

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



**APLICACIÓN DE LA METODOLOGÍA OCTAVE PARA LA
GESTIÓN DE REDES DE COMUNICACIONES DE LA EMPRESA
CONSTRUCTORA PREIMAQ S.A.C**

Tesis para optar el título profesional de
INGENIERO DE SISTEMAS

GREYSI ROXANA GONZALES GARCÍA

PUCALLPA - PERÚ

2025



UNIVERSIDAD NACIONAL DE UCAYALI
FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS
COMISIÓN DE GRADOS Y TÍTULOS



ACTA DE EVALUACIÓN DE SUSTENTACIÓN DE TESIS N° 27-2025

GRADUANDO : GONZALES GARCIA, Greysi Roxana

TEMA : "APLICACIÓN DE LA METODOLOGÍA OCTAVE PARA LA GESTIÓN DE REDES DE COMUNICACIÓN DE LA EMPRESA CONSTRUCTORA PREIMAQ S.A.C"

ASESOR : Mg. CESAR AUGUSTO AGURTO CHERRE

CRITERIOS	PUNTAJE			
	3	2	1	0
I- PRESENTACION				
* MOTIVACION		X		
* TONO DE VOZ		X		
* CALIDAD DE MATERIAL AUDIOVISUAL	X			
II- DESARROLLO DE CONTENIDO				
* SECUENCIA	X			
* DOMINIO DE VOZ		X		
* USO ADECUADO DEL MATERIAL		X		
* VALIDEZ DE LOS HALLAZGOS	X			
III- ABSOLUCION DE PREGUNTAS				
* RESPONDE A LAS PREGUNTAS FORMULADAS POR EL JURADO	X			
IV- APOORTE CIENTIFICO Y TECNOLÓGICO				
* AL DESARROLLO DE LA COMUNIDAD		X		
* A LA PROFESION		X		

EVALUACION

- EXCELENCIA 26 A 30 PUNTOS
- UNANIMIDAD 21 A 25 PUNTOS
- MAYORIA 16 A 20 PUNTOS
- DESAPROBADO 15 A MENOS

CALIFICACION FINAL:

PUNTAJE : 24 / 30

CONCLUSIONES:

APROBADO POR : UNANIMIDAD
 DESAPROBADO POR :

JURADO EVALUADOR


 Dr. Nilton Cesar AYRA APAC
 PRESIDENTE


 Mg. Arturo U/PANQUE VILLANUEVA
 MIEMBRO


 M.Sc. Richard Piero BARDALES LINARES
 MIEMBRO


 M.Sc. CLOTILDE RÍOS HIDALGO DE CERNA
 SECRETARIA ACADÉMICA

PUCALLPA, 04 DE SETIEMBRE DEL 2025



UNIVERSIDAD NACIONAL DE UCAVALI
FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS



COMISION DE GRADOS Y TITULOS

TESIS TITULADA:

"APLICACIÓN DE LA METODOLOGÍA OCTAVE PARA LA GESTIÓN DE REDES DE COMUNICACIÓN DE LA EMPRESA CONSTRUCTORA PREIMAQ S.A.C"

ELABORADO POR:

Bach. GONZALES GARCIA, Greysi Roxana

APROBADO POR:

Dr. Nilton Cesar AYRA APAC

Presidente

Mg. Arturo YUPANQUI VILLANUEVA

Miembro

Mg. Richard Piero BARDALES LINARES

Miembro

Mg. Cesar Augusto AGURTO CHERRE

Asesor



UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº VI/222-2025

La Dirección de Producción Intelectual de la Universidad Nacional de Ucayali, hace constar por la presente, que el trabajo académico de investigación, titulado:

'APLICACIÓN DE LA METODOLOGÍA OCTAVE PARA LA GESTIÓN DE REDES DE COMUNICACIONES DE LA EMPRESA CONSTRUCTORA PREIMAQ S.A.C'

Autor(es) : GONZALES GARCIA, GREYSI ROXANA
Facultad : INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
Escuela : ING. DE SISTEMAS
Asesor(a) : Mg. AGURTO CHERRE, CESAR AUGUSTO

Presenta un porcentaje de similitud de 6%, verificado en el Sistema Antiplagio COMPILATIO, De acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO, el cual indica que todo trabajo de investigación no debe superar el 10%. En tal sentido, se declara, que el presente trabajo de investigación: **SI** Contiene un porcentaje aceptable de similitud, procediéndose a emitir la presente Constancia de Originalidad de Trabajo de Investigación (COTI) a solicitud del asesor.

En señal de conformidad se firma y sella el presente documento.

Fecha: 06/05/2025



Mg. JOSÉ MANUEL CÁRDENAS BERNAOLA
Director de Producción Intelectual



UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo Gregori R. Gonzales Gorda
 Autor de la tesis titulada: Aplicación de la Metodología Activa
para la gestión de Redes de Comunicación de la
Empresa Constructora Pucallpa S.A.S.
 Sustentada el año 2025
 Asesor(a): Mg. Cesar Augusto Aguirre Chorro
 Facultad: de Ingeniería de Sistemas y de Ingeniería Civil
 Escuela Profesional: de Ingeniería de Sistemas

Autorizo la publicación:

PARCIAL

☐

TOTAL

☒

De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

Primero: Otorgo a la Universidad Nacional de Ucayali licencia no exclusiva para reproducir, distribuir, comunicar, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público en general mi tesis (incluido el resumen) a través del Repositorio Institucional de la UNU, en formato digital sin modificar su contenido, en el Perú y en el extranjero; por el tiempo y las veces que considere necesario y libre de remuneraciones.

Segundo: Declaro que la tesis es una creación de mi autoría y exclusiva titularidad, por tanto me encuentro facultado a conceder la presente autorización, garantizando que la tesis no infringe derechos de autor de terceras personas, caso contrario, me hago único(a) responsable de investigaciones y observaciones futuras, de acuerdo a lo establecido en el estatuto de la Universidad Nacional de Ucayali, la Superintendencia Nacional de Educación Superior Universitaria y el Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 04 / 09 / 2025

Email: gonzalezgordagregori@gmail.com Firma: [Firma]
 Teléfono: 964387071 DNI: 47501600

www.repositorio.unu.edu.pe
repositorio@unu.edu.pe

DEDICATORIA

A mis padres, por sus esfuerzos realizados en mi educación y
apoyo incondicional

AGRADECIMIENTO

Agradezco a Dios, por darme la oportunidad de seguir luchando por mis sueños, a mi asesor por guiarme, a la universidad por la oportunidad de seguir aprendiendo, a la empresa que me brindó la información para poder realizar el trabajo

ÍNDICE GENERAL

AGRADECIMIENTO	vii
ÍNDICE DE CONTENIDO	viii
LISTA DE FIGURAS	xii
LISTA DE TABLAS	xi
LISTA DE ANEXOS	xii
RESUMEN	xiv
ABSTRACT	xv
INTRODUCCIÓN	xvi
CAPÍTULO I	17
PLANTEAMIENTO DEL PROBLEMA	17
1.1. ANTECEDENTES DEL PROBLEMA.....	17
1.2. FORMULACIÓN DEL PROBLEMA.....	18
1.2.1. Problema General.	18
1.2.2. Problemas Específicos.....	18
1.3. OBJETIVOS.	18
1.3.1. Objetivo General.	18
1.3.2. Objetivos Específicos.	19
1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES.....	19
1.4.1. JUSTIFICACIÓN.	19
1.4.2. Importancia.....	21
1.4.3. Limitaciones.....	22
1.5. HIPÓTESIS, VARIABLES Y OPERACIONALIZACIÓN DE LAS VARIABLES	22
1.5.1. Hipótesis General.....	22
1.5.2. Hipótesis secundarias	22
1.6. DELIMITACIONES DE LA INVESTIGACIÓN	23
1.6.1. Delimitación Espacial.	23
1.6.2. Delimitación Social.....	23
1.6.3. Delimitación Temporal.....	24
1.6.4. Delimitación Conceptual.....	24
1.7. VARIABLES	25

1.7.1.	Variable independiente:.....	25
1.7.2.	Variable dependiente:	25
1.7.3.	Variable interviniente:.....	25
1.8.	SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES.	26
1.8.1.	Operacionalización de variables.	26
CAPÍTULO II		27
MARCO TEÓRICO		27
2.1.	ANTECEDENTES DE LA INVESTIGACIÓN	27
2.1.1.	Internacionales	27
2.1.2.	Nacionales	29
2.2.	BASES TEÓRICAS	31
2.2.1.	La teoría de Evaluación Operativa Crítica de Amenazas, Activos y Vulnerabilidades	31
2.2.1.1.	Metodología octave	31
2.2.1.2.	Análisis y planificación	32
2.2.1.3.	Concientización	33
2.2.2.	Aseguramiento o Seguridad	34
2.2.3.	Teoría de Gestión de Redes	35
2.2.3.1.	Gestión de redes de comunicaciones	36
2.2.3.2.	Procesos.....	37
2.2.3.3.	Monitoreo.....	37
2.2.3.4.	Seguridad	38
2.3.	DEFINICIÓN DE TÉRMINOS BÁSICOS	39
CAPÍTULO III		41
METODOLOGÍA DE LA INVESTIGACIÓN		41
3.1.	METODOLOGÍA Y TÉCNICAS UTILIZADAS.....	41
3.1.1.	Tipo de investigación.....	41
3.1.2.	Nivel de investigación.....	41
3.1.3.	Método de investigación.....	41
3.1.4.	Diseño de la investigación.....	42
3.2.	POBLACIÓN Y MUESTRA	42
3.3.	INSTRUMENTOS DE RECOLECCIÓN DE DATOS	43
3.4.	PROCEDIMIENTO DE RECOLECCIÓN DE DATOS.....	43
3.5.	TRATAMIENTO DE DATOS.....	43

3.6. GRADO DE CONFIABILIDAD DE LOS DATOS.....	43
CAPÍTULO IV	44
4.1. METODOLOGÍA OCTAVE PARA LA GESTIÓN DE REDES DE COMUNICACIONES.....	44
4.1.1. Metodología de Análisis de Riesgos de Sistemas de información. 44	
1.1.1. Metodología Octave.	64
CAPÍTULO V	71
RESULTADOS Y DISCUSIÓN	71
5.1. Procesamiento de datos del objetivo general.....	71
5.1.1. Procesamiento de datos del primer objetivo específico.....	72
5.2. Prueba de hipótesis	76
5.2.1. Prueba de la hipótesis general.....	76
5.2.2. Prueba de la primera hipótesis específica.....	79
5.2.3. Prueba de la segunda hipótesis específica.....	80
5.2.4. Prueba de la tercera hipótesis específica.....	81
5.3. Discusión de resultados.....	82
CONCLUSIONES	89
RECOMENDACIONES.....	92
BIBLIOGRAFÍAS	93
ANEXOS	98

INDICE DE TABLAS

Tabla 1: Operacionalización de variable	26
Tabla 2: Operacionalización de variable II.....	26
Tabla 3: activos de gestión de redes de comunicaciones	44
Tabla 4: Rangos de Valorización de activos.....	46
Tabla 5: Valorización de activos	46
Tabla 6: Identificación de amenazas.	47
Tabla 7: Valoración de amenazas.	50
Tabla 8: Valoración de impacto.	52
Tabla 9: probabilidad de amenazas.....	54
Tabla 10: Valoración de amenazas porcentual.	56
Tabla 11: Estimación de riesgo.....	57
Tabla 12: Tratamiento de riesgo.	60
Tabla 13: Criterios de evaluación de impacto.....	64
Tabla 14: Identificación de activos.....	64
Tabla 15: Evaluación de prácticas de seguridad.....	65
Tabla 16: Estrategias de seguridad.	66
Tabla 17: Gestión de seguridad.....	66
Tabla 18: Políticas y regulaciones.	67
Tabla 19: Plan de seguridad y recuperación.	67
Tabla 20: Control de acceso físico.....	67
Tabla 21: Activos críticos.	68
Tabla 22: Descripción de activos críticos.....	68
Tabla 23: Distribución de frecuencia del objetivo aplicando la metodología octave para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	71
Tabla 24: Distribución de frecuencia del objetivo específico efectuando la adecuación de las características de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	72
Tabla 25: Distribución de frecuencia del objetivo específico monitorear de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	73
Tabla 26: Distribución de frecuencia del objetivo específico asegurando los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	74
Tabla 27: Prueba de normalidad de las hipótesis.....	78
Tabla 28: Toma de decisión de la prueba de normalidad	78
Tabla 29: Prueba de hipótesis general	79
Tabla 30: Prueba de la primera hipótesis específica.....	80
Tabla 31: Prueba de la primera hipótesis específica.....	81
Tabla 32: Prueba de la primera hipótesis específica.....	82

INDICE DE FIGURAS

Figura 1: Barras porcentuales del objetivo general aplicando la metodología octave para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	71
Figura 2: Barras porcentuales del objetivo específico efectuando la adecuación de las características de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	72
Figura 3: Barras porcentuales del objetivo específico monitores de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	73
Figura 4: Barras porcentuales del objetivo específico asegurando los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	75

INDICE DE ANEXOS

Anexos N° 1: Matriz de consistencia.	99
Anexos N° 2: Cuestionario de preguntas para la recolección de datos	100
Anexos N° 3: Validación de los instrumentos por expertos.....	103
Anexos N° 4: Base de datos del Pre Test	105
Anexos N° 5: Base de datos del Post Test.....	106
Anexos N° 6: Análisis estadístico del alfa de Cronbrach.	107

RESUMEN

En la presente investigación se presenta, despliega un modelo de gestión de riesgos, donde se aplica las etapas correspondientes la metodología Octave para mejorar la gestión de redes de la empresa constructora Preimaq S.A.C, se realiza la identificación de activos y la clasificación de los más relevantes. En el primer capítulo se planteando la definición del problema en cuanto la gestión de riesgos, se definen los objetivos generales y específicos, la justificación, importancia. En el segundo capítulo se detallan los antecedentes de la investigación, el marco teórico y definición de términos básicos. En el tercer capítulo se presenta información la de metodología de la investigación. En el cuarto capítulo se presenta el análisis tomando como referencia la metodología Octave, así como el desarrollo de todas sus etapas. En el quinto capítulo se detalla los resultados y discusión.

Palabras clave: Gestión, riesgo, metodología, octave.

ABSTRACT

In this research, a risk management model is presented and deployed, where the corresponding stages of the Octave methodology are applied to improve the network management of the Preimaq S.A.C company, the identification of assets and the classification of the most relevant ones are carried out. In the first chapter, the definition of the problem in terms of risk management is proposed, the general and specific objectives, justification, and importance are defined. The second chapter details the background of the research, the theoretical framework and definition of basic terms. The third chapter presents information on the research methodology. The fourth chapter presents the analysis taking the Octave methodology as a reference, as well as the development of all its stages. The fifth chapter details the results and discussion.

Keywords: Management, irrigation, methodology, octave.

INTRODUCCIÓN

El proceso de gestión de riesgos abarca desde el desarrollo hasta la implementación de una metodología creada para tal fin, permiten la identificación, obtener la cuantificación, efectuar tareas de mitigación y realizar actividades de monitoreo de riesgos, para así minimizar las amenazas y vulnerabilidades concernientes con la seguridad de la información, en las que se trata los distintos activos de la empresa como son: programas informáticos, hardware entre otros.

La información representa un intangible muy valioso, el cual debe ser gestionada por personal adecuado, garantizando que personal ajeno no cuente con accesos a la misma, esta información debe permanecer disponible, se debe poder acceder de forma oportuna, se debe contar con el respaldo de seguridad.

Un plan de continuidad representa una necesidad importante para las organizaciones y eso debido al avance tecnológico, el cual exige contar con alternativas para garantizar la continuidad de las actividades de la empresa.

El análisis de los riesgos es tratado, en esta investigación, haciendo uso de la metodología Octave, el cual consta de ocho etapas las cuales se encuentran organizadas en cuatro fases: Desarrollo de criterios de medición de riesgo, crear un perfil de cada activo donde se establezcan los límites claros, se debe identificar los requisitos de seguridad.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. ANTECEDENTES DEL PROBLEMA

En la actualidad las empresas de todos los tamaños y sectores subsisten debido a la cantidad de información que ellos gestionan y/o procesan, información externa, interna, producto de su interacción con el mercado, producto de las actividades internas efectuadas como parte de su razón de ser.

Las empresa hacen uso de diferentes tipos de sistemas informáticos, para agilizar o sistematizar sus actividades, para lograr mayor celeridad y control, generando satisfacción en sus clientes y empleados, debido a la facilidad que estos otorgan, dentro de estos sistemas están las herramientas de software, equipos servidores, terminales como laptops, computadoras personales, equipos de impresión; pero estos requieren estar conectados y para ello hacen uso de la tecnología de redes de computadoras, que les permite la interconexión y el intercambio de información entre áreas internas, así como el acceso a información externa a través del internet.

La empresa constructora Preimaq S.A.C, a pesar de contar con tecnológicas como parte de su infraestructura, y según lo argumentado por el personal de TI, carece de un mecanismo de evaluación de riesgos, carencia de controles que permitan minimizar el impacto sobre las vulnerabilidades relacionadas a la tecnología de redes y comunicaciones, esto representan una realidad problemática y de vulnerabilidad; en tal sentido, se ha visto por conveniente realizar una investigación con la finalidad de aplicar una

metodología de gestión de riesgos como lo es la metodología octave y con ello dar solución a la realidad problemática de seguridad.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema General.

¿En qué medida la aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C?

1.2.2. Problemas Específicos.

- ¿Cómo la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.?
- ¿De qué manera la aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.?
- ¿En qué medida la aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.?

1.3. OBJETIVOS.

1.3.1. Objetivo General.

Demostrar que la aplicación de la metodología octave para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

1.3.2. Objetivos Específicos.

- Efectuar la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.
- Determinar que la aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.
- Establecer que a aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES.

1.4.1. JUSTIFICACIÓN.

Justificación teórica.

La aplicación de la metodología OCTAVE para la gestión de redes de comunicaciones, se justifica teóricamente por su enfoque sistemático y holístico en la identificación, análisis y mitigación de riesgos, su alineación con los principios de la gestión de riesgos, la teoría de sistemas complejos y la seguridad de la información, su contribución a la planificación estratégica y su potencial para fortalecer la confianza de los stakeholders. Al adoptar OCTAVE, se podrá fortalecer la seguridad y la resiliencia de su infraestructura de comunicaciones, protegiendo así sus activos críticos y garantizando la continuidad de sus operaciones en un entorno digital cada vez más desafiante.

Justificación práctica.

La justificación práctica para la aplicación de la metodología OCTAVE en la gestión de redes de comunicaciones, radica en su capacidad para proporcionar un enfoque estructurado y colaborativo para la identificación, análisis y mitigación de riesgos específicos para el contexto operativo de la empresa. Su implementación permite priorizar la protección de los activos críticos, desarrollar planes de mitigación más precisos, fortalecer la toma de decisiones en materia de seguridad y, en última instancia, mejorar la resiliencia de la infraestructura, contribuyendo a la continuidad de sus operaciones y a la protección de su valor empresarial.

Justificación metodológica.

La justificación metodológica para la aplicación de OCTAVE en la gestión de riesgos de redes de comunicaciones reside en su enfoque centrado en los activos críticos, su utilización del conocimiento interno, su estructura en fases, su integración con el negocio, su naturaleza iterativa y su énfasis en la documentación. Estos elementos metodológicos proporcionan un marco robusto y adaptable para comprender, evaluar y mitigar los riesgos de seguridad en las redes de comunicaciones de una manera que esté alineada con los objetivos y el contexto específico de la organización.

Justificación operativa.

La justificación operativa para la aplicación de la metodología OCTAVE en la gestión de redes de comunicaciones radica en su enfoque práctico y centrado en el negocio, su dependencia del conocimiento interno, su estructura modular, su orientación a la

creación de planes de acción viables, su fomento de la colaboración interdepartamental y su énfasis en la mejora continua. Al adoptar OCTAVE, una organización puede integrar la gestión de riesgos de seguridad en sus operaciones diarias de manera efectiva, protegiendo sus activos críticos y garantizando la continuidad de sus servicios de comunicación de una forma que sea práctica y sostenible.

1.4.2. Importancia.

En la actualidad, la información es el activo fundamental para las empresas de todos los sectores. La gestión eficiente de esta información, tanto interna como externa, es crucial para el éxito empresarial. Los sistemas informáticos, las redes de computadoras y las herramientas tecnológicas son esenciales para optimizar procesos, mejorar el control y la satisfacción de clientes y empleados.

Sin embargo, esta interconectividad también aumenta el riesgo de ciberataques. La empresa constructora Preimaq S.A.C., al igual que muchas otras, carece de un mecanismo formal para evaluar y gestionar estos riesgos. Esta situación la hace vulnerable a serias amenazas que podrían impactar negativamente en su operación.

La implementación de la metodología Octave para la gestión de riesgos en redes y comunicaciones es fundamental para Preimaq S.A.C., ya que permitirá:

Reducir la probabilidad de ataques cibernéticos, Minimizar el impacto de los incidentes, Mejorar la confianza de clientes y socios, Fortalecer la competitividad de la empresa.

En definitiva, la gestión de riesgos en la tecnología de redes y comunicaciones es una inversión indispensable para cualquier empresa que desee operar de manera segura y eficiente en la era digital.

1.4.3. Limitaciones

La investigación se limitó porque el acceso a la información interna de la información de la empresa en muchas ocasiones fue restringida, en tal medida fue necesario idear métodos distintos para obtener los datos relevantes. Esta circunstancia demandó una dedicación significativamente mayor de tiempo y energía en la localización y el examen de fuentes de información externas, lo que consecuentemente extendió la duración del desarrollo de la investigación.

1.5. HIPÓTESIS, VARIABLES Y OPERACIONALIZACIÓN DE LAS VARIABLES

1.5.1. Hipótesis General

La aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

1.5.2. Hipótesis secundarias

- La aplicación de la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.
- La aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

- La aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

1.6. DELIMITACIONES DE LA INVESTIGACIÓN

1.6.1. Delimitación Espacial.

La investigación se enfocará en la empresa constructora Preimaq S.A.C., ubicada en su sede principal y considerando toda su infraestructura tecnológica, incluyendo redes locales, equipos, software y conexiones a internet.

No se considerarán sucursales, filiales o proyectos específicos de la empresa que se encuentren en otras ubicaciones geográficas.

Esta delimitación espacial permitirá un análisis enfocado y preciso de la situación de riesgo en la red y los sistemas de comunicación de Preimaq S.A.C.

1.6.2. Delimitación Social.

La investigación se enfocará en el personal de la empresa constructora Preimaq S.A.C. que utiliza la red y los sistemas de comunicación, incluyendo:

- Empleados de todas las áreas y departamentos.
- Contratistas y personal externo que acceden a la red.
- Usuarios finales de los sistemas informáticos.

No se considerarán grupos de interés externos a la empresa, como clientes, proveedores o socios comerciales.

1.6.3. Delimitación Temporal

La investigación se enfocará en el período comprendido entre [FECHA DE INICIO] y [FECHA DE FIN], abarcando los siguientes aspectos:

- Análisis de la infraestructura tecnológica existente en Preimaq S.A.C. durante dicho período.
- Evaluación de los riesgos en redes y comunicaciones presentes en la empresa en el marco temporal definido.
- Implementación de la metodología Octave para la gestión de riesgos dentro del período establecido.
- Monitoreo y seguimiento de los resultados de la implementación durante el período de estudio.

No se considerarán eventos o cambios que hayan ocurrido antes o después del período delimitado.

Esta delimitación temporal permitirá un análisis preciso y controlado de la situación de riesgo en la red y los sistemas de comunicación de Preimaq S.A.C., enfocándose en el momento actual y las condiciones específicas del período de estudio.

1.6.4. Delimitación Conceptual

La investigación se enfocará en los siguientes conceptos clave:

- Gestión de riesgos en redes y comunicaciones: Proceso de identificar, evaluar y mitigar los riesgos asociados a la infraestructura tecnológica de una organización.
- Metodología Octave: Un marco de trabajo estandarizado para la gestión de riesgos en redes y comunicaciones, desarrollado por SANS Institute.

- Vulnerabilidades: Debilidades en los sistemas informáticos que pueden ser explotadas por actores maliciosos.
- Amenazas: Eventos o acciones que podrían aprovechar las vulnerabilidades para causar daño.
- Impacto: Consecuencias negativas que podrían derivarse de la materialización de una amenaza.
- Controles de seguridad: Medidas técnicas y organizativas para prevenir, detectar y responder a incidentes de seguridad.
- Empresa constructora Preimaq S.A.C.: Organización objeto de estudio, que requiere implementar una estrategia efectiva de gestión de riesgos para proteger su red y sistemas de comunicación.

1.7. VARIABLES

1.7.1. Variable independiente:

Metodología octave

1.7.2. Variable dependiente:

Gestión de redes de comunicaciones

1.7.3. Variable interviniente:

Empresa constructora Preimaq S.A.C

1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES.

1.8.1. Operacionalización de variables.

Variable: Metodología octave

Tabla 1: Operacionalización de variable

Dimensión	Indicador	Escala
Análisis y planificación.	• Políticas • Gestión de recursos • Seguridad física. • Seguridad de las comunicaciones.	• Malo • Regular • Normal • Bueno • Muy bueno
Concientización	• Reuniones. • Requisitos	
Aseguramiento.	• Perfilamiento de activos • Análisis riesgo • Mitigación	

Fuente: Elaboración propia.

Variable: Gestión de redes de comunicaciones

Tabla 2: Operacionalización de variable II

Dimensión	Indicador	Escala
Procesos	• Herramientas. • Controles	• Malo • Regular • Normal • Bueno • Muy bueno
Monitoreo	• Registros. • Programación.	
Seguridad	• % conformidad	

Fuente: Elaboración propia.

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedentes Internacionales

Estudio para optar el título de Maestría en Seguridad Informática presentado por Muñoz Gutiérrez (2022) realizado en Ecuador, en el que se tuvo como objetivo Establecer una propuesta de un esquema de gestión de riesgos mediante la metodología OCTAVE utilizando el ciclo de mejora continua PHVA para disponer de un marco de referencia que permita gestionar de forma correcta eventos e incidentes de seguridad en un modelo de Infraestructura como servicio "IAAS". En cuanto a la metodología fue cualitativa con un enfoque bibliográfico. Se concluye que la integración de la metodología Octave con el ciclo PHVA establece un marco robusto para gestionar riesgos de seguridad en infraestructuras de nube IAAS, facilitando la identificación de activos críticos y alineando conocimientos organizacionales para implementar estrategias proactivas que aseguran la integridad, disponibilidad y confidencialidad de los servicios.

Estudio de la gestión del riesgo con base en ISO27005 adaptando OCTAVE-S, presentado por Amador Donado, realizado en Universidad Internacional de La Rioja. Colombia en el año 2022, que tiene como título "Gestión del riesgo con base en ISO27005 adaptando OCTAVE-S", con el objetivo de gestionar el riesgo en la seguridad de la información con base en la norma ISO/IEC 27005. El tipo de investigación es exploratoria, de nivel analítico y diseño cuasi-experimental. La población y muestra del estudio incluyen entidades bancarias y financieras, en el cual se utiliza

como instrumento de análisis de datos y simulaciones. Se concluye que la adaptación de OCTAVE-S mejora significativamente la capacidad de las organizaciones para identificar y gestionar riesgos de seguridad de la información (Amador Donado, 2022).

Estudio de la aplicación de la metodología OCTAVE en la gestión de redes de comunicaciones, presentado por V. M. Miranda Jiménez, realizado en Universidad Politécnica Salesiana en el año 2023, que tiene como título "Evaluación de la seguridad de la información con la metodología OCTAVE", con el objetivo de evaluar la seguridad de la información y desarrollar estrategias de protección. El tipo de investigación es correlacional, de nivel explicativo y diseño transversal. La población y muestra del estudio incluyen empresas del sector industrial, en el cual se utiliza como instrumento de encuestas y análisis de riesgos. Se concluye que la metodología OCTAVE proporciona un marco robusto para la evaluación y mejora de la seguridad de la información en redes de comunicaciones (Miranda Jimenez, 2021).

Asimismo, Pacheco, (2022). Seguridad en redes de comunicaciones: Perspectivas y desafíos. Estudio realizado en Chile con el objetivo de analizar las técnicas actuales de protección en redes de comunicación y su impacto en la confidencialidad, integridad y disponibilidad de los datos. Investigación de tipo descriptiva, nivel exploratorio, diseño documental. La población consistió en artículos académicos recientes y la muestra en publicaciones indexadas en revistas científicas. Se utilizaron revisiones sistemáticas de literatura como instrumento de análisis, concluyendo que la

implementación de metodologías como OCTAVE fortalece significativamente la seguridad en redes de comunicación.

2.1.2. Antecedentes Nacionales

Estudio para optar el título de Ingeniero de Sistemas presentado por Gastelo Fernandez (2023), que tuvo como objetivo Desarrollar un modelo de gestión de riesgos basado en la metodología Magerit para minimizar los riesgos de adquisición y uso de TI de una municipalidad de Perú. Caso de estudio: Municipalidad distrital de Cupisnique – Cajamarca. En el campo metodológico la investigación fue de tipo cualitativa, aplicada y técnica. Se concluyó la aplicación de las fases básicas de gestión de riesgos, tales como el Análisis de riesgos, Tratamientos de riesgos y Comunicación de riesgos, basadas en la metodología MAGERIT, junto con el análisis del proceso de adquisición y uso de TI en la Municipalidad de Cupisnique y sus prioridades, permitió un juicio experto adecuado. Esto facilitó la participación de los involucrados en los procesos de gestión, agilizando así el método de selección.

También el estudio presentado por Martos Paredes (2024) Implementar un modelo de procesos de seguridad de la información para una pyme peruana basado en la norma ISO/IEC 27005 y la metodología OCTAVE- S. En el campo metodológico en presente estudio abarcó tipo de investigación cuantitativa y tecnología aplicada, con diseño cuasiexperimental. En consecuencia, la metodología OCTAVE-S se enfocó exclusivamente en las áreas consideradas más críticas. Esto permitió concentrar toda la productividad en las amenazas reales para una Pequeña y Mediana

Empresa (PYME), facilitando así la planificación de un control de estabilidad para la organización.

En el estudio presentado por (Vasquez Atoche & Terrones Moncada, 2023), realizado en Ancash, que tiene como título; mejora de los estándares de seguridad ocupacional para reducir los accidentes mineros en una empresa minera de la región de Ancash, en el 2021, con un enfoque cuantitativo, un tipo de investigación es aplicada, con una población y una muestra de 30 trabajadores, en el cual se utiliza como instrumento de cuestionario de la encuesta, concluyendo que la presente investigación al diseñar un plan de capacitación en base a la mejora de los estándares de seguridad ocupacional, para reducir los accidentes mineros en la empresa minera de la región Ancash, se pudo determinar que el nivel de accidentabilidad en la empresa contratista es leve con un 90% de casos registrados, donde el primer y segundo trimestre del año 2019 junto al primer trimestre del año 2020 se ha registrado mayor frecuencia de accidentes; por otra parte, el nivel de conocimiento de los estándares de seguridad por parte del personal de la empresa es bajo , teniendo un 92.33 %, y un nivel medio de conocimiento con respecto a la Ley N° 29783, generando desaprobación del cumplimiento de las normas mínimas de prevención de riesgos especificados en dicha Ley, debido a la falta de capacitaciones donde se realiza solo una vez al mes, provocando que el 56.7% del personal no conozca las normas.

2.2. BASES TEÓRICAS

2.2.1. La teoría de Evaluación Operativa Crítica de Amenazas, Activos y Vulnerabilidades

2.2.1.1. Metodología octave

Según Allen-Addy (2023), Octave es una metodología de evaluación de vulnerabilidades, activos y amenazas críticas operativas. La tecnología se centra en evaluar los riesgos organizacionales en lugar de los riesgos técnicos, como si una empresa experimenta una violación de datos que podría afectar las operaciones comerciales.

En la implementación del protocolo OCTAVE, se conforman equipos multidisciplinarios integrados por representantes del ámbito empresarial, personal de tecnologías de la información y miembros del sector operacional, quienes desarrollan una labor colaborativa. Dicha colaboración se orienta primordialmente hacia la identificación y satisfacción de los requisitos impuestos por los parámetros de seguridad. Este enfoque requiere el establecimiento de un equilibrio tripartito entre la evaluación de contingencias operativas, los recursos tecnológicos disponibles y los protocolos de seguridad implementados. Esginnova Group, (2021).

Por ende, la metodología OCTAVE destaca por su enfoque integrador que prioriza el impacto organizacional sobre aspectos puramente técnicos, permitiendo identificar vulnerabilidades críticas con mayor precisión mediante la colaboración

multidisciplinaria y el equilibrio entre factores operativos, tecnológicos y de seguridad.

2.2.1.2. Análisis y planificación

La planificación y análisis financiero (FP&A) constituye un conjunto de procesos que ayudan a las organizaciones a planificar, pronosticar y presuponer con exactitud para apoyar decisiones empresariales clave y asegurar la salud financiera futura. Aunque trasciende la contabilidad tradicional, esta sigue siendo fundamental en su desarrollo, por lo que los directores financieros adquirieron software especializado para ejecutar estas funciones críticas (Oracle , 2025).

Así mismo, el análisis de datos evalúa bajo restricciones la importancia relativa de la información mediante la priorización de elementos específicos, mientras que la planificación, derivada de este análisis, establece planes de ejecución que aseguran la disponibilidad de datos y recursos; por consiguiente, estos procesos interdependientes conforman un ciclo integrado donde el análisis fundamenta la planificación y esta implementa las conclusiones analíticas para optimizar la gestión informativa alineada con los objetivos del proyecto. InfoSphere Information Server, (2021).

Por lo tanto, integrar la planificación y análisis constituye un marco metodológico que optimiza la toma de decisiones organizacionales al transformar datos en activos estratégicos mediante identificación sistemática de patrones. Este enfoque

unificado evoluciona hacia arquitecturas predictivas que potencian la anticipación de escenarios, estableciendo un ecosistema informacional que se convierte en fundamento del pensamiento estratégico corporativo.

2.2.1.3. Concientización

La concientización representa un proceso donde los individuos, como sujetos activos del saber y no receptores pasivos, desarrolla gradualmente una comprensión crítica tanto del contexto sociocultural que moldea sus vidas como de su potencial transformador. Esta perspectiva coloca la conciencia como núcleo central, reconociendo al ser humano como entidad pensante capaz de analizar su entorno y actuar sobre él para modificar su realidad según sus necesidades evolutivas. Prada Rodríguez, (2013, pág. 14).

Así mismo, la concientización en materia de ciberseguridad puede conceptualizarse como un conjunto estructurado de metodologías, enfoques estratégicos y lineamientos normativos implementados por las entidades corporativas para salvar la integridad informacional, fundamentados en mecanismos interactivos diseñados para generar efectos beneficiosos en el ecosistema organizacional García Martínez, (2024).

Por ende, la concientización en ciberseguridad emerge como un proceso transformativo donde convergen la comprensión crítica del entorno digital y la implementación metodológica de salvaguardas informacionales. Este paradigma dual posiciona al

individuo como agente activo dentro del ecosistema organizacional, trascendiendo el enfoque meramente normativo para cultivar una cultura de responsabilidad digital colectiva que no solo protege la infraestructura tecnológica, sino que potencia la evolución adaptativa de la organización frente a amenazas emergentes.

2.2.2. Aseguramiento o Seguridad

En el contexto de la metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), la dimensión de aseguramiento o seguridad se refiere a un conjunto de prácticas y procesos destinados a garantizar la protección de los activos críticos de una organización frente a amenazas y vulnerabilidades. Esta dimensión abarca la identificación, evaluación y mitigación de riesgos, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de la información. Baniya & Weech, (2019)

El aseguramiento o seguridad en OCTAVE implica una serie de actividades sistemáticas que incluyen la identificación de activos valiosos, la evaluación de amenazas potenciales y la determinación de vulnerabilidades existentes. A partir de esta evaluación, se desarrollan estrategias de mitigación que buscan reducir el impacto de los riesgos identificados. Estas estrategias pueden incluir la implementación de controles técnicos, administrativos y físicos, así como la formación y concienciación del personal sobre prácticas de seguridad.

La metodología OCTAVE se distingue por su enfoque holístico y participativo, involucrando a diferentes niveles de la organización en el

proceso de evaluación y gestión de riesgos. Esto asegura que las decisiones tomadas reflejen una comprensión integral de las necesidades de seguridad y las prioridades operativas de la empresa.

2.2.3. Teoría de Gestión de Redes

La teoría de redes, componente esencial en programas de maestría en Gestión Comunicacional virtual, proporciona a directivos marcos interpretativos para comprender sus departamentos y organizaciones como estructuras sociales interconectadas. Según Carpenter, Bauer y Erdogan (2010), el rendimiento de estas redes sociales laborales depende de tres principios fundamentales: reciprocidad (homogeneidad funcional entre agentes), intercambio (diferenciación de tareas entre participantes) y similitud (grado de homología entre nodos grupales). USC University of Southern California

La teoría de redes es fundamental en programas de maestría en Gestión Comunicacional virtual, ya que ofrece a los directivos marcos interpretativos para entender sus departamentos y organizaciones como estructuras sociales interconectadas. Según Carpenter, Bauer y Erdogan (2023), el rendimiento de estas redes sociales laborales depende de tres principios fundamentales: reciprocidad, intercambio y similitud.

El principio de reciprocidad se refiere a la homogeneidad funcional entre los agentes de la red. En términos de gestión de redes de comunicaciones, esto implica que los nodos (dispositivos o usuarios) deben colaborar y compartir recursos de manera equitativa. La reciprocidad asegura que los beneficios y responsabilidades se distribuyan de manera justa, promoviendo la estabilidad y la eficiencia

operativa de la red. Este principio es esencial para mantener un flujo de información constante y confiable, ya que cada nodo actúa tanto como proveedor como consumidor de recursos. LibreTexts, (2004).

El principio de intercambio se basa en la diferenciación de tareas entre los participantes de la red. En una red de comunicaciones, esto se traduce en la especialización de funciones y roles, donde cada nodo desempeña tareas específicas que contribuyen al funcionamiento general de la red. La diferenciación de tareas permite una mayor eficiencia y optimización de recursos, ya que cada nodo puede enfocarse en sus fortalezas y capacidades particulares. Este principio también facilita la escalabilidad de la red, permitiendo que se adapte a cambios en la demanda y en el entorno operativo. Castro Garcia, (2024).

El principio de similitud se refiere al grado de homología entre los nodos grupales. En la gestión de redes de comunicaciones, la similitud implica que los nodos con características y funciones similares tienden a agruparse y colaborar más estrechamente. Este agrupamiento facilita la coordinación y la comunicación, ya que los nodos comparten un entendimiento común de sus roles y responsabilidades. La similitud también puede mejorar la resiliencia de la red, ya que los nodos similares pueden respaldarse mutuamente en caso de fallos o interrupciones Castro Garcia, (2024).

2.2.3.1. Gestión de redes de comunicaciones

La gestión de redes de comunicaciones en el contexto de la metodología OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) se refiere a la administración y

supervisión integral de los recursos de red dentro de una organización. Esta gestión abarca la planificación, implementación, monitoreo y mantenimiento de las infraestructuras de comunicación, asegurando que los datos se transmitan de manera eficiente, segura y confiable. La gestión efectiva de redes de comunicaciones es crucial para el funcionamiento óptimo de las operaciones empresariales, permitiendo la conectividad y el intercambio de información entre diferentes sistemas y usuarios ESGinnovaGroup, (2021).

2.2.3.2. Procesos

La dimensión de procesos en la gestión de redes de comunicaciones implica la definición y estandarización de procedimientos que aseguren la operatividad y eficiencia de la red. Esto incluye la configuración de dispositivos de red, la gestión de cambios, la resolución de problemas y la optimización del rendimiento. Los procesos bien definidos permiten una administración coherente y predecible de la red, minimizando el riesgo de interrupciones y mejorando la capacidad de respuesta ante incidentes. En el marco de la metodología OCTAVE, los procesos también abarcan la identificación y evaluación de riesgos, así como la implementación de controles para mitigar dichos riesgos Esginnova Group, (2021)

2.2.3.3. Monitoreo

La dimensión de monitoreo de redes se centra en la supervisión continua de la red para detectar y responder a eventos que

puedan afectar su desempeño y seguridad. El monitoreo incluye la recopilación y análisis de datos sobre el tráfico de red, el estado de los dispositivos y la detección de anomalías. Herramientas avanzadas de monitoreo permiten identificar patrones inusuales que podrían indicar problemas de rendimiento o intentos de intrusión. En el contexto de OCTAVE, el monitoreo es esencial para mantener una visión actualizada de la postura de seguridad de la red y para tomar decisiones informadas sobre la gestión de riesgos. ESGinnovaGroup, (2021).

2.2.3.4. Seguridad

La seguridad de datos, también conocida como seguridad de la información o seguridad informática, es un aspecto esencial de TI en organizaciones de cualquier tamaño y tipo. Se trata de un aspecto que tiene que ver con la protección de datos contra accesos no autorizados y para protegerlos de una posible corrupción durante todo su ciclo de vida Power Data, (2024).

Así mismo, la seguridad de la información se refiere al conjunto de medidas, políticas y prácticas diseñadas para la protección de datos. Así como a los sistemas de una organización contra el acceso no autorizado, el uso indebido, la divulgación, la modificación o la destrucción. Este concepto abarca tres pilares fundamentales: Confidencialidad, Integridad, Disponibilidad Kio IT Services, (2024).

Es decir, la seguridad de datos trasciende la mera protección técnica para constituirse en un paradigma integral de salvaguarda informativa que articula medidas preventivas y reactivadoras a lo largo del ciclo vital de los activos digitales. Este enfoque holístico, fundamentado en la tríada de confidencialidad, integridad y disponibilidad, establece un marco operativo donde la protección contra accesos no autorizados y alteraciones maliciosas se integra orgánicamente con la cultura organizacional, transformando la seguridad informática de requisito técnico a componente estratégico del ecosistema empresarial contemporáneo.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

- Metodología

Según Jansen & Warren (2020), se refieren al “cómo” real de la investigación. Específicamente, se refiere a cómo un investigador diseña sistemáticamente un estudio para proporcionar resultados válidos y confiables consistentes con las metas, objetivos y preguntas del estudio.

- Gestión

Según Byjus (2024), la gestión se puede definir como el proceso de realizar de manera eficiente y efectiva trabajos o tareas necesarias para lograr los objetivos organizacionales.

- Redes de comunicaciones

Según Dremio (2024), la comunicación en red es el proceso clave de intercambio de datos e información entre computadoras. Este intercambio

se produce a través de un medio compartido cableado (como Ethernet) o inalámbrico (como Wi-Fi o 5G).

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. METODOLOGÍA Y TÉCNICAS UTILIZADAS

3.1.1. Tipo de investigación

La investigación es del tipo **Aplicada**.

Según Zamora (2008), Este tipo de investigación se caracteriza por su enfoque en la **exploración y generación de conocimiento** con un **propósito práctico**. A diferencia de otras investigaciones, se centra en **comprender cómo modificar o intervenir en resultados o fenómenos del mundo real**.

3.1.2. Nivel de investigación

El nivel será del tipo **Experimental**.

Según Sampieri (2008), el tipo de investigación es experimental, se centra en **manipular la variable dependiente** del objeto de estudio, la investigación experimental se limita a **aplicar la metodología para ver los resultados en la variable dependiente** de lo que se está investigando.

3.1.3. Método de investigación

El método será **Deductivo – Inductivo**.

Según Newman (2006), el **método deductivo-inductivo** combina dos enfoques de investigación tradicionalmente separados: el **deductivo** y el **inductivo**. Esta metodología busca **obtener conocimiento de una manera más completa y profunda** al aprovechar las fortalezas de ambos enfoques

3.1.4. Diseño de la investigación

Según Sampieri (2008), la investigación es Experimental de tipo preexperimental, donde se manipula las variables independiente y dependiente con el fin de obtener el nivel de influencia, para ello se realizará una evaluación de pre test y luego otro post test.

$$Y_1 \text{ ----- } X \text{ ----- } Y_2$$

Donde:

Y₁: es el grupo antes del experimento.

X: es la aplicación propiamente dicha.

Y₂: es el grupo después del experimento

3.2. POBLACIÓN Y MUESTRA

Población

Lo conforman el grupo de interés, quienes debido a sus condiciones brindaran información para poder determinar la validez de los resultados de la investigación. La población, en esta investigación, son los empleados pertenecientes a la gerencia general y área de TI, quienes en conjunto hacen un total de 13 empleados.

Muestra

Está conformada por una parte de la población, este grupo es elegido, en la mayoría de casos aplicando el muestreo estadístico. En la presente investigación se no es adecuado el muestreo probabilístico debido al número reducido de la población; por lo que la elección será por conveniencia, en ese sentido, el número de la muestra coincide con el total de la población que son 13 empleados

3.3. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El instrumento más adecuado, según las características de la presente investigación es el cuestionario de preguntas, el cual es elaborado en relación a las variables dependiente e independiente, y aplicando la escala de Likert para las respuestas.

3.4. PROCEDIMIENTO DE RECOLECCIÓN DE DATOS

El recojo de datos a través de la aplicación del cuestionario, será previa explicación a los integrantes de la muestra, y será aplicada en dos momentos diferentes, en un pre test y otra pos test.

3.5. TRATAMIENTO DE DATOS.

Se utilizará un programa informático para el procesamiento, sinterización, traficación datos cuantitativos, el software estadístico es el SPSS.

3.6. GRADO DE CONFIABILIDAD DE LOS DATOS.

Será utilizo el coeficiente de alfa de Cronbach, que mide la efectividad del instrumento

CAPÍTULO IV

4.1. METODOLOGÍA OCTAVE PARA LA GESTIÓN DE REDES DE COMUNICACIONES.

4.1.1. Metodología de Análisis de Riesgos de Sistemas de información.

a) Identificación de activos

Para esta etapa inicial se ha visto por conveniente la aplicación de la metodología MAGERIT, el cual nos permite realizar un análisis y gestión de riesgos de seguridad de información. A continuación, se detalla la información correspondiente:

Tabla 3: activos de gestión de redes de comunicaciones

ACTIVOS DE GESTIÓN DE REDES DE COMUNICACIONES DE LA EMPRESA CONSTRUCTORA PREIMAQ S.A.C				
COD.	TIPO	NOMBRE	DESCRIPCIÓN	RESPONSABLE
S001	Servicio	Sistema contable SISCON	Sistema de control de obligaciones.	Área informática
A001	Aplicaciones	SysPreiVen	Sistema para la gestión de ventas de maquinarias y repuestos	Área informática
E001	Equipos TI	Servidor dominio	Sistema que proporciona la resolución de nombres de los equipos conectados a la red	Área informática
E002	Equipos TI	Servidor de Ad	Servidor con el servicio de gestión de usuarios y equipos	Área informática
E003	Equipos TI	Servidor de Base de datos	Servidor alberga al sistema de base de datos de los aplicativos	Área informática
E004	Equipos TI	Servidor de Aplicaciones	Sistema que despliega los aplicativos y programas por la red	Área informática
E005	Equipos TI	Servidor respaldo	Servidor de copia de seguridad de	Área informática

			los datos e información	
E006	Equipos TI	Servidor proxy	Gestiona las solicitudes de acceso a internet	Área informática
E007	Equipos TI	Switch Acceso	Equipo de interconexión de los equipos de la red	Área informática
E008	Equipos TI	Router	Equipo para el acceso a internet	Área informática
R001	Redes	Internet	Servicio de acceso a internet	Área informática
R002	Redes	Wifi	Equipo de comunicación inalámbrica	Área informática
S001	Soporte	Cintas Backup	Cintas para copias de seguridad	Área informática
S002	Soporte	HDD ext	Discos externos	Área informática
S003	Soporte	Sistema eléctrico	Sistema de conexión eléctrica	Área informática
EA001	Equipo Aux	Ups	Sistema de baterías de respaldo	Área informática
EA002	Equipo Aux	Aires acondicionados	Sistema de refrigeración.	Área informática
EA003	Equipo Aux	Grupo electrógeno	Equipo de respaldo eléctrico	Área informática
EA004	Equipo Aux	Cableado	Medios físicos de conexión de la red	Área informática
I001	Instalaciones	DataCenter	Instalación de contiene a los equipos de comunicación y servidores	Área informática
P001	Personal	Personal TI	Asistentes, soporte.	Área informática
P002	Personal	Adm. TI	Encargado de TI	Área informática

Como se puede notar en la tabla anterior, se logró identificar los activos de TI, los cuales fueron catalogados como: servicios, aplicación, equipamiento de TI, redes, soporte, equipos auxiliares, instalaciones y personal.

b) Valorización de activos

Para la valorización se han identificado 05 dimensiones, las cuales se detallan en la siguiente tabla:

Tabla 4: Rangos de Valorización de activos

Item	Dimensión	Rango
1	Disponibilidad	[0, 10]
2	Integridad	[0, 10]
3	Confidencialidad	[0, 10]
4	Autenticidad	[0, 10]
5	Trazabilidad	[0, 10]

Fuente: MAGERIT -V 3.0

A continuación de muestran las valorizaciones de cada activo:

Tabla 5: Valorización de activos

VALORACIÓN DE ACTIVOS								
COD.	TIPO	NOMBRE	DISPO.	INTEG.	CONF.	AUTE.	TRAZ	TOT
S001	Servicio	Sistema contable SISCO	3	0	0	0	0	3
A001	Aplicaciones	SysPreiVen	4	7	0	7	2	5
E001	Equipos TI	Servidor de dominio	3	4	0	4	4	3.8
E002	Equipos TI	Servidor de Ad	3	4	0	4	4	3.8
E003	Equipos TI	Servidor de Base de datos	6	7	1	6	5	5
E004	Equipos TI	Servidor de Aplicaciones	3	4	0	3	4	3.5
E005	Equipos TI	Servidor de respaldo	2	7	0	6	3	4.5
E006	Equipos TI	Servidor proxy	2	0	0	0	0	2
E007	Equipos TI	Switch Acceso	3	0	0	0	1	2
E008	Equipos TI	Router	3	0	0	0	1	2
R001	Redes	Internet	4	0	0	0	2	3
R002	Redes	Wifi	4	0	0	0	2	3
S001	Soporte	Cintas Backup	3	6	0	5	4	4.5
S002	Soporte	HDD ext	3	5	0	4	3	3.8
S003	Soporte	Sistema eléctrico	2	0	0	0	2	2
EA001	Equipo Aux	Ups	4	0	0	0	6	5
EA002	Equipo Aux	Aires acondicionados	4	0	0	0	6	5
EA003	Equipo Aux	Grupo electrógeno	4	0	0	0	6	5
EA004	Equipo Aux	Cableado	4	0	0	0	7	5.5
I001	Instalaciones	DataCenter	4	0	0	0	7	5.5
P001	Personal	Personal TI	3	0	0	0	2	2.5
P002	Personal	Adm. TI	8	0	0	0	3	5.5

Como se puede concluir los más valorados fueron: la aplicación SysPreiVen, el Servidor de Base de datos, el equipo auxiliar Ups, Aires

acondicionados, Grupo electrógeno, Cableado, la instalación del DataCenter y el personal Adm. TI

c) Identificación de amenazas

A continuación se identifican las amenazas de los activos:

Tabla 6: Identificación de amenazas.

IDENTIFICACIÓN DE AMENAZAS				
COD.	ACTIVO		AMENAZA	
	NOMBRE		NOMBRE	DIM. AFECTADA
S001	Sistema contable	SISCON	A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
			A003 Error de usuarios	Integridad
			A004 Falla de Sw	Disponibilidad
A001	SysPreiVen		A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
			A003 Error de usuarios	Integridad
			A004 Falla de Sw	Disponibilidad
			A005 Falla física	Disponibilidad
E001	Servidor de dominio		A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
			A006 Climatización inadecuada	Disponibilidad
			A007 Vulnerabilidad del SW	Integridad
			A008 Error de mantenimiento	Disponibilidad
			A009 Falta de recursos	Disponibilidad
			A010 Incendio	Disponibilidad
			A005 Falla física	Disponibilidad
			A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
E002	Servidor de Ad		A006 Climatización inadecuada	Disponibilidad
			A007 Vulnerabilidad del SW	Integridad
			A008 Error de mantenimiento	Disponibilidad
			A009 Falta de recursos	Disponibilidad
			A010 Incendio	Disponibilidad
			A010 Incendio	Disponibilidad
			A005 Falla física	Disponibilidad
			A001 Corte de fluido eléctrico	Disponibilidad
			A011 Falla de servidor de comunicaciones	Disponibilidad
			A012 Error del administrador	Disponibilidad
E003	Servidor de Base de datos			Confidencialidad
				Integridad
			A008 Error de mantenimiento	Disponibilidad
			A005 Falla física	Disponibilidad
			A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
			A006 Climatización inadecuada	Disponibilidad
			A007 Vulnerabilidad del SW	Integridad
			A008 Error de mantenimiento	Disponibilidad
			A009 Falta de recursos	Disponibilidad
E004	Servidor de Aplicaciones	de	A010 Incendio	Disponibilidad
			A005 Falla física	Disponibilidad
			A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
			A006 Climatización inadecuada	Disponibilidad
E005	Servidor de respaldo		A007 Vulnerabilidad del SW	Integridad
			A008 Error de mantenimiento	Disponibilidad
			A009 Falta de recursos	Disponibilidad
			A010 Incendio	Disponibilidad
			A005 Falla física	Disponibilidad
			A001 Corte de fluido eléctrico	Disponibilidad
			A002 Falla en las comunicaciones	Disponibilidad
			A006 Climatización inadecuada	Disponibilidad

		A007	Vulnerabilidad del SW	Integridad
		A008	Error de mantenimiento	Disponibilidad
		A009	Falta de recursos	Disponibilidad
		A010	Incendio	Disponibilidad
		A010	Incendio	Disponibilidad
		A005	Falla física	Disponibilidad
		A001	Corte de fluido eléctrico	Disponibilidad
		A011	Falla de servidor de comunicaciones	Disponibilidad
E006	Servidor proxy	A012	Error del administrador	Disponibilidad
				Confidencialidad
		A013	Error de configuración	Integridad
				Disponibilidad
				Confidencialidad
E007	Switch Acceso	A009	Falta de recursos	Integridad
				Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
		A011	Falla de servidor de comunicaciones	Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
E008	Router	A012	Error del administrador	Disponibilidad
				Confidencialidad
		A013	Error de configuración	Integridad
				Disponibilidad
				Confidencialidad
		A010	Incendio	Integridad
				Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
R001	Internet	A011	Falla de servidor de comunicaciones	Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
		A012	Error del administrador	Disponibilidad
				Confidencialidad
				Integridad
				Disponibilidad
				Confidencialidad
R002	Wifi	A013	Error de configuración	Integridad
				Confidencialidad
				Integridad
				Disponibilidad
				Disponibilidad
		A010	Incendio	Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
				Disponibilidad
S001	Cintas Backup	A012	Pérdida de equipos	Disponibilidad
				Confidencialidad
				Integridad
		A013	Degradación de los soportes	Disponibilidad
				Disponibilidad
				Disponibilidad

		A014	Robo	Disponibilidad Integridad
		A010	Incendio	Disponibilidad
		A005	Falla física	Disponibilidad
S002	HDD ext	A013	Degradación de los soportes	Disponibilidad
		A003	Error de usuarios	Integridad
		A012	Pérdida de equipos	Disponibilidad
		A010	Incendio	Disponibilidad
		A005	Falla física	Disponibilidad
EA001	Ups	A003	Error de usuarios	Integridad
		A008	Error de mantenimiento	Disponibilidad
		A009	Falta de recursos	Disponibilidad
		A010	Incendio	Disponibilidad
		A005	Falla física	Disponibilidad
		A003	Error de usuarios	Integridad
		A008	Error de mantenimiento	Disponibilidad
		A009	Falta de recursos	Disponibilidad
EA002	Aires acondicionados	A014	Contaminación electromagnética	Disponibilidad
		A001	Corte de fluido eléctrico	Disponibilidad
		A016	Acceso no autorizado	Confidencialidad Integridad
		A010	Incendio	Disponibilidad
		A005	Falla física	Disponibilidad
		A003	Error de usuarios	Integridad
		A008	Error de mantenimiento	Disponibilidad
		A009	Falta de recursos	Disponibilidad
		A017	Indisponibilidad del personal	Disponibilidad
		A010	Incendio	Disponibilidad
		A018	Daños por agua	Disponibilidad
		A019	Contaminación eléctrica	Disponibilidad
EA004	Cableado	A008	Error de mantenimiento	Disponibilidad
		A016	Acceso no autorizado	Confidencialidad Integridad
		A017	Indisponibilidad del personal	Disponibilidad
		A018	Desastre natural	Disponibilidad
		A010	Incendio	Disponibilidad
		A019	Pérdida de equipos	Disponibilidad
		A020	Robo	Disponibilidad
		A017	Indisponibilidad del personal	Disponibilidad
		A008	Error de mantenimiento	Disponibilidad
		A003	Error de usuarios	Integridad
		A021	Divulgación de información	Confidencialidad Disponibilidad
P001	Personal TI	A022	Extorción	Integridad Confidencialidad Disponibilidad
		A023	Ingeniería Social	Integridad Confidencialidad
		A019	Contaminación eléctrica	Disponibilidad
P002	Adm. TI	A006	Climatización inadecuada	Disponibilidad
		A017	Indisponibilidad del personal	Disponibilidad

Como se puede observar se lograron identificar un total de 23 amenazas; a continuación se procede con mostrar los resultados de valoración de amenazas de los activos.

Tabla 7: Valoración de amenazas.

VALORACIÓN DE AMENAZAS												
COD.	ACTIVO		COD.	AMENAZA	D	DIMENSIÓN				TOTAL	NIVEL	
	NOMBRE			NOMBRE		I	C	A	T			
S001	Sistema SISCON	contable	A001	Corte de fluido eléctrico	0.9	0.1				0.9	MUY ALTO	
			A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
			A003	Error de usuarios	0.1					0.1	BAJO	
			A004	Falla de Sw	0.1					0.1	BAJO	
A001	SysPreiVen		A001	Corte de fluido eléctrico	0.9					0.9	MUY ALTO	
			A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
			A003	Error de usuarios	0.1					0.1	BAJO	
			A004	Falla de Sw	0.1					0.1	BAJO	
			A005	Falla física	0.5					0.5	MEDIO	
E001	Servidor de dominio		A001	Corte de fluido eléctrico	0.5					0.5	MEDIO	
			A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
			A006	Climatización inadecuada	0.5					0.5	MEDIO	
			A007	Vulnerabilidad del SW	0.9					0.9	MUY ALTO	
			A008	Error de mantenimiento	0.3					0.3	BAJO	
			A009	Falta de recursos	0.5					0.5	MEDIO	
			A010	Incendio	1					1	MUL ALTO	
			A005	Falla física	0.5					0.5	MEDIO	
			A001	Corte de fluido eléctrico	0.5					0.5	MEDIO	
			A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
E002	Servidor de Ad		A006	Climatización inadecuada	0.5					0.5	MEDIO	
			A007	Vulnerabilidad del SW	0.9					0.9	MUL ALTO	
			A008	Error de mantenimiento	0.3					0.3	BAJO	
			A009	Falta de recursos	0.6					0.6	ALTO	
			A010	Incendio	1					1	MUY ALTO	
			A010	Incendio	1					1	MUY ALTO	
			A005	Falla física	0.5					0.5	MEDIO	
			A001	Corte de fluido eléctrico	0.5					0.5	MEDIO	
			A011	Falla de servidor de comunicaciones	0.5					0.5	MEDIO	
			A012	Error del administrador	0.1					0.1	BAJO	
E003	Servidor de Base de datos		A012	Error del administrador	0.1					0.1	BAJO	
			A008	Error de mantenimiento	0.5					0.5	MEDIO	
			A005	Falla física	0.5					0.5	MEDIO	
			A001	Corte de fluido eléctrico	0.5					0.5	MEDIO	
			A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
			A006	Climatización inadecuada	0.2					0.2	BAJO	
			A007	Vulnerabilidad del SW	0.6					0.6	ALTO	
			A008	Error de mantenimiento	0.5					0.5	MEDIO	
			A009	Falta de recursos	0.5					0.5	MEDIO	
			A010	Incendio	1					1	MUY ALTO	
E004	Servidor Aplicaciones	de		A005	Falla física	0.5					0.5	MEDIO
				A001	Corte de fluido eléctrico	0.5					0.5	MEDIO
				A002	Falla en las comunicaciones	0.5					0.5	MEDIO
				A006	Climatización inadecuada	0.2					0.2	BAJO
				A007	Vulnerabilidad del SW	0.6					0.6	ALTO
				A008	Error de mantenimiento	0.5					0.5	MEDIO
				A009	Falta de recursos	0.5					0.5	MEDIO
				A010	Incendio	1					1	MUY ALTO
				A005	Falla física	0.5					0.5	MEDIO
				A001	Corte de fluido eléctrico	0.5					0.5	MEDIO
E005	Servidor de respaldo		A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
			A006	Climatización inadecuada	0.2					0.2	BAJO	
			A007	Vulnerabilidad del SW	0.6					0.6	ALTO	
			A008	Error de mantenimiento	0.6					0.6	ALTO	
			A009	Falta de recursos	0.2					0.2	BAJO	
			A010	Incendio	1					1	MUY ALTO	
			A010	Incendio	1					1	MUY ALTO	
			A005	Falla física	0.5					0.5	MEDIO	
			A001	Corte de fluido eléctrico	0.5					0.5	MEDIO	
			A002	Falla en las comunicaciones	0.5					0.5	MEDIO	
E006	Servidor proxy		A006	Climatización inadecuada	0.2					0.2	BAJO	
			A007	Vulnerabilidad del SW	0.6					0.6	ALTO	
			A008	Error de mantenimiento	0.6					0.6	ALTO	
			A009	Falta de recursos	0.2					0.2	BAJO	
			A010	Incendio	1					1	MUY ALTO	
			A010	Incendio	1					1	MUY ALTO	
			A005	Falla física	0.5					0.5	MEDIO	
			A001	Corte de fluido eléctrico	0.5					0.5	MEDIO	

E007	Switch Acceso	A011	Falla de servidor de comunicaciones	0.5	0.5	MEDIO
				0.2	0.2	BAJO
		A012	Error del administrador	0.2	0.2	BAJO
				0.2	0.2	BAJO
				0.2	0.2	BAJO
		A013	Error de configuración	0.2	0.2	BAJO
				0.2	0.2	BAJO
		A009	Falta de recursos	0.2	0.2	BAJO
		A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A001	Corte de fluido eléctrico	0.5	0.5	MEDIO
		A011	Falla de servidor de comunicaciones	0.5	0.5	MEDIO
				0.2	0.2	BAJO
		A012	Error del administrador	0.2	0.2	BAJO
				0.2	0.2	BAJO
E008	Router	A013	Error de configuración			
		A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A001	Corte de fluido eléctrico	0.5	0.5	MEDIO
		A011	Falla de servidor de comunicaciones	0.5	0.5	MEDIO
				0.2	0.2	BAJO
		A012	Error del administrador	0.2	0.2	BAJO
				0.2	0.2	BAJO
		A013	Error de configuración			
R001	Internet	A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A001	Corte de fluido eléctrico	0.5	0.5	MEDIO
		A006	Climatización inadecuada	0.5	0.5	MEDIO
				0.2	0.2	BAJO
		A012	Error del administrador	0.2	0.2	BAJO
				0.2	0.2	BAJO
				0.6	0.6	ALTO
		A013	Error de configuración	0.6	0.6	ALTO
				0.6	0.6	ALTO
R002	Wifi	A010	Incendio			
		A005	Falla física	0.5	0.5	MEDIO
		A001	Corte de fluido eléctrico	0.5	0.5	MEDIO
		A012	Pérdida de equipos	0.5	0.5	MEDIO
				0.6	0.6	ALTO
		A013	Denegación de servicios	0.6	0.6	ALTO
S001	Cintas Backup	A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A013	Degradación de los soportes	0.5	0.5	MEDIO
		A003	Error de usuarios	0.5	0.5	MEDIO
		A012	Pérdida de equipos	0.2	0.2	BAJO
				0.2	0.2	BAJO
				0.9	0.9	MUY ALTO
		A014	Robo			
S002	HDD ext			1	1	MUY ALTO
		A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A013	Degradación de los soportes	0.5	0.5	MEDIO
		A003	Error de usuarios	0.5	0.5	MEDIO
		A012	Pérdida de equipos	0.6	0.6	ALTO
EA001	Ups	A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A003	Error de usuarios	0.6	0.6	ALTO
		A008	Error de mantenimiento	0.5	0.5	MEDIO
		A009	Falta de recursos	0.5	0.5	MEDIO

EA002	Aires acondicionados	A010	Incendio	1	1	MUY ALTO
		A005	Falla física	0.5	0.5	MEDIO
		A003	Error de usuarios	0.6	0.6	ALTO
		A008	Error de mantenimiento	0.5	0.5	MEDIO
		A009	Falta de recursos	0.5	0.5	MEDIO
		A014	Contaminación electromagnética	0.2	0.2	BAJO
		A001	Corte de fluido eléctrico	0.5	0.5	MEDIO
		A016	Acceso no autorizado	0.2	0.2	BAJO
EA003	Grupo electrógeno	A010	Incendio	0.2	0.2	BAJO
		A005	Falla física	0.5	0.5	MEDIO
		A003	Error de usuarios	0.6	0.6	ALTO
		A008	Error de mantenimiento	0.5	0.5	MEDIO
		A009	Falta de recursos	0.5	0.5	MEDIO
		A017	Indisponibilidad del personal	0.2	0.2	BAJO
		A010	Incendio	0.2	0.2	BAJO
		A018	Daños por agua	0.2	0.2	BAJO
EA004	Cableado	A019	Contaminación eléctrica	0.2	0.2	BAJO
		A008	Error de mantenimiento	0.5	0.5	MEDIO
		A016	Acceso no autorizado	0.2	0.2	BAJO
		A017	Indisponibilidad del personal	0.6	0.6	ALTO
		A018	Desastre natural	1	1	MUY ALTO
		A010	Incendio	1	1	MUY ALTO
		A019	Perdida de equipos	0.2	0.2	BAJO
		A020	Robo	0.2	0.2	BAJO
I001	DataCenter	A017	Indisponibilidad del personal	0.6	0.6	ALTO
		A008	Error de mantenimiento	0.5	0.5	MEDIO
		A003	Error de usuarios	0.6	0.6	ALTO
		A021	Divulgación de información	0.6	0.6	ALTO
		A022	Extorción	0.2	0.2	BAJO
		A023	Ingeniería Social	0.2	0.2	BAJO
		A019	Contaminación eléctrica	0.2	0.2	BAJO
		A006	Climatización inadecuada	0.2	0.2	BAJO
P002	Adm. TI	A017	Indisponibilidad del personal	0.6	0.6	ALTO

d) Estimación del impacto

A continuación, se procede con mostrar información de la valoración del impacto cuyos valores se obtuvieron del producto del valor del activo por el valor posterior al impacto de amenaza cuando esta se materializa.

Tabla 8: Valoración de impacto.

VALORACIÓN DEL IMPACTO								
ACTIVO		AMENAZA		Valor activo	Desgaste	Impacto	Escala	Nivel
COD.	NOMBRE	COD.	NOMBRE					

S001	Sistema contable	SISCON	A001	Corte de fluido eléctrico	3	0.9	2.7	MEDIO	3
			A002	Falla en las comunicaciones		0.5	1.5	BAJO	2
			A003	Error de usuarios		0.1	0.3	BAJO	2
			A004	Falla de Sw		0.1	0.3	BAJO	2
A001	SysPreiVen		A001	Corte de fluido eléctrico	2	0.9	2.7	MEDIO	3
			A002	Falla en las comunicaciones		0.5	1.5	BAJO	2
			A003	Error de usuarios		0.1	0.3	BAJO	2
			A004	Falla de Sw		0.1	0.3	BAJO	2
E001	Servidor de dominio		A005	Falla física	3.75	0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
			A002	Falla en las comunicaciones		0.5	1.5	BAJO	2
			A006	Climatización inadecuada		0.5	1	BAJO	2
			A007	Vulnerabilidad del SW		0.8	3.1	ALTO	3
			A008	Error de mantenimiento		0.7	2.2	MEDIO	3
			A009	Falta de recursos		0.5	1.5	BAJO	2
			A010	Incendio		1	2	BAJO	2
E002	Servidor de Ad		A005	Falla física	3.75	0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
			A002	Falla en las comunicaciones		0.5	1.5	BAJO	2
			A006	Climatización inadecuada		0.5	1	BAJO	2
			A007	Vulnerabilidad del SW		0.8	3.1	ALTO	3
			A008	Error de mantenimiento		0.7	2.2	MEDIO	3
			A009	Falta de recursos		0.5	1.5	BAJO	2
			A010	Incendio		1	2	BAJO	2
E003	Servidor de Base de datos		A010	Incendio	5	1	2	BAJO	2
			A005	Falla física		0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
			A011	Falla de servidor de comunicaciones		0.5	1.5	BAJO	2
			A012	Error del administrador		2	1	BAJO	2
			A008	Error de mantenimiento		0.7	2.2	MEDIO	3
			A005	Falla física		0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
E004	Servidor de Aplicaciones	de	A002	Falla en las comunicaciones	3.75	0.5	1.5	BAJO	2
			A006	Climatización inadecuada		0.5	1	BAJO	2
			A007	Vulnerabilidad del SW		0.8	3.1	ALTO	3
			A008	Error de mantenimiento		0.7	2.2	MEDIO	3
			A009	Falta de recursos		0.5	1.5	BAJO	2
			A010	Incendio		1	2	BAJO	2
			A005	Falla física		0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
E005	Servidor de respaldo		A002	Falla en las comunicaciones	4.5	0.5	1.5	BAJO	2
			A006	Climatización inadecuada		0.5	1	BAJO	2
			A007	Vulnerabilidad del SW		0.8	3.1	ALTO	3
			A008	Error de mantenimiento		0.7	2.2	MEDIO	3
			A009	Falta de recursos		0.5	1.5	BAJO	2
			A010	Incendio		1	2	BAJO	2
			A010	Incendio		1	2	BAJO	2
			A005	Falla física		0.5	1.5	BAJO	2
E006	Servidor proxy		A001	Corte de fluido eléctrico	2	0.5	1	BAJO	2
			A011	Falla de servidor de comunicaciones		0.5	1.5	BAJO	2
			A012	Error del administrador		2	1	BAJO	2
			A013	Error de configuración		0.2	0.4	BAJO	2
			A009	Falta de recursos		0.5	1.5	BAJO	2
			A010	Incendio		1	2	BAJO	2
			A005	Falla física		0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
E007	Switch Acceso		A011	Falla de servidor de comunicaciones	2	0.5	1.5	BAJO	2
			A012	Error del administrador		2	1	BAJO	2
			A013	Error de configuración		0.2	0.4	BAJO	2
			A010	Incendio		1	2	BAJO	2
			A005	Falla física		0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
			A011	Falla de servidor de comunicaciones		0.5	1.5	BAJO	2
			A012	Error del administrador		2	1	BAJO	2
E008	Router		A013	Error de configuración	2	0.2	0.4	BAJO	2
			A010	Incendio		1	2	BAJO	2
			A005	Falla física		0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
R001	Internet		A011	Falla de servidor de comunicaciones	3	0.5	1.5	BAJO	2
			A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
			A006	Climatización inadecuada		0.5	1	BAJO	2
			A012	Error del administrador		2	1	BAJO	2
			A013	Error de configuración		0.2	0.4	BAJO	2

R002	Wifi	A010	Incendio	3	1	2	BAJO	2
		A005	Falla física		0.5	1.5	BAJO	2
		A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
		A012	Pérdida de equipos		0.9	4.2	ALTO	4
S001	Cintas Backup	A013	Denegación de servicios	4.5	0.6	1.44	BAJO	2
		A010	Incendio		1	2	BAJO	2
		A005	Falla física		0.5	1.5	BAJO	2
		A013	Degradación de los soportes		1	5	ALTO	4
S002	HDD ext	A003	Error de usuarios	3.75	0.1	0.3	BAJO	2
		A012	Pérdida de equipos		0.9	4.2	ALTO	4
		A014	Robo		0.9	4.2	ALTO	4
		A010	Incendio		1	2	BAJO	2
EA001	Ups	A005	Falla física	5	0.5	1.5	BAJO	2
		A003	Error de usuarios		0.1	0.3	BAJO	2
		A008	Error de mantenimiento		0.7	2.2	MEDIO	3
		A009	Falta de recursos		0.5	1.5	BAJO	2
EA002	Aires acondicionados	A010	Incendio	5	1	2	BAJO	2
		A005	Falla física		0.5	1.5	BAJO	2
		A003	Error de usuarios		0.1	0.3	BAJO	2
		A008	Error de mantenimiento		0.7	2.2	MEDIO	3
EA003	Grupo electrógeno	A009	Falta de recursos	5	0.5	1.5	BAJO	2
		A014	Contaminación electromagnética		0.05	0.25	BAJO	2
		A001	Corte de fluido eléctrico		0.9	2.7	MEDIO	3
		A016	Acceso no autorizado		0.1	0.3	BAJO	2
EA004	Cableado	A010	Incendio	5.5	1	2	BAJO	2
		A005	Falla física		0.5	1.5	BAJO	2
		A003	Error de usuarios		0.1	0.3	BAJO	2
		A008	Error de mantenimiento		0.7	2.2	MEDIO	3
I001	DataCenter	A009	Falta de recursos	5.5	0.5	1.5	BAJO	2
		A017	Indisponibilidad del personal		0.9	4.95	ALTO	4
		A010	Incendio		1	2	BAJO	2
		A018	Daños por agua		0.1	0.3	BAJO	2
P001	Personal TI	A019	Contaminación eléctrica	2.5	0.05	0.25	BAJO	2
		A008	Error de mantenimiento		0.7	2.2	MEDIO	3
		A016	Acceso no autorizado		0.1	0.3	BAJO	2
		A017	Indisponibilidad del personal		0.9	4.95	ALTO	4
P002	Adm. TI	A018	Desastre natural	5.5	1	5.5	ALTO	4
		A010	Incendio		1	2	BAJO	2
		A019	Pérdida de equipos		0.9	4.2	ALTO	4
		A020	Robo		1	2	BAJO	2
P001	Personal TI	A017	Indisponibilidad del personal	2.5	0.9	4.95	ALTO	4
		A008	Error de mantenimiento		0.7	2.2	MEDIO	3
		A003	Error de usuarios		0.1	0.3	BAJO	2
		A021	Divulgación de información		0.1	0.3	BAJO	2
P002	Adm. TI	A022	Extorción	5.5	0.1	0.3	BAJO	2
		A023	Ingeniería Social		0.1	0.3	BAJO	2
		A019	Contaminación eléctrica		0.05	0.25	BAJO	2
		A006	Climatización inadecuada		0.5	1	BAJO	2
P002	Adm. TI	A017	Indisponibilidad del personal	5.5	0.9	4.95	ALTO	4

e) Probabilidad de la amenaza

A continuación, se muestra la valoración de la probabilidad de la amenaza.

Tabla 9: probabilidad de amenazas.

PROBABILIDAD DE AMENAZA				
ACTIVO		AMENAZA		VALORACIÓN DE LA PROBABILIDAD
COD.	NOMBRE	COD.	NOMBRE	Nivel
S001		A001	Corte de fluido eléctrico	3
				Normal

	Sistema SISCON	contable	A002	Falla en las comunicaciones	3	Normal
			A003	Error de usuarios	2	Poco frecuente
			A004	Falla de Sw	2	Poco frecuente
A001	SysPreiVen		A001	Corte de fluido eléctrico	3	Normal
			A002	Falla en las comunicaciones	3	Normal
			A003	Error de usuarios	2	Poco frecuente
			A004	Falla de Sw	2	Poco frecuente
			A005	Falla física	2	Poco frecuente
E001	Servidor de dominio		A001	Corte de fluido eléctrico	3	Normal
			A002	Falla en las comunicaciones	3	Normal
			A006	Climatización inadecuada	3	Normal
			A007	Vulnerabilidad del SW	2	Poco frecuente
			A008	Error de mantenimiento	2	Poco frecuente
E002	Servidor de Ad		A009	Falta de recursos	4	Frecuente
			A010	Incendio	2	Poco frecuente
			A005	Falla física	2	Poco frecuente
			A001	Corte de fluido eléctrico	4	Frecuente
			A002	Falla en las comunicaciones	3	Normal
E003	Servidor de Base de datos		A006	Climatización inadecuada	3	Normal
			A007	Vulnerabilidad del SW	2	Poco frecuente
			A008	Error de mantenimiento	2	Poco frecuente
			A009	Falta de recursos	4	Frecuente
			A010	Incendio	2	Poco frecuente
E004	Servidor Aplicaciones	de	A010	Incendio	2	Poco frecuente
			A005	Falla física	2	Poco frecuente
			A001	Corte de fluido eléctrico	3	Normal
			A011	Falla de servidor de comunicaciones	3	Normal
			A012	Error del administrador	2	Poco frecuente
E005	Servidor de respaldo		A008	Error de mantenimiento	2	Poco frecuente
			A005	Falla física	2	Poco frecuente
			A001	Corte de fluido eléctrico	4	Frecuente
			A002	Falla en las comunicaciones	3	Normal
			A006	Climatización inadecuada	3	Normal
E006	Servidor proxy		A007	Vulnerabilidad del SW	2	Poco frecuente
			A008	Error de mantenimiento	2	Poco frecuente
			A009	Falta de recursos	4	Frecuente
			A010	Incendio	2	Poco frecuente
			A010	Incendio	2	Poco frecuente
E007	Switch Acceso		A005	Falla física	2	Poco frecuente
			A001	Corte de fluido eléctrico	3	Normal
			A011	Falla de servidor de comunicaciones	3	Normal
			A012	Error del administrador	2	Poco frecuente
			A013	Error de configuración	2	Poco frecuente
E008	Router		A009	Falta de recursos	4	Frecuente
			A010	Incendio	2	Poco frecuente
			A005	Falla física	2	Poco frecuente
			A001	Corte de fluido eléctrico	4	Frecuente
			A011	Falla de servidor de comunicaciones	3	Normal
R001	Internet		A012	Error del administrador	2	Poco frecuente
			A013	Error de configuración	2	Poco frecuente
			A010	Incendio	2	Poco frecuente
			A005	Falla física	2	Poco frecuente
			A001	Corte de fluido eléctrico	3	Normal
R002	Wifi		A006	Climatización inadecuada	3	Normal
			A012	Error del administrador	2	Poco frecuente
			A013	Error de configuración	2	Poco frecuente
			A010	Incendio	2	Poco frecuente

		A005	Falla física	2	Poco frecuente
		A001	Corte de fluido eléctrico	3	Normal
		A012	Pérdida de equipos	2	Poco frecuente
		A013	Denegación de servicios	3	Normal
		A010	Incendio	2	Poco frecuente
		A005	Falla física	2	Poco frecuente
S001	Cintas Backup	A013	Degradación de los soportes	2	Poco frecuente
		A003	Error de usuarios	5	Muy frecuente
		A012	Pérdida de equipos	2	Poco frecuente
		A014	Robo	2	Poco frecuente
		A010	Incendio	2	Poco frecuente
S002	HDD ext	A005	Falla física	2	Poco frecuente
		A013	Degradación de los soportes	2	Poco frecuente
		A003	Error de usuarios	5	Muy frecuente
		A012	Pérdida de equipos	2	Poco frecuente
		A010	Incendio	2	Poco frecuente
EA001	Ups	A005	Falla física	2	Poco frecuente
		A003	Error de usuarios	2	Poco frecuente
		A008	Error de mantenimiento	2	Poco frecuente
		A009	Falta de recursos	2	Poco frecuente
		A010	Incendio	2	Poco frecuente
		A005	Falla física	2	Poco frecuente
		A003	Error de usuarios	5	Muy frecuente
EA002	Aires acondicionados	A008	Error de mantenimiento	2	Poco frecuente
		A009	Falta de recursos	2	Poco frecuente
		A014	Contaminación electromagnética	2	Poco frecuente
		A001	Corte de fluido eléctrico	3	Normal
		A016	Acceso no autorizado	2	Poco frecuente
		A010	Incendio	2	Poco frecuente
		A005	Falla física	2	Poco frecuente
EA003	Grupo electrógeno	A003	Error de usuarios	5	Muy frecuente
		A008	Error de mantenimiento	2	Poco frecuente
		A009	Falta de recursos	2	Poco frecuente
		A017	Indisponibilidad del personal	2	Poco frecuente
		A010	Incendio	2	Poco frecuente
		A018	Daños por agua	2	Poco frecuente
EA004	Cableado	A019	Contaminación eléctrica	2	Poco frecuente
		A008	Error de mantenimiento	2	Poco frecuente
		A016	Acceso no autorizado	2	Poco frecuente
		A017	Indisponibilidad del personal	2	Poco frecuente
		A018	Desastre natural	2	Poco frecuente
		A010	Incendio	2	Poco frecuente
I001	DataCenter	A019	Perdida de equipos	2	Poco frecuente
		A020	Robo	2	Poco frecuente
		A017	Indisponibilidad del personal	2	Poco frecuente
		A008	Error de mantenimiento	2	Poco frecuente
		A003	Error de usuarios	5	Muy frecuente
P001	Personal TI	A021	Divulgación de información	2	Poco frecuente
		A022	Extorción	2	Poco frecuente
		A023	Ingeniería Social	2	Poco frecuente
		A019	Contaminación eléctrica	2	Poco frecuente
P002	Adm. TI	A006	Climatización inadecuada	3	Normal
		A017	Indisponibilidad del personal	2	Poco frecuente

Como resultado tenemos lo siguiente:

Tabla 10: Valoración de amenazas porcentual.

Valoración	Cantidad	Porcentaje
Poco frecuente	85	73.28%
Normal	26	22.41%
Muy frecuente	5	4.31%
Total	116	100.00%

f) Estimación del riesgo.

A continuación, se muestra escala de valoración de estimación de los riesgos.

Mapa de Calor

PROBABILIDAD	IMPACTO					
		5	4	3	2	1
	5					
	4					
	3					
	2					
	1					

Tabla 11: Estimación de riesgo.

ESTIMACION DEL RIESGO.										
ACTIVO			AMENAZA		IMPACTO	PROBABILIDAD	COD. RIESGP	RIESGO	NIVEL	ESCALA CANTITATIVA
COD.	NOMBRE		COD.	NOMBRE						
S001	Sistema SISCO	contable	A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
			A002	Falla en las comunicaciones	2	3	R2	6	2	Bajo
			A003	Error de usuarios	2	2	R3	4	1	Despreciable
			A004	Falla de Sw	2	2	R4	4	1	Despreciable
A001	SysPreiVen		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
			A002	Falla en las comunicaciones	2	3	R2	6	2	Bajo
			A003	Error de usuarios	2	2	R3	4	1	Despreciable
			A004	Falla de Sw	2	2	R4	4	1	Despreciable
E001	Servidor de dominio		A005	Falla física	2	2	R5	4	1	Despreciable
			A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
			A002	Falla en las comunicaciones	2	3	R2	6	2	Bajo
			A006	Climatización inadecuada	3	3	R6	9	3	Apreciable
			A007	Vulnerabilidad del SW	3	3	R1	9	3	Apreciable
			A008	Error de mantenimiento	3	3	R9	9	3	Apreciable
			A009	Falta de recursos	3	5	R10	15	4	Importante
			A010	Incendio	2	2	R7	4	1	Despreciable
			A005	Falla física	3	5	R5	15	4	Importante
			A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
E002	Servidor de Ad		A002	Falla en las comunicaciones	2	3	R2	6	2	Bajo
			A006	Climatización inadecuada	2	2	R6	4	1	Despreciable
			A007	Vulnerabilidad del SW	2	2	R3	4	1	Despreciable
			A008	Error de mantenimiento	3	3	R9	9	3	Apreciable
			A009	Falta de recursos	3	3	R1	9	3	Apreciable
			A010	Incendio	2	2	R7	4	1	Despreciable
			A010	Incendio	2	2	R7	4	1	Despreciable
			A005	Error de mantenimiento	4	4	R3	16	5	Crítico
E003	Servidor de Base de datos		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
			A011	Falla de servidor de comunicaciones	2	3	R2	6	2	Bajo
			A012	Error del administrador	3	5	R8	15	4	Importante
			A008	Error de mantenimiento	3	5	R9	15	4	Importante

E004	Servidor de Aplicaciones	A005	Falla física	3	3	R5	9	3	Apreciable
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A002	Falla en las comunicaciones	2	3	R2	6	2	Bajo
		A006	Climatización inadecuada	2	2	R6	4	1	Despreciable
		A007	Vulnerabilidad del SW	2	2	R3	4	1	Despreciable
		A008	Error de mantenimiento	3	3	R9	9	3	Apreciable
		A009	Falta de recursos	3	5	R10	15	4	Importante
E005	Servidor de respaldo	A010	Incendio	2	2	R7	4	1	Despreciable
		A005	Falla física	3	5	R5	15	4	Importante
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A002	Falla en las comunicaciones	2	3	R2	6	2	Bajo
		A006	Climatización inadecuada	2	3	R6	6	2	Bajo
		A007	Vulnerabilidad del SW	2	3	R2	6	2	Bajo
		A009	Falta de recursos	3	5	R10	15	4	Importante
E006	Servidor proxy	A008	Error de mantenimiento	4	4	R9	16	5	Crítico
		A010	Incendio	2	3	R7	6	2	Bajo
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	3	5	R5	15	4	Importante
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A011	Falla de servidor de comunicaciones	2	3	R2	6	2	Bajo
		A012	Error del administrador	3	5	R8	15	4	Importante
E007	Switch Acceso	A013	Error de configuración	3	5	R11	15	4	Importante
		A009	Falta de recursos	3	5	R10	15	4	Importante
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	2	3	R5	6	2	Bajo
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A011	Falla de servidor de comunicaciones	2	3	R2	6	2	Bajo
		A012	Error del administrador	3	5	R8	15	4	Importante
E008	Router	A013	Error de configuración	2	3	R11	6	2	Bajo
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	2	3	R5	6	2	Bajo
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A011	Falla de servidor de comunicaciones	2	3	R2	6	2	Bajo
		A012	Error del administrador	3	5	R8	15	4	Importante
		A013	Error de configuración	3	5	R11	15	4	Importante
R001	Internet	A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	3	5	R5	15	4	Importante
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A006	Climatización inadecuada	3	5	R6	15	4	Importante
		A012	Error del administrador	3	5	R8	15	4	Importante
		A013	Error de configuración	3	5	R11	15	4	Importante
		A010	Incendio	2	3	R7	6	2	Bajo
R002	Wifi	A005	Falla física	3	5	R5	15	4	Importante
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A012	Pérdida de equipos	2	3	R14	6	2	Bajo
		A013	Denegación de servicios	3	5	R12	15	4	Importante
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	3	5	R5	15	4	Importante
		A013	Degradación de los soportes	3	5	R13	15	4	Importante
S001	Cintas Backup	A003	Error de usuarios	3	5	R3	15	4	Importante
		A012	Pérdida de equipos	3	5	R14	15	4	Importante
		A014	Robo	2	3	R2	6	2	Bajo
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	2	3	R5	6	2	Bajo
		A013	Degradación de los soportes	3	5	R13	15	4	Importante
		A003	Error de usuarios	3	5	R3	15	4	Importante
S002	HDD ext	A012	Pérdida de equipos	2	3	R14	6	2	Bajo
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	3	5	R5	15	4	Importante
		A003	Error de usuarios	3	5	R3	15	4	Importante
		A008	Error de mantenimiento	3	5	R9	15	4	Importante
		A009	Falta de recursos	3	5	R10	15	4	Importante
		A010	Incendio	2	3	R7	6	2	Bajo
EA001	Ups	A005	Falla física	2	3	R5	6	2	Bajo
		A003	Error de usuarios	3	5	R3	15	4	Importante
		A008	Error de mantenimiento	3	5	R9	15	4	Importante
EA002	Aires acondicionados	A009	Falta de recursos	3	5	R10	15	4	Importante
		A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	2	3	R5	6	2	Bajo
		A003	Error de usuarios	3	5	R3	15	4	Importante

		A008	Error de mantenimiento	3	5	R9	15	4	Importante
		A009	Falta de recursos	3	5	R10	15	4	Importante
		A014	Contaminación electromagnética	2	3	R2	6	2	Bajo
		A001	Corte de fluido eléctrico	3	3	R1	9	3	Apreciable
		A016	Acceso no autorizado	3	5	R15	15	4	Importante
EA003	Grupo electrógeno	A010	Incendio	2	3	R7	6	2	Bajo
		A005	Falla física	3	5	R5	15	4	Importante
		A003	Error de usuarios	3	5	R3	15	4	Importante
		A008	Error de mantenimiento	3	5	R9	15	4	Importante
		A009	Falta de recursos	3	5	R10	15	4	Importante
		A017	Indisponibilidad del personal	3	5	R22	15	4	Importante
		A010	Incendio	2	3	R7	6	2	Bajo
EA004	Cableado	A018	Daños por agua	2	3	R16	6	2	Bajo
		A019	Contaminación eléctrica	2	3	R2	6	2	Bajo
		A008	Error de mantenimiento	4	4	R9	16	5	Crítico
		A016	Acceso no autorizado	3	5	R15	15	4	Importante
		A017	Indisponibilidad del personal	3	5	R22	15	4	Importante
		A018	Desastre natural	2	3	R2	6	2	Bajo
I001	DataCenter	A010	Incendio	2	3	R7	6	2	Bajo
		A019	Perdida de equipos	2	3	R14	6	2	Bajo
		A020	Robo	2	3	R17	6	2	Bajo
		A017	Indisponibilidad del personal	3	5	R22	15	4	Importante
		A008	Error de mantenimiento	4	4	R9	16	5	Crítico
P001	Personal TI	A003	Error de usuarios	3	5	R3	15	4	Importante
		A021	Divulgación de información	2	3	R19	6	2	Bajo
		A022	Extorción	2	3	R18	6	2	Bajo
		A023	Ingeniería Social	2	3	R20	6	2	Bajo
P002	Adm. TI	A019	Contaminación eléctrica	2	3	R21	6	2	Bajo
		A006	Climatización inadecuada	3	5	R6	15	4	Importante
		A017	Indisponibilidad del personal	3	5	R22	15	4	Importante

g) Tratamiento de riesgos

Para esta etapa únicamente se tratarán aquellos riesgos cuyo resultado es importante o crítico.

Tabla 12: Tratamiento de riesgo.

ESTIMACION DEL RIESGO.					ESCALA CUANTITATIVA	TRATAMIENTO DE RIESGO					
ACTIVO		AMENAZA		SALVAGUARDA							
COD.	NOMBRE	COD.	NOMBRE	COD		NOMBRE	DESCRIPCIÓN	TIPO		EFECTO	
								COD	NOMBRE		
E001	Servidor dominio	de	A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
E002	Servidor de Ad		A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
E003	Servidor de Base de datos		A005	Error de mantenimiento	Crítico	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo
			A012	Error del administrador	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
			A008	Error de mantenimiento	Importante	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo
E004	Servidor Aplicaciones	de	A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
E005	Servidor respaldo	de	A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
			A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
			A008	Error de mantenimiento	Crítico	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo
			A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo

		A012	Error del administrador	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
		A013	Error de configuración	Importante	T005	Manuales	Implementar manuales de configuración de equipos y sus respectivas actualizaciones	PR	Preventivo	Preventivo
		A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
E007	Switch Acceso	A012	Error del administrador	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
E008	Router	A012	Error del administrador	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
		A013	Error de configuración	Importante	T005	Manuales	Implementar manuales de configuración de equipos y sus respectivas actualizaciones	PR	Preventivo	Preventivo
R001	Internet	A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
		A006	Climatización inadecuada	Importante	T006	Plan de mantenimiento	Implementar plan de mantenimiento y control de climatización del centro de datos	PR	Preventivo	Preventivo
		A012	Error del administrador	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
		A013	Error de configuración	Importante	T005	Manuales	Implementar manuales de configuración de equipos y sus respectivas actualizaciones	PR	Preventivo	Preventivo
R002	Wifi	A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
		A013	Denegación de servicios	Importante	T007	Control de red	Implementar mecanismos de control de la red de datos.	PR	Preventivo	Preventivo
S001	Cintas Backup	A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
		A013	Degradación de los soportes	Importante	T008	Contingencia de soporte	Mantener una lista de empresas para soporte o mecanismo de cambio de equipamiento	PR	Preventivo	Preventivo
		A003	Error de usuarios	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo

		A012	Pérdida de equipos	Importante	T009	Mecanismos de control de bienes	Implementar mecanismos de control de bienes respecto al traslado y asignación	PR	Preventivo	Preventivo
		A013	Degradación de los soportes	Importante	T008	Contingencia de soporte	Mantener una lista de empresas para soporte o mecanismo de cambio de equipamiento	PR	Preventivo	Preventivo
		A003	Error de usuarios	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
		A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
S002	HDD ext	A003	Error de usuarios	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
		A008	Error de mantenimiento	Importante	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo
		A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
		A003	Error de usuarios	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
EA002	Aires acondicionados	A008	Error de mantenimiento	Importante	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo
		A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
		A016	Acceso no autorizado	Importante	T010	Plan de asignación de accesos	Implementar roles, responsabilidades y control de usuarios	PR	Preventivo	Preventivo
		A005	Falla física	Importante	T002	Verificación permanente	Implementar políticas y procedimientos de verificación programada de recursos y características de los servidores	PR	Preventivo	Preventivo
		A003	Error de usuarios	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
EA003	Grupo electrógeno	A008	Error de mantenimiento	Importante	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo
		A009	Falta de recursos	Importante	T001	Aseguramiento de recursos	Implementar en el POI la adquisición de recursos o la compra de nuevos equipos.	PR	Preventivo	Preventivo
		A017	Indisponibilidad del personal	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
EA004	Cableado	A008	Error de mantenimiento	Crítico	T003	Plan de mantenimiento	Implementar plan de mantenimiento preventivo y correctivo de servidores	PR	Preventivo	Preventivo

		A016	Acceso no autorizado	Importante	T010	Plan de asignación de accesos	Implementar roles, responsabilidades y control de usuarios	PR	Preventivo	Preventivo
		A017	Indisponibilidad del personal	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
I001	DataCenter	A017	Indisponibilidad del personal	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
		A008	Error de mantenimiento	Crítico	T006	Plan de mantenimiento	Implementar plan de mantenimiento y control de climatización del centro de datos	PR	Preventivo	Preventivo
P001	Personal TI	A003	Error de usuarios	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo
P002	Adm. TI	A006	Climatización inadecuada	Importante	T006	Plan de mantenimiento	Implementar plan de mantenimiento y control de climatización del centro de datos	PR	Preventivo	Preventivo
		A017	Indisponibilidad del personal	Importante	T004	Capacitación y verificación	Implementar planes de capacitaciones permanentes y planes de control de procedimientos	PR	Preventivo	Preventivo

1.1.1. Metodología Octave.

a) Fase 1: Compilación de perfiles de amenazas basado en activos

○ Proceso S1: Identificación de información de la empresa.

▪ S1.1 - Criterios de evaluación de impacto

Tabla 13: Criterios de evaluación de impacto.

Tipo Impacto	Muy bajo	Bajo	Medio	Alto	Muy alto
Reputación	Afectación mínima, poco o nada de esfuerzo para la mejora	Poco esfuerzo para mejorar	Esfuerzo regular para mejorar	Mucho esfuerzo requerido	Irremediable.
Costos operativos	Aumento anual de < 1%	Aumento <= 5 % anual	Aumento = 5 % anual	Aumento = 10 % anual	Aumento > 10 % anual
Carga laboral	Aumento de carga < 10% en 1 mes	Aumento de carga = 30% en 1 mes	Aumento de carga = 50% en 1 mes	Aumento de carga = 70% en 1 mes	Aumento de carga = 100% en 1 mes
Interrupción de servicio	Interrupción < 4 horas	Interrupción entre 5 y 10 horas	Interrupción entre 11 y 16 horas	Interrupción entre 16 y 24 horas	Interrupción superior a 36 horas
Administración	Puede impedir casi nada	Puede impedir un poco	Puede impedir regular	Puede impedir totalmente	Puede impedir y llegar al cierre
Vida	No existe amenazas	Amenaza mínima	Puede afectar la vida, con recuperación rápida	Con recuperación lenta	Perdida de vida
Salud	Incapacidad < 2 días	Incapacidad entre 3 y 7 días	Incapacidad entre 8 y 15 días	Incapacidad entre 16 y 28 días	Incapacidad > 28 días
Multas	No genera	Genera, pero no significativas	Llamada de atención	Significativas	Sanciones económicas, legales

Todos los niveles de evaluación se efectúan con la participación activa de los usuarios involucrados y sus propios criterios como dueños de los activos.

▪ S1.2 – Identificación de los activos

Tabla 14: Identificación de activos.

COD	SISTEMA	INFORMACIÓN	APLICACIONES Y SERVICIOS	OTROS
S001	Sistema contable SICON	Nominas, planillas, debes, haberes, gastos, pagos de servicios, etc	Sistema contable	Servidor de aplicaciones, equipos de comunicación, terminales
A001	SysPreiVen	Ventas, registros de clientes, mercancías, etc.	Sistema de ventas	Servidor de aplicaciones, equipos de comunicación, terminales
E001	Servidor de dominio		Internet	Internet, UPS, Sistemas O. Firewall, equipos de comunicación.
E002	Servidor de Ad		Internet	Internet, UPS, Sistemas O.

E003	Servidor de Base de datos		Internet	Firewall, equipos de comunicación. Internet, UPS, Sistemas O.
E004	Servidor de Aplicaciones		Internet	Firewall, equipos de comunicación. Internet, UPS, Sistemas O.
E005	Servidor de respaldo		Internet	Firewall, equipos de comunicación. Internet, UPS, Sistemas O.
E006	Servidor proxy		Internet	Firewall, equipos de comunicación. Internet, UPS, Sistemas O.
E007	Switch Acceso		Internet	Cableado
E008	Router		Internet	Cableado
R001	Internet		Internet	
R002	Wifi		Internet	Sistema eléctrico
S001	Cintas Backup	Dispositivos de respaldo		
S002	HDD ext	Dispositivos de almacenamiento		
S003	Sistema eléctrico	Sistema de cables, tableros, etc		
EA001	Ups	Respaldo de alimentación eléctrica		
EA002	Aires acondicionados	Mantenimiento de climatización		
EA003	Grupo electrógeno	Respaldo eléctrico		
EA004	Cableado	Interconexión		
I001	DataCenter	Espacio de trabajo		
P001	Personal TI			Personal
P002	Adm. TI			Personal

▪ S1.3 – Evaluar las prácticas de Seguridad de la organización

Evaluación de prácticas de seguridad

Tabla 15: Evaluación de prácticas de seguridad.

Descripción	Seguridad, entrenamiento									
	¿En qué nivel esta afirmación se refleja en la empresa?				¿Qué está haciendo bien su empresa en esta área?	¿Qué NO está haciendo bien su empresa en esta área?	¿Cuál es el nivel de efectividad de la implementación de las prácticas en esta área?			
El personal conoce sus roles de seguridad y está documentada y verificado	SI	ALGO	NO	NO SABE	No se posee la cultura de divulgación de información	Tiempo de adecuación en los roles y responsabilidades asignadas	Rojos	Amarillo	Verde	NO aplica
Existe suficiente experiencia interna para todos los servicios y está documentada y verificado	SI	ALGO	NO	NO SABE	Las funciones se encuentran definidas	Carencia de documentación de procedimientos				
Existe la presencia de	SI	ALGO	NO	NO SABE	Capacitaciones regulares	Capacitación poco frecuente				

Tabla 16: Estrategias de seguridad.

Estrategias de seguridad - ES										
Descripción	¿En qué nivel esta afirmación se refleja en la empresa?				¿Qué está haciendo bien su empresa en esta área?	¿Qué NO está haciendo bien su empresa en esta área?	¿Cuál es el nivel de efectividad de la implementación de las prácticas en esta área?			
Las ES incorporan consideraciones de seguridad	SI	ALGO	NO	NO SABE		Presentan consideraciones de forma parcial.	Rojo	Amarillo	Verde	NO aplica
Las ES y políticas se basan en objetivos del negocio.	SI	ALGO	NO	NO SABE		No alineados estrechamente a los objetivos				
Las ES metas y objetivos se encuentran documentados	SI	ALGO	NO	NO SABE		Carencia de documentación detallada				

Tabla 17: Gestión de seguridad.

Gestión de seguridad - GS										
Descripción	¿En qué nivel esta afirmación se refleja en la empresa?				¿Qué está haciendo bien su empresa en esta área?	¿Qué NO está haciendo bien su empresa en esta área?	¿Cuál es el nivel de efectividad de la implementación de las prácticas en esta área?			
Se asignan fondos para actividades de GS	SI	ALGO	NO	NO SABE		No se asignan fondos.	Rojo	Amarillo	Verde	NO aplica
Los roles y responsabilidades de Gs están definidos para todos	SI	ALGO	NO	NO SABE		No se definen para todos				
Las contrataciones y culminación laboral cuentan con GS	SI	ALGO	NO	NO SABE		No se cuenta con mecanismos de GS				
Se gestionan los riesgos de seguridad de Información.	SI	ALGO	NO	NO SABE		No se gestionan.				

Políticas y regulaciones

Tabla 18: Políticas y regulaciones.

Políticas y regulaciones - PR											
Descripción	¿En qué nivel esta afirmación se refleja en la empresa?				¿Qué está haciendo bien su empresa en esta área?	¿Qué está haciendo bien su empresa en esta área?	NO	¿Cuál es el nivel de efectividad de la implementación de las prácticas en esta área?			
Se cuenta con políticas actuales	SI	ALGO	NO	NO SABE		NO se cuenta		Rojó	Amarillo	Verde	NO aplica
Se cuenta con procedimientos	SI	ALGO	NO	NO SABE		No se cuenta					
Se cuenta con políticas y/o procedimientos para evaluación de PR	SI	ALGO	NO	NO SABE		No se cuenta					
Se refuerzan policiacas de forma periódica	SI	ALGO	NO	NO SABE		No se cuenta					

Plan de seguridad y recuperación

Tabla 19: Plan de seguridad y recuperación.

Plan de recuperación y desastres - PRAD											
Descripción	¿En qué nivel esta afirmación se refleja en la empresa?				¿Qué está haciendo bien su empresa en esta área?	¿Qué está haciendo bien su empresa en esta área?	NO	¿Cuál es el nivel de efectividad de la implementación de las prácticas en esta área?			
Se posee el análisis operacional y de aplicaciones críticas	SI	ALGO	NO	NO SABE		NO se cuenta		Rojó	Amarillo	Verde	NO aplica
Se cuenta con documentación aprobada sobre PRAD	SI	ALGO	NO	NO SABE		No se cuenta					

Control de acceso físico.

Tabla 20: Control de acceso físico.

Control de acceso físico - CAS										
Descripción	¿En qué nivel esta afirmación se refleja en la empresa?				¿Qué está haciendo bien su empresa en esta área?	¿Qué NO está haciendo bien su empresa en esta área?	¿Cuál es el nivel de efectividad de la implementación de las prácticas en esta área?			
Los planes de seguridad física y sus restricciones están documentadas.	SI	ALGO	NO	NO SABE		No se cuenta	Rojo	Amarillo	Verde	NO aplica
Se cuenta con regulaciones para visitantes	SI	ALGO	NO	NO SABE		No se cuenta				
Se cuenta con procedimiento para el acceso físico a las áreas de trabajo	SI	ALGO	NO	NO SABE		NO se cuenta				
Los componentes se encuentran salvaguardados	SI	ALGO	NO	NO SABE		No se encuentran salvaguardados				

○ **Proceso S2: Perfiles de las amenazas.**

▪ **S2.1 – Activos críticos**

Tabla 21: Activos críticos.

COD	ACTIVO	DESCRIPCIÓN
A1	Sistema contable	Es el sistema que gestiona todas las operaciones contables de la empresa
A2	Servidor de base de datos	Contiene información de los sistemas
A3	Firewall	Gestiona las peticiones de red
A4	Adm TI	Personal encargado de gestionar el área de TI

Descripción de activos críticos

Tabla 22: Descripción de activos críticos.

Activo	Razón de selección
Servidor de base de datos	Es la ubicación donde se almacena toda la información de los sistemas que se utilizan en la organización, que es indispensable para su funcionamiento.

▪ **S2.2 – Requisitos de seguridad.**

- **Confidencialidad:** Únicamente personal con autorización puede gestionar el servidor
- **Integridad:** Las modificaciones o alteraciones de información deben ejecutarse previo permiso.
- **Disponibilidad:** El servidor debe estar disponible durante el desarrollo de las actividades.

▪ S2.3 – Identificar amenazas de los activos críticos.

AMENAZA		ACTORES DE AMENAZA		MOTIVO																																		
¿Para cual rama existe una posibilidad no despreciable de amenaza? ¿Para cual rama restante hay una posibilidad despreciable o nula de amenaza?		¿Qué actores representan las mayores amenazas?		¿Que tan fuerte es el motivo? ¿Que tanto confia de la estimación?																																		
ACTIVO	ACCESO	ACTOR	MOTIVO	RESULTADO																																		
Sistema contable	Físico	Adentro	Accidental	Revelación Modificación Pérdida Interrupción	Persona que actua de forma accidental	<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>																																
Intencional	Revelación Modificación Pérdida Interrupción	Persona que actua de forma intensional	<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>																																			
Afuera	Accidental	Revelación Modificación Pérdida Interrupción	Persona externo que actua de forma accidental	<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>																																		
	Intencional	Revelación Modificación Pérdida Interrupción	Persona externo que actua de forma intensional	<table border="1"> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> <tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr> </table>																																		

b) Fase 2: Identificación de vulnerabilidades

a. Proceso S3: Examinar la infraestructura de TI con los activos.

▪ S3.1 – Examinar rutas de acceso

SISTEMA DE INTERES			
¿Que sistemas estan relacionados con el activo critico?			
Activos virtuales y acceso remoto			
SISTEMA DE INTERES	PUNTOS DE ACCESO	ACCESO AL SISTEMA	ALMACENAMIENTO
¿Cual de los componentes son parte del sistema de interes?	¿Cual de los componentes son utilizados para transferir informacion y cuales sirven de puntos de acceso?	¿Cual de los componentes son utilizados por el personal para el acceso?	¿Cual de los componentes son utilizados para almacenamiento?
☐ Servidor ☐ Redes internas ☐ Estacion de trabajo ☐ Otros	☐ Redes internas ☐ Redes externas ☐ otros ☐	☐ Estación de trabajo ☐ Laptops ☐ Estacion de trabajo desde fuera ☐ Otros	☐ Discos externos - respaldo ☐ Otros

▪ S3.2 – Identificar y analizar los riesgos

AMENAZA					IMPACTO				
ACTIVO	ACCESO	ACTOR	MOTIVO	RESULTADO	REPUTACIÓN	PRODUCTIVIDAD	MULTAS Y PENAS LEGALES	SEGURIDAD	FINANCERA
Activos virtuales y acceso remoto	Red	Adentro	Accidental	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	medio	bajo	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	medio	bajo	bajo	bajo	bajo
			Intencionado	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo
		Afuera	Accidental	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	medio	bajo	bajo	bajo
				Interrupción	bajo	medio	bajo	bajo	bajo
			Intencionado	Revelación	bajo	bajo	bajo	bajo	bajo
				Modificación	bajo	medio	bajo	bajo	bajo
				Pérdida	bajo	bajo	bajo	bajo	bajo
				Interrupción	bajo	bajo	bajo	bajo	bajo

CAPÍTULO V

RESULTADOS Y DISCUSIÓN

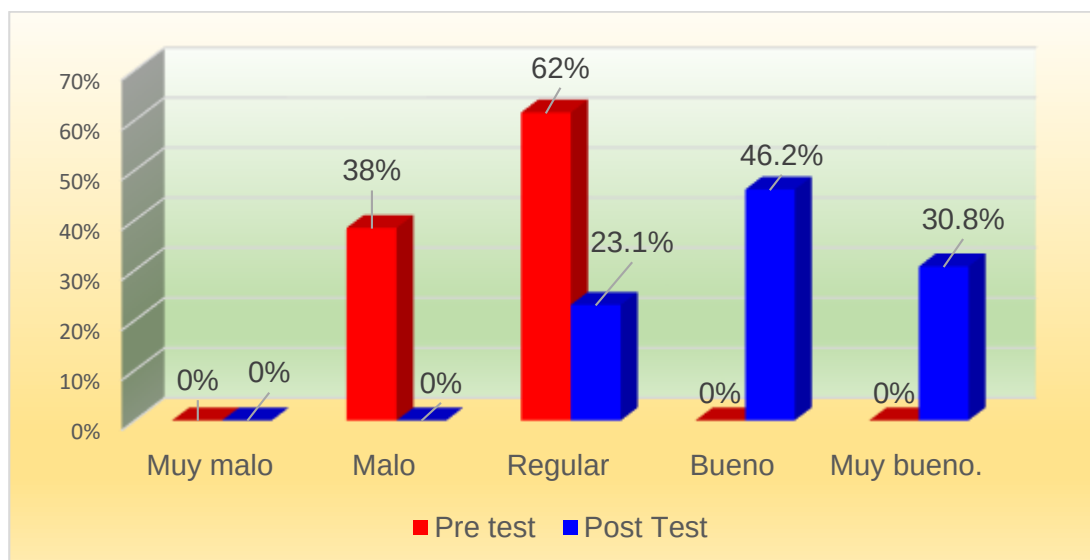
5.1. Procesamiento de datos del objetivo general

Tabla 23: Distribución de frecuencia del objetivo aplicando la metodología octave para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

Gestión de redes de comunicaciones	Pre test		Post Test	
	Frecuencia	Porcentajes	Frecuencia	Porcentajes
Muy malo	0	0%	0	0%
Malo	5	38%	0	0%
Regular	8	62%	3	23.1%
Bueno	0	0%	6	46.2%
Muy bueno.	0	0%	4	30.8%
Total	13	100%	13	100%

Nota. Datos obtenidos en el pre y post test y registrados en una base de datos.

Figura 1: Barras porcentuales del objetivo general aplicando la metodología octave para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.



Nota. Tabla 1

La tabla y figura 1, evidencia que, tras la implementación de la metodología OCTAVE, la gestión de redes de comunicaciones, experimentó una mejora significativa, ya que en el pre test predominaban evaluaciones negativas con un 38% en la categoría "Malo" y un 62% en la categoría "Regular", mientras que, en el post test, dichas categorías disminuyeron

drásticamente, desapareciendo por completo la primera y reduciéndose la segunda al 23.1%; además, surgieron resultados positivos, destacándose un 46.2% en la categoría "Bueno" y un 30.8% en la categoría "Muy Bueno".

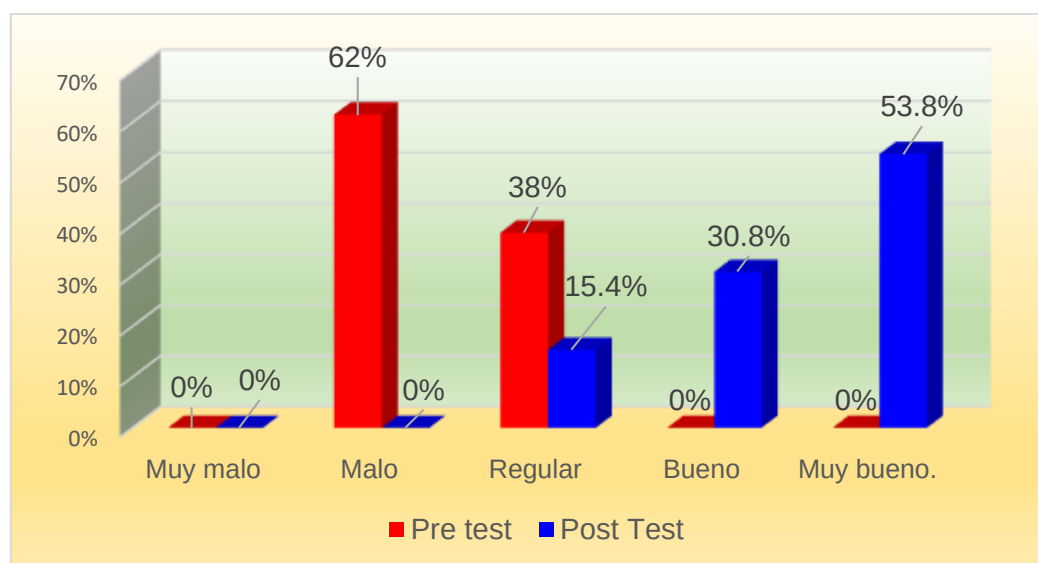
5.1.1. Procesamiento de datos del primer objetivo específico

Tabla 24: Distribución de frecuencia del objetivo específico efectuando la adecuación de las características de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimac S.A.C.

Procesos	Pre test		Post Test	
	Frecuencia	Porcentajes	Frecuencia	Porcentajes
Muy malo	0	0%	0	0%
Malo	8	62%	0	0%
Regular	5	38%	2	15.4%
Bueno	0	0%	4	30.8%
Muy bueno.	0	0%	7	53.8%
Total	13	100%	13	100%

Nota. Datos obtenidos en el pre y post test y registrados en una base de datos.

Figura 2: Barras porcentuales del objetivo específico efectuando la adecuación de las características de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimac S.A.C.



Nota. Tabla 2

El análisis estadístico presentado en la tabla y figura 2 refleja un impacto positivo en la implementación de la metodología OCTAVE para mejorar la gestión de redes de comunicaciones. Antes de la intervención, los resultados del pre test mostraron una predominancia de procesos deficientes, con un 62% de las evaluaciones categorizadas como "Malo"

y un 38% como "Regular", destacando claramente las debilidades estructurales y operativas iniciales en la gestión. Sin embargo, los resultados del post test revelan una redistribución significativa hacia categorías superiores, eliminándose por completo la categoría "Malo" y reduciéndose "Regular" al 15.4%. De manera destacable, emergen las categorías "Bueno" y "Muy Bueno", alcanzando un 30.8% y un 53.8%, respectivamente.

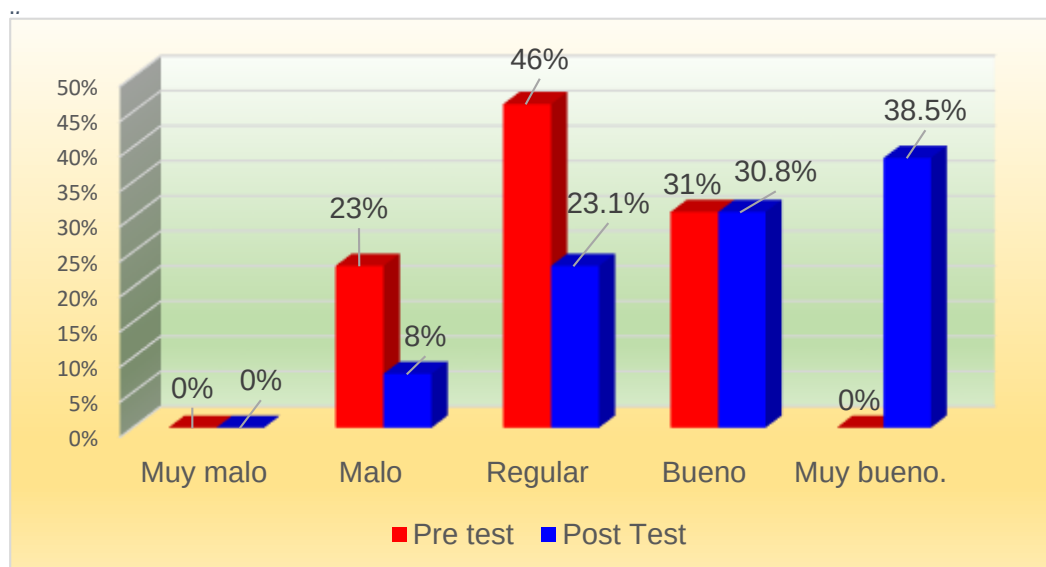
5.1.2. Procesamiento de datos del segundo objetivo específico

Tabla 25: Distribución de frecuencia del objetivo específico monitorear de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

Monitoreo	Pre test		Post Test	
	Frecuencia	Porcentajes	Frecuencia	Porcentajes
Muy malo	0	0%	0	0%
Malo	3	23%	1	8%
Regular	6	46%	3	23.1%
Bueno	4	31%	4	30.8%
Muy bueno.	0	0%	5	38.5%
Total	13	100%	13	100%

Nota. Datos obtenidos en el pre y post test y registrados en una base de datos.

Figura 3: Barras porcentuales del objetivo específico monitores de los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C



Nota. Tabla 3

El análisis de los resultados estadísticos presentados en la tabla y figura 3, evidencia que la metodología OCTAVE, fue diseñada para optimizar la gestión de redes de comunicaciones en la empresa constructora Preimac S.A.C. Inicialmente, en el pre test, se observa que un 23% de las evaluaciones fueron clasificadas como "Malo" y un 46% como "Regular", mientras que solo un 31% alcanzaron la categoría "Bueno" y no se registraron resultados en las categorías superiores. Sin embargo, los resultados del post test revelan un progreso notable, evidenciado por la eliminación casi total de la categoría "Malo", que se reduce al 8%, así como por la disminución de la categoría "Regular" al 23.1%. Paralelamente, se mantiene un 30.8% en la categoría "Bueno" y emerge un significativo 38.5% en la categoría "Muy Bueno", lo que demuestra una mejora integral en el monitoreo de los procesos.

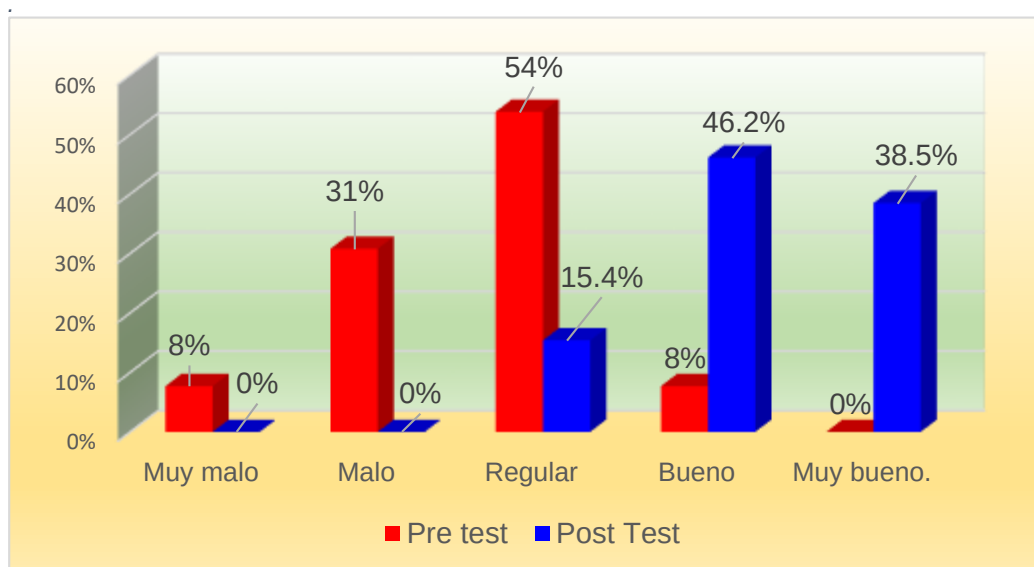
5.1.3. Procesamiento de datos del tercer objetivo específico

Tabla 26: Distribución de frecuencia del objetivo específico asegurando los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimac S.A.C.

Seguridad	Pre test		Post Test	
	Frecuencia	Porcentajes	Frecuencia	Porcentajes
Muy malo	1	8%	0	0%
Malo	4	31%	0	0%
Regular	7	54%	2	15.4%
Bueno	1	8%	6	46.2%
Muy bueno.	0	0%	5	38.5%
Total	13	100%	13	100%

Nota. Datos obtenidos en el pre y post test y registrados en una base de datos.

Figura 4: Barras porcentuales del objetivo específico asegurando los procesos para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C



Nota. Tabla 4

El análisis de los datos estadísticos presentados en la tabla y figura 4, refleja una evolución sustancial en la seguridad de los procesos tras la implementación de la metodología OCTAVE, diseñada para optimizar la gestión de redes de comunicaciones en la empresa constructora Preimaq S.A.C. En el pre test, se observaba una predominancia de debilidades en los procesos, con un 8% de las evaluaciones en la categoría "Muy Malo", un 31% en "Malo" y un 54% en "Regular", dejando en evidencia deficiencias importantes en el enfoque inicial hacia la gestión de la seguridad. Por el contrario, los resultados del post test muestran un avance significativo, evidenciado por la completa eliminación de las categorías "Muy Malo" y "Malo", así como por la reducción de la categoría "Regular" al 15.4%, lo que denota una clara disminución en los niveles de riesgo. Además, se observa un aumento considerable en las categorías superiores, con un 46.2% de las evaluaciones clasificadas como "Bueno" y un 38.5% en "Muy Bueno",

lo que refleja una consolidación en las capacidades de protección, control y mitigación de riesgos.

5.2. Prueba de hipótesis

El análisis de una hipótesis estadística se describe como un procedimiento orientado a verificar una presunción en el ámbito de la estadística. Este método, caracterizado por su enfoque sistemático en la toma de decisiones, permite evaluar la validez de dos postulados opuestos: por un lado, la hipótesis nula, conocida como H_0 , y, por el otro, la hipótesis alternativa, denominada H_1 . Este proceso reflexivo encuentra su base en un examen exhaustivo de los datos recabados de un conjunto representativo de elementos seleccionados aleatoriamente dentro de la población objeto de estudio. De esta forma, se busca determinar, con precisión metodológica, si se debe aceptar o rechazar la premisa inicial expresada en la hipótesis nula (Córdova Zamora , 2003, pág. 432).

Asimismo, se establecen procedimientos destinados a demostrar la validez de la hipótesis en cuestión, conforme a lo señalado por (Agurto Mejía & Alvarado Pintado , 2009 , pág. 518)

- 1) Plantear la hipótesis nula y la hipótesis alternativa.
- 2) Seleccionar el nivel de significancia.
- 3) Calcular el valor estadístico de prueba.
- 4) Formular la regla de decisión.
- 5) Tomar una decisión.

5.2.1. Prueba de la hipótesis general

1. Establecer la hipótesis nula y la hipótesis alternativa:

H_0 : La aplicación de la metodología octave no mejora la gestión de

redes de comunicaciones de la empresa constructora Preimaq S.A.C.

H₁: La aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

2. Seleccionar los niveles de significación

El margen de error es del 5% $\alpha = 0.05$

Nota: Este proceso no se considera en las demás pruebas de hipótesis debido que tendrá el mismo valor.

3. Seleccionar la prueba estadística

Se realizó un estudio transversal y se aplicó la prueba de Prueba de t de Student.

La prueba de Normalidad menciona que se debe corroborar que la variable aleatoria en ambos grupos se distribuya normalmente. Para ellos se utilizó la prueba de **Shapiro- Wilk** por que el tamaño de la muestra es menor que 50. El criterio para determinar si la (VA) se distribuye normalmente es:

- a) **P- valor $\geq \alpha$, aceptar la H₀** = los datos provienen de una distribución normal.
- b) **P- valor $< \alpha$, aceptar la H₁** = los datos no provienen de una distribución normal.

Nota: Este proceso no se considera en las demás hipótesis debido a que siempre es la misma.

Tabla 27: Prueba de normalidad de las hipótesis

Prueba de Normalidad		Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre test	Gestión de redes de comunicaciones	0.939	13	0.446
	Procesos	0.970	13	0.889
	Monitoreo	0.929	13	0.331
	Seguridad	0.953	13	0.643
Post test	Gestión de redes de comunicaciones	0.904	13	0.151
	Procesos	0.786	13	0.005
	Monitoreo	0.936	13	0.408
	Seguridad	0.876	13	0.063

Nota. Datos tomados del Cuestionario de Preguntas del pre y post test.

Tabla 28: Toma de decisión de la prueba de normalidad

PRUEBA DE NORMALIDAD

P- valor de la variable Gestión de redes de comunicaciones en el pre test =
 $0.446 > \alpha = 0.050$

P- valor de la variable Gestión de redes de comunicaciones en el post test
 $= 0.151 > \alpha = 0.050$

Conclusión: De acuerdo a la prueba de normalidad de La variable: Gestión de redes de comunicaciones se comporta normalmente, en el pre test y post test, por tanto, los datos provienen de una distribución normal, es por ello que se aplica la Prueba de t de Student.

Nota. tabla 5

Nota: Este proceso no se realizará en las demás hipótesis debido a que será la misma.

4. Formular la regla de decisión.

Tabla 29: Prueba de hipótesis general

Prueba de muestras emparejadas								
Diferencias emparejadas								
95% de intervalo de confianza de la diferencia								
		Desv.	Desv. Error			t	gl	Sig. (bilateral)
	Media	Desviación	promedio	Inferior	Superior			
Par 1	Gestión Pre - Gestión Post	- 1,43590	,72101	,19997	-1,87160 -1,00020	- 7,180	12	,000

Nota: Datos tomados del Cuestionario de Preguntas del pre y post test.

5. Toma de decisión

Sig. Asintótica (bilateral) = 0.000 < $\alpha = 0.05$

Lo que significa que se rechaza la hipótesis nula y se acepta la hipótesis alternativa lo que demuestra que la aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

5.2.2. Prueba de la primera hipótesis específica

1. Establecer la hipótesis nula y la hipótesis alternativa:

H₀: La aplicación de la metodología octave no mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

H₁: La aplicación de la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

2. Formular la regla de decisión.

Tabla 30: Prueba de la primera hipótesis específica

		Rangos		
		N	Rango promedio	Suma de rangos
Proceso Post - Proceso Pre	Rangos negativos	1 ^a	1,00	1,00
	Rangos positivos	12 ^b	7,50	90,00
	Empates	0 ^c		
	Total	13		

a. Proceso Post < Proceso Pre

b. Proceso Post > Proceso Pre

c. Proceso Post = Proceso Pre

Estadísticos de prueba^a

	Proceso Post - Proceso Pre
Z	-3,123 ^b
Sig. asintótica(bilateral)	,002

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

Nota: Datos tomados del Cuestionario de Preguntas del pre y post test.

3. Toma de decisión

Sig. Asintótica (bilateral) = 0.002 < $\alpha = 0.05$

Lo que significa que se rechaza la hipótesis nula y se acepta la hipótesis alternativa lo que demuestra que la aplicación de la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

5.2.3. Prueba de la segunda hipótesis específica

1. Establecer la hipótesis nula y la hipótesis alternativa:

H₀: La aplicación de la metodología octave no mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

H₁: La aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

2. Formular la regla de decisión.

Tabla 31: Prueba de la primera hipótesis específica

Prueba de muestras emparejadas									
		Diferencias emparejadas							
			Desv.	Desv. Error	95% de intervalo de confianza de la diferencia				Sig.
		Media	Desviación	promedio	Inferior	Superior	t	gl	(bilateral)
Par	Monitoreo Pre	-	,97031	,26912	-1,50943	-,33672	-	12	,005
1	- Monitoreo	,92308					3,430		
	Post								

Nota: Datos tomados del Cuestionario de Preguntas del pre y post test.

3. Toma de decisión

Sig. Asintótica (bilateral) = 0.005 < $\alpha = 0.05$

Lo que significa que se rechaza la hipótesis nula y se acepta la hipótesis alternativa lo que demuestra que la aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

5.2.4. Prueba de la tercera hipótesis específica

1. Establecer la hipótesis nula y la hipótesis alternativa:

H₀: La aplicación de la metodología octave no mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

H₁: La aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

2. Formular la regla de decisión.

Tabla 32: Prueba de la primera hipótesis específica

		Prueba de muestras emparejadas							
		Diferencias emparejadas							
				Desv. Error		95% de intervalo de confianza de la diferencia		t	Sig. (bilateral)
		Media	Desviación	promedio		Inferior	Superior		
Par	Seguridad	-	1,2647	,3508		-2,4181	-,8896	- 12	,001
1	Pre - Seguridad Post	1,6538						4,715	

Nota: Datos tomados del Cuestionario de Preguntas del pre y post test.

3. Toma de decisión

Sig. Asintótica (bilateral) = 0.001 < $\alpha = 0.025$

Lo que significa que se rechaza la hipótesis nula y se acepta la hipótesis alternativa lo que demuestra que la aplicación de la metodología OCTAVE mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

5.3. Discusión de resultados

Luego de haber demostrado la hipótesis general en la que se establece como una interpretación exhaustiva de los hallazgos obtenidos mediante la aplicación de la metodología OCTAVE en la empresa constructora Preimaq S.A.C. Se confirma que dicha metodología transformó la gestión de las redes de comunicación, evidenciando un cambio significativo en la calidad evaluativa. Las categorías negativas iniciales de "Malo" (38%) y "Regular" (62%) desaparecieron o disminuyeron drásticamente, dando lugar a evaluaciones positivas como "Bueno" (46.2%) y "Muy Bueno" (30.8%). Estos resultados reflejan una mejora contundente en la gestión, respaldada

por un análisis estadístico con una significancia asintótica bilateral de 0.000, lo que valida la hipótesis propuesta en el estudio.

En comparación con el antecedente proporcionado por Amador Donado (2022), su estudio sobre la adaptación de OCTAVE-S en la gestión de riesgos de seguridad en redes de información en Colombia muestra resultados consistentes con los de esta investigación. Amador concluyó que OCTAVE-S es una herramienta eficaz para identificar y gestionar riesgos de seguridad, beneficiando principalmente a entidades financieras. En este sentido, la presente investigación coincide en que la metodología OCTAVE potencia las capacidades organizacionales para mejorar la gestión integral de redes, aunque en un contexto más industrial y empresarial.

Ambos estudios se encuentran aparados en la metodología OCTAVE, según Allen-Addy (2023), es una metodología diseñada para evaluar vulnerabilidades y amenazas en el contexto operativo, priorizando los riesgos organizacionales sobre los técnicos. Este enfoque permite establecer un marco colaborativo entre diferentes sectores de la empresa, evaluando contingencias operativas, recursos tecnológicos y protocolos de seguridad. Con base en esta definición, el análisis realizado concluye que el impacto positivo de OCTAVE en la gestión de redes de Preimac S.A.C. no solo es significativo, sino que está alineado con las capacidades y objetivos inherentes a la metodología, consolidando su eficacia en contextos organizacionales diversos.

Asimismo, luego de comprobar que los resultados obtenidos en esta investigación evidencian una transformación significativa en la gestión de

procesos de las redes de comunicaciones de la empresa constructora Preimaq S.A.C. Antes de la implementación de la metodología OCTAVE, los procesos específicos presentaban graves deficiencias estructurales, con un 62% de evaluaciones en la categoría "Malo" y un 38% en "Regular". Posterior a la intervención, se registró una redistribución cualitativa notable: la categoría "Malo" fue eliminada completamente, la categoría "Regular" se redujo al 15.4%, mientras que las categorías "Bueno" y "Muy Bueno" alcanzaron un 30.8% y 53.8%, respectivamente. Este cambio fue validado mediante un análisis estadístico que arrojó una significancia asintótica bilateral de 0.002, valor que confirma la mejora en la gestión y valida la hipótesis planteada en esta tesis.

Comparativamente, el estudio realizado por Gastelo Fernández (2023) sobre la gestión de riesgos basado en la metodología MAGERIT en la Municipalidad Distrital de Cupisnique, Cajamarca, comparte similitudes con la presente investigación en cuanto al enfoque de mejora de procesos a través de metodologías estructuradas. Gastelo concluye que la aplicación de las fases de análisis y tratamiento de riesgos, sustentadas en un juicio experto y en la colaboración de los actores involucrados, resultó en una gestión más eficiente y participativa. Aunque la metodología utilizada fue distinta (MAGERIT en lugar de OCTAVE), ambos estudios destacan la importancia de implementar procedimientos metódicos para alcanzar mejoras significativas en la gestión.

Estos hallazgos se amparan cuando, la gestión de procesos en redes de comunicaciones se define como el conjunto de actividades sistemáticas destinadas a asegurar la operación eficiente y continua de la infraestructura

de red. Esto incluye tareas como la configuración de dispositivos, gestión de cambios, monitoreo, resolución de problemas y optimización del rendimiento. Según Esginnova Group (2021), el enfoque metodológico de OCTAVE permite no solo identificar y mitigar riesgos, sino también establecer un equilibrio funcional entre los recursos tecnológicos, las contingencias operativas y los parámetros de seguridad. Dicho marco conceptual sustenta los hallazgos de esta investigación, consolidando la efectividad de OCTAVE como una herramienta estratégica en la mejora de la gestión de procesos de redes de comunicaciones.

También luego de haber demostrado la segunda hipótesis específica de la presente investigación confirma que la aplicación de la metodología OCTAVE ha generado un impacto significativo en la gestión del monitoreo de redes de comunicaciones en la empresa constructora Preimac S.A.C. Inicialmente, el diagnóstico indicó la existencia de vulnerabilidades importantes en los procesos de monitoreo, con un 23% de evaluaciones calificadas como "Malo" y un 46% como "Regular", mientras que solo el 31% alcanzaba la categoría de "Bueno". Tras la implementación de OCTAVE, se evidenció una optimización sustancial en las evaluaciones: la categoría "Malo" se redujo drásticamente al 8%, "Regular" disminuyó al 23.1%, "Bueno" se mantuvo en un 30.8%, y emergió un 38.5% en la categoría "Muy Bueno". Este avance fue respaldado estadísticamente con una significancia asintótica bilateral de 0.005, corroborando que la hipótesis planteada –la mejora en la gestión de monitoreo de redes– es válida.

En comparación, el estudio desarrollado por Vásquez Atoche y Terrones Moncada (2023) en Ancash, titulado Mejora de los estándares de seguridad

ocupacional para reducir los accidentes mineros en una empresa minera de la región de Ancash, presenta similitudes metodológicas y de resultados. Este trabajo, de enfoque cuantitativo y tipo aplicado, evidenció que la implementación de estándares mejorados de seguridad ocupacional tuvo un efecto significativo en la reducción de accidentes. Aunque el contexto y la variable principal de ambas investigaciones difieren, en esencia, ambos estudios destacan la importancia de una metodología estructurada para optimizar procesos críticos: en el caso de Vásquez y Terrones, la seguridad ocupacional; en el caso de esta investigación, la gestión del monitoreo en redes de comunicaciones.

Amabas conclusiones se encuentran amparadas en la definición de la dimensión de monitoreo de redes de comunicaciones, según ESGinnova Group (2021), consiste en la supervisión constante de la infraestructura tecnológica para identificar eventos que puedan comprometer el rendimiento o la seguridad. Incluye actividades como la recopilación y análisis de datos sobre el tráfico de red, la evaluación del estado de dispositivos y la detección de anomalías. En el marco de la metodología OCTAVE, esta dimensión no solo garantiza la integridad del sistema, sino que también proporciona una base sólida para la toma de decisiones estratégicas en la gestión de riesgos. Los resultados de esta investigación reafirman que un enfoque metodológico en el monitoreo no solo mitiga vulnerabilidades, sino que también optimiza el desempeño general de las redes de comunicaciones.

Por último, en la demostración de la tercera hipótesis específica se demuestra que la implementación de la metodología OCTAVE ha generado

una mejora sustancial en la gestión de seguridad de las redes de comunicaciones de la empresa constructora Preimac S.A.C. Antes de la intervención, los diagnósticos reflejaban una situación preocupante, con un 8% de evaluaciones clasificadas como "Muy Malo", un 31% como "Malo" y un 54% como "Regular", lo cual evidenciaba vulnerabilidades críticas en la protección de los activos informáticos. Tras la aplicación de la metodología OCTAVE, los resultados mejoraron significativamente; las categorías "Muy Malo" y "Malo" fueron completamente eliminadas, y la categoría "Regular" se redujo al 15.4%. Además, se registró un aumento en las evaluaciones positivas: un 46.2% se ubicó en la categoría "Bueno" y un 38.5% en la categoría "Muy Bueno". Este cambio fue respaldado por el análisis estadístico, que arrojó una significancia asintótica bilateral de 0.001, confirmando que la metodología OCTAVE fortalece la gestión de seguridad en redes de comunicación.

En el marco de la comparación con estudios previos, se destaca el trabajo realizado por Pacheco (2022), titulado Seguridad en redes de comunicaciones: Perspectivas y desafíos. Este estudio realizado en Chile tuvo como objetivo analizar las técnicas actuales de protección en redes de comunicación y su impacto en la confidencialidad, integridad y disponibilidad de los datos. De tipo descriptivo y nivel exploratorio, la investigación utilizó como instrumento de análisis una revisión sistemática de literatura, abordando una muestra de artículos académicos recientes. Sus conclusiones coinciden con los hallazgos de esta investigación, pues demuestran que la aplicación de metodologías como OCTAVE refuerza la

seguridad de las redes de comunicación, evidenciando así la relevancia y aplicabilidad de esta metodología en diferentes contextos organizacionales. Por último, la variable de estudio, la seguridad de la información, constituye un componente esencial en el ámbito de las tecnologías de la información, al abarcar medidas, políticas y prácticas orientadas a proteger los datos contra accesos no autorizados, mal uso, divulgación, modificación o destrucción, garantizando tres pilares fundamentales: confidencialidad, integridad y disponibilidad (KIO IT SERVICES, 2024; Power Data, 2024). Este enfoque integral trasciende la protección técnica, articulando estrategias preventivas y correctivas que aseguren la salvaguarda de los activos digitales a lo largo de su ciclo de vida. En el contexto de la metodología OCTAVE, estas medidas se implementan para establecer un marco operativo que permita la gestión eficiente de riesgos y vulnerabilidades, consolidando así la seguridad como un elemento estratégico en el ecosistema empresarial.

CONCLUSIONES

- La aplicación de la metodología OCTAVE ha demostrado ser un elemento transformador en la gestión integral de las redes de comunicaciones. Inicialmente, el diagnóstico reveló un panorama preocupante, donde predominaban evaluaciones negativas con un 38% categorizadas como "Malo" y un 62% como "Regular". Esta situación cambió radicalmente tras la intervención metodológica, evidenciándose una mejora sustancial en la calidad de gestión: la categoría "Malo" desapareció por completo, la categoría "Regular" se redujo al 23.1%, mientras emergieron calificaciones positivas con un 46.2% en "Bueno" y un 30.8% en "Muy Bueno". El análisis estadístico corrobora esta transformación con una significancia asintótica bilateral de 0.000, valor inferior al umbral establecido ($\alpha = 0.025$), lo que permite confirmar que la aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.
- En cuanto a la gestión de procesos específicos en las redes de comunicaciones, los resultados preliminares mostraban deficiencias estructurales significativas, con un 62% de evaluaciones en la categoría "Malo" y un 38% en "Regular". La implementación metodológica provocó una redistribución cualitativa hacia estándares superiores, eliminando por completo la categoría "Malo" y reduciendo la categoría "Regular" a solo un 15.4%. Particularmente destacable resulta la emergencia de categorías que denotan excelencia operativa: "Bueno" con un 30.8% y "Muy Bueno" con un 53.8%. Esta evolución queda validada estadísticamente con una significancia asintótica bilateral de 0.002, valor inferior al umbral crítico

establecido ($\alpha = 0.025$), permitiendo afirmar que la aplicación de la metodología OCTAVE mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimac S.A.C.

- Respecto al componente de monitoreo, el diagnóstico inicial identificó vulnerabilidades considerables, con un 23% de evaluaciones clasificadas como "Malo" y un 46% como "Regular", mientras que solo un 31% alcanzó la categoría "Bueno", sin registros en niveles superiores. Tras la intervención, se constató una optimización sustancial: la categoría "Malo" se redujo al 8%, "Regular" disminuyó al 23.1%, "Bueno" se mantuvo estable en un 30.8% y emergió un significativo 38.5% en la categoría "Muy Bueno". El análisis estadístico respalda esta evolución positiva con una significancia asintótica bilateral de 0.005, valor inferior al parámetro crítico ($\alpha = 0.025$), confirmando que la aplicación de la metodología OCTAVE mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimac S.A.C.
- Finalmente, en el ámbito crítico de la seguridad, el diagnóstico inicial reveló un escenario preocupante: 8% de evaluaciones en la categoría "Muy Malo", 31% en "Malo" y 54% en "Regular", evidenciando vulnerabilidades significativas en la protección de activos de información. La transformación post-implementación resultó particularmente notable, con la eliminación total de las categorías "Muy Malo" y "Malo", y la reducción de "Regular" al 15.4%. Paralelamente, se registró un fortalecimiento significativo en los niveles de protección, con un 46.2% de evaluaciones en "Bueno" y un 38.5% en "Muy Bueno". El análisis estadístico confirma esta transformación con una significancia asintótica bilateral de 0.001, valor inferior al umbral crítico ($\alpha = 0.025$), validando que la metodología OCTAVE mejora sustancialmente la

aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.

RECOMENDACIONES

A continuación, se presentan recomendaciones que debe ser efectuadas en adelante:

- Creer un comité de seguridad permanente con el personal estable para garantizar una continuidad y mejora de los controles de seguridad, evaluaciones producto de los nuevos cambios se que se presentaran, siendo estos de forma permanente.
- Programar capacitaciones periódicas a todo el personal en los temas de seguridad de la información, sin dejar de lado la metodología aplicada para su implementación.
- Elaborar un software para automatizar la gestión de seguridad de la información y así poder hacer un seguimiento y control mas preciso con acceso de forma más rápida a la información.

BIBLIOGRAFIAS

Allen-Addy (2023). Metodología OCTAVE en la gestión de redes de Preimaq S.A.C. Loreto. Perú

Amador Donado (2022). Gestión del riesgo con base en ISO27005 adaptando OCTAVE-S. Universidad Internacional de La Rioja. Colombia

Bibliotecas, & duoc. (2022). *Investigación Aplicada*. Obtenido de [https://bibliotecas.duoc.cl/investigacion-aplicada/definicion-proposito-investigacion-aplicada#:~:text=La%20Investigaci%C3%B3n%20Aplicada%20tiene%20por,del%20desarrollo%20cultural%20y%20cient%C3%ADfico](https://bibliotecas.duoc.cl/investigacion-aplicada/definicion-proposito-investigacion-aplicada#:~:text=La%20Investigaci%C3%B3n%20Aplicada%20tiene%20por,del%20desarrollo%20cultural%20y%20cient%C3%ADfico.). Rev 05/10/2024

Bigelow, S. (2023). Obtenido de <https://www.techtarget.com/searchitchannel/definition/solution.> Rev 08/10/2024

Careerexplorer. (2023). Obtenido de <https://www.careerexplorer.com/careers/solution-architect/>. Rev 12/10/2024

Cisco. (06 de 09 de 2023). Obtenido de https://www.cisco.com/c/es_mx/solutions/cloud/what-is-cloud-computing.html. Rev 05/10/2024

Crowdstrike. (2021). Obtenido de <https://www.crowdstrike.com/cybersecurity-101/it-security/>. Rev 05/11/2024

- Cruz diaz, m. A. (2017). *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica medcam Perú sac*. Lima: usmp. Rev 06/10/2024
- Carpenter, Bauer y Erdogan. (2010). Rasgos adicionales como la autoeficacia, la autoestima y la personalidad proactiva. et al USC University of Southern California
- Gastelo Fernández (2023). Gestión de riesgos basado en la metodología MAGERIT en la Municipalidad Distrital de Cupisnique, Cajamarca.
- Gartner. (2023). Obtenido de <https://www.gartner.com/en/information-technology/glossary/solution>
- Geneva. (2021). *wipo*. Obtenido de https://www.wipo.int/pressroom/es/articles/2021/article_0008.html. Rev 15/12/2024
- Imperva. (25 de 06 de 2023). Obtenido de <https://www.imperva.com/learn/data-security/information-security-infosec/>. Rev 05/10/2024
- Indeed. (2023). Obtenido de <https://ca.indeed.com/career-advice/career-development/what-is-it-solution>. Rev 12/10/2024
- Internationalit. (2022). Obtenido de <https://www.internationalit.com/post/qu%C3%A9-es-la-gesti%C3%B3n-de-red-y-por-qu%C3%A9-es-importante?lang=es>. Rev 09/10/2024
- lacamara. (2022). *lacamara*. Obtenido de <https://lacamara.pe/empresas-en-peru-invierten-9-en-tecnologia/>. Rev 03/12/2024
- larepublica. (2022). *larepublica*. Obtenido de <https://larepublica.pe/economia/2020/11/17/inversion-en-el-sector-tic-alcanzara-mas-de-3-millones-entre-el-2020-y-2024>. Rev 05/10/2024

- Méndez gálvez, c. (2020). *Desarrollo de un plan de seguridad de la información basado en estándares para empresa de seguros*. Pimentel: uss. Rev 09/11/2024
- Mitchell, B. (2020). Obtenido de <https://www.lifewire.com/introduction-information-technology-817815>. Rev 09/10/2024
- Molano espinel, r. (2017). *Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma iso 27001 en el área de ti para la empresa market mix*. Bogota: ucc. Rev 25/11/2024
- Mora guaman, r. J. (2022). *Analisis y diseño de un modelo para establecer un sistema de gestion de la seguridad de la informacion dentro de un mbiente cloud computing, aplicando la norma iso 27001. En la empresa data-fiber*. Babahoyo: utb. Rev 05/10/2024
- Moreno, J. (2023). Obtenido de <https://blog.hubspot.es/service/que-es-soporte-tecnico>. Rev 16/10/2024
- Muñoz Gutiérrez (2022). Gestión de riesgos mediante la metodología OCTAVE utilizando el ciclo de mejora continua PHVA para disponer de un marco de referencia que permita gestionar de forma correcta eventos e incidentes de seguridad en un modelo de Infraestructura como servicio "IAAS
- Muniucayali. (2024). Obtenido de <https://www.muniucayali.gob.pe/>
- Oarc. (05 de 07 de 2023). Obtenido de <https://stats.oarc.ucla.edu/spss/faq/what-does-cronbachs-alpha-mean/>. Rev 05/10/2024
- Otgroup. (2022). Obtenido de <https://www.otgroup.ca/business-technology-insights/it-solutions-definition-what-does-it-mean-can-it-help-your-company>. Rev 16/11/2024

- Oviedo, J. (2010). *scielo*. Obtenido de [http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0034-74502005000400009#:~:text=El%20coeficiente%20alfa%20fue%20descrito,correlacionados%20\(3%2C17\)](http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0034-74502005000400009#:~:text=El%20coeficiente%20alfa%20fue%20descrito,correlacionados%20(3%2C17).). Rev 07/10/2024
- Pacheco (2022). Seguridad en redes de comunicaciones: Perspectivas y desafíos. Chile
- Porras ruiz, m. (2019). *Sistema de gestión de seguridad de la información para la gestión de riesgos en*. Huancayo: upda. Rev 14/10/2024
- Ramiro alejandro, g. (2017). *“sistema de gestión de seguridad de la información basado en la norma iso/iec 27001 para el departamento de ecnologías de la información y comunicación del distrito*. Ecuador: uta. Rev 05/12/2024
- Rojas viera, c. K. (2015). *“sistema de gestión de seguridad de información (sgsi) basado en la norma iso/iec27001 para mejorar la seguridad del área de operaciones y tecnología de global bpo center allus chiclayo - 2015*. Lambayeque: unprg. Rev 25/11/2024
- Sampieri (2008). Metodologia de la investigacion 6ta edicion. Mcgraw-hill / interamericana editores, S.A. DE C.V
- Servicenow. (2023). Obtenido de <https://www.servicenow.com/products/itsm/what-are-it-solutions.html>. Rev 05/10/2024
- Suarez barros, I. D. (2021). *Sistema de gestión de seguridad de la información bajo la norma iso/iec 27001:2015- en la empresa magdaniel ltda. En el distrito especial, turístico y cultural de riohacha*. Guajira: u. Guajira. Rev 11/11/2024

Sumologic. (2023). Obtenido de
<https://www.sumologic.com/glossary/information-security-management/>
Unir. (2023). Obtenido de <https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/> Rev 05/10/2024

ANEXOS

Anexos N° 1: Matriz de consistencia.

Título: Aplicación de la metodología Octave para la Gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C													
FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES/DIMENSIONES E INDICADORES	METODOLOGÍA DE LA INVESTIGACIÓN									
¿En qué medida la aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C?	Demostrar que la aplicación de la metodología octave para mejorar la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	La aplicación de la metodología octave mejora la gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	Variable independiente: Metodología octave Dimensiones: • Análisis y planificación. • Concientización • Aseguramiento. Variable dependiente: Gestión de redes de comunicaciones Dimensiones: ▪ Procesos ▪ Monitoreo ▪ Seguridad	Tipo de investigación: Aplicada Nivel de investigación: Descriptiva. Población: Muestra: Diseño de la investigación: Experimental de tipo pre experimental. Ge: Y1 ---- X ----Y2 Donde: Ge: Grupo experimental O1 : Pretest O1 : Posttest X : Modelo de Gestión del conocimiento									
¿Cómo la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.?	Efectuar la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	La aplicación de la metodología octave mejora la gestión de procesos de redes de comunicaciones de la empresa constructora Preimaq S.A.C.		<table><tr><th>Fuentes</th><th>Técnicas</th><th>Instrumentos</th></tr><tr><td>Primaria</td><td>Encuesta</td><td>Cuestionarios</td></tr><tr><td>Secundaria</td><td>Análisis documental</td><td>Resumen de autores.</td></tr></table>	Fuentes	Técnicas	Instrumentos	Primaria	Encuesta	Cuestionarios	Secundaria	Análisis documental	Resumen de autores.
Fuentes	Técnicas	Instrumentos											
Primaria	Encuesta	Cuestionarios											
Secundaria	Análisis documental	Resumen de autores.											
¿De qué manera la aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.?	Determinar que la aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	La aplicación de la metodología octave mejora la gestión de monitoreo de redes de comunicaciones de la empresa constructora Preimaq S.A.C.											
¿En qué medida la aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.?	Establecer que a aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.	La aplicación de la metodología octave mejora la gestión de seguridad de redes de comunicaciones de la empresa constructora Preimaq S.A.C.											

Anexos N° 2: Cuestionario de preguntas para la recolección de datos

CUESTIONARIO DE PREGUNTAS SOBRE LA INVESTIGACIÓN

“Aplicación de la metodología Octave para la Gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C”

El presente cuestionario tiene como finalidad recopilar información de indicadores correspondientes a las variables principales de la investigación, se le solicita responder las preguntas con la mayor seguridad y exactitud, a fin de poder contar con datos relevantes.

INDICACIONES

- Marque con X en el cuadro que considere el valor adecuado como respuesta a las preguntas específicas.

Escala de Likert

Valor	Significado
1	Muy malo
2	Malo
3	Regular
4	Bueno
5	Muy bueno.

Variable dependiente: Gestión de redes de comunicaciones.

P1: ¿Según su apreciación personal/ profesional que calificativo le asignaría a las herramientas identificados en los procesos para garantizar la seguridad y continuidad de las redes de comunicaciones?

a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P2: ¿Según su apreciación personal/ profesional que calificativo le asignaría a las herramientas implementadas en los procesos para garantizar la seguridad y continuidad de las redes de comunicaciones?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P3: ¿Según su apreciación personal/ profesional que calificativo le asignaría a los controles identificados y propuestos relacionados con la gestión de redes de comunicaciones?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P4: ¿Según su apreciación personal/ profesional que calificativo le asignaría a los controles implementados y propuestos relacionados con la gestión de redes de comunicaciones?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P5: ¿Según su apreciación personal/ profesional que calificativo les asignaría a los registros de incidencias identificados como parte del proceso de monitoreo de las redes de comunicación?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P6: ¿Según su apreciación personal/ profesional que calificativo les asignaría a los registros de incidencias implementados como parte del proceso de monitoreo de las redes de comunicación?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P7: ¿Según su apreciación personal/ profesional que calificativo le asignaría a las programaciones de actividades de monitoreo encontradas para la gestión de las redes de comunicación?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P8: ¿Según su apreciación personal/ profesional que calificativo le asignaría a las programaciones de actividades de monitoreo implementadas para la gestión de las redes de comunicación?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P9: ¿Según su apreciación personal/ profesional que calificativo le asignaría al nivel de conformidad referido a la seguridad de las redes de comunicación?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

P10: ¿Según su apreciación personal/ profesional que calificativo le asignaría al nivel de conformidad de la gestión de las redes de comunicación?

- a) Malo b)Regular c)Normal d)Bueno e)Muy bueno

Anexos N° 3: Validación de los instrumentos por expertos



UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE INGENIERIA DE SISTEMAS

**I. DATOS GENERALES**

- 1.1. APELLIDOS Y NOMBRES: EUCLIDES PANDURO PADILLA
- 1.2. GRADO ACADÉMICO: MAGISTER
- 1.3. INSTITUCIÓN QUE LABORA: UNIVERSIDAD NACIONAL DE UCAYALI.
- 1.4. TÍTULO DE LA INVESTIGACIÓN: Aplicación de la metodología Octave para la Gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.
- 1.5. AUTOR DEL INSTRUMENTO: Greysi Roxana Gonzales García
- 1.6. GRADO ACADÉMICO: ESTUDIANTE DE PREGRADO
- 1.7. NOMBRE DEL INSTRUMENTO: **CUESTIONARIO**
- 1.8. CRITERIOS DE APLICABILIDAD:

(a) De 01 a 09: (No válido, reformular)
 (d) De 16 a 18 (Válido, precisar)

(b) De 10 a 12: (No válido, modificar)
 (e) De 19 a 20: (Válido, aplicar)

(c) De 13 a 15: (Válido, mejorar)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS – CUANTITATIVOS	Deficiente (01 - 09)	Regular (10 - 12)	Bueno (13 - 15)	Muy bueno (16 - 18)	Excelente (19 - 20)
1. CALIDAD	Esta formulado con lenguaje apropiado					19
2. OBJETIVIDAD	Esta expresado con conductas observables					19
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					19
4. ORGANIZACIÓN	Existe organización y lógica					19
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					19
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					19
7. CONSISTENCIA	Basado en aspecto teórico científico y del tema de estudio					19
8. COHERENCIA	Entre las variables, dimensiones e indicadores					19
9. METODOLOGÍA	La estrategia responde al propósito del estudio					19
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					19
SUB TOTAL						19
TOTAL						19

VALORACIÓN CUANTITATIVA : 18
VALORACIÓN CUALITATIVA : MUY BUENO
OPINIÓN DE APLICABILIDAD : APLICABLE.

Lugar y Fecha: 15/04/2025.



 Firma y post firma del experto
 DNI: 40820337



UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE INGENIERIA DE SISTEMAS



III. DATOS GENERALES

- 1.9. APELLIDOS Y NOMBRES: CLOTIDE RIOS HIDALGO DE CERNA
- 1.10. GRADO ACADÉMICO: MAGISTER
- 1.11. INSTITUCIÓN QUE LABORA: UNIVERSIDAD NACIONAL DE UCAYALI.
- 1.12. TÍTULO DE LA INVESTIGACIÓN: Aplicación de la metodología Octave para la Gestión de redes de comunicaciones de la empresa constructora Preimaq S.A.C.
- 1.13. AUTOR DEL INSTRUMENTO: Greysi Roxana Gonzales García
- 1.14. GRADO ACADÉMICO: ESTUDIANTE DE PREGRADO
- 1.15. NOMBRE DEL INSTRUMENTO: **CUESTIONARIO**
- 1.16. CRITERIOS DE APLICABILIDAD:
- (a) De 01 a 09: (No válido, reformular) (b) De 10 a 12: (No válido, modificar) (c) De 13 a 15: (Válido, mejorar)
- (d) De 16 a 18 (Válido, precisar) (e) De 19 a 20: (Válido, aplicar)

IV. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS – CUANTITATIVOS	Deficiente (01 - 09)	Regular (10 - 12)	Bueno (13 - 15)	Muy bueno (16 - 18)	Excelente (19 - 20)
1. CALIDAD	Esta formulado con lenguaje apropiado					19
2. OBJETIVIDAD	Esta expresado con conductas observables					19
3. ACTUALIDAD	Adecuado al avance de la ciencia y tecnología					19
4. ORGANIZACIÓN	Existe organización y lógica					19
5. SUFICIENCIA	Comprende los aspectos en cantidad y calidad					19
6. INTENCIONALIDAD	Adecuado para valorar los aspectos de estudio					19
7. CONSISTENCIA	Basado en aspecto teórico científico y del tema de estudio					19
8. COHERENCIA	Entre las variables, dimensiones e indicadores					19
9. METODOLOGÍA	La estrategia responde al propósito del estudio					19
10. CONVENIENCIA	Genera nuevas pautas para la investigación y construcción de teorías					19
SUB TOTAL						19
TOTAL						19

VALORACIÓN CUANTITATIVA : 18
 VALORACIÓN CUALITATIVA : MUY BUENO
 OPINIÓN DE APLICABILIDAD : APLICABLE.

Lugar y Fecha: 15/04/2025.

Firma y post firma del experto
 DNI: 18198286

Anexos N° 4: Base de datos del Pre Test

Codigo	Procesos					Monitoreo					Seguridad			Variable dependiente
	P 1	P 2	P 3	P 4		P 5	P 6	P 7	P 8		P 9	P 10		
1	3	2	2	1	2	2	2	3	3	3	1	2	2	2
2	1	4	1	3	2	2	1	4	2	2	3	2	3	2
3	3	1	1	4	2	3	4	4	4	4	3	2	3	3
4	3	2	2	3	3	1	1	3	3	2	2	4	3	3
5	2	4	3	2	3	3	2	3	4	3	2	2	2	3
6	2	3	1	3	2	3	4	4	1	3	2	2	2	2
7	4	3	2	3	3	4	4	2	4	4	1	1	1	3
8	2	4	3	4	3	4	4	4	2	4	2	4	3	3
9	2	2	1	1	2	4	4	4	1	3	4	1	3	2
10	2	3	3	2	3	2	3	4	1	3	3	4	4	3
11	1	1	3	2	2	1	4	3	3	3	2	4	3	3
12	3	1	2	3	2	4	4	4	3	4	3	2	3	3
13	2	2	3	1	2	1	2	1	4	2	1	3	2	2

Anexos N° 5: Base de datos del Post Test

Gestión de redes de comunicaciones														
Codigo	Procesos					Monitoreo					Seguridad			Variable dependiente
	P 1	P 2	P 3	P 4		P 5	P 6	P 7	P 8		P 9	P 10		
1	4	4	5	5	5	5	5	5	5	5	5	4	5	5
2	4	5	4	5	5	3	5	5	5	5	3	4	4	4
3	5	5	3	5	5	4	5	4	5	5	5	5	5	5
4	5	4	3	4	4	3	3	3	3	3	2	3	3	3
5	4	3	4	4	4	4	5	4	3	4	4	4	4	4
6	5	4	4	5	5	3	5	5	5	5	5	5	5	5
7	5	5	3	5	5	4	3	3	3	3	3	5	4	4
8	3	2	3	3	3	4	4	5	3	4	2	3	3	3
9	3	4	4	3	4	2	2	2	2	2	5	5	5	4
10	5	3	3	5	4	3	4	3	3	3	3	5	4	4
11	5	5	3	5	5	3	4	5	3	4	4	4	4	4
12	5	4	5	4	5	5	5	4	4	5	5	5	5	5
13	3	4	3	3	3	5	3	3	3	4	4	3	4	3

Anexos N° 6: Análisis estadístico del alfa de Cronbach.

CONFIABILIDAD

ANÁLISIS ESTADÍSTICO ALFA DE CRONBACH

Variable: Reparación civil de la víctima por lesiones y homicidio

$$\alpha = \left(\frac{k}{k-1} \right) \left(1 - \frac{\sum V_i}{\sum V_T} \right)$$

$$\alpha = \left(\frac{13}{12} \right) \cdot \left(1 - \frac{8.7900}{37.6500} \right)$$

$$\alpha = 0.83$$

ALFA DE CRONBACH	Ítems
0,83	13

Fuente: Salida del SPSS V24

Interpretación: El estadístico **ALFA DE CRONBACH**, aplicado al instrumento de investigación, arrojó 0,83. Por ende el instrumento tiene un grado de confiabilidad **MUY ALTA**, para la investigación, por el resultado que se obtuvo. Por tanto, se recomienda su aplicación.

Pucallpa; 05 de abril del 2021



 Marco Antonio Díaz Apac
 Lic. Especialidad de Matemática