridad para mitigarlos, estas medidas pueden presentarse de cuatro maneras: Evitar, Transmitir, Aceptar y Reducir

3.5.8. Fase 8: Reporte de resultados

En esta fase se espera reportar los resultados encontrados después de análisis de riesgo a la Dirección de tecnología de la empresa y proveedores de tecnología a través del jefe del departamento de TI/Sistemas, con el objetivo de que el análisis aporte a al SGSI se presenta un resumen de los resultados encontrados a lo largo de este análisis para que puedan hacer uso según lo requieran.

3.5.9. Fase 9: Manual de Buenas Prácticas

De acuerdo con los objetivos establecidos de crear una cultura de seguridad que este conformada por el personal y soluciones tecnológicas se realizará un documento que contemple una serie de políticas de seguridad y salvaguardas dirigidas para los empleados que manejan información de la empresa y para el jefe de TI/Sistemas para impulsar y mejorar el tratamiento de riegos con el objetivo de fortalecer el sistema de seguridad de la información del negocio.

4. CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS

Para determinar el grado de confianza y cumplimiento de las normas y políticas establecidas por el SGSI de la empresa, se procedió a evaluar la cultura de seguridad por porte de los empleados hasta los altos mandos y de las herramientas tecnológicas que forman parte de este entorno de SI. Lo cual permitirá dar forma a una parte del estado actual de la seguridad de los activos de información y su nivel de resiliencia frente a un caso de ataque.

4.1.Análisis de Resultados de las Encuesta

Para analizar el ambiente de seguridad de la información del negocio se procedido a realizar encuestas dirigidas hacia un grupo específico de empleados (Anexo 1), que permite recopila información para medir el grado de confianza y cumplimiento de las políticas de seguridad en relación con los objetivos previstos con este proyecto para la empresa Four Points by Sheraton Cuenca. A continuación, se muestra los resultados obtenidos:

- **¿Qué áreas considera usted son las principales responsables de la gestión de riesgo cibernético?**

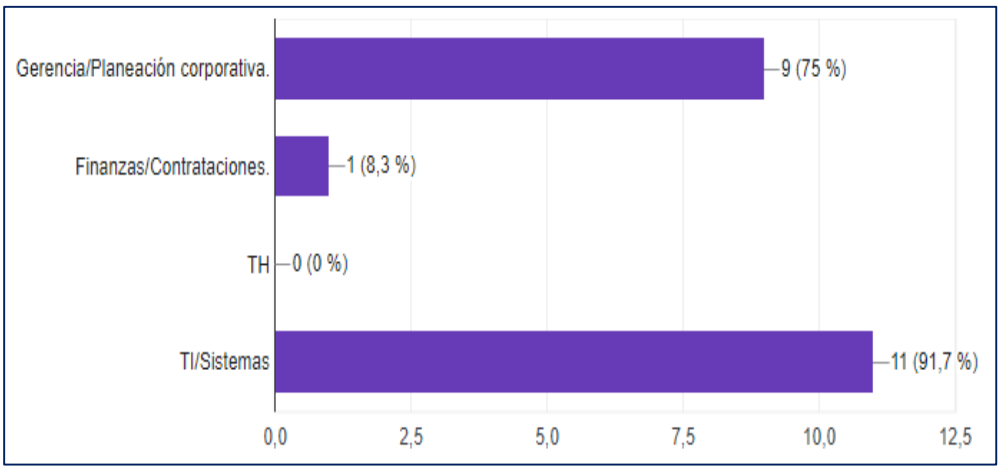

Figura 5: *Resultado de la pregunta 1 en la encuesta.*
Fuente: *(Autor, 2019).*

Con esta pregunta se busca conocer cuáles son los principales departamentos que tienen responsabilidades sobre la gestión de riesgos de la información por lo general el área de TI/Sistemas es el encargado de diligenciar todos los asuntos relacionados. Casi un 92% atribuye esta responsabilidad al departamento de TI/Sistemas lo que significa un nivel de confianza bastante alto y positivo en esta área por parte de las demás, otro de los roles que tuvieron un resultado del 75% de nivel de compromiso con la gestión de riesgos fue la Gerencia/Planeación corporativa lo que significa que ambas áreas también se encuentran relacionados y existe un apoyo y seguimiento al proyecto de seguridad en la empresa.

- **¿En qué nivel usted cree que la inversión de nuevas tecnologías ayuda a controlar las amenazas de ciberataques?**

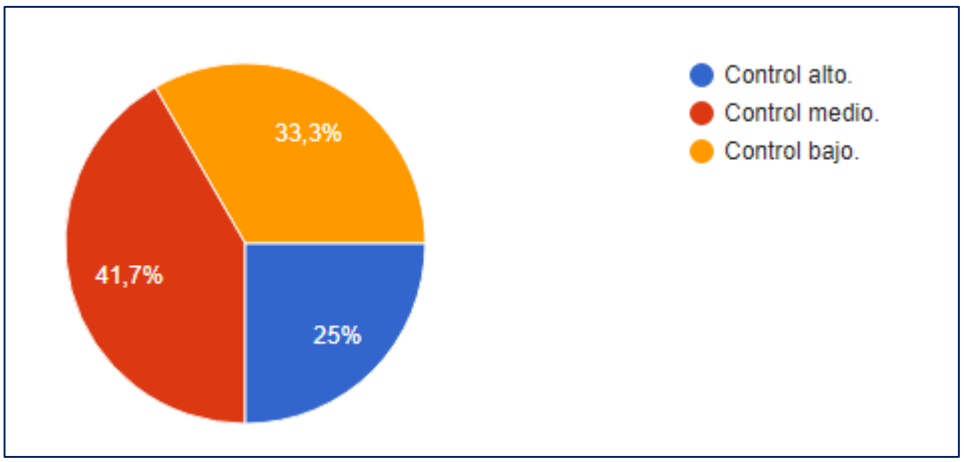

***Figura 6**: Resultados de la pregunta 2 en la encuesta.*
***Fuente:** (Autor, 2019).*

Las aplicaciones de nuevas tecnologías aparte de ayudar a controlar las amenazas de ciberataque son también uno de los proyectos que más recursos necesita. El 42% indica que cree que la adopción de estas emergentes tecnologías mantiene un control medio y un 33% cree que tiene un control bajo sobre las amenazas y por otro lado un 25% cree que es alto, lo que indica que existe un cierto nivel de incertidumbre sobre su función, los pros y contras que podría tener este tipo de proyectos.

- **En este último año ha recibido capacitaciones sobre la gestión de riesgos cibernéticos.**

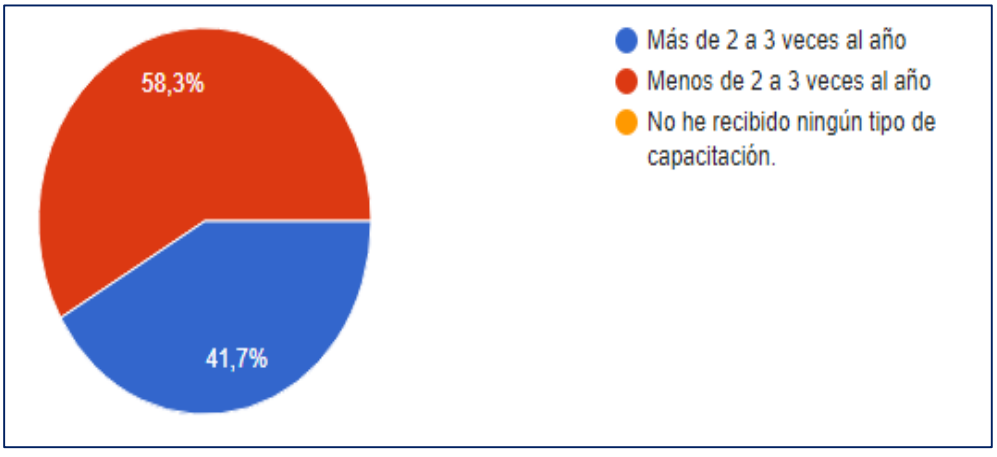

***Figura 7:** Resultados de la pregunta 3 en la encuesta.*
***Fuente:** (Autor, 2019).*

Las capacitaciones ayudan a fortalecer y crear una cultura de seguridad informática entre todas las áreas que componen la organización para prevenir la materialización de amenazas, Casi un 58% dijo que ha recibido más de 2 a 3 veces al año una capacitación sobre ciberseguridad y un casi 42% indico que lo recibía más de 2 a 3 veces al año, lo que indica de la empresa se encuentra en una constante evaluación de riesgos que puede asegurar que los empleados mantienen conocimientos sobre las amenazas que puede llegar a tener la empresa y como controlar su materialización. Los que llevan más de 2 a 3 veces al año son por lo general los jefes de cada área y la otra parte el 58% son empleados de los departamentos.

- **Indique cuál de las siguientes afirmaciones refleja mejor la adopción de políticas de seguridad de la información en su empresa.**

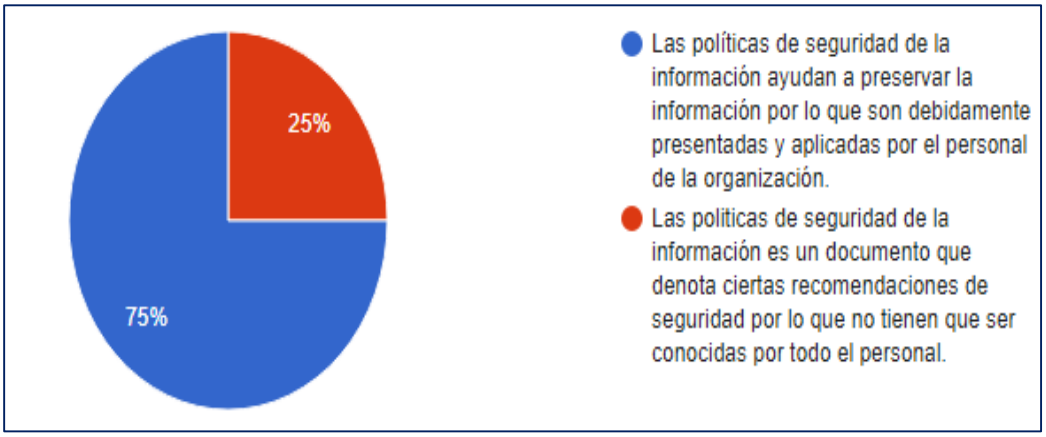

Figura 8: *Resultados de la pregunta 4 en la encuesta.*
Fuente: *(Autor, 2019)*

Las políticas de seguridad de la información son un elemento fundamental para ayudar a preservar la información, Un 75% afirmo que las políticas establecidas en la empresa representan un papel fundamental y la importancia de comunicar el documento hacia todo el personal que maneja información de la empresa, por lo que se puede decir que los empleados en cuanto a conocimiento sobre estas políticas están en un nivel muy bueno.

- **¿En qué nivel usted considera que la organización está en la capacidad para enfrentar el riesgo cibernético?**

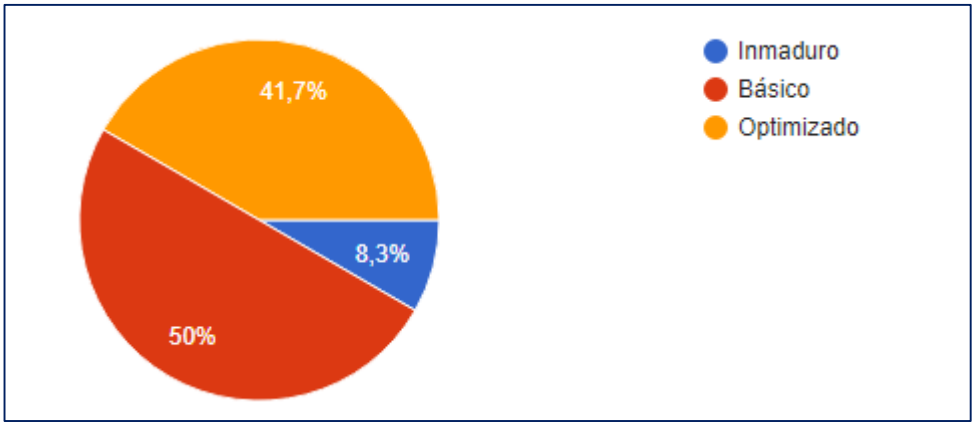

Figura 9: *Resultados de la pregunta 5 en la encuesta.*
Fuente: *(Autor, 2019)*

La baja confianza que pueden tener las empresas representa un problema en sus habilidades para mitigar un riesgo así también como la falta de conocer su capacidad para enfrentarse a estas situaciones. Un 50% dijo que su nivel para enfrentar cualquier tipo de materialización de amenazas es básico y casi un 42% afirma que pueden asumir un ataque cibernético, es decir una parte confían completamente en los procesos para prevención de amenazas tanto en la empresa como fuera de la misma y otra asume que están listos para enfrentar estos casos, esto puede indicar que existe por parte de algunos empleados un desconocimiento de cuanto puede ser la resiliencia de la empresa o si es seguro que la empresa está más que lista para enfrentar los riesgos, con un análisis especifico se podrá tener una idea más clara de la situación.

- **Indique cuál de las siguientes afirmaciones refleja mejor la actitud de la empresa.**

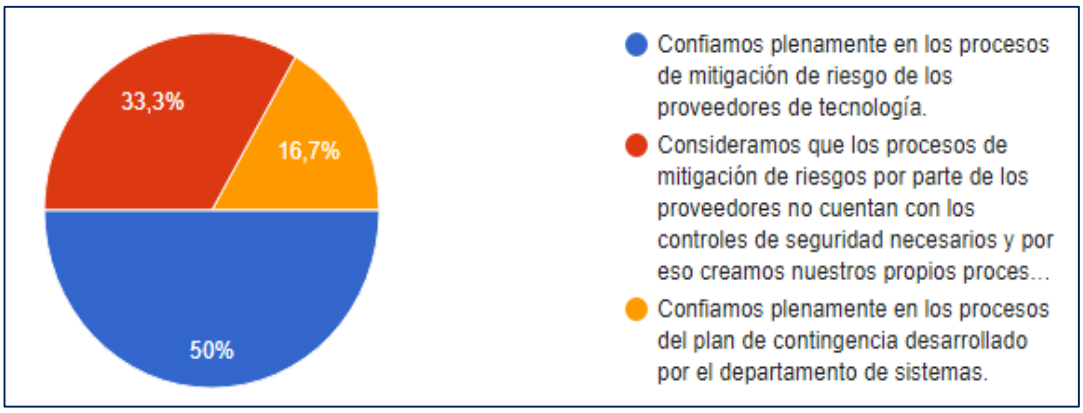

Figura 10: *Resultados de la pregunta 6 en la encuesta.*
Fuente: *(Autor, 2019)*

Un 33% asume que los proveedores traen consigo las amenazas que pueden afectar a la empresa mientras que un 50% confía en los procesos de mitigación de riesgos de los proveedores. Se puede asumir que la empresa tiene un nivel de confianza más alto en los procesos que ofrecen los proveedores de tecnología que su propia área de seguridad.

- **¿Considera que el departamento de sistemas fortalece constantemente la seguridad de los equipos informáticos en su área de trabajo?**

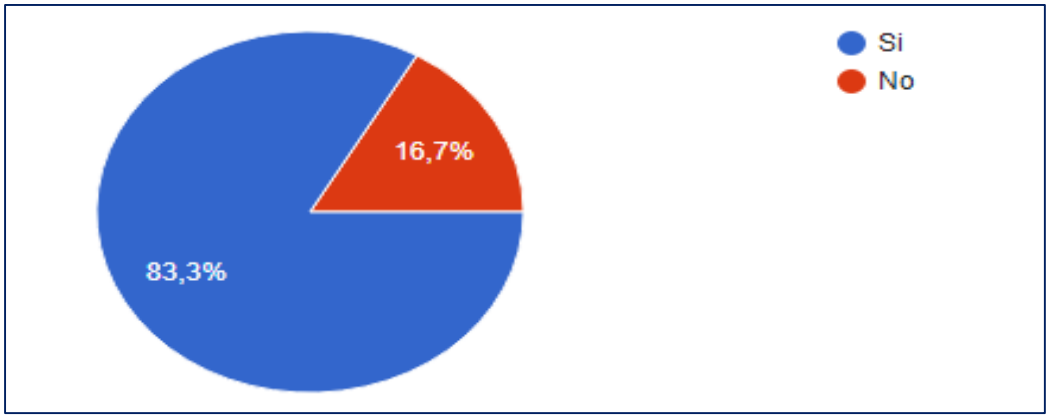

Figura 11: *Resultados de la pregunta 7 en la encuesta.*
Fuente: *(Autor, 2019).*

Un 83% afirmo tener plena confianza y seguridad de que el departamento de sistemas fortalece los procesos de seguridad para los activos de información que se encuentran en cada área de trabajo.

- **Considera usted que las verdaderas amenazas cibernéticas:**

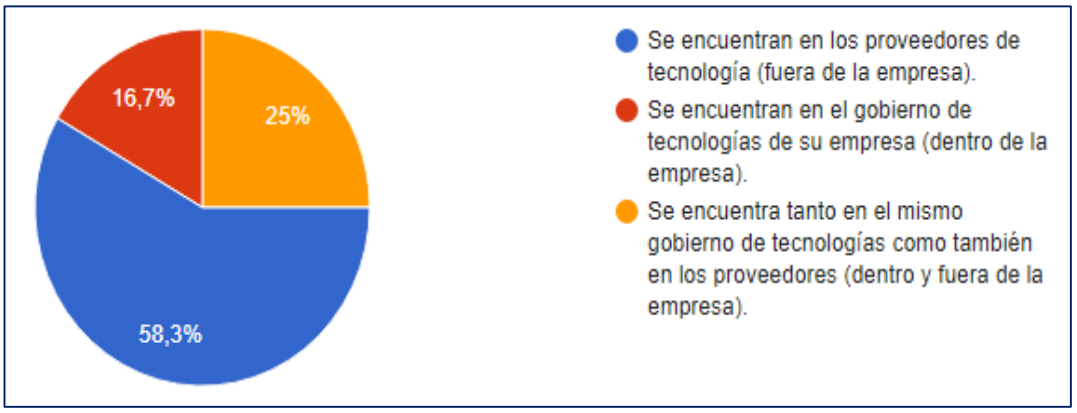

Figura 12: *Resultados de la pregunta 8 en la encuesta.*
Fuente: *(Autor, 2019).*

Un 58% afirmo que las verdaderas amenazas se encuentran fuera de la empresa, es decir que la falta de normas y políticas de seguridad por parte de los proveedores de tecnología trae consigo consecuencias graves para la seguridad de la información y la falta de definición de acuerdos con terceros es uno de los mayores riesgos para enfrenta la empresa.

- **¿La empresa cuenta con un documento que recoge las buenas prácticas a aplicar con el objetivo de formar un entorno seguro y un soporte de capacitación que previenen los riesgos informáticos?**

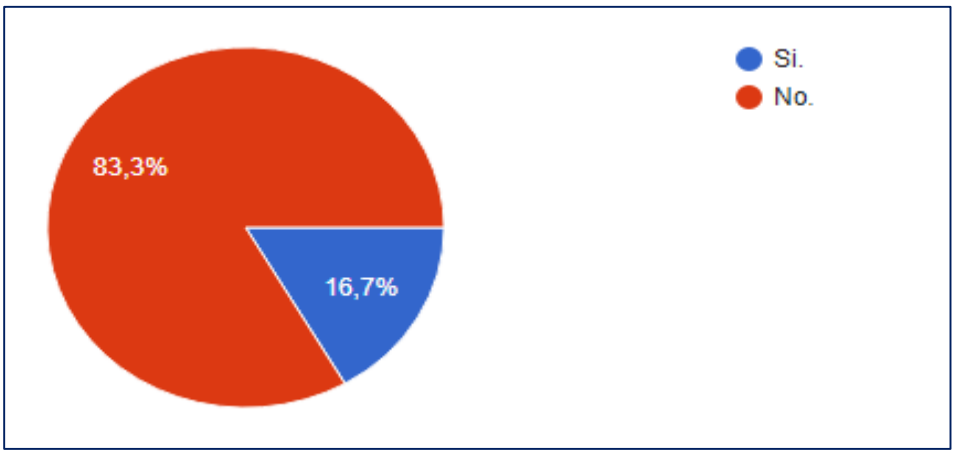

Figura 13: *Resultados de la pregunta 9 en la encuesta.*
Fuente: *(Autor, 2019).*

El manual de buenas prácticas en seguridad informática representa un factor clave para desarrollar una cultura para la protección de la información, en donde no solo las soluciones de seguridad son importantes si no también la educación de los empleados que manejan la información, un 82% afirma que no existe un documento como tal que recoja este tipo de pautas de seguridad, por lo que tener uno resulta un factor importante y sería muy útil que existiera.

Como observaciones finales de esta encuesta podemos identificar que el entorno de seguridad que vive la empresa por parte de los empleados es una comunidad que ha ido mejorando año tras año ya que han sabido dar importancia a las nuevas tecnologías y al riesgo que conlleva aplicarlas en el entorno de trabajo, el área de TI/Sistemas no maneja solo esta gestión si no que existen otras áreas que se involucran y dan seguimiento a los procesos de seguridad lo que mantiene en un nivel bastante alto y existe mayor confianza en los procesos de seguridad que toman los proveedores correspondiente a cada sistema informático que esta implementado en su SGSI.

4.2. Análisis de Resultados Sobre el Estado Actual del SGSI con Gap

Generar un informe de análisis GAP con el objetivo de establecer brechas existentes entre el grado de aplicación de los controles de seguridad y los requerimientos para un SGSI cumpliendo con las normas y requisitos necesarios que comprende un sistema de

información, como también permitir establecer mejores procesos para optimizar el nivel de maduración actual de la organización.

De acuerdo con lo mencionado anteriormente el siguiente informe de brechas de información pretende determinar el grado de cumplimiento que tiene la empresa Four Points by Sheraton Cuenca con respecto a los lineamientos establecidas por la norma ISO 27001. El análisis es cualitativo y cuantitativo, hace hincapié en identificar las actividades de mayor riesgo de seguridad en un SI, todos los datos necesarios para la evaluación fueron obtenidos en apoyo con el jefe de TI/Sistemas así también como la presentación de los resultados. Los niveles de madures para la empresa tienen 6 estados, los cuales están justificados en la siguiente tabla:

Tabla 4: *Niveles de madures GAP.*

Estado	Descripción
0- Inmaduro	Las salvaguardas no existen, no existe un proceso de ningún tipo donde se pueda gestionar. Su éxito depende de tener personal de la alta calidad.
1- Básico	La medida de seguridad no corresponde a procesos documentados, es decir de una manera totalmente informal (con procedimientos propios, informales), no existe ningún seguimiento
2- Gestionado	El control se aplica conforme a un procedimiento documentado, de acuerdo a la planificación y realizándose un seguimiento.
3- Establecido	Existen procesos definidos donde se gestionan. Cada implementación de un proceso se hace utilizando procedimientos creados según un estándar y documentados
4- Predecible	La organización gestiona los procesos conforme a documentación y de manera cuantitativamente.
5- Optimizado	Se mejora continuamente los procesos para cumplir los objetivos de la empresa

La valoración de las normas de madurez según GAP (Elaboración propia).

Utilizando estos niveles se pudo identificar el rango de madurez por cada dominio, los cuales se encuentran definidos en el anexo B, permitiendo evidenciar lo siguiente:

En la (Figura 12) se presenta los resultados de los dominios que fueron plasmados en un gráfico de radar el cual muestra el nivel que alcanzan los factores representados de una manera cuantitativa con el fin de mostrar perfiles de máximos y mínimos, además demuestra gráficamente el equilibrio o desequilibrio entre los dominios.

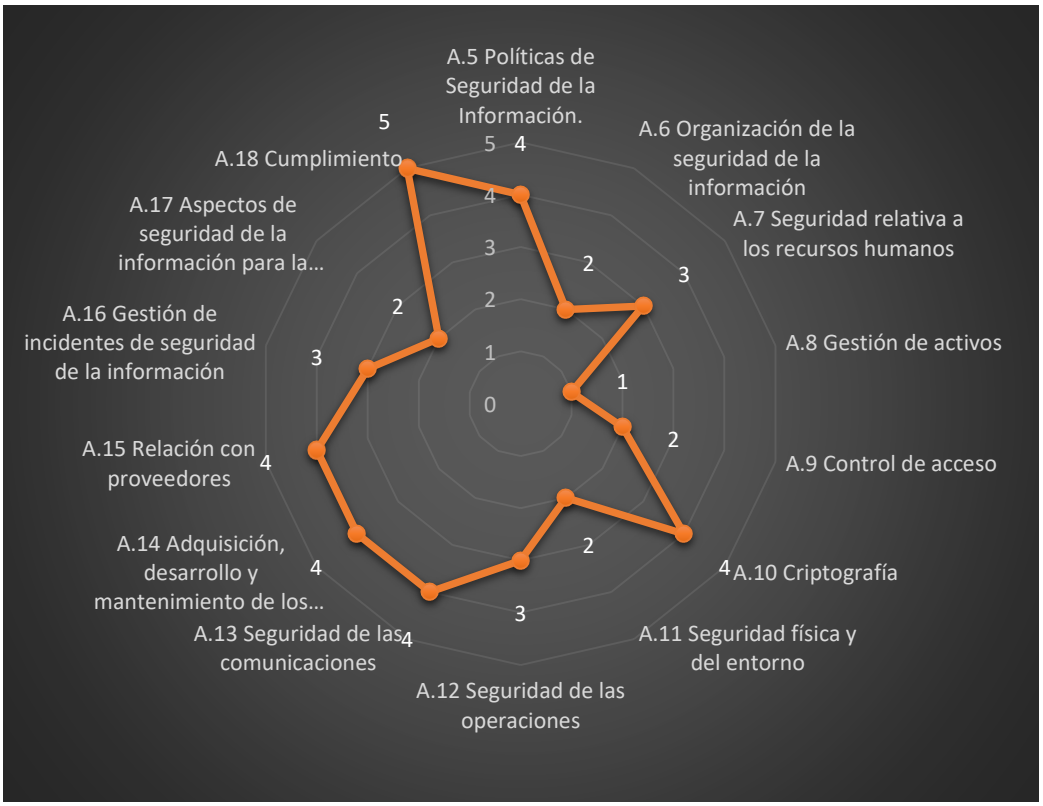

Figura 14: *Alcance de los dominios GAP.*
Fuente: *(Autor, 2019)*

Según la escala dispuesta anteriormente el nivel de cumplimiento se obtuvieron las siguientes calificaciones para cada dominio:

El valor por el cual una entidad demuestra tener procesos mínimos seguros es del 70% y la porción de requerimientos para un SGSI por cumplimiento de requisitos es de un 60% sobre el estado de cumplimiento que en total es el 100% lo que permite evidenciar un nivel establecido sobre el requerido demostrando que la empresa se encuentra en cumplimiento con los requerimientos, pero existen dominios que se deben fortalecer.

Tabla 5: *Resultado Análisis GAP*

Estado	Descripción	Proporción de requerimientos de un análisis de riesgos	Proporción de Controles de Seguridad de la Información
0- Inmaduro	Las salvaguardas no existen, no existe un proceso de ningún tipo donde se pueda gestionar. Su éxito depende de tener personal de la alta calidad.	4%	10%

1- Básico	La medida de seguridad no corresponde a procesos documentados, es decir de una manera totalmente informal (con procedimientos propios, informales), no existe ningún seguimiento	9%	8%
2- Gestionado	El control se aplica conforme a un procedimiento documentado, de acuerdo a la planificación y realizándose un seguimiento.	16%	14%
3- Establecido	Existen procesos definidos donde se gestionan. Cada implementación de un proceso se hace utilizando procedimientos creados según un estándar y documentados	11%	22%
4- Predecible	La organización gestiona los procesos conforme a documentación y de manera cuantitativamente.	18%	27%
5- Optimizado	Se mejora continuamente los procesos para cumplir los objetivos de la empresa	2%	20%
		54%	100%

Los resultados del análisis de GAP (Elaboración propia).

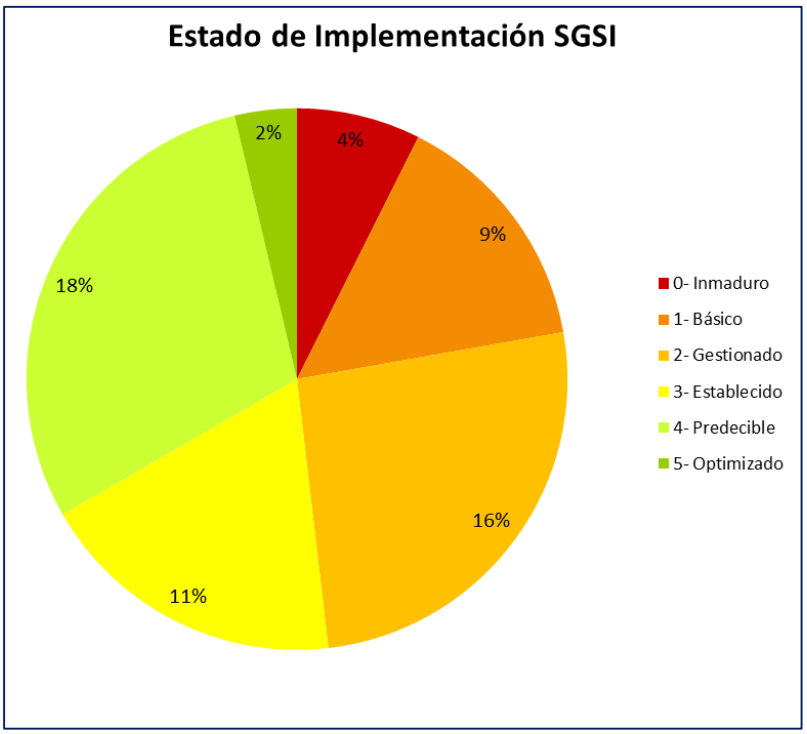

Figura 15: *Resultados de Análisis GAP.*
Fuente: *(Autor, 2019)*

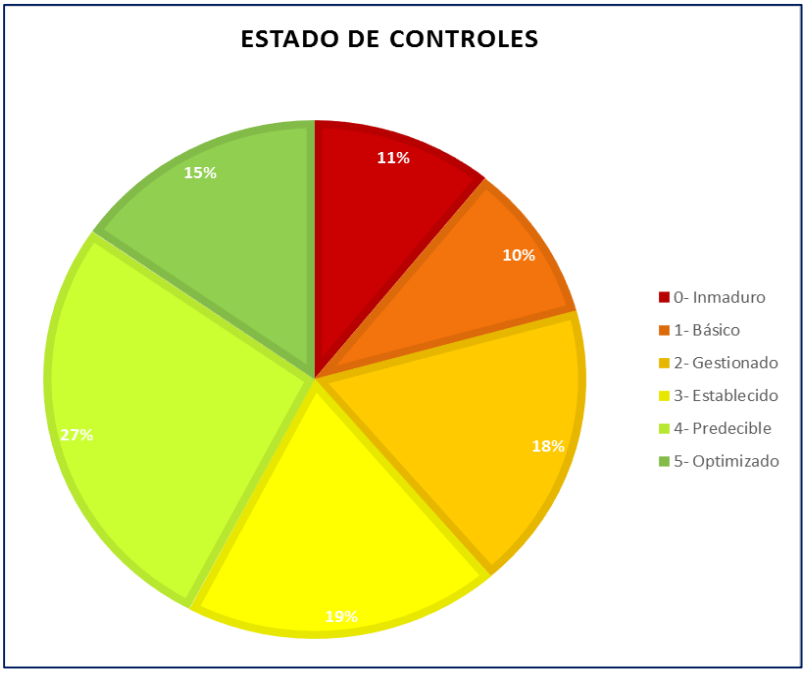

Figura 16: *Estado de controles GAP.*
Fuente: *(Autor, 2019).*

A través de este estudio se pudo establecer siete brechas que describen de mejor manera la distancia existente entre los controles de seguridad de la información y los requerimientos de un SGSI aplicados en la empresa:

Brecha 1. _Organización de la seguridad de la información

- Crear una política para dispositivos móviles para que limitar y controlar el uso de los dispositivos móviles para controlar la propagación de amenazas.

Brecha 2. _ Gestión de Activos

- Realizar un inventario de activos con su respectiva categorización ya que la existente en la empresa no se encuentra actualizada.
- Definir la clasificación de la información según su importancia ya que en procesos de recuperación de desastres la empresa restaura toda la información almacenada en los equipos comprometidos hasta la cierta información que no tiene ningún tipo de relación con sus operaciones, esta información muchas veces es almacenada por los empleados en equipos de la empresa ocupando espacio innecesario.
- Crear una política documentada para gestionar las unidades removibles que contienen información sensible para la empresa, debido a que existen empleados que utilizan el mismo dispositivo para guardar información de todo tipo y suelen prestarse entre si lo que puede ocasionar fugas de información confidencial.

Brecha 3. _ Control de acceso

- Definir un documento formal en donde se registre los usuarios que tienen todo tipo de accesos a la red interna, existen procesos para el registro, pero no genera ningún tipo de documentación.

Brecha 4. _ Seguridad Física y del entorno

- Mantener el ambiente libre de documentos físicos, notas, contraseñas importantes para la empresa y apagar los equipos de cómputo una vez que salgan cerrar las puertas de los departamentos porque existen información confidencial sobre los escritorios y podrían ser hurtados por terceros.
- Concientizar a los empleados acerca de la política que cubre la integridad de los equipos al momento de que salgan de la empresa y los riesgos que implica debido a que existe personal que sale con el equipo fuera de las instalaciones.
- Al formatear los ordenadores en el memento de que se restaura la información suele ser muy a menudo que no se elimina la información de la sesión anterior por lo que se debe crear una política para la eliminación segura de la información.

Brecha 5. _ Aspectos de seguridad para la gestión de la continuidad del negocio

- Mantener revisiones periódicas sobre los requisitos futuros del SGSI en respuesta a nuevas vulnerabilidades.

Brecha 6. _ Aspectos de seguridad para la gestión de la continuidad del negocio

- Crear un proceso para la designar los datos para pruebas (actualmente en desarrollo por la misma organización).

Brecha 7. _ Gestión de incidentes de seguridad de la información

- Documentar de manera específica las responsabilidades administrativas sobre incidentes para identificar y direccionar los reportes de los casos más relevantes.

4.3.Resultados del Análisis de Riesgo de Seguridad de la Información

El análisis de riesgo de seguridad de la información para la empresa Four Points by Sheraton pretende identificar y evaluar las amenazas a los que se exponen los activos de información con el objetivo de recomendar los controles apropiados y un manual de buenas prácticas aplicando la metodología MAGERIT.

Como primer paso para realizar el análisis de riesgos fue construir un inventario de los activos más relevantes para la empresa y su valoración según el impacto que tiene para la organización. Mediante técnicas como la observación directa y la ayuda del jefe de TI/Sistemas se pudo identificar los activos de información más significativos que forman parte de la empresa.

Los niveles de valoración son mediante una escala cualitativa y cuantitativa detallada de 5 valores, los cuales están justificados en la siguiente tabla:

Tabla 6: *Valoración de activos.*

Valor	Porcentaje	Criterio	Estado
5- Extremo	**22 - 25**	daño extremadamente grave	23%
4- Muy alto	**18 - 21**	daño muy grave	28%
3- Alto	**14 - 17**	daño grave	28%
2- medio	**10 - 13**	daño importante	9%
1- Bajo	**6 - 9**	daño menor	9%
0- Despreciable	**0 - 5**	irrelevante a efectos prácticos	2%
			100%

El resultado de la valoración de los activos (Elaboración propia).

En la tabla 7 se agrupan los activos de información de acuerdo a su nivel, permitiendo establecer cuales son más susceptibles a recibir un ataque informático y de sufrir una materialización de amenazas y el impacto que tendría en la organización.

La empresa cuenta con activos que pueden significar una gran pérdida al momento de enfrentarse a un riesgo, para el análisis se tomó en cuenta los activos que se encuentran en los siguientes niveles; extremo con 23%, muy alto con 28%, alto con un 28% y se descartan los demás niveles porque no representan un mayor impacto.

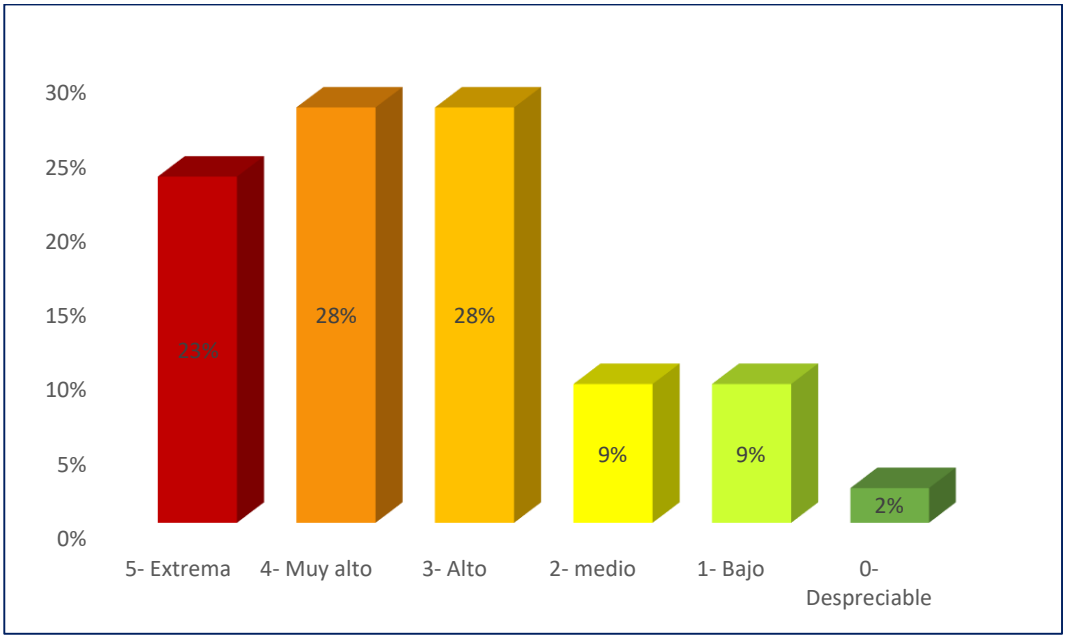

Figura 17: *Diagrama de barras según la valoración de activos.*
Fuente: *(Autor, 2019)*

4.3.1. Revisión de requisitos para el análisis de riesgo.

Tabla 7: *Requisitos para el análisis de riesgo.*

Verificación del estado de implementación del sistema de gestión de seguridad de información en la empresa Four Points by Sheraton Cuenca para el desarrollo del presente análisis de riesgo.	
Observaciones	• En la empresa se han desarrollo aprobado y publicado, por parte de la Dirección de Tecnología de la cadena hotelera, 32 políticas de seguridad de la información.

	• Las políticas de seguridad se crearon en base a la reglamentación de la ley ecuatoriana. • La empresa desarrolló un conjunto de políticas puntuales que tienen un cierto grado de alcance. **<u>Recomendación</u>** *Se sugiere una reevaluación de las políticas y sus alcances.* • Se toma en consideración para el desarrollo del análisis de riesgo las últimas pruebas de hacking ético realizadas en la empresa con apoyo de la Dirección de tecnología y las recomendaciones sugerida por parte del auditor de SI. • No se realizaron nuevas pruebas de penetración al sistema debido a la falta de tiempo para preparar los espacios de prueba y la selección de datos ya que la empresa maneja un gran volumen de datos y no se puede proceder a infiltrarse en la red de comunicación sin antes obtener permisos de la Dirección de tecnología. **<u>Recomendación</u>** *Agendar un nuevo proyecto para pruebas de hacking ético en el siguiente año, con el fin de encontrar nuevas vulnerabilidades y reevaluar el nivel de seguridad de los SI.*

Revisión de requisitos para el análisis de riesgo (Elaboración propia).

4.3.2. Resultados del análisis de riesgo.

Tabla 8: *Resultados del análisis de riesgo.*

Analizar los resultados de las actividades que se desarrollaron en la aplicación de la propuesta.	
Observaciones	• En el cuadro de riesgos se identificaron un total de 21 riesgos para los activos de la seguridad de la información, resultado de la fase final de este análisis, se listan los riesgos con una mayor probabilidad de ocurrencia, los cuales se describen en función a la amenaza (causa por error o mala intención). Ejemplo: ✓ Destrucción de la información por error de los usuarios. ✓ Accesos no autorizados a documentos. ✓ Alteración accidental de la información. ✓ Errores secuenciales de registro de actividades. ✓ Uso no previsto de los servicios. • En el departamento de TI/Sistemas de la empresa se encuentra realizando un plan de actividades para la evaluación de riesgos tomando en cuenta los riegos descubiertos en este análisis, con la intervención del auditor encargado para analizar los procesos metodológicos, mapa de riesgos y los planes de mitigación. **Recomendación:** *Para mantener un enfoque centrado de las vulnerabilidades y amenazas se propone la lista*

	puede pasar a una reevaluación por parte del departamento de TI/Sistemas y el apoyo de los jefes de áreas también responsables para este proceso. • En el ANEXO A se muestra el análisis de riesgo general de los activos dela información, se pueden observan datos como; la identificación de amenazas y vulnerabilidades que se encuentran presentes en los diferentes grupos de activos, identificador del riesgo, la descripción del riesgo y por último la valoración del riesgo. En esta documentación no se muestra el nivel de clasificación de la información asociada con los activos debido a los acuerdos de confidencialidad con la empresa. **Recomendación:** *Para futuros análisis de riesgo incluir los resultados los valores de los niveles de clasificación de la información (pública, reservada o confidencial).* • Con relación al mapa de calor para los riesgos del análisis de riesgo de la información se observó que no se estableció criterios de evaluación financiera costo-beneficio para la mitigación del riesgo que ayudarían a determinar el alcance y los riesgos residuales siendo este proceso importante para adoptar acciones y decisiones de la aplicabilidad de este proyecto por parte de la institución. **Recomendación:** *Es importante que la Dirección de tecnología incluya el nivel de tolerancia al riesgo estableciendo los criterios financieros que permita tomar la mejor*

	opción de mitigación según el costo y esfuerzos que estén en posibilidad de la empresa para así calcular el riesgo residual. • Se observa que ciertos controles de seguridad se encuentran aplicados, pero no documentados, de estos se derivan ciertas amenazas que no se incluyen en la lista de riesgo porque ya se encuentran controladas mediante controles. **Recomendación:** *Es importante que el departamento de TI/Sistemas documente sus procesos de seguridad y estén aceptados por la Dirección de tecnología.* • La metodología MAGERIT está incluida en los estándares ISO, lo que sirve como un punto de partida para los procesos de certificación para la empresa. **Recomendación:** *Es importante que el departamento de TI/Sistemas tome en cuenta los resultados de este proyecto y los adapte a la metodología propia de los directivos de seguridad GHL, ya que Magerit es una de las más moldeables para todo tipo de metodologías.* • De la empresa depende la aplicabilidad total o parcial del proyecto al su SGSI y seguir un proceso de certificación debido a que este proyecto, por temas de seguridad y protección de información, no cuenta con especificaciones como la clasificación de su información y el costo-beneficio de los controles.

	<u>Recomendación:</u> *Es importante que el departamento de TI/Sistemas y a quien corresponda adapte los resultados del análisis de riesgo e incluya la valoración de la clasificación de su información y el costo-beneficio al SGSI de la empresa.* **<u>Recomendación:</u>** *Se propone desarrollar un manual de buenas prácticas de seguridad de la información con el fin de prevenir y disminuir los ataques de ciberseguridad a través de la educación.*

Analizar los resultados de las actividades de la propuesta. (Elaboración propia).

5. Capítulo V

Desarrollo de la Propuesta del Desarrollo

5.1.Antecedentes de da Empresa

El hotel inicio su operación en el año 2017 y se inauguró el 27 de octubre del mismo año. La Empresa “Four Points by Sheraton” fue insertada en la ciudad de Cuenca como una de las franquicias operadas por la cadena hotelera GHL en Ecuador; esta empresa cuenta con estándares de calidad en todos los procedimientos en atención al cliente y una excelente calificación en la prestación de servicios.

5.2.Infraestructura Informática

Actualmente la infraestructura informática de la Empresa Four Points by Sheraton Cuenca se encuentra distribuida por10 pisos, está conformado por equipos de hardware, cada cuarto tiene cierto número de switches que prestan los recursos a cada uno de los departamentos, todos estos están conectados a un switch central, desde el piso 10 hasta el piso 1 se recoge por fibra óptica, todo el sistema de cableado es estructurado cumple las normas y los estándares dispuestos por la Dirección de tecnología y posee capacidad de soportar tecnología Gigabyte Ethernet hasta las estaciones de trabajo. El centro de cableado se encuentra en el Data Center.

A continuación, se muestra un diagrama de la infraestructura informática y como se encuentra distribuida por el edificio de la empresa

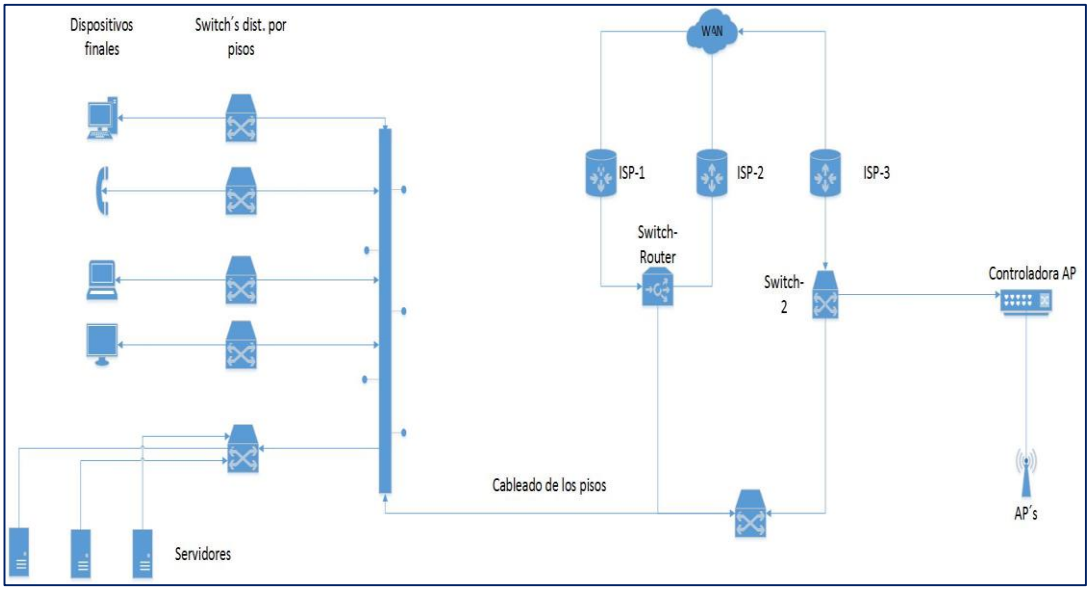

Figura 18: *Diagrama de la estructura informática de la empresa.*
Fuente: *(Autor, 2019)*

5.2.1. Conexiones en cada Piso del Edificio

Existen cuartos de bastidores en ciertos pisos del edificio, se muestra que en cada piso existen de uno a dos switch los cuales se conectan con los diferentes equipos ubicados en los departamentos o habitaciones, para luego conectarse al PP y llevar todo el cableado hacia la troncal. No todos los bastidores son iguales.

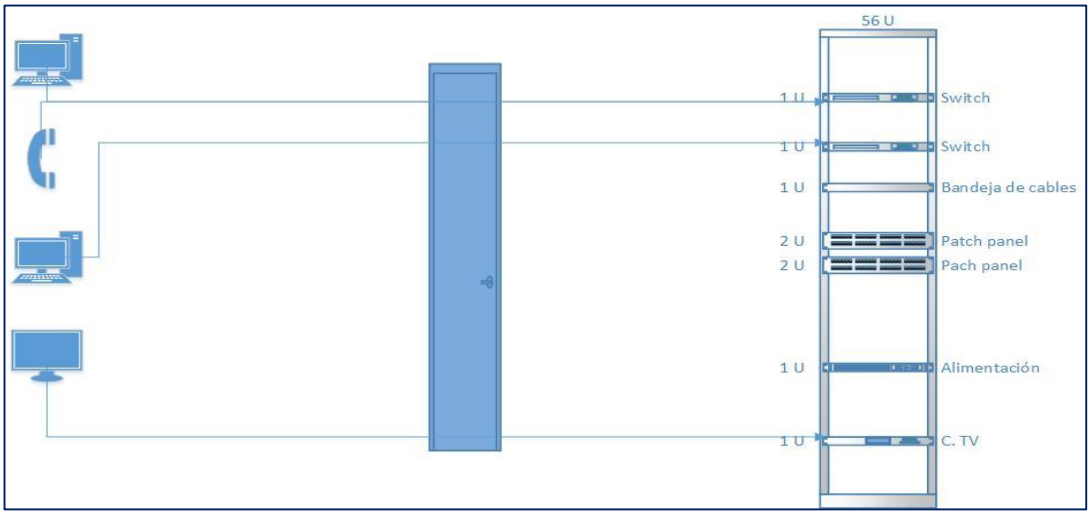

Figura 19: *Diagrama de la estructura informática de la empresa.*
Fuente: *(Autor, 2019).*

5.3.Desarrollo del Análisis GAP

Para evaluar la situación actual se utilizó una métrica del 0 al 5, donde 0 son los controles que no se encuentran aplicados en ninguna de las áreas entrevistadas y 5 es la total optimización y cumplimiento de las salvaguardas en la empresa.

Tabla 9: *Niveles de evaluación GAP.*

Estado	Descripción
0- Inmaduro	Las salvaguardas no existen, no existe un proceso de ningún tipo donde se pueda gestionar. Su éxito depende de tener personal de la alta calidad.
1- Básico	La medida de seguridad no corresponde a procesos documentados, es decir de una manera totalmente informal (con procedimientos propios, informales), no existe ningún seguimiento
2- Gestionado	El control se aplica conforme a un procedimiento documentado, de acuerdo a la planificación y realizándose un seguimiento.
3- Establecido	Existen procesos definidos donde se gestionan. Cada implementación de un proceso se hace utilizando procedimientos creados según un estándar y documentados
4- Predecible	La organización gestiona los procesos conforme a documentación y de manera cuantitativamente.
5- Optimizado	Se mejora continuamente los procesos para cumplir los objetivos de la empresa

Niveles de evaluación para controles y dominios. (Elaboración propia).

Durante la ejecución del servicio, se realizó entrevistas con las diferentes áreas de la compañía con el ánimo de identificar la situación actual de la misma, comparando contra las mejores prácticas o normativas vigentes respecto a la seguridad de la información. A continuación, se muestra la evaluación de Controles de Seguridad y una valoración de los requerimientos de un SGSI en la empresa:

Tabla 10: *Estados por dominios.*

DOMINIO	ESTADO POR DOMINIO	ESTADO
A.5	Políticas de Seguridad de la Información.	**4- Predecible**
A.6	Organización de la seguridad de la información	**2- Gestionado**
A.7	Seguridad relativa a los recursos humanos	**3- Establecido**
A.8	Gestión de activos	**1- Básico**
A.9	Control de acceso	**2- Gestionado**
A.10	Criptografía	**4- Predecible**
A.11	Seguridad física y del entorno	**2- Gestionado**
A.12	Seguridad de las operaciones	**3- Establecido**
A.13	Seguridad de las comunicaciones	**4- Predecible**
A.14	Adquisición, desarrollo y mantenimiento de los sistemas de información	**4- Predecible**
A.15	Relación con proveedores	**4- Predecible**
A.16	Gestión de incidentes de seguridad de la información	**3- Establecido**
A.17	Aspectos de seguridad de la información para la gestión de la continuidad del negocio	**2- Gestionado**
A.18	Cumplimiento	**5- Optimizado**

La valoración de los estados por dominio (Elaboración propia).

La tabla de estado por dominio era una visión global en donde se comprende todos los controles. A continuación, se muestra la tabla de cumplimiento por cada control mediante los cuales se califican su grado de cumplimiento de manera que se pueda obtener un porcentaje específico de la aplicación de normas.

Tabla 11: *Estados por control.*

Estándar	Control	Cumplimiento
A.5.1	Directrices de gestión de la seguridad de la información	**3- Establecido**
A.6.1	Organización interna	**4- Predecible**
A.6.2	Los dispositivos móviles y el teletrabajo	**2- Gestionado**
A.7.1	Antes del empleo	**3- Establecido**

A.7.2	Durante el empleo	**3- Establecido**
A.7.3	Finalización del empleo o cambio en el puesto de trabajo	**3- Establecido**
A.8.1	Responsabilidad sobre los activos	**2- Gestionado**
A.8.2	Clasificación de la información	**1- Básico**
A.8.3	Manipulación de los soportes	**1- Básico**
A.9.1	Requisitos de negocio para el control de acceso	**2- Gestionado**
A.9.2	Gestión de acceso de usuario	**3- Establecido**
A.9.3	Responsabilidades del usuario	**3- Establecido**
A.9.4	Control de acceso a sistemas y aplicaciones	**4- Predecible**
A.10.1	Controles criptográficos	**4- Predecible**
A.11.1	Áreas seguras	**2- Gestionado**
A.11.2	Seguridad de los equipos	**2- Gestionado**
A.12.1	Procedimientos y responsabilidades operacionales	**3- Establecido**
A.12.2	Protección contra el software malicioso (malware)	**3- Establecido**
A.12.3	Copias de seguridad	**4- Predecible**
A.12.4	Registros y supervisión	**3- Establecido**
A.12.5	Control del software en explotación	**3- Establecido**
A.12.6	Gestión de la vulnerabilidad técnica	**2- Gestionado**
A.12.7	Consideraciones sobre la auditoría de sistemas de información	**4- Predecible**
A.13.1	Gestión de la seguridad de redes	**3- Establecido**
A.13.2	Intercambio de información	**4- Predecible**
A.14.1	Requisitos de seguridad en los sistemas de información	**3- Establecido**
A.14.2	Seguridad en el desarrollo y en los procesos de soporte	**3- Establecido**
A.14.3	Datos de prueba	**1- Básico**
A.15.1	Seguridad en las relaciones con proveedores	**4- Predecible**
A.15.2	Gestión de la provisión de servicios del proveedor	**1- Básico**
A.16.1	Gestión de incidentes de seguridad de la información y mejoras	**1- Básico**
A.17.1	Continuidad de la seguridad de la información	**1- Básico**
A.17.2	Redundancias	**4- Predecible**
A.18.1	Cumplimiento de los requisitos legales y contractuales	**5- Optimizado**
A.18.2	Revisiones de la seguridad de la información	**1- Básico**

La valoración de los estados por control (Elaboración propia).

Se procede a valorar todos los requerimientos actuales en la empresa a nivel de implementación y su estado según la tabla de valoración para identificar la proporción de requerimientos del análisis de riesgos establecido en la actualidad por la empresa.

Tabla 12: *requerimientos de un análisis de riesgos*

Análisis de brechas para el sistema de gestión de seguridad de la información		
Cláusula	**Gestión**	**Estado**
4	**Contexto de la Organización**	
4.1	Contexto de la Organización	**2- Gestionado**
4.2	Partes Interesadas	**2- Gestionado**
		2- Gestionado
4.3	Alcance del SGSI	**3- Establecido**
4.4	Implementación del SGSI	**4- Predecible**
5	**Liderazgo**	
5.1	Liderazgo y Compromiso	**4- Predecible**
5.2	Política	**4- Predecible**
5.3	Roles y Responsabilidades	**2- Gestionado**
6	**Planeación**	
6.1	Acciones para la administración del riesgo	
6.1.1	Consideraciones generales	**4- Predecible**
6.1.2	Apreciación de riesgos de seguridad de la información	**3- Establecido**
6.1.3	Tratamiento de los riesgos de seguridad de la información	**2- Gestionado**
6.2	Objetivos de Seguridad de la Información	**2- Gestionado**
7	**Soporte**	
7.1	Asignación de Recursos	**4- Predecible**
7.2	Competencia	**2- Gestionado**
7.3	Concientización	**4- Predecible**
7.4	Comunicación	**1- Básico**
7.5	Documentación de Información	
7.5.1	Consideraciones generales	**1- Básico**

7.5.2	Creación y documentación	**0- Inmaduro**
7.5.2	Control de la información documentada	**1- Básico**
8	**Operación**	
8.1	Plan y Control Operacional	**5- Optimizado**
8.2	Apreciación de los riesgos de seguridad de la información	**4- Predecible**
8.3	Tratamiento de los riesgos de seguridad de la información	**3- Establecido**
9	**Evaluación del Desempeño**	
9.1	Seguimiento, medición, análisis y evaluación	**0- Inmaduro**
9.2	Auditoria Interna	**3- Establecido**
9.3	Revisión de la Dirección	**1- Básico**
10	**Mejora**	
10.1	No conformidad y acciones correctivas	**3- Establecido**
10.2	Mejora continua	**4- Predecible**

Valorar todos los requerimientos actuales en la empresa (Elaboración propia).

5.4. Desarrollo del Análisis de Riesgo de Seguridad de la Información

Para realizar el análisis de riesgo se utilizó la metodología MAGERIT que beneficia a la empresa con la reevaluación de su SGSI con el objetivo de identificar claramente los activos de información y determinar los riesgos a los que se exponen y planificar el tratamiento oportuno para mantener los riesgos bajo control mediante la mitigación de los mismos.

5.4.1. Fase 1: Levantamiento de los activos de información

Se realizó el levantamiento de información y de los activos de departamentos, de la red de comunicaciones y de los cuartos de rack. Los cuales se clasificaron en diez categorías. Para identificar los activos se realizó entrevistas con el jefe de TI/Sistemas, revisiones del inventario y recorridos por las instalaciones- A continuación, se muestra los activos los cuales están agrupados de la siguiente manera basado en el libro de Magerit – Catalogo de elementos:

Tabla 13: *Clasificación de los activos*

Arquitectura del sistema	
ID	**Descripción**
sap	punto de [acceso al] servicio
ip	punto de interconexión
ext	proporcionado por terceros
DATOS / INFORMACIÓN (D)	
files	ficheros
backup	copias de respaldo
conf	datos de configuración
int	datos de gestión interna
password	credenciales
auth	datos de validación de credenciales
acl	datos de control de acceso
log	registro de actividad
Servicios (S)	
ID	**Descripción**
anon	anónimo (sin requerir identificación del usuario)
pub	al público en general (sin relación contractual)
ext	a usuarios externos (bajo una relación contractual)
int	interno (a usuarios de la propia organización)

www	world wide web
telnet	acceso remoto a cuenta local
email	correo electrónico
file	almacenamiento de ficheros
ftp	transferencia de ficheros
edi	intercambio electrónico de datos
dir	servicio de directorio
idm	gestión de identidades
ipm	gestión de privilegios
pki	PKI - infraestructura de clave pública
Software - Aplicaciones informáticas (SW)	
ID	**Descripción**
prp	desarrollo propio (in house)
sub	desarrollo a medida (subcontratado)
std	estándar (off the shelf)
browser	navegador web
www	servidor de presentación
app	servidor de aplicaciones
email_client	cliente de correo electrónico
email_server	servidor de correo electrónico
file	servidor de ficheros
dbms	sistema de gestión de bases de datos
tm	monitor transaccional
office	ofimática
av	anti virus
os	sistema operativo
hypervisor	gestor de máquinas virtuales
ts	servidor de terminales
backup	sistema de backup
hardware - Equipos informáticos (HW)	
ID	**Descripción**
host	grandes equipos
mid	equipos medios
pc	informática personal
mobile	informática móvil
pda	agendas electrónicas
vhost	equipo virtual
backup	equipamiento de respaldo
peripheral	periféricos
print	medios de impresión
scan	escáneres

crypto	dispositivos criptográficos
bp	dispositivo de frontera
network	soporte de la red
modem	módems
hub	concentradores
switch	conmutadores
router	encaminadores
bridge	pasarelas
firewall	cortafuegos
wap	punto de acceso inalámbrico
pabx	centralita telefónica
ipphone	teléfono IP
Redes de comunicaciones (COM)	
ID	**Descripción**
PSTN	red telefónica
ISDN	rdsi (red digital)
X25	X25 (red de datos)
ADSL	ADSL
pp	punto a punto
radio	comunicaciones radio
wifi	red inalámbrica
mobile	telefonía móvil
sat	por satélite
LAN	red local
MAN	red metropolitana
Internet	Internet
Soportes de información (Media)	
ID	**Descripción**
disk	discos
vdisk	discos virtuales
san	almacenamiento en red
disquette	disquetes
cd	cederrón (CD-ROM)
usb	memorias USB
dvd	DVD
tape	cinta magnética
mc	tarjetas de memoria
ic	tarjetas inteligentes

Equipamiento auxiliar (Media)	
ID	**Descripción**

power	fuentes de alimentación
ups	sistemas de alimentación ininterrumpida
gen	generadores eléctricos
ac	equipos de climatización
cabing	cableado
wire	cable eléctrico
fiber	fibra óptica
robot	robots
tape	de cintas
disk	... de discos
supply	suministros esenciales
destroy	equipos de destrucción de soportes de información
furniture	mobiliario: armarios
safe	cajas fuertes
Instalaciones (L)	
ID	**Descripción**
site	recinto
building	edificio
local	cuarto
mobile	plataformas móviles
Personal (P)	
ID	**Descripción**
ue	usuarios externos
ui	usuarios internos
op	operadores
adm	administradores de sistemas
com	administradores de comunicaciones
dba	administradores de BBDD
sec	administradores de seguridad

Tipos de activos de la información. (Elaboración propia).

En la tabla 21 se muestra el inventario de los activos de información con su respectiva clasificación:

Tabla 14: *Listado de los activos y su clasificación.*

Clasificación de los activos de información		
Arquitectura del sistema (arch)		
ID_arch	**Nombre del Activo**	**Categoría**
arch1	Red de área local -LAN	ext
arch2	Red de área local inalámbrica -WLAN	ext
arch3	Servicio ISP	ext
arch4	Cuartos de Red	sap
arch5	Data Center	sap
arch6	Central Telefónica	sap
arch7	AP's inalámbricos	ip
Datos / información (D)		
ID_D	**Nombre del Activo**	**Categoría**
D1	Discos extraíbles de Backup	backup
D2	Documentos Administrativos	int
D3	Manuales de aplicación	int
D4	Manuales operacionales	int
D5	Base de Datos	int
D6	Facturas	int
D7	Libros Contables	int
D8	Documentos Financieros	int
D9	Manuales Administrativos	int
D10	Manuales de planificación estratégica	int
D11	Presupuesto de operaciones	int
D12	Documentos de carácter jurídico	int
D13	Contratos	files
D14	Documentos de políticas organizacionales	files
D15	Documentación Física de T.H.	files
D16	Registros Físicos	files
D17	Nominas	files
D18	Registros de Habitaciones	files
D19	Procesos de Operaciones	log
D20	Asistencia y registro de personal	log
Servicios (S)		

ID_S	Nombre del Activo	Categoría
S1	Red de área local -LAN	int
S2	Red de área local inalámbrica -WLAN	int
S3	Registro de correo	email
S4	Transferencia de ficheros	ftp
Software - aplicaciones informáticas (SW)		
ID_SW	**Nombre del Activo**	**Categoría**
SW1	Servidor de interfaces	app
SW2	Servidor de aplicaciones	app
SW3	Servidor de ficheros	file
SW4	Antivirus	av
SW5	Navegador web	browser
SW6	Base de Datos	dbms
SW7	Ofimática	office
SW8	S.O.	os
SW9	Servidor	os
SW10	Software de Gestión Hotelera	sub
SW11	Software Gestión Administrativa	sub
SW12	Software Facturación Electrónica	sub
SW13	Software autonomína	sub
Hardware - equipos informáticos (HW)		
ID_HW	**Nombre del Activo**	**Categoría**
HW1	Bandejas para Rack	bridge
HW2	Central Telefónica	pabx
HW3	Router	router
HW4	Router - HotSpot	router
HW5	Controlador	router
HW6	Servidor virtual	vhost
HW7	Discos extraíbles	backup
HW8	Switch- Router	firewall
HW9	Teléfono VoIP	ipphone
HW10	Teléfono analógico	ipphone
HW11	Smartphone	mobile
HW12	Equipo de mesa	pc
HW13	Computadora 2 en 1	pc
HW14	Laptop	pc

HW15	Aire Acondicionado	peripheral
HW16	AP	peripheral
HW18	Cámaras de vigilancia	peripheral
HW19	Impresoras	peripheral
HW20	Switch	switch
Redes de comunicaciones (COM)		
ID_COM	**Nombre del Activo**	**Categoría**
COM1	Servicio ISP	Internet
COM2	Red Voz Habitaciones	LAN
COM3	Red Datos Habitaciones	LAN
COM4	Red Voz Admin	LAN
COM5	Red Datos Admin	LAN
COM6	Red de área local -LAN	LAN
COM7	Red de área local -WLAN	wifi
Soportes de información (MEDIA)		
ID_MEDIA	**Nombre del Activo**	**Categoría**
MEDIA2	Discos extraibles	disk
MEDIA3	Almacenamiento de red	san
Equipamiento auxiliar (AUX)		
ID_AUX	**Nombre del Activo**	**Categoría**
AUX1	Patch Cords	cabing
AUX2	RACK	cabing
AUX3	cable eléctrico	wire
AUX4	Aire Acondicionado	ac
AUX5	fibra óptica	fiber
AUX6	armarios	furniture
AUX7	fuentes de alimentación	power
AUX8	sistemas de alimentación ininterrumpida	ups
Instalaciones (L)		
ID_L	**Nombre del Activo**	**Categoría**
L1	RED LAN - ESTRUCTURA	building
L2	RED WLAN - ESTRUCTURA	building
L3	DATA CENTER	local
L4	CUARTOS DE RED	local
Personal (P)		
ID_P	**Nombre del Activo**	**Categoría**
P1	Jefe de Sistemas	adm
P2	Jefe de Seguridad	sec
P3	jefe de Talento Humano	ui

P4	jefe de Ama de Llaves	ui
P5	Tesorera	ui
P6	Contralora	ui
P7	Gerente de Mercadeo	ui
P8	Gerente General	ui
P9	Jefe de Eventos	ui

Catálogo de los activos, clasificación y valoración. (Elaboración propia).

5.4.2. Fase 2: Clasificación de la información

En las operaciones de la empresa Four Points by Sheraton se maneja y se comparte un volumen cuantioso de información por lo que existen diferentes tipos de datos que depende de las actividades que se realicen, se encuentran presente en diferentes medios informáticos que se debería tratar de manera específica dependiendo del contexto en el que se aplique por lo que la valoración de un activo dependerá también que tipo de información se almacena o procesa en los dispositivos.

Otro factor importante que intervienen en la clasificación de la información son los activos de información, ya que con la ayuda de estos pueden desarrollar sus actividades que permite su transmisión y su disponibilidad para los usuarios que la requieran y con esto también conlleva una gran responsabilidad de seguridad.

Después de haber desarrollado el levantamiento de activos gracias a la clasificación de MAGERIT que permitió dividir los activos en 8 tipos, se procede a identificar los siguientes datos necesarios para la clasificación de la información:

Tabla 15: *Información procesada por la empresa.*

Datos / Información (D)	***Descripción***
D1	Discos extraíbles de Backup
D2	Documentos Administrativos
D3	Manuales de aplicación
D4	Manuales operacionales
D5	Base de Datos de los clientes
D6	Facturas
D7	Libros Contables

D8	Documentos Financieros
D9	Manuales Administrativos
D10	Manuales de planificación estratégica
D11	Presupuesto de operaciones
D12	Documentos de carácter jurídico
D13	Contratos
D14	Documentos de políticas organizacionales
D15	Documentación Físico de T.H.
D16	Registros Físicos
D17	Nominas
D18	Registros de Habitaciones
D19	Procesos de Operaciones
D20	Asistencia y registro de personal

Listado de la información de maneja la empresa (Elaboración propia).

Para desarrollar esta clasificación se debe tomar en cuenta que esta lista de la *tabla 23* está conformado por activos de nivel superior que después serán evaluados por las propiedades de la información en la siguiente fase, el objetivo que tienen este paso es conocer el valor que tiene un cierto grupo de información para la empresa y como se relacionan con los demás activos de información.

A continuación, se muestra en la *tabla 24* la lista de clasificación de la información:

***Tabla 16**: Clasificación de la información.*

Nombre de Información	Características de la información	Activos relacionados	Responsables
Discos extraíbles de Backup	Información Privada	Servicio (S) Aplicaciones (SW) Equipamiento informático (HW) Soportes de información (Media) Personal (P)	Jefe de TI/Sistemas Jefes de administración
Documentos Administrativos	Información Semiprivada	Servicio (S) Aplicaciones (SW) Equipamiento informático (HW) Soportes de información (Media) Personal (P)	Director General Jefes de administración
Manuales de aplicación	Información Privada	Soportes de información (Media) Personal (P)	Director General Jefes de administración
Manuales operacionales	Información Semiprivada	Soportes de información (Media) Personal (P)	jefes Operacionales Jefes de administración
Base de Datos de los clientes	Información Privada	Servicio (S) Aplicaciones (SW) Equipamiento informático (HW) Soportes de información (Media) Personal (P)	Jefe de TI/Sistemas Jefes de administración
Facturas	Información Publica	Aplicaciones (SW)	jefes Operacionales Jefes de administración
Libros Contables	Información Privada	Servicio (S) Aplicaciones (SW) Equipamiento informático (HW) Soportes de información (Media) Personal (P)	Jefes de administración

Documentos Financieros	Información Privada	Aplicaciones (SW) Personal (P)	Director General Jefes de administración
Manuales Administrativos	Información Semiprivada	Aplicaciones (SW) Personal (P)	Jefes de administración
Manuales de planificación estratégica	Información Semiprivada	Personal (P)	Director General Jefes de administración
Presupuesto de operaciones	Información Semiprivada	Personal (P)	jefes Operacionales Jefes de administración
Documentos de carácter jurídico	Información Semiprivada	Personal (P)	Director General
Contratos	Información Publica	Personal (P)	Jefes de administración
Documentos de políticas organizacionales	Información Publica	Personal (P)	jefes Operacionales Jefes de administración
Documentación Físico de T.H.	Información Semiprivada	Personal (P)	Jefes de administración
Registros Físicos	Información Semiprivada	Aplicaciones (SW) Personal (P)	jefes Operacionales Jefes de administración
Nominas	Información Privada	Servicio (S) Aplicaciones (SW) Equipamiento informático (HW) Personal (P)	jefes Operacionales Jefes de administración
Registros de Habitaciones	Información Semiprivada	Aplicaciones (SW) Personal (P)	jefes Operacionales
Procesos de Operaciones	Información Privada	Personal (P)	jefes Operacionales
Asistencia y registro de personal	Información Semiprivada	Aplicaciones (SW) Equipamiento informático (HW) Personal (P)	jefes Operacionales Jefes de administración

La clasificación de los activos de información relacionados a los activos informáticos que los maneja (Elaboración propia).

5.4.3. Fase 3: Valoración de los activos de información.

Para la calificación se determinó una escala del 0 al 5 siendo el 5 el activo de mayor importancia y el 0 el menos importante para el análisis de riesgos, para calcular el valor total se utiliza la formula acumulativa dispuesta en la tabla 23 y según los resultados se asigna un valor cualitativo y cuantitativo de acuerdo a la tabla 24:

VT (valor total) = Disponibilidad + Integridad + Confidencialidad + Autenticidad + Tranzabilidad

Tabla 17: *Valoración acumulativa para activos.*

Valor	Porcentaje	Criterio
5- Extrema	**22 - 25**	Daño extremadamente grave
4- Muy alto	**18 - 21**	Daño muy grave
3- Alto	**14 - 17**	Daño grave
2- medio	**10 - 13**	Daño importante
1- Bajo	**6 - 9**	Daño menor
0- Despreciable	**0 - 5**	Irrelevante a efectos prácticos

Se presentan los parámetros de evaluación para un activo (Elaboración propia).

En base a la metodología MAGERIT para realizar la valoración de los activos de información se utilizaron cinco dimensiones que ayudaron a determinar qué tan importante es un activo para la organización.

A continuación, se muestra las tablas que ayudaron a justificar la calificación de un activo por cada dimensión que lo compone:

Disponibilidad

¿Cuál sería la importancia tendría que el activo no estuviera disponible?

Tabla 18: *Valoración de la disponibilidad.*

Valor	Disponibilidad [D]	Descripción
5- Extrema	Interrupción del servicio.	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización.
	Administración y gestión	Probablemente impediría seriamente la operación efectiva de la Organización.
	Tiempo de Recuperación.	Tiempo tolerable de interrupción menor a 3 horas
4- Muy alto	Interrupción del servicio.	Probablemente cause una interrupción seria de las actividades propias de la Organización
	Administración y gestión	probablemente impediría la operación efectiva de la Organización
	Tiempo de Recuperación.	Tiempo tolerable mayor a 3 horas y menor a 5 horas
3- Alto	Interrupción del servicio.	Probablemente cause la interrupción de actividades propias de la Organización
	Administración y gestión	probablemente impediría la operación efectiva de más de una parte de la Organización
	Tiempo de Recuperación.	Tiempo tolerable mayor a 5 horas y menor a 1 día
2- medio	Administración y gestión	probablemente impediría la operación efectiva de una parte de la Organización
	Interrupción del servicio.	Pudiera causar la interrupción de actividades propias de la Organización
1- Bajo	Tiempo de Recuperación.	Tiempo tolerable mayor a 1 día y menor a 3 días
	Administración y gestión	pudiera impedir la operación efectiva de una parte de la Organización
0- Despreciable	Tiempo de Recuperación.	Tiempo tolerable mayor a 3 días y menor a 7 días

La disponibilidad de los activos. (Elaboración propia).

- **Integridad**

¿Cuál sería la importancia de que la información sea modificada sin autorización?

Tabla 19: *Tabla de valoración de la integridad.*

Valor	Integridad [I]	Descripción
5- Extrema	Información clasificada	Secreto
	Seguridad	probablemente sea causa de un incidente excepcionalmente serio de seguridad
4- Muy alto	Información clasificada	Reservado

	Seguridad	probablemente sea causa de un serio incidente de seguridad
3- Alto	Información clasificada	Confidencial
	Seguridad	probablemente sea causa de un grave incidente de seguridad
2- medio	Seguridad	probablemente sea causa de una merma en la seguridad
1- Bajo	Seguridad	pudiera causar una merma en la seguridad
0- Despreciable	Seguridad	pudiera no causar una merma en la seguridad

La disponibilidad de los activos. (Elaboración propia).

- **Confidencialidad**

¿Cuál sería el impacto que la información sea revelada a terceros?

Tabla 20: *Valoración de la confidencialidad.*

Valor	Confidencialidad [C]	Descripción
5- Extrema	Obligaciones legales	Probablemente quebrante seriamente leyes o regulaciones y afecte gravemente a un individuo.
	Intereses comerciales o económicos	Vulnerable a la divulgación a personas o sistemas que no se encuentran autorizados.
4- Muy alto	Obligaciones legales	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	Intereses comerciales o económicos	De muy significativas ganancias o ventajas para individuos u organizaciones.
3- Alto	Obligaciones legales	probablemente cause un incumplimiento leve grave de una ley o regulación
	Intereses comerciales o económicos	De alto interés para la competencia
2- medio	Intereses comerciales o económicos	De cierto interés y valor para la competencia
1- Bajo	Intereses comerciales o económicos	De bajo interés y valor para la competencia
0- Despreciable	Intereses comerciales o económicos	De pequeño valor comercial

La confidencialidad de los activos. (Elaboración propia).

- **Autenticidad**

¿Cuál sería la importancia de que quien accede al servicio no sea realmente quien se cree?

Tabla 21: *Tabla de valoración de la autenticidad.*

Valor	Autenticidad [A]	Descripción
5- Extrema	Controles	Información que requiere controles estrictos para su protección
4- Muy alto	Controles	Información que requiere controles preventivos para su protección
3- Alto	Controles	Información que requiere controles concurrentes para su protección
2- medio	Controles	Información que requiere controles eventuales para su protección
1- Bajo	Controles	Información que requiere controles mínimo para su protección
0- Despreciable	Controles	Información que no requiere controles para su protección

La autenticidad de los activos. (Elaboración propia).

- **Tranzabilidad**

¿Cuál sería la importancia de que no quedara constancia del acceso a los datos?

Tabla 22: *Valoración de la trazabilidad.*

Valor	Trazabilidad [T]	Descripción
5- Extrema	acceso	Información que requiere estrictamente constancia del acceso a los datos
	Persecución de delitos	dificulta la investigación de incidentes excepcionalmente serios
4- Muy alto	acceso	Información que requiere preventiva constancia del acceso a los datos
	Persecución de delitos	dificulta la investigación de incidentes serios
3- Alto	acceso	Información que requiere concurrente constancia del acceso a los datos
	Persecución de delitos	dificulta la investigación de incidentes graves

2- medio	acceso	Información que requiere eventualmente constancia del acceso a los datos
1- Bajo	acceso	Información que requiere mínima constancia del acceso a los datos
0- Despreciable	acceso	Información que no requiere constancia del acceso a los datos

La Tranzabilidad de los activos. (Elaboración propia).

En la siguiente tabla se especifica los activos más importantes que se consideraron para el análisis de riesgo:

Tabla 23: Valoración de activos.

DIMENSIONES									
ID_arch	**Nombre del Activo**	**D**	**I**	**C**	**A**	**T**	**Cuantitativa**	**Categoría**	**Cualitativa**
Datos / Información (D)									
D1	Discos extraíbles	5	5	4	4	5	**23**	backup	**5- Extrema**
D2	Documentos Administrativos	5	5	4	5	4	**23**	int	**4- Muy alto**
D3	Manuales de aplicación	3	4	4	4	3	**18**	int	
D4	Manuales operacionales	4	4	5	5	4	**22**	int	
D5	Base de Datos	5	5	4	4	5	**23**	int	
D6	Facturas	4	4	3	3	2	**16**	int	
D7	Libros Contables	5	4	5	3	3	**20**	int	
D8	Documentos Financieros	5	5	4	4	5	**23**	int	
D9	Manuales Administrativos	5	4	5	3	4	**21**	int	
D10	Manuales de planificación estratégica	5	4	3	4	4	**20**	int	
D11	Presupuesto de operaciones	5	5	4	4	4	**22**	int	
D12	Documentos de carácter jurídico	3	2	3	2	1	**11**	int	
D13	Contratos	5	3	2	3	3	**16**	files	**3- Alto**
D14	Documentos de políticas organizacionales	5	5	4	4	3	**21**	files	
D15	Documentación Físico de T.H.	5	5	4	4	4	**22**	files	
D16	Registros Físicos	5	3	4	3	4	**19**	files	
D17	Nominas	3	2	1	3	0	**9**	files	
D18	Registros de Habitaciones	4	3	4	2	2	**15**	files	
D19	Procesos de Operaciones	5	5	5	4	4	**23**	log	**5- Extrema**
D20	Asistencia y registro de personal	5	4	5	5	4	**23**	log	
Servicio (S)									

S1	Red de área local –LAN	4	5	5	5	4	**23**	int	**5- Extrema**
S2	Red de área local inalámbrica -WLAN	5	4	4	4	3	**20**	int	
S4	Registro de correo	5	4	4	3	4	**20**	email	**4- Muy alto**
S5	Transferencia de ficheros	3	4	4	3	3	**17**	ftp	**3- Alto**
Software - Aplicaciones informáticas (SW)									
SW1	Servidor de interfaces	4	4	4	3	3	**18**	app	**3- Alto**
SW2	Servidor de aplicaciones	4	4	3	3	3	**17**	app	
SW3	Servidor de ficheros	4	4	3	4	4	**19**	file	**4- Muy alto**
SW4	Antivirus	5	4	4	4	3	**20**	av	**4- Muy alto**
SW5	Navegador web	4	3	4	3	3	**17**	browser	**3- Alto**
SW6	Base de Datos	5	4	5	5	4	**23**	dbms	**5- Extrema**
SW7	Ofimática	4	4	3	2	2	**15**	office	**1- Bajo**
SW8	S.O.	4	5	4	4	3	**20**	os	**4- Muy alto**
SW9	Servidor	4	5	5	3	3	**20**	os	
SW10	Software de Gestión Hotelera	5	5	3	3	2	**18**	sub	**3- Alto**
SW11	Software Gestión Administrativa	5	5	4	3	2	**19**	sub	
SW12	Software Facturación Electrónica	4	3	1	3	3	**14**	sub	
SW13	Software auto nómina	4	4	2	2	1	**13**	sub	
hardware - Equipos informáticos (HW)									
HW1	Bandejas para Rack	0	0	1	1	0	**2**	bridge	**0- Despreciable**
HW2	Central Telefónica	4	3	3	3	3	**16**	pabx	**3- Alto**
HW3	Router	5	5	2	3	4	**19**	router	**3- Alto**
HW4	Router – HotSpot	5	4	3	3	3	**18**	router	
HW5	Controlador	5	4	3	3	2	**17**	router	
HW6	Servidor virtual	4	5	5	3	3	**20**	vhost	**3- Alto**

HW7	Discos extraíbles	5	5	5	5	5	**25**	backup	**5- Extrema**
HW8	Switch- Router	5	5	5	2	3	**20**	firewall	**4- Muy alto**
HW9	Teléfono VoIP	5	5	5	5	4	**24**	ipphone	**3- Alto**
HW10	Teléfono analógico	2	3	2	2	1	**10**	ipphone	
HW11	Smartphone	4	4	4	5	5	**22**	mobile	**5- Extrema**
HW12	Equipo de mesa	5	5	4	4	5	**23**	pc	**5- Extrema**
HW13	Computadora 2 en 1	5	5	4	4	5	**23**	pc	
HW14	Laptop	5	5	4	4	5	**23**	pc	
HW15	Aire Acondicionado	5	5	4	4	2	**20**	peripheral	**3- Alto**
HW16	AP	4	5	5	4	4	**22**	peripheral	
HW17	Reloj Biométrico	5	3	4	2	2	**16**	peripheral	
HW18	Cámaras de vigilancia	5	5	4	4	4	**22**	peripheral	
HW19	Impresoras	2	1	1	0	0	**4**	peripheral	
HW20	Switch	5	5	4	3	3	**20**	switch	**4- Muy alto**
hardware - Equipos informáticos (HW)									
COM1	Servicio ISP	4	3	5	5	4	**21**	Internet	**4- Muy alto**
COM2	Red Voz Habitaciones	4	4	4	5	4	**21**	LAN	**4- Muy alto**
COM3	Red Datos Habitaciones	5	4	5	4	3	**21**	LAN	
COM4	Red Voz Admin	5	4	5	4	3	**21**	LAN	
COM5	Red Datos Admin	5	3	5	3	4	**20**	LAN	
COM6	Red de área local –LAN	5	3	5	4	5	**22**	LAN	
COM10	Red de área local -WLAN	4	4	4	3	4	**19**	wifi	**3- Alto**
Soportes de información (Media)									
MEDIA2	Discos extraíbles	4	5	4	3	4	**20**	disk	**3- Alto**
MEDIA3	Almacenamiento de red	4	4	4	2	2	**16**	san	**2- medio**
Equipamiento auxiliar (AUX)									

AUX1	Patch Cords	1	0	0	0	0	**1**	cabing	**1- Bajo**
AUX2	RACK	4	3	1	2	1	**11**	cabing	
AUX3	cable eléctrico	5	5	2	2	1	**15**	wire	**2- medio**
AUX4	Aire Acondicionado	4	3	4	2	3	**16**	ac	**2- medio**
AUX5	fibra óptica	4	4	2	2	1	**13**	fiber	**1- Bajo**
AUX6	Armarios	3	2	2	2	1	**10**	furniture	**1- Bajo**
AUX7	fuentes de alimentación	3	4	5	5	4	**21**	power	**4- Muy alto**
AUX8	sistemas de alimentación ininterrumpida	5	5	4	4	5	**23**	ups	**5- Extrema**
Instalaciones (L)									
L1	RED LAN - ESTRUCTURA	5	4	5	3	4	**21**	building	**5- Extrema**
L2	RED WLAN - ESTRUCTURA	5	3	5	5	4	**22**	building	
L3	DATA CENTER	5	5	4	5	3	**22**	local	**4- Muy alto**
L4	CUARTOS DE RED	3	4	5	3	2	**17**	local	
Personal (P)									
P1	Jefe de Sistemas	5	5	4	5	5	**24**	adm	**5- Extrema**
P2	Jefe de Seguridad	5	4	4	4	3	**20**	sec	**4- Muy alto**
P3	jefe de Talento Humano	4	3	2	3	4	**16**	ui	**2- medio**
P4	jefe de Ama de Llaves	1	3	1	0	0	**5**	ui	
P5	Tesorera	3	4	4	1	1	**13**	ui	
P6	Contralora	4	4	3	3	4	**18**	ui	
P7	Gerente de Mercadeo	3	2	2	4	4	**15**	ui	
P8	Gerente General	4	5	4	5	4	**22**	ui	
P9	Jefe de Eventos	2	1	0	0	0	**3**	ui	

La lista de los activos valorados. (Elaboración propia).

5.4.4. Fase 4: Identificación de amenazas

Los activos de información están expuestos a una serie de amenazas tanto dentro y fuera de la empresa, los cuales pueden presentarse como un error o puede generarse también como un ataque cibernético. MAGERIT brida un cataloga bastante amplio el cual se presenta como un documento adjunto llamado (IDENTIFICACIÓN DE AMENAZAS) y a presar de que sea una lista extensa es necesario tomarlas encuentra, después de su evaluación se podrán descartar las que tienen menos probabilidad.

A continuación, se alinean los errores con los ataques mostrando la correlación que existe entre los tipos de amenaza:

Tabla 24: *Correlación entre ataques y errores.*

Número	Error	Ataque
1	Errores de los usuarios	
2	Errores del administrador	
3	Errores de monitorización (log)	Manipulación de los registros de actividad
4	Errores de configuración	Manipulación de la configuración
5		Suplantación de la identidad del usuario
6		Abuso de privilegios de acceso
7	Deficiencias en la organización	Uso no previsto
8	Difusión de software dañino	Difusión de software dañino
9	Errores de [re-]encaminamiento	[Re-]encaminamiento de mensajes
10	Errores de secuencia	Alteración de secuencia
11		Acceso no autorizado
12		Análisis de tráfico
13		Repudio
14		Interceptación de información (escucha)
15	Alteración accidental de la información	Modificación deliberada de la información
18	Destrucción de información	Destrucción de información
19	Fugas de información	Divulgación de información
20	Vulnerabilidades de los programas (software)	
21	Errores de mantenimiento / actualización de programas (software)	
22		Manipulación de programas

23	Errores de mantenimiento / actualización de equipos (hardware)	Manipulación de los equipos
24	Caída del sistema por agotamiento de recursos	Denegación de servicio
25	Pérdida de equipos	Robo
26		Ataque destructivo
27		Ocupación enemiga
28	Indisponibilidad del personal	Indisponibilidad del personal
29		Extorsión
30		Ingeniería social (picaresca)

La lista de correlación que existe entre las diferentes amenazas. (Elaboración propia).

En la tabla 27 se muestra el catálogo de amenazas asociados a cada tipo activo que ofrece MAGERIT:

Tabla 25: *Catálogo de amenazas.*

Tipo de Activos	Nombre de activo	**Amenazas**
Datos / Información (D)	[int] datos de gestión interna	Falta de cuidado sobre el manejo de información.
		Acceso no autorizado a documentos.
	[files] Ficheros	Alteración accidental de la información
		Fugas de información.
		Modificación deliberada de la información.
		Destrucción de información
		Divulgación de información
		Repudio
	[log] registro de actividad	Errores de secuencia al registrar actividades
		Manipulación de los registros de actividad

	[backup] copias de respaldo	Eliminación de las copias de respaldo
Servicio (S)	[int] interno (a usuarios de la propia organización)	Uso no previsto de los servicios.
		Acceso no autorizado
		Errores de los usuarios al utilizar un servicio
	[ftp] transferencia de ficheros	Problemas de rendimiento
	[email] correo electrónico	[Re-]encaminamiento de mensajes
Software - Aplicaciones informáticas (SW)	[app] servidor de aplicaciones	Error de inicio o reinicio del servidor
	[file] servidor de ficheros	Acceso no autorizado al servidor
	[browser] navegador web	Uso no previsto de navegador web
	[dbms] sistema de gestión de BD	Acceso no autorizado a la base de datos
	[email_server] servidor de correo electrónico	Difusión de software dañino intencionado
	[av] antivirus	Divulgación de información por malware
		Difusión de software dañino.
	[os] sistema operativo	Instalación de software desconocido.
		Errores de mantenimiento / actualización de programas (software)
		Suplantación de la identidad del usuario para inicio de sesión
		Errores del administrador al instalar/actualizar software
	[sub] desarrollo a medida [office] ofimática	Alteración accidental de la información por programas de gestión
		Abuso de privilegios de acceso a programas de gestión
		Desbordamiento de búfer

		Manipulación de programas
hardware - Equipos informáticos (HW)	[pc] informática personal. [firewall] cortafuegos. [peripheral] periféricos. [pabx] centralita telefónica. [switch] conmutadores. [backup] equipamiento de respaldo.	Fuego
		Daños por agua
		Desastres naturales
		Avería de origen físico del hardware
		Corte del suministro eléctrico
		Errores del administrador al instalar equipos
		Pérdida de equipos
		Manipulación de los equipos
		Ataque destructivo
	[vhost] equipo virtual.	Abuso de privilegios de acceso a los equipos.
	[mobile] informática móvil.	Robo de laptops y equipos móviles.
	[Ipphone] teléfono IP.	Uso no previsto de los equipos
Redes de comunicaciones (COM)	[LAN] red local	Errores del administrador al compartir sus credenciales.
		Falta de registro de los eventos en caso de ataques a las redes.
		Caída del sistema por agotamiento de recursos
		Suplantación de la identidad del usuario
		Abuso de privilegios de acceso a la red
		Demasiadas aplicaciones que operan sobre la red.
	[internet] internet	Errores de administración de cuentas con privilegios.

	[wifi] red inalámbrica	Análisis de tráfico
		Interceptación de información (escucha)
		Errores de [re-]encaminamiento
Soportes de información (Media)	[disk] discos.	Acceso no autorizado
		Eliminación accidental de la información
Equipamiento auxiliar (AUX)	[ac] equipos de climatización	Manipulación de los equipos de climatización
	[ups] sistemas de alimentación ininterrumpida	
	[power] fuentes de alimentación	Daños de los equipos de suministro eléctrico
	[cabing] cableado [wire] cable eléctrico [fiber] fibra óptica	Ataque destructivo del cableado.
		Desgaste normal que un sistema de cableado
Instalaciones (L)	[building] edificio [local] cuarto	Fuego
		Daños por agua
		Ausencia de vigilancia por cámaras de seguridad.
		Desastres naturales
PERSONAL (P)	[adm] administrador de sistemas [sec] administrador de seguridad [ui] usuarios internos.	Ingeniería social (picaresca)
		Extorsión
		Ausencia deliberada del puesto de trabajo
		Indisponibilidad del personal
		Compromiso por la seguridad informática.

Catálogo de amenazas (Elaboración propia).

5.4.5. Fase 5: Identificación y valoración de vulnerabilidades

La siguiente fase consiste en identificar los puntos débiles de los activos, también conocido como vulnerabilidades que pone en riesgo la seguridad de la información que un atacante puede comprometer. A continuación, veremos los niveles de valoración y los criterios que se toman en cuenta para identificarlas y calificarlas:

Tabla 26: *Valoración de vulnerabilidades.*

Descripción	Valor	Porción de riesgo total
Muy bajo (MB)	1	Es de severidad y exposición menor, no afecta a los componentes del sistema, no existen la probabilidad de vulnerabilidades adicionales. No tienen un potencial de daño.
Bajo (B)	2	Es de severidad y exposición controlable, afecta a muy pocos de los componentes del sistema, no existen la probabilidad de vulnerabilidades adicionales. Tienen un potencial bajo de daño.
Medio (M)	3	Es de severidad y exposición moderada, afecta a muy pocos de los componentes del sistema, existen la probabilidad de vulnerabilidades adicionales. Tienen un potencial medio de daño.
Alto (A)	4	Es de severidad y exposición alta, afecta a casi todos los componentes del sistema, existen la probabilidad de vulnerabilidades adicionales. Tienen un potencial alto de daño.
Muy alto (MA)	5	Es de severidad y exposición muy alta, afecta a casi todos los componentes del sistema, existen vulnerabilidades adicionales. Tienen un potencial peligroso de daño.

Niveles de valoración de las vulnerabilidades (Elaboración propia).

Se muestran los parámetros utilizados para la evaluación cuantitativa de las vulnerabilidades identificadas en la empresa:

Tabla 27: *Parámetros de valoración de vulnerabilidades: exposición.*

	Valor	Descripción
Exposición	**1**	**Exposición Menor:** Los efectos de la vulnerabilidad son mínimos. No incrementa la probabilidad de que vulnerabilidades adicionales sean explotadas.
	2	**Exposición Moderada:** La vulnerabilidad puede afectar a más de un elemento o componente del sistema. La explotación de la vulnerabilidad aumenta la probabilidad de explotar vulnerabilidades adicionales.

	3	**Exposición Alta:** La vulnerabilidad afecta a la mayoría de los componentes del sistema. La explotación de la vulnerabilidad aumenta significativamente la probabilidad de explotar vulnerabilidades adicionales.

Niveles de exposición de activos. (Elaboración propia).

Tabla 28: *Parámetros de valoración de vulnerabilidades: severidad.*

	Valor	Descripción
Severidad	**1**	**Severidad Menor:** Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene poco potencial de pérdida o daño en el activo.
	2	**Severidad Moderada:** Se requiere una cantidad significativa de recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo
	3	**Severidad Alta:** Se requieren pocos recursos para explotar la vulnerabilidad y tiene un potencial significativo de pérdida o daño en el activo.

Niveles de severidad de las vulnerabilidades (Elaboración propia).

Las vulnerabilidades se encuentran asociadas con los activos de información y son el resultado de ciertas debilidades o fallos en el SI de las empresas también conocida como brechas que pueden ser aprovechadas para la materialización de las amenazas. En la siguiente tabla se muestran las vulnerabilidades identificadas y su valoración de acuerdo al nivel de exposición y severidad que permite medir la posibilidad de hacer susceptible una amenaza, calculada con la siguiente fórmula:

Vulnerabilidad = Severidad + exposición – 1

Para identificar las vulnerabilidades se procedió primero a listar los posibles fallos tanto conocidos y desconocidos que pudieran tener los activos de información, para luego mediante la valoración de los mismos que a través de un análisis de los informes de auditorías, políticas y controles los cuales son realizados por los directivos de seguridad, proveedores de tecnología y el jefe de área TI/Sistemas se pudiera obtener un catálogo reducido de amenazas, que ayudará a desarrollar la próxima fase, que se presenta a continuación:

Tabla 29: *Valoración de vulnerabilidades en relación con las amenazas.*

Tipo de Activos	Nombre de activo	**Amenazas**	**Vulnerabilidad**	Severidad	Exposición	Valor Cuantitativo	Valor Cualitativo
DATOS / INFORMACIÓN (D)	[int] datos de gestión interna	Falta de cuidado sobre el manejo de información.	Perdidas/eliminación de datos por desconocimiento de su nivel de importancia para la empresa.	3	1	**3**	**Medio (M)**
		Acceso no autorizado a documentos.	El atacante consigue acceder a documentos importantes para la empresa.	2	1	**2**	**Bajo (B)**
	[files] Ficheros	Alteración accidental de la información	Alteraciones accidentales de información por parte de las personas que la manipulan.	2	1	**2**	**Bajo (B)**
		Fugas de información.	Revelación por indiscreción producida por la incontinencia verbal de los empleados sobre información concentrada en documentos confidenciales.	3	1	**3**	**Medio (M)**
		Modificación deliberada de la información.	Alteración intencional de la información de las actividades, solicitudes, trámites, proyectos y apuestas con el fin de conseguir un beneficio.	2	1	**2**	**Bajo (B)**
		Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	2	1	**2**	**Bajo (B)**
		Divulgación de información	Revelación intencionada de información por parte de ex empleados o empleados con privilegios al acceso de la información.	2	1	**2**	**Bajo (B)**
		Repudio	Negación de haber recibido el documento/Negación de haber recibido un mensaje para su entrega a otro.	2	1	**2**	**Bajo (B)**
	[log] registro de actividad	Errores de secuencia al registrar actividades	Errores no intencionados producidos cuando se procesa o almacena la información de registro de actividades.	3	2	**4**	**Alto (A)**

		Manipulación de los registros de actividad	Manejo intencionado de la información con intensión de modificar/eliminar registros por parte de un atacante para sus fines propios.	1	3	**3**	**Medio (M)**
	[backup] copias de respaldo	Eliminación de las copias de respaldo	Eliminación intencional por parte del atacante de las copias de respaldo para perjudicar u obtener beneficio.	1	2	**2**	**Bajo (B)**
Servicio (S)	[int] interno (a usuarios de la propia organización)	Uso no previsto de los servicios.	Utilización de los servicios para fines típicamente de interés personal como almacenamiento de datos personales.	3	2	**4**	**Alto (A)**
		Acceso no autorizado	El atacante consigue por medio de un fallo de autenticidad acceder al servicio, con el fin de disfrutar de los privilegios.	1	2	**2**	**Bajo (B)**
		Errores de los usuarios al utilizar un servicio	Equivocaciones no intencionadas de las personas cuando usan los servicios con fines que no corresponde a las tareas definidas.	1	1	**1**	**Muy bajo (MB)**
	[ftp] transferencia de ficheros	Problemas de rendimiento	Cuando la carga de trabajo es desmesurada provoca la carencia de recursos que a su vez desemboca en la caída del sistema	2	2	**3**	**Medio (M)**
	[email] correo electrónico	[Re-]encaminamiento de mensajes	Cuando la carga de trabajo es desmesurada provoca la carencia de recursos que a su vez desemboca en la caída del sistema	2	3	**4**	**Alto (A)**
Software - Aplicaciones informáticas (SW)	[app] servidor de aplicaciones	Errores de inicio o reinicio del servidor.	Es posible que se produzca este problema si la red es lenta.	2	2	3	**Medio (M)**
	[file] servidor de ficheros	Acceso no autorizado al servidor	El atacante consigue acceder al servidor sin autorización debido a un fallo del sistema de identificación.	2	2	3	**Medio (M)**
	[browser] navegador web	Uso no previsto de navegador web	Utilización del navegador web para fines no previstos, típicamente de interés personal: juegos, redes sociales y consultas personales en Internet.	3	2	4	**Alto (A)**

	[dbms] sistema de gestión de BD	Acceso no autorizado a la base de datos	El atacante consigue acceder al servidor de BD sin autorización debido a un fallo del sistema de identificación y autorización.	2	3	4	**Alto (A)**
	[email_server] servidor de correo electrónico	Difusión de software dañino intencionado	El atacante difunde malware mediante la infiltración a los sistemas por la fallas de firewall.	2	2	3	**Medio (M)**
	[av] antivirus	Divulgación de información por malware	Revelación de información no autorizada por del atacante con el uso de malware	2	2	3	**Medio (M)**
		Difusión de software dañino.	Propagación de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc. Por falta de protección del antivirus y por medio el usuario que se redirige a páginas, rutas infectadas o manipulación de archivos corruptos.	1	2	2	**Bajo (B)**
	[os] sistema operativo	Instalación de software desconocido.	Instalar en equipos finales de programas de distribuidores desconocidos o que pueden estar infectados.	3	1	3	**Medio (M)**
		Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos de actualización de versiones de SO que permiten que sigan utilizándose programas con defectos conocidos.	1	3	3	**Medio (M)**
		Suplantación de la identidad del usuario para inicio de sesión	Cuando un atacante consigue las credenciales de inicio de sesión en SO para ingresar con fines de beneficio propio.	1	1	1	**Muy bajo (MB)**
		Errores del administrador al instalar/actualizar software	Equivocaciones del jefe de sistemas al instalar versiones incompatibles/con errores de software.	2	1	2	**Bajo (B)**
	[sub] desarrollo a medida [office] ofimática	Alteración accidental de la información por programas de gestión	Modificación por error de la información gestionada por medio de las aplicaciones que manejan un grupo de usuarios.	2	1	2	**Bajo (B)**

		Abuso de privilegios de acceso a programas de gestión	Cada usuario disfruta de un nivel de privilegios para un determinado propósito; cuando un usuario abusa de su nivel de privilegios para realizar tareas que no son de su competencia, hay problemas.	2	1	2	**Bajo (B)**
		Desbordamiento de búfer	Defecto de un programa que no controla adecuadamente la cantidad de datos que se copian sobre un área de memoria reservada	1	2	2	**Bajo (B)**
		Manipulación de programas	Alteración intencionada del funcionamiento de los programas, por parte de un atacante persiguiendo un beneficio.	1	1	1	**Muy bajo (MB)**
hardware - Equipos informáticos (HW)	[pc] informática personal. [firewall] cortafuegos. [peripheral] periféricos. [pabx] centralita telefónica. [switch] conmutadores. [backup] equipamiento de respaldo.	Fuego	Incendios: posibilidad de que el fuego acabe con recursos de hardware del sistema.	1	3	3	**Medio (M)**
		Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos de hardware del sistema.	1	2	2	**Bajo (B)**
		Desastres naturales	Otros incidentes que se producen sin intervención humana como: rayo, tormenta eléctrica, terremoto.	2	1	2	**Bajo (B)**
		Avería de origen físico del hardware	Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema.	1	3	3	**Medio (M)**
		Corte del suministro eléctrico	Los equipos se quedan sin alimentación eléctrica por corte de servicios o por fallas de las instalaciones.	2	1	2	**Bajo (B)**
		Errores del administrador al instalar equipos	Equivocaciones de personas con responsabilidades de instalar equipos (configuraciones erróneas, equipos incorrectos).	1	2	2	**Bajo (B)**
		Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios o averías graves de los equipos.	2	2	3	**Medio (M)**
		Manipulación de los equipos	Alteración intencionada del funcionamiento de los equipos, persiguiendo un beneficio.	1	3	3	**Medio (M)**

		Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal.	2	2	3	**Bajo (B)**
	[vhost] equipo virtual.	Abuso de privilegios de acceso a los equipos.	Abuso de los privilegios de su nivel de privilegios para manejar equipos que no son de su competencia.	2	1	2	**Bajo (B)**
	[mobile] informática móvil.	Robo de laptops y equipos móviles.	Hurto de los equipos que puede producirse dentro de la empresa como fuera de la misma que son de uso exclusivo para la empresa.	3	2	4	**Muy alto (MA)**
	[ipphone] teléfono IP.	Uso no previsto de los equipos	Utilización de los recursos del sistema para fines no previstos, típicamente de interés personal: almacenamiento de datos personales, etc.	3	1	3	**Medio (M)**
Redes de comunicaciones (COM)	[LAN] red local	Errores del administrador al compartir sus credenciales.	Equivocaciones de los administradores al compartir sus datos y contraseñas con otras personas que dan apoyo técnico o a proveedores de tecnología.	2	2	3	**Medio (M)**
		Falta de registro de los eventos en caso de ataques a las redes.	El administrador no lleva un registro de los eventos de ataques hacia la red local para futuras revisiones.	2	1	2	**Bajo (B)**
		Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	2	2	3	**Medio (M)**
		Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un administrador de red gracias a sus credenciales para ingresar como administrador.	2	2	3	**Medio (M)**
		Abuso de privilegios de acceso a la red	El usuario abusa de su nivel de privilegios sobre la red y puede ingresar a la información sensible.	2	2	3	**Medio (M)**
		Demasiadas aplicaciones que operan sobre la red.	Se instalan programas que se conectan a internet que sobrecargan inútilmente la red.	1	1	1	**Muy bajo (MB)**

	[internet] internet	Errores de administración de cuentas con privilegios.	Equivocaciones al dejar cuentas abandonadas sin retirarles los privilegios.	3	1	3	**Medio (M)**
	[wifi] red inalámbrica	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.	3	2	4	**Alto (A)**
		Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	2	2	3	**Medio (M)**
		Errores de [re-]encaminamiento	Envío accidental de información a través de un canal equivocado en la red.	2	1	2	**Bajo (B)**
Soportes de información (Media)	[disk] discos.	Acceso no autorizado	El atacante consigue acceder a los discos que contienen información confidencial por fallo del sistema de autorización.	2	2	3	**Medio (M)**
		Eliminación accidental de la información	Eliminación accidental de información por no mantener los discos en un lugar seguro o por sobre montar información.	2	3	4	**Alto (A)**
Equipamiento auxiliar (AUX)	[ac] equipos de climatización	Manipulación de los equipos de climatización	Alteración intencionada del funcionamiento de los sistemas de climatización persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza.	2	1	2	**Bajo (B)**
	[ups] sistemas de alimentación ininterrumpida						
	[power] fuentes de alimentación	Daños de los equipos de suministro eléctrico	Los equipos de alimentación se dañan por deterioro o alguna falla técnica.	2	1	2	**Bajo (B)**
	[cabing] cableado [wire] cable	Ataque destructivo del cableado.	El atacante destruye ya sea por vandalismo, terrorismo, acción militar, etc.	1	2	2	**Bajo (B)**

	eléctrico [fiber] fibra óptica	Desgaste normal que un sistema de cableado	Problemas en el estado físico el cableado por el paso del tiempo.	2	1	2	**Bajo (B)**
Instalaciones (L)	[building] edificio [local] cuarto	Fuego	Incendios: posibilidad de que el fuego acabe con la infraestructura	2	2	3	**Medio (M)**
		Daños por agua	Inundaciones: posibilidad de que el agua acabe con la infraestructura	2	2	3	**Medio (M)**
		Ausencia de vigilancia por cámaras de seguridad.	Cuando los cuartos de red y las entradas del edificio se encuentran sin vigilancia, por lo que los intrusos pudieran aprovecharse de ello.	1	1	1	**Muy bajo (MB)**
		Desastres naturales	Otros incidentes que se producen sin intervención humana: terremoto y corrimiento de tierras.	1	1	1	**Muy bajo (MB)**
PERSONAL (P)	[adm] administrador de sistemas [sec] administrador de seguridad [ui] usuarios internos.	Ingeniería social (picaresca)	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	2	3	4	**Alto (A)**
		Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	3	2	4	**Alto (A)**
		Ausencia deliberada del puesto de trabajo	Como huelgas, absentismo laboral, bajas no justificadas.	2	1	2	**Bajo (B)**
		Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público.	2	1	2	**Bajo (B)**
		Compromiso por la seguridad informática.	El personal no muestra el interés suficiente para aplicar las políticas de seguridad.	2	2	3	**Medio (M)**

Valoración de vulnerabilidades (Elaboración propia).

5.4.6. Fase 6: Valoración del Riesgo (Impacto potencial)

La valoración de riesgo tiene como objetivo determinar el impacto potencial de las amenazas al momento de concretarse y como esto puede afectar a la seguridad de la información. El resultado obtenido en gracias a una estimación de la probabilidad de ocurrencia de una amenaza tomando en consideración los activos de mayor riesgo, la identificación de amenazas y la valoración de las vulnerabilidades.

Para calcular la materialización se utiliza dos elementos importantes como lo son: la probabilidad e impacto, que ayudar a determinan el nivel del riesgo. A continuación, las tablas de valoración del riesgo:

Tabla 30: *valoración según las ocurrencias.*

Impacto (cualitativo)	Valor (cuantitativo)	Descripción
Muy alto (MA)	**5**	Afecta de manera crítica la confidencialidad de la información y a su seguridad
		La información puede resultar demasiado complicado de recuperar.
		La imagen de la empresa se ve afectada extremadamente ante los proveedores y terceros.
		El desarrollo de las actividades no puede realizarse con normalidad y afectan negativamente las decisiones estratégicas y la continuidad del negocio.
Alto (A)	**4**	Afecta de manera muy grave la confidencialidad de la información y a su seguridad
		La información puede resultar muy difícil de recuperar y pudría producir muy graves afecciones de integridad.
		La imagen de la empresa se ve afectada muy gravemente ante los proveedores y terceros.
		Genera demasiados obstáculos para el desarrollo de actividades
Medio (M)	**3**	Afecta de manera grave la confidencialidad de la información y a su seguridad
		La información se puede recuperar en cierto tiempo pero con graves afecciones de integridad.
		La imagen de la empresa se ve afectada gravemente ante los proveedores y terceros.
		Se presenta obstáculos normalizados en las actividades
Bajo (B)	**2**	Afecta levemente la confidencialidad de la información y a su seguridad

		La información se puede recuperar en un tiempo prudente pero con mínimas afecciones de integridad.
		La imagen de la empresa se ve afectada muy poco ante los proveedores y terceros.
		La seguridad de la información tiene procesos que presentan muy poca importancia.
Muy bajo (MB)	**1**	No afecta a la confidencialidad de la información, es de bajo interés.
		La información se puede recuperar en un tiempo prudente y con la misma integridad.
		No se daña la imagen de la empresa ante los proveedores y terceros.
		La seguridad de la información tiene procesos que no presentan mucha importancia.

Valoración de riesgo en base a las amenazas (Elaboración propia).

***Tabla 31**: Valoración de la probabilidad según su ocurrencia*

Probabilidad (cualitativo)	Valor (cualitativo)	Descripción
Muy alto (MA)	5	Por lo menos una vez cada quince días
Alto (A)	4	Por lo menos una vez cada mes
Medio (M)	3	Por lo menos una vez cada trimestre
Bajo (B)	2	Por lo menos una vez cada semestre
Muy bajo (MB)	1	Por lo menos una vez cada año

Valoración de riesgo en base a la probabilidad (Elaboración propia).

Después de haber definido los criterios de valoración se procede a desarrollar una escala que permita determinar el grado de importancia que adquiere el riesgo frente a las vulnerabilidades, con esta evaluación debe ser posible reconocer los riesgos aceptables donde, aquellos que no necesitan control porque ya existen procedimientos de seguridad que solo necesitan una revisión rutinaria por parte de los encargados de seguridad.

Para determinar el cálculo del riesgo se precisa un mapa de probabilidad - impacto tanto cualitativa como cuantitativa, además de definirlos con colores según su grado de riesgo, la operación que se realiza es la siguiente:

RIESGO = PROBABILIDAD * IMPACTO

Tabla 32: *Probabilidad – impacto cualitativo.*

PROBABILIDAD	IMPACTO				
	Muy bajo (MB)	Bajo (B)	Medio (M)	Alto (A)	Muy alto (MA)
Muy bajo (MB)	Muy bajo (MB)	Muy bajo (MB)	Bajo (B)	Bajo (B)	Medio (M)
Bajo (B)	Muy bajo (MB)	Bajo (B)	Medio (M)	Medio (M)	Alto (A)
Medio (M)	Bajo (B)	Medio (M)	Medio (M)	Alto (A)	Alto (A)
Alto (A)	Bajo (B)	Medio (M)	Alto (A)	Muy alto (MA)	Muy alto (MA)
Muy alto (MA)	Medio (M)	Alto (A)	Alto (A)	Muy alto (MA)	Muy alto (MA)

Mapa de calor Probabilidad cualitativa

Tabla 33: Probabilidad – impacto cuantitativo.

PROBABILIDAD	IMPACTO				
	Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy alto (5)
Muy bajo (1)	1	2	3	4	5
Bajo (2)	2	4	6	8	10
Medio (3)	3	6	9	12	15
Alto (4)	4	8	12	16	20
Muy alto (5)	5	10	15	20	25

Mapa de calor Probabilidad cuantitativa. (Elaboración propia).

La valoración presentada a continuación suministra un medio que permite el priorizar los riesgos que representan una mayor amenaza para la organización y después aplicar un tratamiento adecuado.

Los riesgos que se toman en cuenta para la siguiente fase son: 6 (Medio), 8(ALTO), 10(MUY ALTO), 12(ALTO), 16(MUY ALTO), 20(MUY ALTO).

La tabla 34 muestra con más detalle los riesgos que se incluyen en esta lista:

Tabla 34: *Mapa de calor de riesgos.*

PROBABILIDAD	IMPACTO				
	Muy bajo (1)	Bajo (2)	Medio (3)	Alto (4)	Muy alto (5)
Muy bajo (1)	R17, R22	R11, R12, R19, R30, R32, R33	R13, R20, R28, R31, R34	R18, R24, R25, R26	R10, R36
Bajo (2)			R14, R16	R3, R4, R6, R8, R23, R37	R1, R7, R27, R29
Medio (3)				R2, R35	R5, R15, R38
Alto (4)					R9. R21
Muy alto (5)					

Mapa de calor de riesgos. (Elaboración propia).

En la *tabla 35* se presenta un resumen de los riesgos que necesitan de mitigación:

Tabla 35: *Valoración del riesgo.*

Tipo de Activos	Nombre de activo	Amenazas	ID Riesgo	Riesgo de seguridad	Probabilidad	Impacto	Total	Nivel de riego
Datos / Información (D)	[int] datos de gestión interna	Falta de cuidado sobre el manejo de información.	R1	Daños a la integridad y autenticidad por falta de registros documentados de los privilegios otorgados a los usuarios para el manejo de la información.	2	5	**10**	**Alto (A)**
	[files] Ficheros	Fugas de información.	R2	Daños a la integridad de la información por falta de la repartición de responsabilidades para disminuir la probabilidad de modificaciones no autorizadas.	3	4	**12**	**Alto (A)**
	[log] registro de actividad	Errores de secuencia al registrar actividades	R3	Dificultad para las investigaciones frente a la materialización de un riesgo debido a la falta de revisión regular de las actividades del personal que opera la información	2	4	**8**	**Medio (M)**
		Manipulación de los registros de actividad	R4	Alteración de la información por falta de registro de las modificaciones realizadas sobre la información que afecta su integridad.	2	4	**8**	**Medio (M)**
Servicio (S)	[int] interno (a usuarios de la propia organización)	Uso no previsto de los servicios.	R5	Indisponibilidad de los servicios debido al mal uso de los mismos por parte de los usuarios con fines de interés propios.	5	3	**15**	**Alto (A)**
	[ftp] transferencia de ficheros	Problemas de rendimiento	R6	Daños a la disponibilidad por sobrecarga de tareas que provoca la pérdida del servicio para realizar las actividades.	2	4	**8**	**Medio (M)**
	[email] correo electrónico	[Re-]encaminamiento de mensajes	R7	Alteración grave de envió de mensajes por correo electrónico suplantando la identidad de un usuario para tener acceso a su usuario de correo.	2	5	**10**	**Alto (A)**

Software - Aplicaciones informáticas (SW)	[app] servidor de aplicaciones	Errores de inicio o reinicio del servidor.	R8	No disponibilidad del servidor de aplicaciones a causa de que no arranca o arranca con errores	2	4	**8**	**Medio (M)**
	[file] servidor de ficheros	Acceso no autorizado al servidor	R9	Error en el almacenamiento de copias de seguridad debido a una mala configuración de las necesidades de mantenimiento que afectan la integridad y disponibilidad de la información.	4	5	**20**	**Muy alto (MA)**
	[browser] navegador web	Uso no previsto de navegador web	R10	Ataque de malware a causa de abrir paginas no autorizadas en el navegador web, comprometiendo la disponibilidad de los sistemas que se ven afectados.	1	5	**5**	**Medio (M)**
	[dbms] sistema de gestión de BD	Acceso no autorizado a la base de datos	R11	Daños a la integridad y disponibilidad de los sistemas de gestión de BD debido a la separación inadecuada de los ambientes de desarrollo y pruebas.	1	2	**2**	**Muy bajo (MB)**
	[email_server] servidor de correo electrónico	Difusión de software dañino intencionado	R12	Problemas de disponibilidad del servidor de correo debido a fallos producidos por la incorrecta configuración del mismo en los puntos finales.	1	2	**2**	**Muy bajo (MB)**
	[av] antivirus	Divulgación de información por malware	R13	Indisponibilidad del antivirus debido a fallo de mantenimiento/actualización de versiones más recientes.	1	3	**3**	**Bajo (B)**
	[os] sistema operativo	Instalación de software desconocido.	R14	Daños de integridad por falta de control sobre las instalaciones de software de fabricantes desconocidos.	3	2	**6**	**Medio (M)**
		Errores de mantenimiento / actualización de programas (software)	R15	Problemas de disponibilidad del sistema operativo debido a errores de actualización de parches.	3	5	**15**	**Alto (A)**
hardware		Avería de origen físico del hardware	R16	Problemas de disponibilidad de los equipos finales por avería de hardware.	3	2	**6**	**Medio (M)**

- Equipos informáticos (HW)	[pc] informática personal.	Pérdida de equipos	R17	Daños a la disponibilidad y confidencialidad del equipo informático causado por hurto de los dispositivos que lo componen E/S.	1	1	**1**	**Muy bajo (MB)**
	[firewall] cortafuegos.	Manipulación de los equipos	R18	Problemas de autenticidad y tranzabilidad debido a la falta de procesos formales donde se registre a los usuarios responsables de los equipos.	1	4	**4**	**Bajo (B)**
	[peripheral] periféricos.	Pérdida de equipos	R19	Daños o robos a los equipos informáticos debido a la falta de registro de entrada y salida de equipos de la empresa.	1	2	**2**	**Muy bajo (MB)**
	[switch] conmutadores.	Manipulación de los equipos	R20	Abuso de privilegios para el acceso a equipos que no son de la competencia para ciertos usuarios provocando daños en su funcionamiento.	1	3	**3**	**Bajo (B)**
	[mobile] informática móvil, laptops.	Robo de laptops y equipos móviles.	R21	Daños a la confidencialidad por falta de controles sobre el uso de dispositivos móviles dentro de la empresa.	4	5	**20**	**Muy alto (MA)**
	[ipphone] teléfono IP.	Uso no previsto de los equipos	R22	Mal uso de los teléfonos por parte de los usuarios para su propio beneficio.	1	1	**1**	**Muy bajo (MB)**
Redes de comunicaciones (COM)	[LAN] red local	Errores del administrador al compartir sus credenciales.	R23	Problemas de confidencialidad por revelar credenciales de administrador a proveedores de tecnología.	2	4	**8**	**Medio (M)**
		Caída del sistema por agotamiento de recursos	R24	No disponibilidad de la red LAN por no contar con los recursos necesarios para soportar la sobrecarga de datos.	2	2	**4**	**Bajo (B)**
		Suplantación de la identidad del usuario	R25	Daños de tranzabilidad por falta de un ataque de suplantación de identidad para tomar control de la red.	2	2	**4**	**Bajo (B)**

		Abuso de privilegios de acceso a la red	R26	Daños de tranzabilidad por falta de registros documentados de privilegios de usuarios en una red.	2	2	**4**	**Bajo (B)**
		Demasiadas aplicaciones que operan sobre la red.	R27	Daños de disponibilidad porque existen programas que sobrecargan la red haciendo conexión aun sin estar en uso.	2	5	**10**	**Alto (A)**
Soportes de información (Media)	[disk] discos.	Acceso no autorizado	R28	Robo o pérdida de los discos de información por la falta de controles para el registro de entrada y salida de personal externo en los cuartos donde se almacenan.	1	3	**3**	**Bajo (B)**
		Eliminación accidental de la información	R29	Pérdida parcial/total de la información almacenada en los discos por la falta de procesos para la eliminación segura de hardware con información.	2	5	**10**	**Alto (A)**
Instalaciones (L)	[building] edificio	• Fuego	R30	Perjudicar la estructura del edificio debido a un Incendio.	1	2	**2**	**Muy bajo (MB)**
		• Daños por agua	R31	Deterioro de la infraestructura de la empresa debido a daños por agua.	1	3	**3**	**Bajo (B)**
	[local] cuarto	• Fuego	R32	Perjudicar la estructura de los cuartos provocado por un incendio.	1	2	**2**	**Muy bajo (MB)**
		• Daños por agua	R33	Daños por agua a la infraestructura de los cuartos de red.	1	2	**2**	**Muy bajo (MB)**
PERSONAL (P)	[adm] administrador de sistemas	• Compromiso por la seguridad informática.	R34 R35	Falta de preocupación por impulsar la seguridad de la información en cada área de trabajo.	1	3	**3**	**Bajo (B)**

	[sec] administrador de seguridad	• Compromiso por la seguridad informática.	R36	Problemas de disponibilidad de la información por la falta de aplicación de políticas de seguridad.	3	4	**12**	**Alto (A)**
		• Ingeniería social (picaresca)	R37	Daños graves de confidencialidad por divulgación de la información por empleados o ex empleados.	1	5	**5**	**Medio (M)**
	[ui] usuarios internos.	• Extorsión	R38	Problemas de confidencialidad de la información por empleados que son obligados mediante extorción a revelar información.	2	4	**8**	**Medio (M)**
		• Compromiso por la seguridad informática.	R39	Problemas de integridad y confidencialidad por la falta de capacitación del usuario sobre el manejo de información sensible.	1	5	**5**	**Medio (M)**

Valoración de los riesgos según su probabilidad – impacto. (Elaboración propia).

5.4.7. Fase 7: Tratamiento del riesgo

Luego de valorar los riesgos de seguridad de la información es conveniente presentar ciertas medidas de protección para mantener bajo control las vulnerabilidades que se encontraron en la infraestructura lógica del hotel, los riesgos que han sido descubiertos se pueden prevenir, impedir, reducir o controlar de acuerdo a las necesidades. Todas las opciones posibles para el tratamiento del riesgo son consideradas para su aplicabilidad según lo disponga la Dirección de Seguridad de la información de la empresa.

El integrar medidas de control conlleva el consumo de recursos por un lado técnicos y por otro financiero por tal motivo se compara la rentabilidad contra el beneficio de la mitigación:

Tabla 36: *Tipos de Mitigación.*

ID	Tratamiento del Riesgo	Rentabilidad vs Beneficio
TR1	Evitar el Riesgo.	Evitar el riesgo conlleva que la rentabilidad es inversamente proporcional al beneficio que se espera obtener.
TR2	Transferir el Riesgo.	Al transferir el riesgo a terceros el beneficio es oportuno para la empresa debido a que es proporcional m al costo, resultando más económico que al tratarlo de manera interna.
TR3	Aceptar el Riesgo.	La rentabilidad de asumir el riesgo sin contar con ningún tipo de control no es proporcional con el beneficio a obtener, por lo que existe un aumento de recursos implicados y el costo de tiempo invertido en monitorear continuamente el riesgo.
TR4	Reducir el riesgo.	Al reducir el riesgo, el costo de la implementación de los controles resulta ser adecuada con los beneficios que se espera.

Mitigación de riesgo. (Elaboración propia).

La principal estrategia que se adoptó en este caso de estudio fue analizar todas las situaciones en las que se puede presentar un riesgo con el objetivo de encaminar las decisiones por el sendero correcto.

Tabla 37: *Valoración del riesgo.*

Valoración del riesgo			Tratamiento del riesgo		
ID Riesgo	**Riesgo de seguridad**	**Nivel de riego**	**Tratamiento del riesgo**	**Id**	**Descripción del control**
R1	Daños a la integridad y autenticidad por falta de registros documentados de los privilegios otorgados a los usuarios para el manejo de la información.	**Alto (A)**	Reducir el riesgo.	**C1**	Documentar los registros otorgados a los diferentes usuarios según su perfil, tomando en cuenta si es necesario conceder el privilegio de acceso.
R2	Daños a la integridad de la información por falta de la repartición de responsabilidades para disminuir la probabilidad de modificaciones no autorizadas.	**Alto (A)**	Reducir el riesgo.	**C2**	Establecer controles para la asignación de responsabilidades dentro de la empresa del manejo de la información con el objetivo de conocer quién es el usuario responsable.
R3	Dificultad para las investigaciones frente a la materialización de un riesgo debido a la falta de revisión regular de las actividades del personal que opera la información	**Medio (M)**	Aceptar el Riesgo.	**C3**	Estipular un seguimiento y la documentación de los cambios en el registro de actividades solo si el motivo es relevante para seguir con el proceso de modificación.
R4	Alteración de la información por falta de registro de las modificaciones realizadas sobre la información que afecta su integridad.	**Medio (M)**	Aceptar el Riesgo.	**C4**	Realizar revisiones continuas de las actividades desarrolladas por usuarios que manejan información sensible en la empresa para lego evaluar su importancia según las políticas de seguridad.
R5	Indisponibilidad de los servicios debido al mal uso de los mismos por parte de los usuarios con fines de interés propios.	**Alto (A)**	Reducir el riesgo.	**C5**	Construir un política en la cual se defina el uso que se debe dar a los servicios disponibles para cada usuario y el compromiso les corresponde, además dar a conocer a los usuarios esta información para reducir el riesgo de uso inadecuado de los servicios.
R6	Daños a la disponibilidad por sobrecarga de tareas que provoca la pérdida del servicio para realizar las actividades.	**Medio (M)**	Transferir el Riesgo.	**C6**	Proveedores de tecnología

R7	Alteración grave de envió de mensajes por correo electrónico suplantando la identidad de un usuario para tener acceso a su usuario de correo.	**Alto (A)**	Transferir el Riesgo.	**C7**	Proveedores de tecnología
R8	No disponibilidad del servidor de aplicaciones a causa de que no arranca o arranca con errores	**Medio (M)**	Aceptar el Riesgo.	**C7**	Proveedores de tecnología
R9	Error en el almacenamiento de copias de seguridad debido a una mala configuración de las necesidades de mantenimiento que afectan la integridad y disponibilidad de la información.	**Muy alto (MA)**	Reducir el riesgo.	**C8**	Elegir los tipos de backup (incremental, diferencial o total) que se utilizaran en los dispositivos de almacenamiento de información que mejor se adapte a las necesidades, dependiendo del volumen de la información y su valor.
R10	Ataque de malware a causa de abrir paginas no autorizadas en el navegador web, comprometiendo la disponibilidad de los sistemas que se ven afectados.	**Medio (M)**	Transferir el Riesgo.	**C9**	Proveedores de tecnología
R11	Daños de integridad por falta de control sobre las instalaciones de software de fabricantes desconocidos.	**Medio (M)**	Reducir el riesgo.	**C10**	Bloquear la instalación libre de software en los dispositivos finales, administrado desde el servidor para que nadie que no sea el administrador pueda instalar cualquier tipo de archivo ejecutable.
R12	Problemas de disponibilidad del sistema operativo debido a errores de actualización de parches.	**Alto (A)**	Aceptar el Riesgo.	**C11**	Realizar una revisión periódica de las actualizaciones del sistema operativo antes de su instalación, existen parches que no son estables y se debe esperar para su actualización cuando esté disponible uno que sea estable o necesario.
R13	Problemas de disponibilidad de los equipos finales por avería de hardware.	**Medio (M)**	Reducir el riesgo.	**C12**	Desarrollar un mantenimiento preventivo de los equipos finales para evitar daños de su funcionamiento.

R14	Daños a la confidencialidad por falta de controles sobre el uso de dispositivos móviles dentro de la empresa.	**Muy alto (MA)**	Reducir el riesgo.	**C13**	Crear una política de uso de dispositivos móviles externos a la empresa donde se defina el personal que está autorizado a su uso por razones de trabajo y los usuarios a los cuales se les prohíbe.
			Reducir el riesgo.	**C14**	Establecer una política para controlar el almacenamiento de información personal en los dispositivos móviles que pertenecen a la empresa para prevenir que en un robo quede expuesto la información privada del personal.
R15	Problemas de confidencialidad por revelar credenciales de administrador a proveedores de tecnología.	**Medio (M)**	Aceptar el Riesgo.	**C15**	Generar una política para controlar la revelación de contraseñas hacia los proveedores de tecnología solo si es necesario y su compromiso con la discreción de esta información.
R16	Daños de disponibilidad porque existen programas que sobrecargan la red haciendo conexión aun sin estar en uso.	**Alto (A)**	Transferir el Riesgo.	**C16**	Proveedores de tecnología
R17	Pérdida parcial/total de la información almacenada en los discos por la falta de procesos para la eliminación segura de hardware con información.	**Alto (A)**	Reducir el riesgo.	**C17**	Crear procesos seguros para el respaldo y la eliminación de la información de dispositivos auxiliares.
R18	Problemas de disponibilidad de la información por la falta de aplicación de políticas de seguridad.	**Alto (A)**	Reducir el riesgo.	**C18**	Asegurarse mediante evaluaciones sobre la comunicación entre los jefes de los departamentos y los empleados de las correspondientes áreas si están siendo controladas sus actividades relacionadas con la seguridad de la información antes de ejecutarse, con la supervisión de los jefes.
R19	Daños graves de confidencialidad por divulgación de la información por empleados o ex empleados.	**Medio (M)**	Reducir el riesgo.	**C19**	Crear políticas que aseguren la no divulgación de los ex empleados de información privada de la empresa porque existen problemas

					legales que afectarían a estas personas por violación de confidencialidad.
R20	Problemas de confidencialidad de la información por empleados que son obligados mediante extorción a revelar información.	**Medio (M)**	Evitar el Riesgo.	**C20**	Asegurar la comunicación de los empleados frente a problemas de seguridad de la información a la dirección de TI de la empresa para tomar acciones.
R21	Problemas de integridad y confidencialidad por la falta de capacitación del usuario sobre el manejo de información sensible.	**Medio (M)**	Evitar el Riesgo.	**C21**	Realizar capacitaciones de seguridad de la información a los usuarios que manejan hasta el mínimo volumen de datos para crear un entorno de seguridad desde los empleados operacionales.

Mitigación de riesgo. (Elaboración propia).

5.4.8. Fase 8: Reporte de resultados

Para afianzar la seguridad de la información en la empresa es necesario comunicar los resultados encontrados a través del desarrollo de este análisis de riesgos al jefe de TI/Sistemas de la organización con el objetivo de asegurar que las brechas con mayor impacto puedan ser controladas a tiempo. El tratamiento que se realizó a los riesgos es presentado y valorados para la consideración de la Dirección de Tecnología.

En el ANEXO A se muestra un resumen puntual del análisis de riesgo, el cual sirvió como apoyo para demostrar junto a los resultados el estado actual de la seguridad de la información del negocio.

5.4.9. Fase 9: Manual de buenas prácticas

En vista de la situación en la que se encuentra la empresa se propuso desarrollar un manual de buenas prácticas como una medida de seguridad que permita minimizar en lo posible la materialización de los riesgos y garantizar la confidencialidad, integridad y la disponibilidad de la información. Este manual recoge estrategias de formación y admite la concientización para fortalecer el ambiente de ciberseguridad en el personal para la organización, hay que tomar en cuenta que técnicamente es imposible alcanzar al 100% la seguridad de la información en una empresa, pero la aplicación de buenas prácticas puede ayudar a reducir los posibles ataques por parte de atacantes.

Para la elaboración del documento se tomó en cuenta el análisis del estado de los controles y el análisis de riesgo en la empresa para definir los objetivos a alcanzar con su desarrollo y se recibió el apoyo necesario por parte del departamento de TI/Sistemas.

El documento adjunto en los archivos del proyecto llamado “Manual de buenas prácticas en seguridad de la información para el Hotel Four Points by Sheraton Cuenca” muestra el manual que está compuesto por:

- Seguridad de los dispositivos móviles.
- Seguridad de dispositivos de almacenamiento removibles.
- Aseguramientos del sistema operativo y aplicaciones.
- Seguridad del correo electrónico corporativo.

- Seguridad en los navegadores web.
- Seguridad en la red.
- Seguridad para los respaldos
- Seguridad física del entorno y del personal.

CRONOGRAMA DE ACTIVIDADES

Nombre de tarea	Duración	Comienzo	Fin	% completado
Análisis de riesgo	**43 días**	**lun 21/10/19**	**mié 18/12/19**	**100%**
Planificación	**8 días**	**lun 21/10/19**	**mié 30/10/19**	**100%**
Determinar alcances y delimitaciones	4 días	lun 21/10/19	jue 24/10/19	100%
Entrega de propuesta a la empresa	4 días	mié 23/10/19	lun 28/10/19	100%
Desarrollo de una encuenta con los jefes de área	4 días	vie 25/10/19	mié 30/10/19	100%
Análisis de la situación actual GAP	**16 días**	**vie 25/10/19**	**vie 15/11/19**	**100%**
Análisis de la estructura organizacional	2 días	vie 25/10/19	lun 28/10/19	100%
Análisis de la red LAN	3 días	mar 29/10/19	jue 31/10/19	100%
Análisis del SGSI establecido en la empresa.	2 días	vie 01/11/19	lun 04/11/19	100%
1ra entrevista con el jefes claves	2 días	mar 05/11/19	mié 06/11/19	100%
Análisis del cumplimiento de controles.	2 días	jue 07/11/19	vie 08/11/19	100%
Reporte del cumplimiento de las normas ISO 27001	3 días	vie 08/11/19	mar 12/11/19	100%
2da estrevista con los jefes claves	2 días	lun 11/11/19	mar 12/11/19	100%
Análsis de riesgo	**25 días**	**mié 13/11/19**	**mar 17/12/19**	**100%**
Fase 1: Levantamiento de activos	3 días	mié 13/11/19	vie 15/11/19	100%
Fase 2: Clasificación de la información	2 días	lun 18/11/19	mar 19/11/19	100%
Revisiones de las areás tecnologicas y puntos finales	3 días	mié 20/11/19	vie 22/11/19	100%
Fase 3: Valoración de activos	2 días	lun 25/11/19	mar 26/11/19	100%
Fase 4: Identificación de amenazas	3 días	mié 27/11/19	vie 29/11/19	100%
Análisis de reportes, documento, manuales, etc.	2 días	lun 02/12/19	mar 03/12/19	100%
Fase 5: Identificacion y valoración de vulnerabilidades	2 días	mié 04/12/19	jue 05/12/19	100%
Fase 6: Valoración del riesgo	2 días	vie 06/12/19	lun 09/12/19	100%
Fase 7: Tratamiento de riesgo potencial	2 días	mar 10/12/19	mié 11/12/19	100%
Fase 8: Reporte de resultados.	1 día	jue 12/12/19	jue 12/12/19	100%
Fase 9: Manual de buenas prácticas	2 días	vie 13/12/19	lun 16/12/19	100%
Entrega del manual de buenas prácticas	1 día	mar 17/12/19	mar 17/12/19	100%

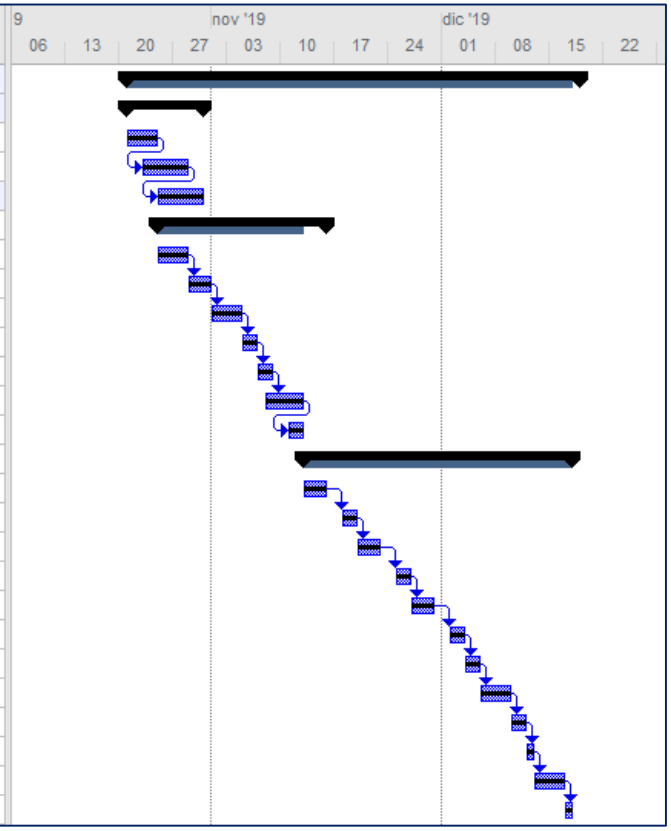

Figura 20: *Cronograma de actividades*
Fuente: *(Autor, 2019).*

CONCLUSIONES

En la empresa Four Points by Sheraton Cuenca se maneja un volumen considerable de datos por lo que la información es activo esencial para desarrollar sus actividades y ofrecer servicios de calidad a sus clientes, lo que conlleva a la adaptación de las nuevas tecnologías para mejorar y agilizar sus procesos operacionales, la información siendo el pilar fundamental en el que se apoya todo tipo de empresas puede verse vulnerable a estos cambios y presentar riesgos potenciales que afecten las propiedades de los activos de información.

La importancia de contar con un SGSI que abarque las necesidades de la empresa supone una herramienta valiosa para resguardar la información de posibles amenazas, siendo prudente recordar que, así como se expande la tecnología también crecen los ataques cibernéticos volviéndose cada vez más complejas y sofisticadas. Las empresas deben entender que manejar información privada conlleva una gran responsabilidad y puede tener consecuencias desastrosas si llegase a caer en manos equivocadas.

La finalidad de este proyecto fue desarrollar un análisis de riesgo que presente la reevaluación del catálogo de vulnerabilidades de la empresa con el objetivo de proteger la información y crear una cultura de buenas prácticas de seguridad de la información, a través del levantamiento de activos, analizar un conjunto de amenazas a las que se exponen los activos, identificar las vulnerabilidades y la gestión de riesgos siendo todos estos procesos necesarios para fortalecer un SGSI.

Existen muchas metodologías para en análisis de riesgo pero se debe tomar en cuenta que no todas sirven para un mismo propósito, dependiendo de la disponibilidad de los implicados y el tiempo máximo para ver los resultados de la implementación podría ser una u otra, en este caso se estableció un análisis de riesgo con ayuda de MAGERIT porque mantiene bien fundamentadas las decisiones que se toman y puede ser fácilmente defendibles, ofrece un método sistematizado para el tratamiento del riesgo y aplicar mediada necesarias para su gestión.

Una de las maneras para fomentar las buenas prácticas de seguridad es construir una manual con salvaguardas para educar a todos los empleados y reducir las amenazas de tipo errores no intencionados por parte de los propios miembros de la empresa.

RECOMENDACIONES

En base al análisis de la situación actual de los controles aplicados en la empresa se puede recomendar aplicar las medidas que en la evaluación presentaron una valoración con mayores falencias:

Brecha 1. _Organización de la seguridad de la información

- Crear una política para dispositivos móviles para que limitar y controlar el uso de los dispositivos móviles para controlar la propagación de amenazas.

Brecha 2. _ Gestión de Activos

- Realizar un inventario de activos con su respectiva categorización ya que la existente en la empresa no se encuentra actualizada.
- Definir la clasificación de la información según su importancia ya que en procesos de recuperación de desastres la empresa restaura toda la información almacenada en los equipos comprometidos hasta la cierta información que no tiene ningún tipo de relación con sus operaciones, esta información muchas veces es almacenada por los empleados en equipos de la empresa ocupando espacio innecesario.
- Crear una política documentada para gestionar las unidades removibles que contienen información sensible para la empresa, debido a que existen empleados que utilizan el mismo dispositivo para guardar información de todo tipo y suelen prestarse entre si lo que puede ocasionar fugas de información confidencial.

Brecha 3. _ Control de acceso

- Definir un documento formal en donde se registre los usuarios que tienen todo tipo de accesos a la red interna, existen procesos para el registro, pero no genera ningún tipo de documentación.

Brecha 4. _ Seguridad Física y del entorno

- Mantener el ambiente libre de documentos físicos, notas, contraseñas importantes para la empresa y apagar los equipos de cómputo una vez que salgan cerrar las puertas de los departamentos porque existen información confidencial sobre los escritorios y podrían ser hurtados por terceros.
- Concientizar a los empleados acerca de la política que cubre la integridad de los equipos al momento de que salgan de la empresa y los riesgos que implica debido a que existe personal que sale con el equipo fuera de las instalaciones.
- Al formatear los ordenadores en el memento de que se restaura la información suele ser muy a menudo que no se elimina la información de la sesión anterior por lo que se debe crear una política para la eliminación segura de la información.

Brecha 5. _ Aspectos de seguridad para la gestión de la continuidad del negocio

- Mantener revisiones periódicas sobre los requisitos futuros del SGSI en respuesta a nuevas vulnerabilidades.

Brecha 6. _ Aspectos de seguridad para la gestión de la continuidad del negocio

- Crear un proceso para la designar los datos para pruebas (actualmente en desarrollo por la misma organización).

Brecha 7. _ Gestión de incidentes de seguridad de la información

- Documentar de manera específica las responsabilidades administrativas sobre incidentes para identificar y direccionar los reportes de los casos más relevantes.

Por otra parte, también se puede recomendar políticas para mejorar las que se encuentran establecidas actualmente, estas también fueron expuestas en el manual de buenas prácticas que se entregó a la empresa, las cuales son:

- Evitar el acceso de dispositivos móviles dentro de las instalaciones de la empresa a todos los usuarios que no tienen autorización para manejarlos durante la jornada laboral.
- Los usuarios tienen la responsabilidad sobre los dispositivos móviles o portátiles que se le han facilitado para su desempeño laboral tanto fuera como dentro de la empresa y responderán por los que hayan sido destruidos, dañados o robados mientras haya estado bajo si custodia.
- Los usuarios requieren seguir las buenas prácticas de seguridad para el uso de dispositivos móviles.
- El uso de dispositivos de almacenamiento removibles debe ser solamente autorizado por el administrador encargado de la seguridad de la información, cualquier dispositivo externo que no mantenga un registro y autorización por parte de esta entidad se considera una amenaza y el que lo utilice tendrá que responder por las sanciones establecidas por violación a la seguridad de la información.
- El administrador deberá mantener un control documentado de cuáles son los dispositivos con estos permisos de funcionamiento y que tipo de información mantienen almacenados.
- El administrador deberá proveer de acciones de cifrado para la encriptación de la información según su clasificación y nivel de confidencialidad.
- Los administradores tienen la responsabilidad de construir procesos seguros de eliminación de la información almacenada en estos dispositivos, este proceso se lleva a cabo cuando los datos son obsoletos o el tiempo de vida de estos medios haya finalizado.
- El personal autorizado deberá gestionar y coordinar las actualizaciones del sistema operativo y las aplicaciones de los equipos finales conectados a la

red administrativa, además de asegurar que todos los equipos tengan actualizados los parches de seguridad que ofrece el fabricante.

- Es responsabilidad de los usuarios que tengan acceso a un correo corporativo de la empresa aplicar las medidas preventivas que se ofrecen en el manual de buenas prácticas y tienen la obligación de informar cualquier incidente que le resulte sospechoso y pueda afectar la seguridad de la información.
- El administrador deberá automatizar las actualizaciones necesarias del navegador web para el desarrollo de las actividades de los usuarios. Así también debe mantenerse pendiente de las comunicaciones entrantes y salientes que son bloqueadas por el firewall.
- Es responsabilidad del administrador de la red LAN corporativa realizar un análisis y gestión de riesgos para medir el nivel de seguridad de la infraestructura tecnológica, mediante la aplicación de test de penetración con el objetivo de crear planes estratégicos para evitar los ataques de ciberseguridad.
- Es responsabilidad de la Dirección de tecnología y el administrador de TI educarse y educar al personal que se encuentra conectado a la red de comunicación con el objetivo de formar la primera línea de protección contra vulnerabilidades.
- Los proveedores de tecnología tienen la obligación de trabajar conjuntamente con el administrador de seguridad de la información para brindar servicios de protección confiables y establecer medidas a nivel de hardware y software para la organización.
- El administrador de TI tiene la obligación de establecer controles documentados para la asignación de privilegios hacia los usuarios dentro de la red corporativa evitando el acceso de usuario no requeridos.
- El usuario tiene la responsabilidad de seguir las buenas prácticas de seguridad para el uso de los servicios y la red.
- El equipo de seguridad debe realizar un plan documentado para los

respaldos de seguridad de la información de toda la empresa y desarrollar

controles de supervisión periódicos para asegurar los respaldos de en cada equipo final.

- Todo empleado que maneje en cualquier nivel la información de la empresa debe aceptar las condiciones de confidencialidad, el uso adecuado de los equipos informáticos y deberá cumplir con las políticas de seguridad establecidas
- Todo empleado deberá comprometerse a usar los servicios que se le ofrecen para que realice sus actividades diarias según lo establezcan las políticas de seguridad actuales.
- El empleado que haya culminado su vínculo contractual deberá entregar todos los equipos informáticos proporcionados por la empresa y cumplir con las condiciones de seguridad que fueron definidas al aceptar su contrato, como lo son el acuerdo de confidencialidad.
- Durante su periodo contractual el empleado tiene la responsabilidad de avisar de manera inmediata los incidentes de seguridad que comprometa a la información o cualquier actividad sospechosa por otros empleados o terceros.
- Los empleados que manejen volumen de datos se les asignaran responsabilidades sobre el manejo, modificación, eliminación y pérdida de información. Con la finalidad de conocer al responsable/ los responsables de las modificaciones que pudiera sufrir la información y la perjudique en sus procesos de tranzabilidad, autenticidad e integridad.
- El equipo de seguridad designado deberé realizar revisiones de las actividades desarrolladas por los empleados que manejan información sensible cada cierto tiempo o cuando suscite alguna actividad sospechosa.
- Realizar capacitaciones sobre la seguridad de la información tanto a los jefes de área como a los demás empleados que mantienen relación con los departamentos operacionales y administrativos.

BIBLIOGRAFÍA

Arbesú, L. P. (2018). Seguridad desde el inicio. *TechTarget*, 15.

Daniel Benchimol. (2011). *Hacking desde cero.* Buenos Aires: Redusers.

Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2011). *Magerit versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

Goez, L. (2014). *Libro Virtual Seguridad Informatica.* Medellín: Calameo.

Gómez, R., Pérez, D., Donoso, Y., & Herrera, A. (2017). *Metodología y gobierno de la gestión de riesgos de tecnología de la información.* Bogotá.

Ministerio de Administraciones Públicas. (2011). *Magerit versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

Nilo, F., & Salinas, V. (2017). *Auditoría de seguridad física de la Empresa AGROKASA Supe.* Huacho: Universidad San Pedro.

Santos, S. (2009). *Una al día - Once años de seguridad informática.* Madrid: Hispasec Sistemas.

FUENTES ELECTRÓNICAS

Alvarado, J., Pacheco, J., & Martillo, I. (Noviembre de 2018). *Revista Contribuciones a las Ciencias Sociales.* Obtenido de El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT: https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html

BACSCIRT. (31 de Octubre de 2018). *Ciberataques: Las estrategias delictivas del mundo digital.* Obtenido de https://www.ba-csirt.gob.ar/files/boletines/B46_AtaquesCiberneticos.pdf

GIAC Certifications. (2013). *GIAC Certifications*. Obtenido de Documento de certificación Global de Information Assurance: https://www.giac.org/paper/gsec/3018/security-lifecycle/105040

Giraldo, Á. (18 de 10 de 2014). *ISO 27001 para PYMES.* Obtenido de UNIR: https://reunir.unir.net/bitstream/handle/123456789/3128/AngelaMaria_Parra_Giraldo.pdf?sequence=1&isAllowed=y

Goana, R. (Octubre de 2013). *Aplicación de la metodología MAGERIT para el análisis y gestión de riesgos de seguridad de la información aplicada a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala.* Obtenido de upc: https://dspace.ups.edu.ec/bitstream/123456789/5272/1/UPS-CT002759.pdf

INCIBE. (20 de Marzo de 2017). *INCIBE*. Obtenido de INCIBE: : https://www.incibe.es/protege-tu-empresa/blog/amenaza-vs-vulnerabilidad-sabes-se-diferencian

ISO27k. (2013). *ISO / CEI 27001: 2013 - Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos*

(segunda edición) . Obtenido de iso27001security: https://www.iso27001security.com/html/27001.html

Joyce Boland. (27 de Febrero de 2019). *El líder financiero moderno*. Obtenido de Oracle latinoamerica Blog: https://blogs.oracle.com/modernfinance/how-to-cloud-first-steps-to-successful-oracle-cloud-erp-project

López, D., & Vásquez , S. (2017). *Universidad del Azuay*. Obtenido de Respositorio Institucional: http://dspace.uazuay.edu.ec/handle/datos/5391

MARSH & McLennan. (2019). *Percepción del Riesgo Cibernético en Latinoamérica 2019.* Obtenido de MARSH Company: https://www.marsh.com/uy/es/insights/research/marsh-microsoft-encuesta-percepcion-riesgo-cibernetico-2019.html

Mendoza, M. Á. (16 de Julio de 2015). *ESET*. Obtenido de De la identificación y análisis a la gestión de riesgos de seguridad: https://www.welivesecurity.com/la-es/2015/07/16/analisis-gestion-de-riesgos-seguridad/

Ministerio de Administraciones Públicas. (2011). *Magerit versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid.

Nilo, F., & Salinas, V. (2017). *Auditoría de seguridad física de la Empresa AGROKASA Supe.* Huacho: Universidad San Pedro.

Perdomo, M., & Frankye, M. (2018). *distrital.* Obtenido de Diseño de un sistema de gestión de seguridad (SGSI) para la empresa manufacturera persianas y enrollables SAFRA SAS basado en los estándares de la norma ISO 27001: http://repository.udistrital.edu.co/bitstream/11349/14200/1/MateusAlfonsoFrankyeSteven2018.pdf

Rodríguez, J. M., & Peralta, I. (2013). *Gestión de riesgos con MAGERIT.* Obtenido de tiThink: https://www.tithink.com/publicacion/MAGERIT.pdf

Santos, S. (2009). *Una al día - Once años de seguridad informática.* Madrid: Hispasec Sistemas.

Segovia, A. J. (2013). *Centro de Consulta Online sobre ISO 27001 y ISO 22301*. Obtenido de Centro de Consulta Online sobre ISO 27001 y ISO 22301: https://advisera.com/27001academy/es/que-es-iso-27001/

GLOSARIO

Backup: se entiende como una copia de seguridad de los datos originales que se almacenan en equipos informáticos o lugares intangibles

Brecha de seguridad: se entiende como la vulnerabilidad que es aprovechada por un atacante para introducirse en los sistemas de información sin ninguna buena intensión, la mayoría de veces persiguen un beneficio económico.

Ciberseguridad: se refiere a la relación que existe entre con la informática y los equipos informáticos y de telecomunicación con el objetivo de brindar seguridad a los sistemas de información.

Pentesting: se entienden como las técnicas de intrusión hacia los sistemas de información con el objetivo de demostrar que existen falencias de seguridad.

Salvaguardas: se refiere a las medidas de protección para resguarda la información y reducir la probabilidad de ocurrencia de una amenaza dentro de un SI.

SGSI: se refiere como un sistema de gestión de seguridad de la información que supone una herramienta para analizar y permite gestionar, mantener y supervisar la seguridad de la información.

SI: corresponde a un sistema de información que maneja un conjunto de datos que se disponen entre sí para permitir su gestión en los procesos organizacionales de las empresas.

TI: se entiende como la tecnología de la información que se aplica en los equipos finales y de telecomunicación en el contexto de las empresas.

ANEXOS

ANEXO A: Catálogo de amenaza

						Valoración del riesgo			
Tipo de Activos	Nombre del activos de información	**ID Amenaza**	**Amenazas**	**ID Riesgo**	**Riesgo de seguridad**	**Probabilidad**	**Impacto**	**Total**	**Nivel de riego**
DATOS / INFORMACIÓN (D)	[int] datos de gestión interna	AM1	• Errores de los usuarios al deshacerse de documentos importantes.	R1	Daños a la integridad y autenticidad por falta de registros documentados de los privilegios otorgados a los usuarios para el manejo de la información.	2	5	**10**	**Alto (A)**
	[files] Ficheros	AM2	• Fugas de información.	R2	Daños a la integridad de la información por falta de la repartición de responsabilidades para disminuir la probabilidad de modificaciones no autorizadas.	3	4	**12**	**Alto (A)**
	[log] registro de actividad	AM3	• Errores de secuencia al registrar actividades	R3	Perdida de información por modificaciones deliberadas de los registros de actividad provocando dificultades para la investigación de las mismas.	3	4	**12**	**Alto (A)**
				R4	Dificultad para las investigaciones frente a la	2	4	**8**	**Medio (M)**

					materialización de un riesgo debido a la falta de revisión regular de las actividades del personal que opera la información				
			• Manipulación de los registros de actividad	R5	Perdida de información por errores de almacenamiento de documentos del usuarios de la empresa afectando su integridad.	4	3	**12**	**Alto (A)**
				R6	Alteración de la información por falta de registro de las modificaciones realizadas sobre la información que afecta su integridad.	2	4	**8**	**Medio (M)**
	[backup] copias de respaldo	AM3	• Eliminación de las copias de respaldo	R7	Daños a la confidencialidad y autenticidad de la información por falta del control de contraseñas	4	5	**20**	**Muy alto (MA)**
Servicio (S)	[int] interno (a usuarios de la propia organización)	AM4	• Uso no previsto de los servicios.	R8	Indisponibilidad de los servicios debido al mal uso de los mismos por parte de los usuarios con fines de interés propios.	5	3	**15**	**Alto (A)**
	[ftp] transferencia de ficheros	AM5	• Denegación de servicio	R9	Daños a la confidencialidad y autenticidad por fallos de autenticación del acceso al servicio que desencadenan el acceso a usuarios no permitidos.	1	5	**5**	**Medio (M)**
	[email] correo electrónico	AM6	• [Re-]encaminamiento de mensajes	R10	Alteración grave de envió de mensajes por correo electrónico	1	2	**2**	**Muy bajo (MB)**

					suplantando la identidad de un usuario para tener acceso a su usuario de correo.				
Software - Aplicaciones informáticas (SW)	[app] servidor de aplicaciones	AM7	• Errores de inicio o reinicio del servidor.	R11	No disponibilidad del servidor de aplicaciones a causa de que no arranca o arranca con errores	1	2	**2**	**Muy bajo (MB)**
	[file] servidor de ficheros	AM8	• Destrucción de información del servidores	R12	Error en el almacenamiento de copias de seguridad debido a una mala configuración de las necesidades de mantenimiento que afectan la integridad y disponibilidad de la información.	1	3	**3**	**Bajo (B)**
	[browser] navegador web	AM9	• Uso no previsto de navegador web	R13	Ataque de malware a causa de abrir paginas no autorizadas en el navegador web, comprometiendo la disponibilidad de los sistemas que se ven afectados.	1	5	**5**	**Medio (M)**
				R14	Uso incorrecto del navegador web por parte de los usuarios comprometiendo así la disponibilidad de los servicios.	4	3	**12**	**Alto (A)**
	[dbms] sistema de gestión de BD	AM10	• Acceso no autorizado a la base de datos	R15	Daños a la integridad y disponibilidad de los sistemas de gestión de BD debido a la separación inadecuada de los ambientes de desarrollo y pruebas.	1	2	**2**	**Muy bajo (MB)**
	[email_server] servidor de	AM11	• Difusión de software dañino intencionado	R16	Problemas de disponibilidad del servidor de correo debido a fallos producidos por la	1	2	**2**	**Muy bajo (MB)**

	correo electrónico				incorrecta configuración del mismo en los puntos finales.				
	[av] antivirus	AM12	• Divulgación de información por malware	R17	Indisponibilidad del antivirus debido a fallo de mantenimiento/actualización de versiones más recientes.	1	3	**3**	**Bajo (B)**
	[os] sistema operativo	AM13	• Instalación de software desconocido.	R18	Daños de disponibilidad por falta de control sobre los cambios de sistema operativo cuando finaliza su vida útil.	1	2	**2**	**Muy bajo (MB)**
			• Errores de mantenimiento / actualización de programas (software)	R19	Problemas de disponibilidad del sistema operativo debido a errores de actualización de parches.	3	5	**15**	**Alto (A)**
EQUIPOS INFORMÁTICOS (HW)	[pc] informática personal.	AM14	• Avería de origen físico del hardware	R20	Problemas de disponibilidad de los equipos finales por avería de hardware.	3	2	**6**	**Medio (M)**
			• Pérdida de equipos	R21	Daños a la disponibilidad y confidencialidad del equipo informático causado por hurto de los dispositivos que lo componen.	1	1	**1**	**Muy bajo (MB)**
			• Falta de procesos para registro de responsables	R22	Problemas de autenticidad y tranzabilidad debido a la falta de procesos formales donde se registre a los usuarios responsables de los equipos.	1	4	**4**	**Bajo (B)**
	[firewall] cortafuegos.	AM15	• Manipulación de los equipos	R23	Problemas de disponibilidad de los equipos finales por manipulación de terceros.	1	3	**3**	**Bajo (B)**
	[peripheral] periféricos.	AM16	• Pérdida de equipos	R24	Daños o robos a los equipos informáticos debido a la falta de	1	2	**2**	**Muy bajo (MB)**

					registro de entrada y salida de equipos de la empresa.				
	[switch] conmutadores.	AM17	• Manipulación de los equipos	R25	Daños a disponibilidad de los switches por manipulación por medio de atacantes mediante puertos.	2	2	**4**	**Bajo (B)**
				R26	Daños a la disponibilidad al momento de asignar VLAN'S a los puertos de red.	2	2	**4**	**Bajo (B)**
				R27	Abuso de privilegios para los accesos a equipos que no son de la competencia para cierto usuario provocando daños en su funcionamiento.	1	3	**3**	**Bajo (B)**
	[backup] equipamiento de respaldo.	AM18	• Avería de origen físico del hardware	R28	Problemas de disponibilidad e integridad de la información almacenada de los equipos de backup por avería de hardware.	1	2	**2**	**Muy bajo (MB)**
	[mobile] informática móvil, laptop´s.	AM19	• Robo de laptops y equipos móviles.	R29	Daños a la confidencialidad por falta de controles sobre el uso de dispositivos móviles dentro de la empresa.	4	5	**20**	**Muy alto (MA)**
				R30	Problemas graves de confidencialidad por el robo de dispositivos móviles que trabajan con información dentro de la empresa.	1	5	**5**	**Medio (M)**
	[ipphone] teléfono IP.	AM20	• Uso no previsto de los equipos	R31	Mal uso de los teléfonos por parte de los usuarios para su propio beneficio.	1	1	**1**	**Muy bajo (MB)**
	[LAN] red local	AM21	• Errores del administrador al	R32	Problemas de disponibilidad de la red local debido a la	2	4	**8**	**Medio (M)**

Redes de comunicaciones (COM)			compartir sus credenciales.		sobrecarga de datos que pasa por la misma.				
			• Error en mantener un registro de eventos de ataques a las redes.	R33	Daños a la disponibilidad de la red debido a la deficiencia del diseño de la red LAN por mantenerse obsoleta.	1	2	**2**	**Muy bajo (MB)**
			• Caída del sistema por agotamiento de recursos	R34	Problemas graves de confidencialidad por compartir credenciales de administrador con personas externas a la empresa.	2	5	**10**	**Alto (A)**
			• Suplantación de la identidad del usuario	R35	Daños de tranzabilidad por falta de registros documentados de ataques hacia la red interna que dificultan los procesos de investigación tras un incidente.	2	2	**4**	**Bajo (B)**
			• Abuso de privilegios de acceso a la red	R36	Pérdida parcial/total de la información por causa de atacantes que realizan análisis de tráfico en la red LAN.	2	2	**4**	**Bajo (B)**
			• Errores de administración de cuentas con privilegios.	R37	Problemas de disponibilidad del servicio de internet.	3	4	**12**	**Alto (A)**
	[wifi] red inalámbrica	AM22	• Análisis de tráfico	R38	Pérdida parcial/total de la información por causa de atacantes que realizan análisis de tráfico en la red wifi.	1	2	**2**	**Muy bajo (MB)**
			• Interceptación de información (escucha)	R39	Daños de tranzabilidad por falta de registros documentados de ataques hacia la red wifi que dificultan los procesos de investigación tras un incidente.	2	2	**4**	**Bajo (B)**

Soportes de información (Media)	[disk] discos.	AM23	• Acceso no autorizado	R40	Robo o pérdida de los discos de información por la falta de controles para el registro de entrada y salida de personal externo en los cuartos donde se almacenan.	1	3	**3**	**Bajo (B)**
			• Eliminación accidental de la información	R41	Pérdida parcial/total de la información almacenada en los discos por la falta de procesos para la eliminación segura de hardware con información.	2	5	**10**	**Alto (A)**
Instalaciones (L)	[building] edificio	AM24	• Fuego	R42	Perjudicar la estructura del edificio debido a un Incendio.	1	2	**2**	**Muy bajo (MB)**
			• Daños por agua	R43	Deterioro de la infraestructura de la empresa debido a daños por agua.	1	3	**3**	**Bajo (B)**
	[local] cuarto	AM25	• Fuego	R44	Perjudicar la estructura de los cuartos provocado por un incendio.	1	2	**2**	**Muy bajo (MB)**
			• Daños por agua	R45	Daños por agua a la infraestructura de los cuartos de red.	1	2	**2**	**Muy bajo (MB)**
PERSONAL (P)	[adm] administrador de sistemas	AM26	• Compromiso por la seguridad informática.	R46	Falta de preocupación por impulsar la seguridad de la información en cada área de trabajo.	1	3	**3**	**Bajo (B)**
				R47	Falta de elaboración de procesos documentados para respuesta oportuna contra incidentes.	1	3	**3**	**Bajo (B)**
		AM27	• Compromiso por la seguridad informática.	R48	Problemas de disponibilidad de la información por la falta de	3	4	**12**	**Alto (A)**

	[sec] administrador de seguridad				aplicación de políticas de seguridad.				
			• Ingeniería social (picaresca)	R49	Daños graves de confidencialidad por divulgación de la información por empleados o ex empleados.	1	5	**5**	**Medio (M)**
	[ui] usuarios internos.	AM28	• Extorsión	R50	Problemas de confidencialidad de la información por empleados que son obligados mediante extorción a revelar información.	2	4	**8**	**Medio (M)**
			• Compromiso por la seguridad informática.	R51	Problemas de integridad y confidencialidad por la falta de capacitación del usuario sobre el manejo de información sensible.	1	5	**5**	**Medio (M)**