

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS



**GESTIÓN DE RIESGO PARA MEJORAR LA GESTIÓN DE
SERVICIOS DE LA RED DE DATOS EN LA EMPRESA
COMPARTAMOS FINANCIERA S.A.**

Tesis para optar al título profesional de

INGENIERO DE SISTEMAS

JORGE MICHAEL JUNIOR DÁVILA RÍOS

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° 03-2025

GRADUANDO : DAVILA RIOS, JORGE MICHAEL JUNIOR

TEMA : "GESTIÓN DE RIESGOS PARA MEJORAR LA GESTIÓN DE SERVICIOS DE LA RED DE DATOS EN LA EMPRESA COMPARTAMOS FINANCIERA S.A"

ASESOR : Mg. EUCLIDES PANDURO PADILLA

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
- UNANIMIDAD
- MAYORIA
- DESAPROBADO

26 A 30 PUNTOS
21 A 25 PUNTOS
16 A 20 PUNTOS
15 A MENOS

CALIFICACION FINAL:

PUNTAJE : 16 / 30

CONCLUSIONES:

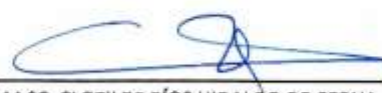
APROBADO POR : MAYORIA
DESAPROBADO POR :

JURADO EVALUADOR


Dr. NILTON CESAR AYRA APAC
PRESIDENTE


Mg. ARTURO YUPANQUI VILLANUEVA
MIEMBRO


Msc. OSCAR AMADO RUIZ TORRES
MIEMBRO


M.SC. CLOTILDE RÍOS HIDALGO DE CERNA
SECRETARIA ACADÉMICA

PUCALLPA, 23 DE ENERO 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

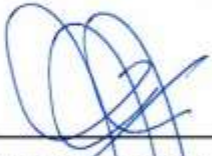
TESIS TITULADA:

"GESTIÓN DE RIESGOS PARA MEJORAR LA GESTIÓN DE SERVICIOS
DE LA RED DE DATOS EN LA EMPRESA COMPARTAMOS FINANCIERA
S.A"

ELABORADO POR:

Bach. DAVILA RIOS, JORGE MICHAEL JUNIOR

APROBADO POR:



Dr. NILTON CESAR AYRA APAC

Presidente



Mg. Arturo YUPANQUI VILLANUEVA

Miembro



Msc. Oscar Amado RUIZ TORRES

Miembro



Mg. Euclides PANDURO PADILLA

Asesor



UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº V/0516-2024.

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

"GESTIÓN DE RIESGO PARA MEJORAR LA GESTIÓN DE SERVICIOS DE LA RED DE DATOS EN LA EMPRESA COMPARTAMOS FINANCIERA S.A"

Autor(es) : DÁVILA RÍOS, JORGE MICHAEL JUNIOR
Facultad : INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL
Escuela : ING. DE SISTEMAS
Asesor(a) : M.Sc. PANDURO PADILLA, EUCLIDES

Presenta un **porcentaje de similitud de 8%**, 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: 01/10/2024



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, Jorge Michael Junior Danilo Ríos

Autor de la tesis titulada: Creación de Riegos para mejorar la gestión de servicios de la red de datos en la empresa Compañía Financiera S.A.

Sustentada el año 2025

Asesor(a): Ing. Eulides Paredano Padilla

Facultad: Ingeniería de Sistemas e Ingeniería Civil

Escuela Profesional: 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: 23 / 01 / 2025

Email: jorgedaniario10@gmail.com

Firma: [Firma]

Teléfono: 930340077

DNI: 76336399

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

DEDICATORIA

Deseo dedicar esta investigación con profundo cariño a mi padre, madre, hermana y sobrina, quienes han sido mi fuente constante de fortaleza e inspiración. Su amor incondicional, sus palabras de aliento y su presencia en cada etapa de mi vida han sido el impulso que me ha motivado a seguir adelante, a no rendirme y a perseverar con determinación en la búsqueda de mis metas.

AGRADECIMIENTO

A Dios, por ser mi guía constante, por brindarme fortaleza, sabiduría y la oportunidad de vivir este proceso. Sin su presencia en mi vida, nada de esto hubiera sido posible.

Agradezco profundamente a mi familia por su apoyo incondicional, por sus palabras de aliento y por estar siempre presentes, especialmente en los momentos más difíciles. Su amor y comprensión han sido pilares fundamentales en este logro.

A la Universidad Nacional de Ucayali, por acogerme durante estos años de formación académica, brindándome no solo conocimientos, sino también valores que marcarán mi vida profesional.

Expreso mi sincero agradecimiento a los docentes de la Facultad de Ingeniería de Sistemas, por su dedicación, enseñanza y compromiso con nuestra formación. Cada uno de ustedes ha contribuido significativamente a mi crecimiento académico y personal.

ÍNDICE GENERAL

	Pág.
DEDICATORIA	vi
AGRADECIMIENTO	vii
ÍNDICE GENERAL.....	viii
ÍNDICE DE TABLAS	xi
ÍNDICE DE FIGURAS.....	xv
RESUMEN	xix
ABSTRACT	xx
INTRODUCCIÓN	xxi
CAPÍTULO I. EL PROBLEMA DE INVESTIGACIÓN.....	1
1.1. DESCRIPCIÓN DEL PROBLEMA.....	1
1.2. FORMULACIÓN DEL PROBLEMA	2
1.2.1. Problema general.	2
1.2.2. Problemas específicos.....	2
1.3. OBJETIVOS.	3
1.3.1. Objetivo general.....	3
1.3.2. Objetivos específicos.....	3
1.4. JUSTIFICACIÓN.	3
1.5. IMPORTANCIA.	4
1.6. LIMITACIONES.....	5
1.7. DELIMITACIONES DE LA INVESTIGACIÓN.....	5
1.8. HIPÓTESIS Y/O SISTEMA DE HIPÓTESIS	6
1.8.1. Hipótesis general	6
1.8.2. Hipótesis específicas	6

1.9. VARIABLES	7
1.9.1. Variable independiente	7
1.9.2. Variable dependiente	7
1.9.3. Variable interviniente	7
1.9.4. Operacionalización de las variables	7
CAPÍTULO II. MARCO TEÓRICO	9
2.1. ANTECEDENTES DE LA INVESTIGACIÓN	9
2.1.1. Antecedentes internacionales.....	9
2.1.2. Antecedentes nacionales.....	11
2.2. BASES TEÓRICAS.....	13
2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS.....	24
CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN	25
3.1. METODOLOGÍA Y TÉCNICAS UTILIZADAS	25
3.1.1. Tipo de investigación	25
3.1.2. Nivel de investigación.....	25
3.1.3. Método de investigación.....	25
3.1.4. Diseño de la investigación	26
3.2. POBLACIÓN Y MUESTRA.....	26
3.3. INSTRUMENTOS DE RECOLECCIÓN DE DATOS	27
3.4. PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS	27
3.5. TRATAMIENTO DE DATOS.....	27
3.6. GRADO DE CONFIABILIDAD DE LOS DATOS.....	28
CAPÍTULO IV. RESULTADOS Y DISCUSIÓN	29
4.1. RESULTADOS DE LA INVESTIGACIÓN PRE-TEST.....	29
4.2. RESULTADOS DE LA INVESTIGACIÓN POST-TEST	43

4.3. MEDICIÓN DE NORMALIDAD	57
4.4. PRUEBA DE HIPÓTESIS	59
CONCLUSIONES	66
RECOMENDACIONES	68
REFERENCIAS BIBLIOGRÁFICAS.....	69
ANEXOS	71

ÍNDICE DE TABLAS

En el texto:	Pág.
Tabla 1. Operacionalización de las variables.....	8
Tabla 2. ¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?.....	29
Tabla 3. ¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?	30
Tabla 4. ¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?.....	31
Tabla 5. ¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?.....	32
Tabla 6. ¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?.....	33
Tabla 7. ¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?.....	34
Tabla 8. ¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?.....	35
Tabla 9. ¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?.....	36
Tabla 10. ¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?.....	37
Tabla 11. ¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?.....	38

Tabla 12. ¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	39
Tabla 13. ¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	40
Tabla 14. ¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?.....	41
Tabla 15. ¿Cuál es su punto de vista sobre las actividades de mejora continua empleados en la Gestión de servicios de la red de datos?.....	42
Tabla 16. ¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?.....	43
Tabla 17. ¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?.....	44
Tabla 18. ¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?.....	45
Tabla 19. ¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?.....	46
Tabla 20. ¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?.....	47
Tabla 21. ¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?.....	48
Tabla 22. ¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?.....	49

Tabla 23. ¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?.....	50
Tabla 24. ¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?.....	51
Tabla 25. ¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?.....	52
Tabla 26. ¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	53
Tabla 27. ¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	54
Tabla 28. ¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?.....	55
Tabla 29. ¿Cuál es su punto de vista sobre las actividades de mejora continuad empleados en la Gestión de servicios de la red de datos?.....	56
Tabla 30. Pruebas de normalidad.....	58
Tabla 31. Prueba de los rangos con signo de Wilcoxon – HG.....	59
Tabla 32. Estadística de Wilcoxon – HG.....	60
Tabla 33. Prueba de los rangos con signo de Wilcoxon – HE1.....	61
Tabla 34. Estadística de Wilcoxon – HE1.....	61
Tabla 35. Prueba de los rangos con signo de Wilcoxon – HE2.....	63
Tabla 36. Estadística de Wilcoxon – HE2.....	63
Tabla 37. Prueba de los rangos con signo de Wilcoxon – HE3.....	64

Tabla 38. Estadística de Wilcoxon – HE3.....	65
En el anexo:	
Tabla 1A. Diagnóstico inicial.....	82
Tabla 2A. Clasificación de amenazas.....	86
Tabla 3A. Valoración de impacto.....	87
Tabla 4A. Mapa de color evaluación de impacto.....	87
Tabla 5A. Clasificación de amenazas y cálculo de riesgo.....	88
Tabla 6A. Riesgos por amenazas.....	89
Tabla 7A. Causas y efectos.....	90
Tabla 8A. Riesgos residuales.....	91
Tabla 9A. Matriz de impacto residuales.....	92

ÍNDICE DE FIGURAS

En el texto:	Pág.
Figura 1. Estrategias de Oportunidades y riesgos.....	21
Figura 2. R&O.....	23
Figura 3. ¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?.....	29
Figura 4. ¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?	30
Figura 5. ¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?.....	31
Figura 6. ¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?.....	32
Figura 7. ¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?.....	33
Figura 8. ¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?.....	34
Figura 9. ¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?.....	35
Figura 10. ¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?.....	36
Figura 11. ¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?.....	37
Figura 12. ¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?.....	38

Figura 13.	¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	39
Figura 14.	¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	40
Figura 15.	¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?.....	41
Figura 16.	¿Cuál es su punto de vista sobre las actividades de mejora continua empleados en la Gestión de servicios de la red de datos?.....	42
Figura 17.	¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?.....	43
Figura 18.	¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?.....	44
Figura 19.	¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?.....	45
Figura 20.	¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?.....	46
Figura 21.	¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?.....	47
Figura 22.	¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?.....	48
Figura 23.	¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?.....	49

Figura 24. ¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?.....	50
Figura 25. ¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?.....	51
Figura 26. ¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?.....	52
Figura 27. ¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	53
Figura 28. ¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?.....	54
Figura 29. ¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?.....	55
Figura 30. ¿Cuál es su punto de vista sobre las actividades de mejora continuad empleados en la Gestión de servicios de la red de datos?.....	56
Figura 31. Curva de distribución normal estándar en una prueba de hipótesis bilateral.....	60
Figura 32. Curva de distribución normal con regiones de rechazo y de aceptación en una prueba de hipótesis bilateral – HE1.....	62
Figura 33. Curva de distribución normal con regiones de aceptación y rechazo en una prueba de hipótesis bilateral (nivel de significancia $\alpha = 0.05$).....	63

Figura 34. Curva de distribución normal estándar con regiones de aceptación y rechazo para una prueba de hipótesis bilateral...	65
--	----

En el anexo:

Figura 1A. Formatos análisis de riesgo.....	94
Figura 2A. Formatos activos.....	95
Figura 3A. Formatos amenazas.....	95
Figura 4A. Formatos análisis de RAPI	96

RESUMEN

El Sistema de gestión de la seguridad de la información, con siglas SGSI, y su relación con la mejora del proceso de gestión de servicios de la red de datos en la empresa Compartamos Financiera S.A., tiene su origen a partir de las situaciones problemáticas en la transmisión de datos, debido a la saturación de red, falta de controles de seguridad adecuados, presencia de ataques de virus por falta de control, lentitud en el acceso a los servicios desde los servidores. La presente investigación, tuvo por finalidad determinar la mejora del proceso de gestión de servicio de datos a través de la implementación de un sistema de gestión de riesgos, tomando como marco de referencia la Norma Técnica Peruana NTP ISO/IEC 27001:2014. La investigación contó con el enfoque cuantitativo haciendo uso de una herramienta de captura de datos y procesamiento a través del cual se obtuvo resultados y conclusiones.

Palabras claves: Gestión, riesgo, servicio, redes.

ABSTRACT

The information security management system, with the acronym SGSI, and its relationship with the improvement of the data network service management process in the company Compartamos Financiera S.A., has its origin from the problematic situations in the data transmission, due to network saturation, lack of adequate security controls, presence of virus attacks due to lack of control, slow access to services from servers. The purpose of this research is to determine the improvement of the data service management process through the implementation of a risk management system, taking the Peruvian Technical Standard NTP ISO/IEC 27001:2014 as a framework of reference. The research has a quantitative approach using a data capture and processing tool through which results and conclusions were obtained.

Keywords: Management, risk, service, networks.

INTRODUCCIÓN

Si observamos nuestro entorno, las organizaciones, empresas de cualquier nivel que tengan o hagan uso de la tecnología encontramos las redes de computadoras, a través del cual se transmiten datos e información denominado información digital, esta estructura de redes facilita la comunicación, agiliza los procesos, permite el acceso a información multimedia, facilita la búsqueda de información, entre otros.

En nuestro país la tecnología de redes de computadoras se adapta a las distintas características geográficas de cada región y/o ciudad. Asimismo, esta interconexión llega a la empresa, para quienes representa un recurso primordial ya que permite el uso de recursos de red denominado red de área local o también podría ser de tipo Red área metropolitana con la conexión de sucursales.

Así como esta tecnología de apoyo, también genera la presencia de problemas relacionado a las vulnerabilidades, amenazas latentes, riesgos existentes, pérdida, robo, daño de activos de información, accesos sin autorización, entre otros, cuya principal razón es la falta o deficiente administración, carencia de controles de seguridad a nivel organizacional. Esta situación problemática se mejora aplicado o implementado un sistema de gestión de la seguridad de la información SGSI, que consiste en el aseguramiento de la información a través del control de la integridad, configuración de la confidencialidad y el aseguramiento de la disponibilidad de la información, en este caso, que se transmiten a través de las redes de área local.

El SGSI es el tema central de esta investigación, se implementará y de demostrará que con su aplicación mejora la gestión de servicio de la red de datos de la empresa Compartamos Financiera S.A.

Para una mejor organización de la presente investigación, este documento fue separado en capítulos, respetando lo establecido por los reglamentos de la Universidad Nacional de Ucayali.

CAPÍTULO I

EL PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

El cambio tecnológico es constante e imparable y uno de los objetivos de la misma es garantizar la seguridad y calidad de la información y servicio, también representa el medio de comunicación eficaz para las organizaciones y las personas, pero también representa la vulnerabilidad de la información que las empresas deben efectuar el aseguramiento de la información a través de la implementación un sistema de gestión de seguridad.

La empresa compartamos financiera S.A. ha ido creciendo de forma notablemente, eso le ha permitido invertir en tecnología de la información permitiéndoles procesar mayor cantidad de información, la cual se realiza, según observaciones, con controles de seguridad muy básicos lo cual afecta negativamente la disponibilidad de datos, integridad de la información y la confidencialidad de accesos a los datos e información.

La empresa posee una infraestructura de red LAN y con el paso del tiempo ha sufrido pérdidas de información afectando su productividad debido a que la empresa no cuenta con un Sistema de Gestión de Seguridad de la Información (SGSI) para poder mejorar la calidad de servicio proporcionados a través de la red LAN que es gestionada el área de Tecnología de Información, a continuación, se describen situaciones problemáticas detectadas: Saturación de datos a través de la red Carencia de Controles de seguridad o controles desactualizados. Ataque a través de

programas maliciosos como virus, troyanos, etc. Falta de controles adecuados de accesos a los servidores.

Como se puede apreciar existen irregularidades la cual implica diseñar y aplicar un sistema de gestión de riesgos y aplicación de controles; lo cual, viene a ser la finalidad por de la presente investigación.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. Problema general

- ¿La implementación de la gestión de riesgo mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?

1.2.2. Problemas específicos

- ¿De qué manera las condiciones de la confiabilidad mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?
- ¿Cuáles son las características del aseguramiento de la información para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?
- ¿Cómo la capacidad de respuesta de los servicios de red mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?

1.3. OBJETIVOS

1.3.1. Objetivo general

- Implementar la gestión de riesgo para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

1.3.2. Objetivos específicos

- Determinar las condiciones de la confiabilidad del servicio de red para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.
- Identificar las características del aseguramiento de la información para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.
- Optimizar la capacidad de respuesta de los servicios de red para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

1.4. JUSTIFICACIÓN

1.4.1. Justificación teórica

El mundo moderno actual y cambiante tecnológicamente las redes de transmisión de datos representan uno de los componentes que avanza constantemente; como es en la mejora del proceso de transmisión, los

medios, los equipos de control, los mecanismos de seguridad entre otros. Con la presente investigación se pretende hacer uso de los conocimientos en el campo de la seguridad de la información para beneficio de los usuarios finales.

1.4.2. Justificación práctica

Con la implementación de un sistema que garantice la gestión de riesgos en la empresa COMPARTAMOS FINANCIERA S.A. se logra la relevancia de carácter práctico, y con valor, ya que proveerá una solución moderna y eficiente para la gestión de los procesos relacionados con de la red de datos, se implementarán controles de seguridad y así garantizar los servicios y salvaguardar la información de los usuarios.

1.4.3. Justificación metodológica

La metodología utilizada en la implementación de la gestión de riesgos en los procesos de gestión de la red de datos, parte de efectuar un análisis detallado de la situación actual, para determinar cómo se viene llevando el proceso de gestión de riesgos, para luego proponer mejoras y alternativas de solución que garanticen la seguridad y la reducción del nivel de riesgos de seguridad.

1.5. IMPORTANCIA

La importancia de la presente investigación radica en que nos va a permitir reducir los riesgos de pérdida de información a los que está expuesta la empresa, de igual con la confidencialidad de los datos de

nuestros clientes, la integridad, la disponibilidad de los datos y por sobre todo que nos permitirá monitorear cualquier operación que se haya podido realizar en la empresa.

1.6. LIMITACIONES

Las principales limitaciones encontradas en la presente investigación fueron principalmente al tema de la seguridad de la información de los clientes, porque al tratarse de una empresa dedicada al rubro financiero, el acceso a esta ha sido limitado.

1.7. DELIMITACIONES DE LA INVESTIGACIÓN

1.7.1. Delimitación espacial

La presente investigación se realizó sobre los servicios de gestión de redes y servidores, labor que es realizado por el personal de área de TI de la empresa Compartamos Financiera S.A.

1.7.2. Delimitación social

En la presente investigación participa un egresado de la Facultad de Ingeniería de Sistemas e Ingeniería Civil quien, con su investigación dio solución a una realidad problemática presentada en la empresa Compartamos Financiera S.A.

1.7.3. Delimitación temporal

La presente investigación fue iniciada en el abril del año 2023 y se

cumplió con los requisitos temporales impuestos por la Oficina de Grados y Títulos de la FISEIC de la UNU.

1.7.4. Delimitación conceptual

En la presente investigación se utilizan y aplican conceptos referidos al sistema de gestión de seguridad de datos, los cuales contribuyen con la solución de la realidad problemática, aplicando un sistema de gestión y seguimiento de los mismo.

1.8. HIPÓTESIS Y/O SISTEMA DE HIPÓTESIS

1.8.1. Hipótesis general

- La implementación de la gestión de riesgo mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

1.8.2. Hipótesis específicas

- Las condiciones la confiabilidad del servicio de red mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.
- Las características del aseguramiento de la información identificadas mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

- La optimización de la capacidad de respuesta de los servicios de red mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

1.9. VARIABLES

1.9.1. Variable independiente

- Gestión de riesgos: Es el proceso para identificar, realizar una evaluación y aplicar control a los riesgos que perjudican a una organización (Ibm, 2024).

1.9.2. Variable dependiente

- Gestión de servicios de la red de datos: Viene a ser un sistema de protección de los recursos de una red a través de la administración y supervisión permanente (Hpe, 2024).

1.9.3. Variable interviniente

- Compartamos Financiera S.A.

1.9.4. Sistema de variables, dimensiones e indicadores

- Se describe en la siguiente tabla:

Tabla 1***Operacionalización de variables***

Variable	Dimensión	Indicador	Escala
Gestión de riesgos	• Prevención	• Medios • Métodos • Factores	• Malo • Regular
	• Diagnostico	• Perspectiva • Grado	• Normal • Bueno
	• Valoración	• Comparación • Alternativas	• Muy bueno
	• Confiabilidad	• Eficiencia • Efectividad	• Malo • Regular
Gestión de servicios de la red de datos	• Aseguramiento	• Confianza • Credibilidad	• Normal • Bueno
	• Capacidad de respuesta	• Tiempo de respuesta. • Mejora continua	• Muy bueno

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedentes internacionales

Según Cárdenas (2019), en la investigación “Análisis de riesgos de seguridad de la información para la empresa Pijaos telecomunicaciones del municipio de Cajamarca en el departamento del Tolima”, finalizó argumentado: Los riesgos actuales se pueden reducir a niveles mínimos o aceptables mediante el uso de procesos diseñados para lograr los objetivos de la empresa Pijaos Telecomunicaciones S.A.S. actualmente tiene riesgos informáticos importantes y con el apoyo de la alta dirección y de todos los empleados se pueden mitigar los riesgos existentes. Es importante recordar que en las empresas del futuro es necesario brindar una buena capacitación a todos los empleados y directivos para que comprendan la gravedad del problema de los ataques informáticos por la falta de controles legales y políticas que dañan el capital humano imagen, marca, presupuesto y la propia empresa.

Según Molina (2018), en la investigación “Diseño de una política para la clasificación y etiquetado de la información basada en riesgos para instituciones públicas en el Ecuador”, finalizó argumentado: Entre las agencias responsables de supervisar las cooperativas y asociaciones, se cree que la tecnología, los procesos y las personas constituyen los tres pilares que sustentan la seguridad de la información: las agencias gubernamentales suelen tener grandes presupuestos para implementar

tecnología y definir procesos, ignorando el talento y por lo tanto convirtiéndose en el pilar más débil. , motivar a las personas Integrar una cultura de seguridad de la información es fundamental. Al desarrollar políticas de clasificación y etiquetado de la información basada en riesgos, principalmente mediante el uso de un conjunto de estándares: ISO 27001:2013 y MAGERIT y luego ISO 27002:2017 para establecer mecanismos de control, las inconsistencias en la gestión de la información institucional son responsables de la regulación de las cooperativas y asociaciones. En la carta, el departamento de seguridad de la información expresó su satisfacción con los hallazgos.

Según Rosero (2019), en la investigación relacionado al análisis de riesgo de la seguridad de la red LAN de la matriz en la contraloría general del estado, se planteó ejecutar el análisis relacionado con los riesgos de seguridad en la red LAN de la CGE haciendo uso de Megerit como metodología, y logro obtener la siguiente conclusión: El apoyo tanto de la dirección como de varios directivos, las áreas tecnológicas como infraestructura, proyectos y servicios jugaron un papel importante brindando información que me permitió evaluar y gestionar los activos tecnológicos, el mayor beneficio de seguridad Información significa disponer de una adecuada evaluación de riesgos que oriente las inversiones y minimice las consecuencias en caso de incidencias, independientemente de la metodología elegida, la seguridad de la información no es responsabilidad exclusiva del sector tecnológico; debe extenderse desde la alta dirección a todos los procesos de negocio, un Comité de Seguridad de la Información, compuesto por líderes de cada

región, aumenta el compromiso para garantizar el cumplimiento de las políticas de seguridad de la información, si la seguridad de la información depende únicamente de TI, entonces la probabilidad de que no se implemente es del 100%, los recursos financieros de una organización deben invertirse de la mejor manera posible, siempre con vistas al retorno de la inversión, la organización debe entender la seguridad como un proceso que nunca termina, la inseguridad es una propiedad inherente a los recursos informáticos y gestionarla es la única manera de medirla y reducirla.

2.1.2. Antecedentes nacionales

Según Cáceres (2018), en la investigación “La gestión de riesgos y su impacto en la rentabilidad de las empresas de telecomunicaciones ubicadas en Lima Metropolitana 2012 – 2015”. Finalizó argumentado: Como puede ver, herramientas de gestión La información gestionada por las empresas de telecomunicaciones tiene un impacto significativo en el nivel de desempeño financiero teniendo en cuenta los requisitos de diversas administraciones, el desarrollo de la economía nacional es atípico. Así, se ha demostrado que el cumplimiento normativo tiene un impacto directo en la reducción de los sobrecostos operativos de las empresas de telecomunicaciones; Reducir la carga operativa y legal asociada al proceso de Supervisión.

Según Valverde (2022), en la investigación “Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021”. Finalizó argumentado:

Inicialmente, la agencia de publicidad no contaba con un inventario de activos; posteriormente, luego de aplicar el método Magerit, se identificaron los activos y se realizó una valoración de los mismos. Al implementar la metodología Magerit, las agencias de publicidad pueden identificar los riesgos a los que están expuestos los activos y posteriormente realizar una evaluación de riesgos. Al implementar el enfoque Magerit, las agencias de publicidad están desarrollando planes de acción y controles aún no definidos para mitigar el riesgo.

Según Huaurea (2019), en la investigación “Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones”, finalizó argumentado: En resumen, la Ley de Protección de Datos Personales es preocupante, ya que más del 50% de los encuestados desconocen la ley y su impacto en la protección de la información privada de los usuarios. O las empresas que cotizan en bolsa están obligadas a implementar esto. El estudio, que tardó seis (6) meses en completarse, muestra que el uso de NTP ISO/IEC 31000 puede mejorar el éxito de la gestión e integración de riesgos en todos los niveles de la empresa. En consecuencia, puede fortalecer los controles existentes e introducir otros nuevos. Una gestión adecuada de los riesgos de seguridad de la información conduce a la retroalimentación, el refuerzo y el aprendizaje en toda la empresa, y aumenta la confianza de todos los participantes (comités, propietarios de procesos y clientes).

Según Maquera (2022), en la investigación “Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes Lan en la municipalidad distrital de Ilabaya”, finalizó argumentado:

Para la prueba de correlación de Pearson, se determinó que el valor del coeficiente de correlación era $r = 0,540$ (valor de $p = 0,000$, por lo tanto, existe un efecto directo y significativo entre el SGSI y la calidad del servicio de la red LAN en el área de Ilabaya); Con base en el análisis estadístico realizado se concluyó que “existe una relación directa y significativa entre el SGSI y la calidad de servicio de las redes LAN en la región de Ilabaya” y se concluyó que: Se presentaron las evidencias necesarias para iniciar la implementación del SGSI a las unidades responsables del desarrollo del SGSI, iniciando con un análisis de la situación en la organización y el posterior desarrollo de una política de seguridad y medidas de control para el municipio del Ilabaya región. Asimismo, es necesario resaltar los riesgos que enfrenta la seguridad de la información en las redes LAN físicas, por lo que se desarrollan sistemas de gestión de riesgos como parte del SGSI físico para poder monitorear riesgos de información específicos.

2.2. BASES TEÓRICAS

2.2.1. Gestión de riesgos

La gestión de riesgos, de acuerdo con CFI (2024), implica identificar, analizar y responder a los factores de riesgo que forman parte del ciclo de vida empresarial. Una gestión de riesgos eficaz significa intentar controlar los resultados futuros tanto como sea posible siendo proactivo en lugar de reactivo. Por lo tanto, una gestión eficaz del riesgo puede reducir la probabilidad de que ocurra un riesgo y su impacto potencial.

El propósito de establecer marcos de gestión de riesgos no es simplemente señalar los riesgos existentes. Un buen marco de gestión de riesgos también debería considerar las incertidumbres y anticipar su impacto en el negocio. Por tanto, el resultado es una elección entre aceptar el riesgo o rechazarlo. Aceptar o rechazar el riesgo depende del nivel de tolerancia que una empresa se haya determinado.

Si una organización establece la gestión de riesgos como un proceso disciplinado y continuo para identificar y abordar riesgos, el marco de gestión de riesgos se puede utilizar para respaldar otros sistemas de mitigación de riesgos. Estos incluyen planificación, organización, control de costos y elaboración de presupuestos. En este caso, las empresas normalmente no enfrentan muchas sorpresas porque la atención se centra en la gestión proactiva de riesgos.

Importancia de la gestión de riesgos

Según SafetyCulture (2024), la gestión de riesgos tiene como objetivo proteger a una organización de posibles pérdidas o amenazas a sus operaciones en curso. Esto puede incluir pérdidas financieras, daños a la reputación de la organización o lesiones a los empleados. Recuerde, no existe una solución única cuando se trata de gestión de riesgos. Cada organización es única y enfrenta diferentes tipos de riesgos. Por eso es tan importante que las organizaciones desarrollen un plan de gestión de riesgos. El plan de gestión de riesgos contiene todos los riesgos evaluados que enfrenta la organización y los pasos correspondientes para mitigarlos.

Al adoptar un enfoque proactivo para la gestión de riesgos y capacitar continuamente a los empleados, las organizaciones pueden reducir la probabilidad de que algo salga mal y minimizar las pérdidas cuando ocurren incidentes como este. La gestión de riesgos es una parte importante de cualquier organización y debe recibir la atención que merece.

¿Por qué administrar el riesgo?

La gente suele preguntarse por qué la gestión de riesgos no puede permanecer dentro de la dirección general. Esto es cierto, pero la gestión de riesgos se centra específicamente en los riesgos por las siguientes razones:

Gobierno corporativo

Legislaciones como la PFMA y la MFMA, así como códigos de gobierno corporativo como el King II, exigen que las instituciones implementen programas de gestión de riesgos. Las partes interesadas no quieren quedarse sin preparación para eventos riesgosos debido a fallas organizativas pasadas. Esperan que los controles internos y otros mecanismos de mitigación de riesgos se basen en una evaluación de riesgos exhaustiva en toda la agencia.

Anteriormente, los miembros del órgano contable no participaban en los detalles de la gestión de riesgos, ya que se consideraba una función operativa.

Las partes interesadas deben asegurarse de que la dirección haya tomado las medidas necesarias para proteger sus intereses. Por lo tanto, el gobierno corporativo asigna la responsabilidad de la gestión de riesgos a los órganos/funcionarios contables.

Las administraciones, los organismos contables, los funcionarios contables y las partes interesadas ahora quieren saber más sobre los riesgos que enfrentan las instituciones. Esto es comprensible en un entorno donde las expectativas de prestación de servicios son complejas y desafiantes.

Planificación y organización

El valor de la gestión de riesgos se materializa mejor cuando los principios y prácticas de gestión de riesgos se aplican a la planificación institucional y a los procesos organizacionales. Dada la mayor volatilidad e incertidumbre, los planes, especialmente los plurianuales, deben incorporar una evaluación integral de riesgos y estrategias de mitigación.

Para ello, además del modelo de gestión de riesgos institucionales, se pueden utilizar herramientas y técnicas existentes como el análisis FODA, el análisis PEST, el modelo de Porter y las auditorías internas. Por tanto, está claro que la planificación, la organización y la gestión de riesgos son interdependientes.

Procesos de gestión de riesgos

Las cuatro etapas principales del proceso de gestión de riesgos son:

- Identificar riesgos.

- Evaluar el riesgo.
- Toma riesgos.
- Monitorear y reportar riesgos.

Paso 1: Identificación de riesgos

El primer paso en el proceso de gestión de riesgos es identificar todos los eventos que podrían tener un impacto negativo (riesgo) o positivo (oportunidad) en los objetivos del proyecto:

- Principales etapas del proyecto.
- Trayectoria financiera del proyecto.
- Alcance del proyecto.

Estos eventos pueden ingresarse en una matriz de riesgos y luego registrarse en el registro de riesgos.

Un riesgo (u oportunidad) se caracteriza por su descripción, causas y consecuencias, evaluación cualitativa, evaluación cuantitativa y plan de mitigación. También puede caracterizarse por quién es responsable de sus acciones. Cada una de estas características es necesaria para que un riesgo (u oportunidad) sea efectivo.

Para una gestión eficaz, los riesgos y oportunidades (R&O) identificados deben ser lo más precisos y específicos posible. Los nombres de los riesgos y oportunidades deben ser breves, auto explicativos y claramente definidos.

Todos los participantes del proyecto pueden y deben determinar la R&O de la cual es responsable el propietario del riesgo (u oportunidad). El

administrador de riesgos es responsable de garantizar que se implemente un proceso formal para identificar riesgos y desarrollar planes de respuesta a través de la comunicación con los propietarios de riesgos. Explicaremos cada función con más detalle en nuestro próximo artículo sobre funciones en un equipo de gestión de riesgos.

A continuación, se muestran ejemplos de herramientas para ayudar a identificar R&O:

- Análisis de archivos existentes.
- Entrevista a experto
- Idea genial
- Utilice enfoques metodológicos estándar como modos de fallo, análisis de efectos y criticidad (FMECA), árboles de causas, etc.
- Considere las lecciones aprendidas de la experiencia de R&O en proyectos anteriores.
- Utilice una lista de verificación o cuestionario prediseñado (estructura de desglose de riesgos o RBS) que cubra diferentes áreas del proyecto.

Paso 2: Evaluación de riesgos

Hay dos tipos de evaluaciones de riesgos y oportunidades: cualitativas y cuantitativas. Las evaluaciones cualitativas analizan la gravedad en función de la probabilidad y el impacto de un evento. La evaluación cuantitativa analiza las consecuencias o beneficios financieros de un evento. Ambos son necesarios para evaluar plenamente los riesgos y oportunidades.

Evaluación cualitativa

Los propietarios y gestores de riesgos clasificarán y priorizarán cada riesgo y oportunidad identificados según la probabilidad de que ocurra y la gravedad del impacto en función de la criticidad del proyecto.

- **Estimar la probabilidad de ocurrencia (P):** Esto se determina mejor por la experiencia, el progreso del proyecto o la conversación con un experto en riesgos y oscila entre el 1 y el 99%.

Por ejemplo, supongamos el siguiente riesgo: existe un 50% de posibilidades de que “Proveedor”. Esto se puede determinar basándose en la retroalimentación y el análisis de la carga de trabajo del proveedor.

- **Califique la gravedad del impacto (I):** Para evaluar el impacto general, es necesario evaluar la gravedad de cada impacto identificado a nivel de proyecto. Se utilizan escalas para clasificar diferentes impactos y su gravedad. Esto garantiza que las evaluaciones de riesgos y oportunidades estén estandarizadas y sean confiables.

La criticidad de un riesgo u oportunidad está determinada por la fórmula: $\text{Criticidad} = P \times I$.

El propósito de una evaluación cualitativa es garantizar que el equipo de gestión de riesgos dé prioridad a las respuestas a las preguntas clave.

Cuantificación

En la mayoría de los proyectos, el propósito de la cuantificación es proporcionar una estimación financiera del impacto de un riesgo o el beneficio de una oportunidad si ocurre. Este paso lo lleva a cabo el propietario del riesgo, el gestor de riesgos (con el apoyo de los responsables de las evaluaciones y los datos) o el responsable del tratamiento, dependiendo de la estructura organizativa de la empresa. Estos montos representan costos adicionales potenciales (o ganancias potenciales, si hablamos de oportunidades) que no estaban incluidos en el presupuesto del proyecto. Para hacer esto necesitas:

Estime los costos adicionales incurridos en relación con la auditoría financiera:

- Tiempo de ingeniería interna.
- Relojes subcontratados.
- Se requiere más trabajo.
- Cambios de contrato y/o reclamaciones, etc.

Calcule el costo de las consecuencias de un evento inesperado sumando estos valores.

En esta etapa, se evaluarán las necesidades presupuestarias adicionales en relación con los riesgos y oportunidades del proyecto.

Paso tres: gestión de riesgos

Para responder a los riesgos, una organización debe primero determinar su estrategia de respuesta mediante el desarrollo de un plan de

respuesta. El propósito de un plan de tratamiento de riesgos es reducir la probabilidad de que ocurra el riesgo (acciones preventivas) y/o reducir el impacto del riesgo (acciones de mitigación). Con respecto al azar, el objetivo del plan de tratamiento es aumentar la probabilidad de que ocurra el azar y/o aumentar su beneficio. Determine la estrategia de respuesta para el proyecto en función de la naturaleza del riesgo u oportunidad. Aquí hay 7 estrategias que puede utilizar:

Gráfico de embudo que muestra 7 estrategias para responder a riesgos u oportunidades.

Figura 1

Estrategias de Oportunidades y riesgos



7 estrategias

- Aceptar: No se toma ninguna medida, pero el seguimiento continúa.

- Mitigación/intensificación: Reducir (por riesgo) o aumentar (por oportunidad) la probabilidad de que ocurra y/o la gravedad de un impacto.
- Transferir/compartir: Transferir la responsabilidad del riesgo a un tercero que es responsable de las consecuencias del problema (compartir los beneficios de las oportunidades realizadas).
- Evitar/explotar: Eliminar por completo la incertidumbre/explotación.

El seguimiento del progreso del plan de tratamiento es responsabilidad del propietario del riesgo. Deberán informar periódicamente al gestor de riesgos, quien deberá actualizar el registro de riesgos.

Nota. El costo del plan de mitigación de riesgos debe incluirse en el presupuesto del proyecto.

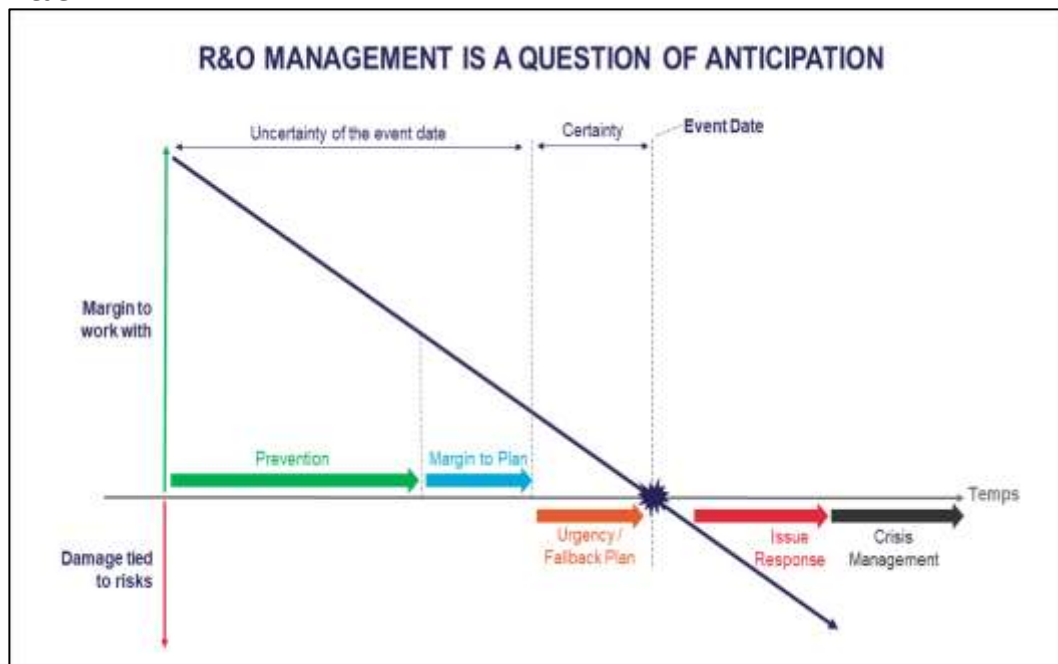
Al desarrollar un plan de tratamiento:

- Cada acción comienza con un verbo de acción y tiene un propósito claro.
- Cada acción tiene un objetivo y un plazo.
- Las actividades que pueden generar costos deben rastrearse y contabilizarse dentro del proyecto.
- Por ejemplo: para reducir el riesgo de que mi coche se averíe, un plan de tratamiento podría consistir en llevarlo a un taller de reparación una vez al año.

¿Cuándo el riesgo se convierte en un problema?

Figura 2

R&O



A pesar de las medidas tomadas para reducir o prevenir el riesgo, la probabilidad de riesgo puede aumentar y alcanzar el 100%. Una vez que se identifica un riesgo, ya no lo llamamos riesgo, lo llamamos problema. Luego, el administrador de riesgos debe notificar a las distintas partes interesadas del proyecto, quienes informarán que el riesgo se ha convertido en un problema y lo trasladarán al registro de problemas.

Paso 4: Monitoreo e informes de riesgos

Es necesario monitorear y comunicar los riesgos y oportunidades, y sus planes de tratamiento. La frecuencia de esto depende del riesgo/severidad del enemigo. Al establecer un marco de seguimiento y presentación de informes, se garantizará que existan foros de escalada adecuados y que se adopten las respuestas adecuadas a los riesgos.

En un artículo anterior, identificamos el Plan de Gestión de Riesgos y Oportunidades (ROMP) como uno de los cinco elementos esenciales de la gestión de riesgos del proyecto. Debe incluir no sólo a las partes interesadas del proyecto y a los miembros de la gestión, sino también una cadencia de gestión para monitorear e informar sobre los riesgos y oportunidades. El método de su organización y gestión lo deciden conjuntamente el gestor de riesgos y el director del proyecto.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

- **Gestión:** Según Parodi (2020). La gestión se refiere a las acciones prácticas de establecimiento de objetivos. Soy el líder responsable de gestionar los procesos, los problemas y en última instancia la gestión de la empresa y la responsabilidad.
- **Riesgo:** Según Santos (2024). El riesgo es una medida del grado de daño en una situación peligrosa. El riesgo se mide teniendo en cuenta la vulnerabilidad específica a cada tipo de amenaza.
- **Servicio:** Según Sánchez (2024). Un servicio es un conjunto de acciones encaminadas a satisfacer las necesidades del cliente.
- **Redes:** Según Implika (2024). La infraestructura de red de datos crea formas de comunicar información a través de interacciones de datos.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. METODOLOGÍA Y TÉCNICAS UTILIZADAS

3.1.1. Tipo de investigación

La investigación fue aplicada, se concentra en la investigación y la búsqueda del conocimiento, acoge un enfoque diferente a las otras investigaciones al explorar cómo pueden alterarse los resultados o fenómenos del mundo real (Hernández, Fernández y Baptista, 2014).

3.1.2. Nivel de investigación

El nivel es descriptivo, explora el “qué” del objeto de estudio, en mayor medida que el “por qué” Busca describir y explicar lo que se está investigando, pero no brinda las razones por las que se dan las cosas. (Barrantes, 2002)

3.1.3. Método de investigación

El método fue Deductivo – Inductivo, inductivo es el enfoque utilizado en la investigación científica, porque buscó inferir conclusiones tipo general teniendo en cuenta observaciones específicas. Y deductivo, porque se parte de una premisa de carácter general para luego aplicar la lógica y llegar a una conclusión específica (Suárez, 2024).

3.1.4. Diseño de la investigación

La investigación fue Experimental de tipo preexperimental, donde se manipula la variable independiente para establecer su efecto en la variable dependiente; para ello, se utilizó un grupo experimental al cual se aplicó una prueba de pre test y post test respectivamente (Hernández, Fernandez y Batista, 2014).

Y1 ----- X----- Y2

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

3.2.1. Población

La población estuvo representada por todos los individuos relacionados con el estudio, siendo estos el personal del Área de Informática que conforman un total de 13 empleados.

3.2.2. Muestra

La muestra en una parte representativa de la población de estudio, pero al notar que la población estuvo conformada por un número pequeño, no es necesario emplear el método probabilístico, y siendo el más

adecuado la elección por conveniencia, debido a ello el total de la muestra fue la misma cantidad de la población siendo estos 13 empleados.

3.3. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

El instrumento adecuado para este tipo de estudio fue el cuestionario de preguntas donde se tiene en cuenta la variable dependiente e independiente de la investigación al momento de elaborar las preguntas.

3.4. PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS

La recolección de datos se empleó en dos instantes, uno antes de implementar y otro posterior a la implementación de la solución, y de esta forma medir el grado de mejora.

El cuestionario fue aplicado a la muestra de empleados elegidos, y posterior a la respectiva capacitación sobre temas técnicos si fuera necesario.

3.5. TRATAMIENTO DE DATOS

Para el tratamiento de datos se utilizó una herramienta de software estadístico, en este caso el SPSS de IBM, a través del cual se obtuvieron resúmenes de información, gráficos y valores adecuados para determinar el resultado de la investigación.

3.6. GRADO DE CONFIABILIDAD DE LOS DATOS

Se utilizó el alfa de Cronbach que viene a ser el coeficiente utilizado para determinar la consistencia del instrumento aplicado.

CAPÍTULO V

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS DE LA INVESTIGACIÓN PRE-TEST

Tabla 2

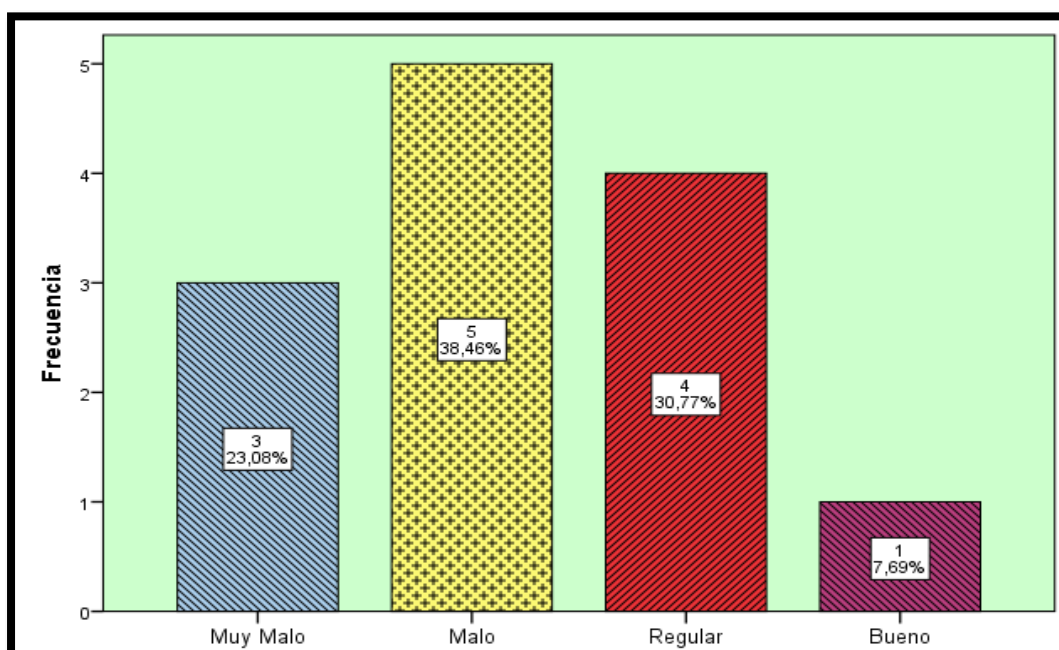
¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	3	23,1	23,1	23,1
	Malo	5	38,5	38,5	61,5
	Regular	4	30,8	30,8	92,3
	Bueno	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 3

¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?



Fuente: Tabla 2.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 23,08% afirma sobre los medios utilizados para efectuar una correcta gestión de riesgos son muy malas, un 38,46% lo consideran malo, un 30,77% afirma que es regular y por último un 7,69% cree que es bueno.

Tabla 3

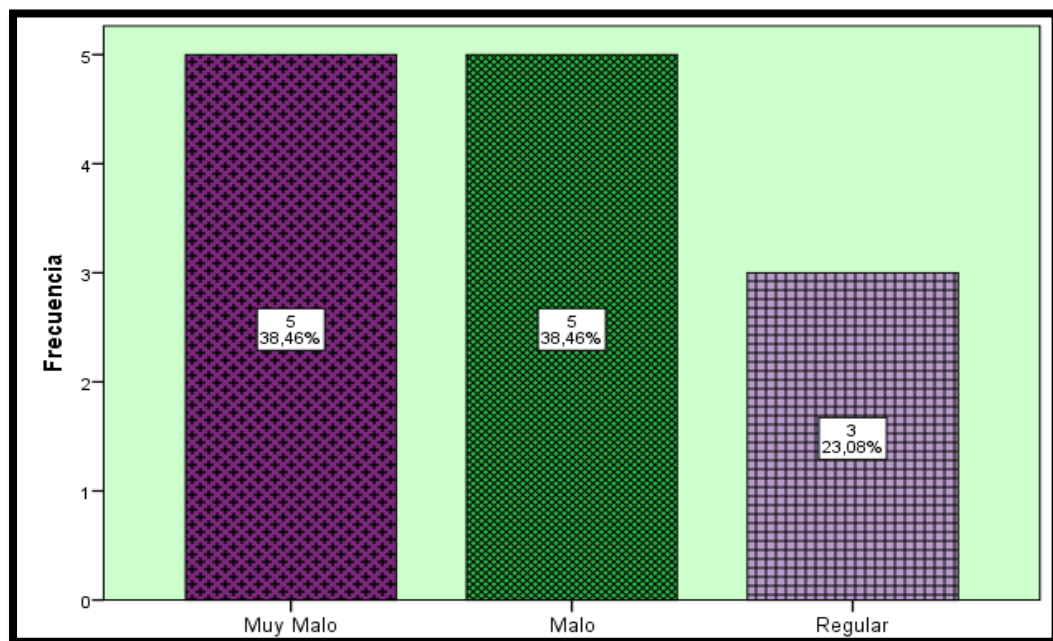
¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Muy Malo	5	38,5	38,5	38,5
Malo	5	38,5	38,5	76,9
Regular	3	23,1	23,1	100,0
Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 4

¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?



Fuente: Tabla 3.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% considera sobre los métodos utilizados para efectuar una correcta gestión de riesgos es muy mala, un 38,46% lo consideran malo, y por último un 23,08% manifiesta que es regular.

Tabla 4

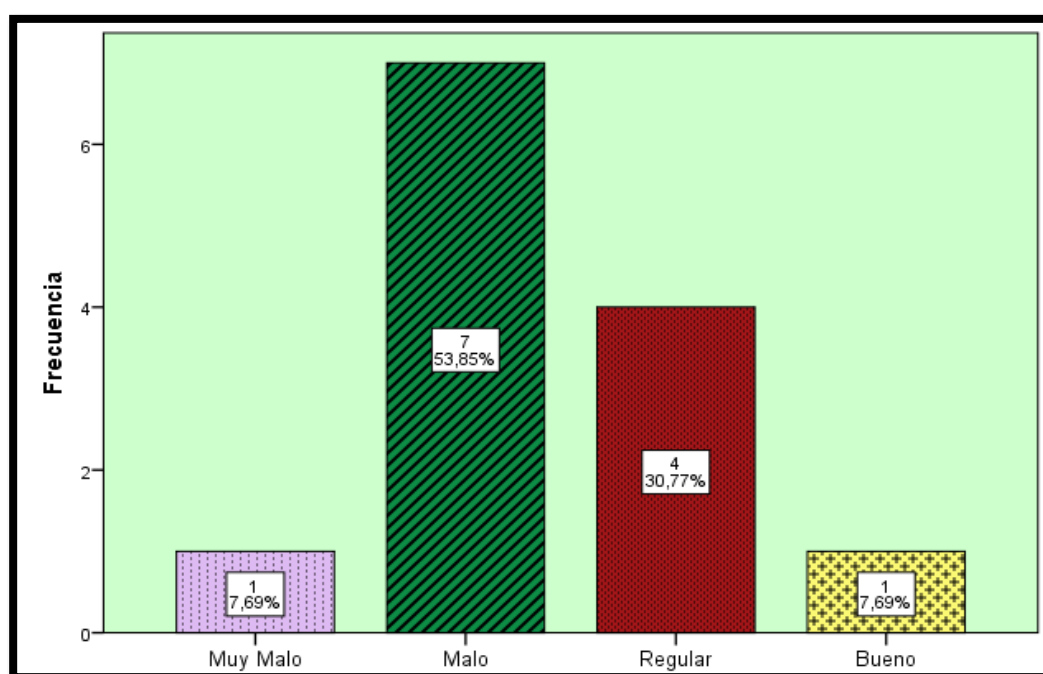
¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	1	7,7	7,7	7,7
	Malo	7	53,8	53,8	61,5
	Regular	4	30,8	30,8	92,3
	Bueno	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 5

¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?



Fuente: Tabla 4.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 7,69% afirma sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgos son muy malas, un 53,85% lo consideran malo, un 30,77% afirma que es regular y por último un 7,69% cree que es bueno.

Tabla 5

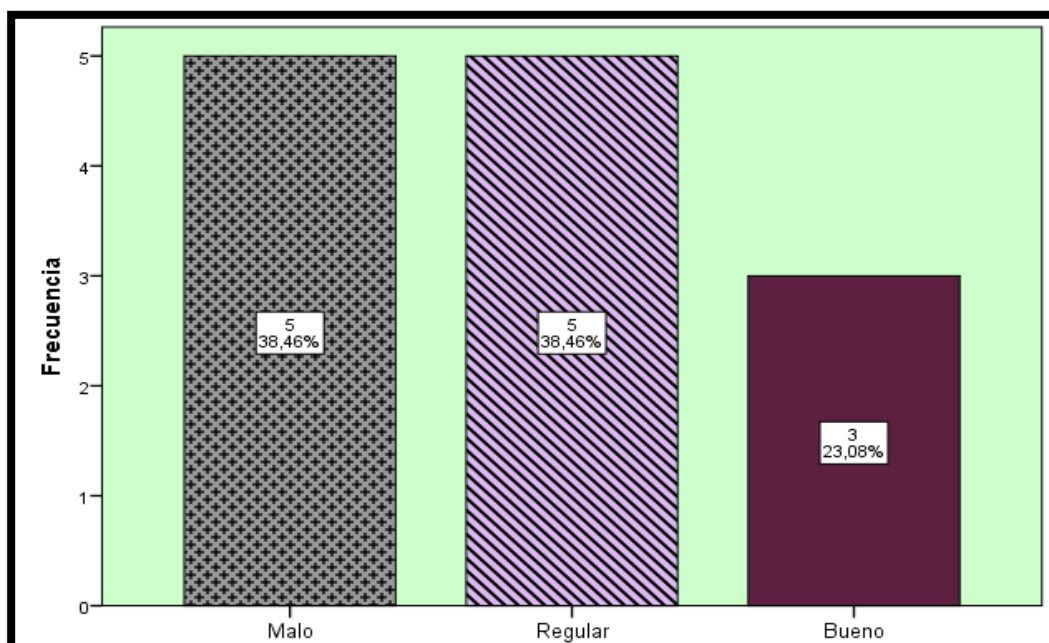
¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Malo	5	38,5	38,5	38,5
	Regular	5	38,5	38,5	76,9
	Bueno	3	23,1	23,1	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 6

¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?



Fuente: Tabla 5.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% considera sobre las perspectivas de diagnóstico empleadas en la gestión de riesgos es muy mala, un 30,77% lo consideran regular, y por último un 23,08% manifiesta que es bueno.

Tabla 6

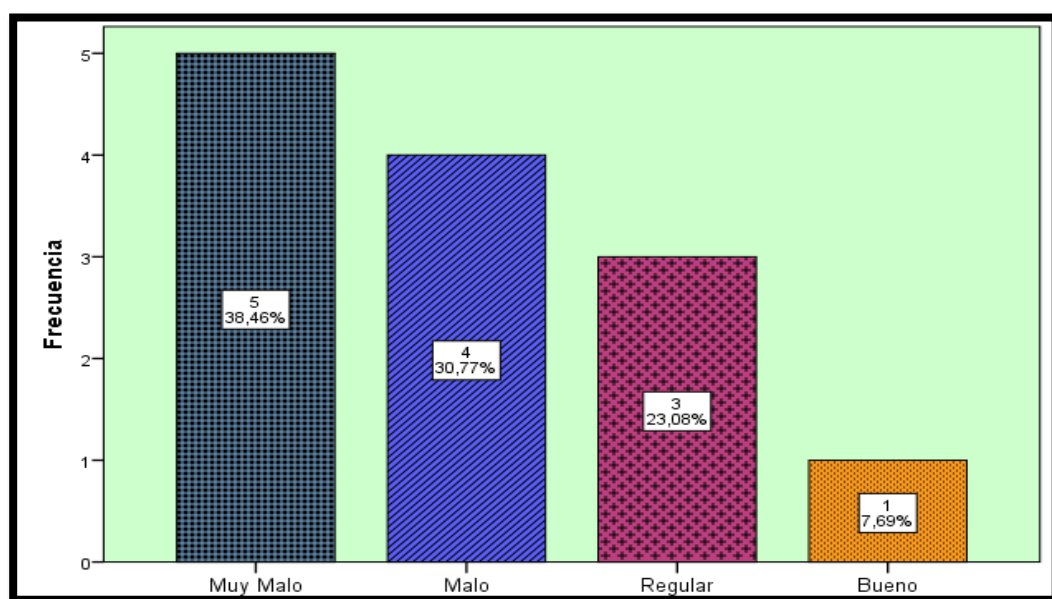
¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	5	38,5	38,5	38,5
	Malo	4	30,8	30,8	69,2
	Regular	3	23,1	23,1	92,3
	Bueno	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 7

¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?



Fuente: Tabla 6.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% afirma sobre el grado de diagnóstico obtenido en la gestión de riesgo es muy malo, un 30,77% lo consideran malo, un 23,08% afirma que es regular y por último un 7,69% afirma que es bueno.

Tabla 7

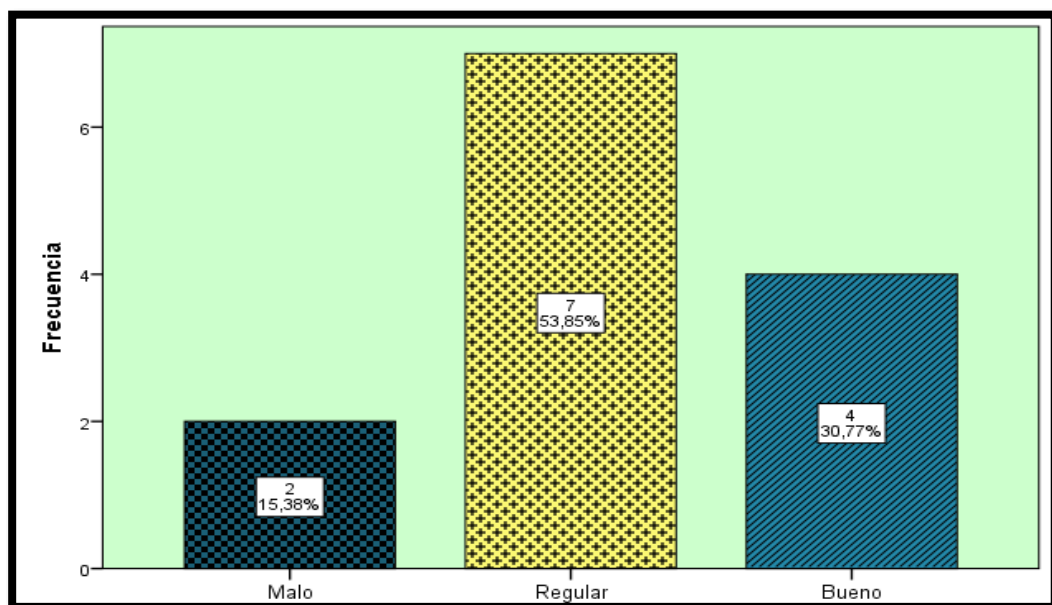
¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Malo	2	15,4	15,4	15,4
	Regular	7	53,8	53,8	69,2
	Bueno	4	30,8	30,8	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 8

¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?



Fuente: Tabla 7.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 15,38% considera sobre la comparación entre controles de seguridad para la gestión de riesgo es mala, un 53,85% lo consideran regular, y por último un 30,77% manifiesta que es bueno.

Tabla 8

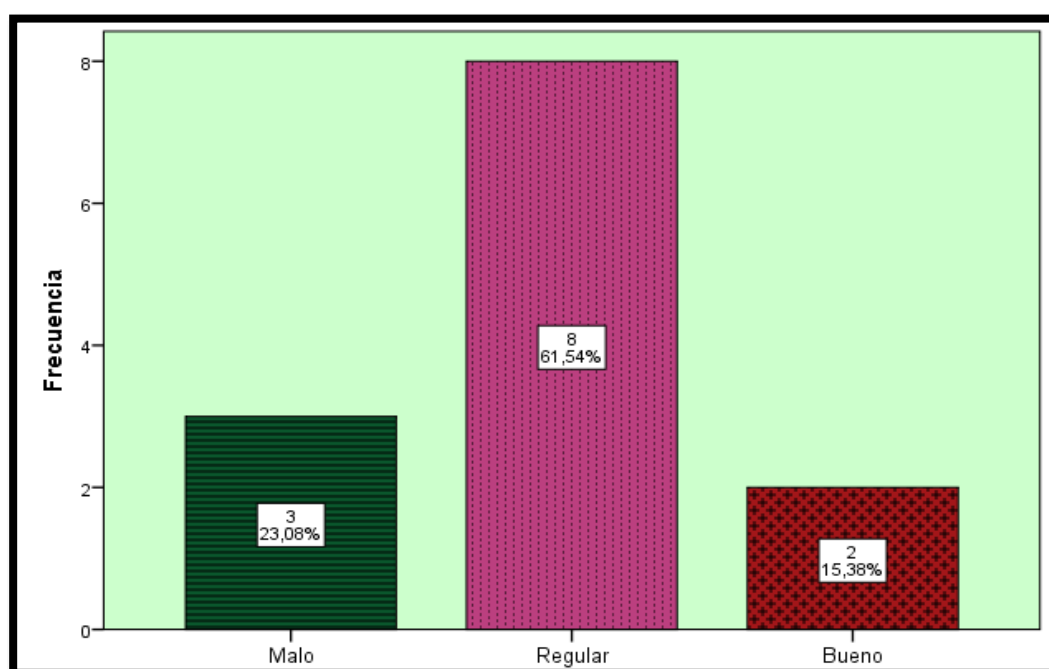
¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Malo	3	23,1	23,1	23,1
	Regular	8	61,5	61,5	84,6
	Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 9

¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?



Fuente: Tabla 8.

Interpretación: En la figura y tabla mostrada del total de las 13 personas encuestadas, un 23,08% considera sobre las alternativas identificadas para la gestión de riesgo es mala, un 61,54% lo consideran regular, y por último un 15,38% manifiesta que es bueno.

Tabla 9

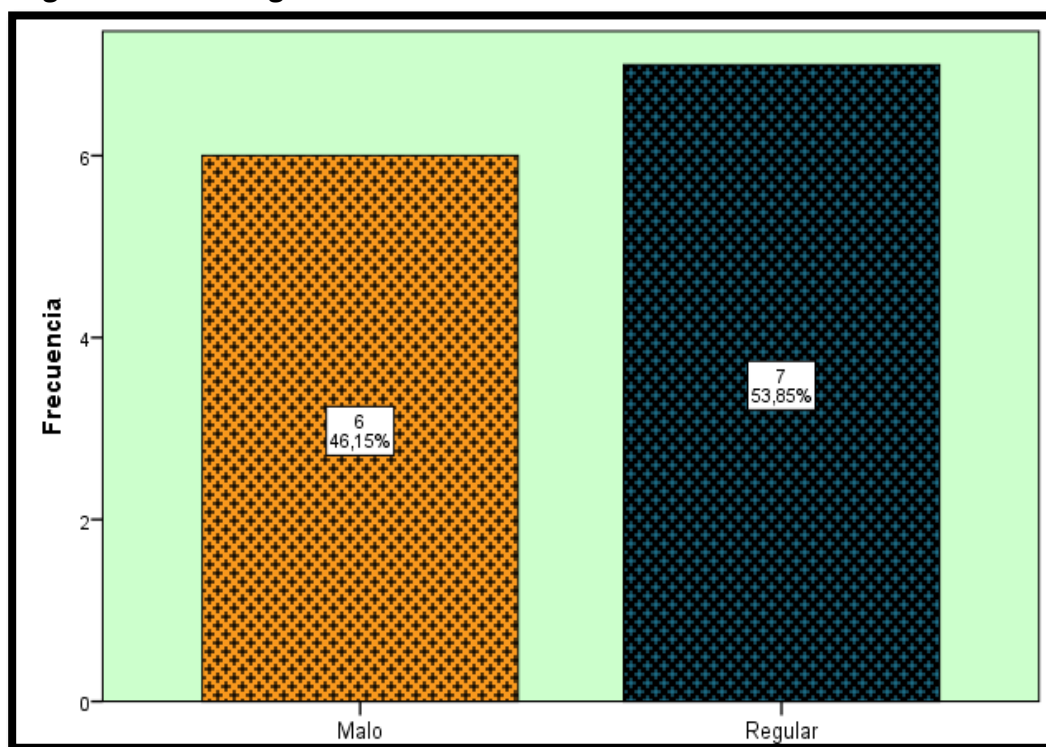
¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Malo	6	46,2	46,2	46,2
Válidos Regular	7	53,8	53,8	100,0
Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 10

¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?



Fuente: Tabla 9.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 46,15% considera sobre las alternativas seleccionadas para la gestión de riesgo es mala, mientras que un 53,85% lo consideran regular

Tabla 10

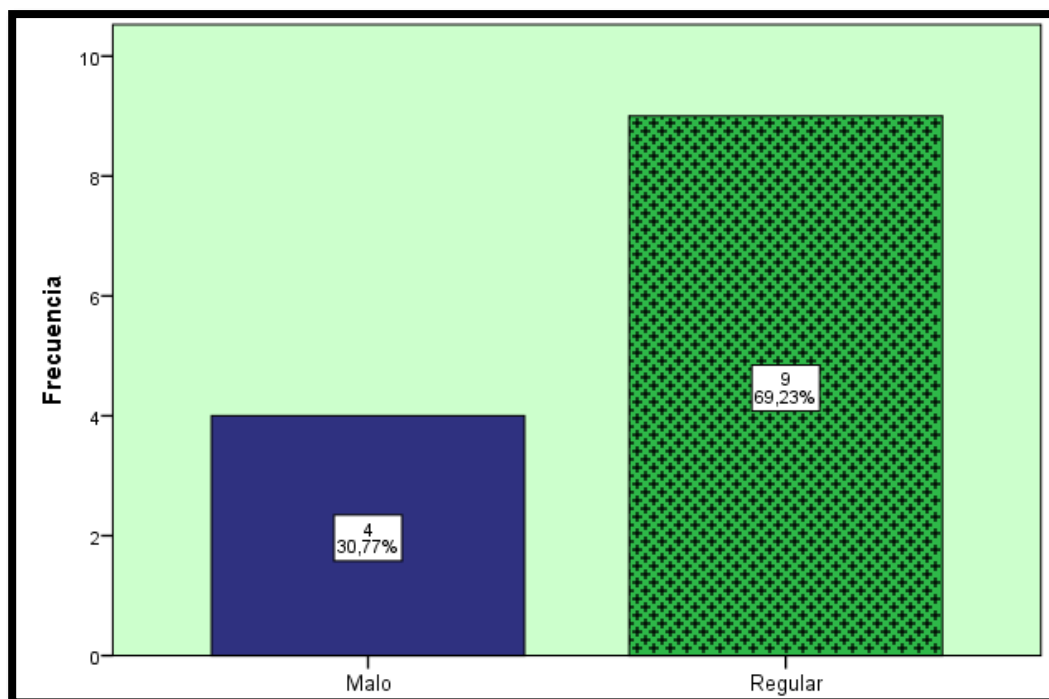
¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Malo	4	30,8	30,8	30,8
	Regular	9	69,2	69,2	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 11

¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?



Fuente: Tabla 10.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 30,77% considera sobre el grado de eficiencia empleado para la gestión de servicios de la red datos es mala, mientras que un 69,23% lo consideran regular.

Tabla 11

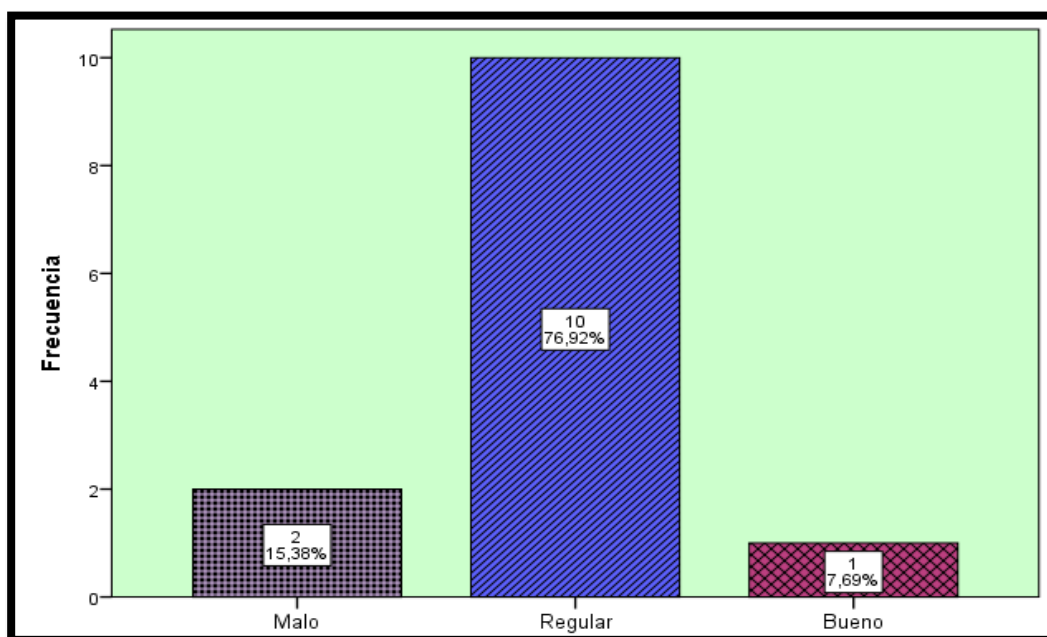
¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Malo	2	15,4	15,4	15,4
	Regular	10	76,9	76,9	92,3
	Bueno	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 12

¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?



Fuente: Tabla 11.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 15,38% considera sobre el grado de efectividad empleado para la gestión de servicios de la red de datos es mala, un 76,92% lo consideran regular, y por último un 7,69% manifiesta que es bueno.

Tabla 12

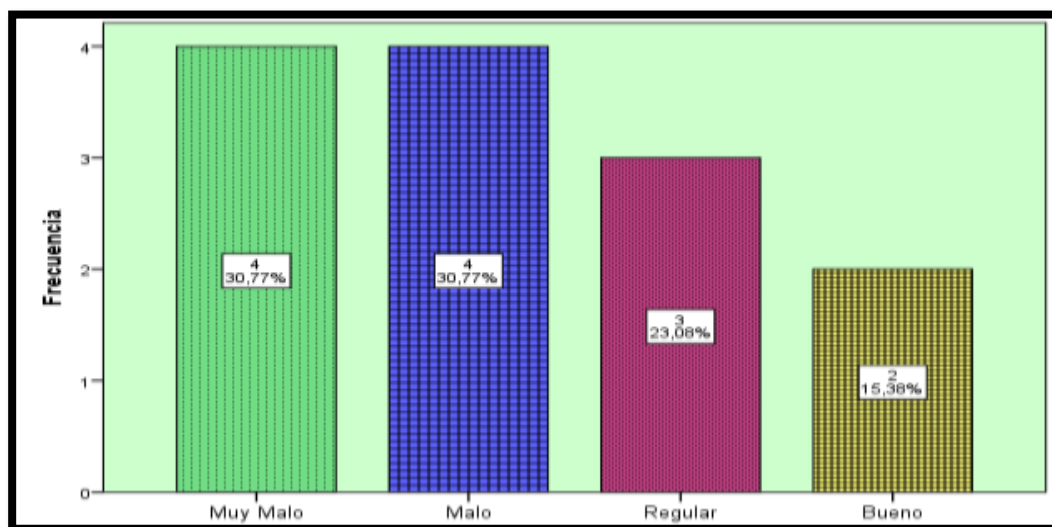
¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	4	30,8	30,8	30,8
	Malo	4	30,8	30,8	61,5
	Regular	3	23,1	23,1	84,6
	Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 13

¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?



Fuente: Tabla 12.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 30,77% afirma sobre el grado de confianza que emiten los controles y/o mecanismos empelados para la gestión de servicios de la red de datos es muy malo, un 30,77% lo consideran malo, un 23,08% afirma que es regular y por último un 15,38% afirma que es bueno.

Tabla 13

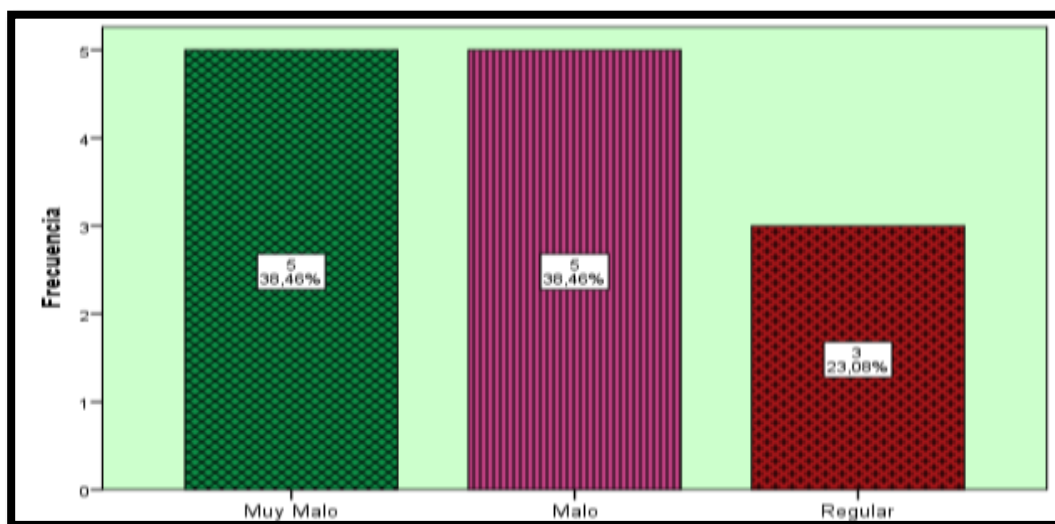
¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	5	38,5	38,5	38,5
	Malo	5	38,5	38,5	76,9
	Regular	3	23,1	23,1	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 14

¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?



Fuente: Tabla 13.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% considera sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la gestión de servicios de la red de datos es muy mala, un 38,46% lo consideran malo, y por último un 23,08% manifiesta que es regular.

Tabla 14

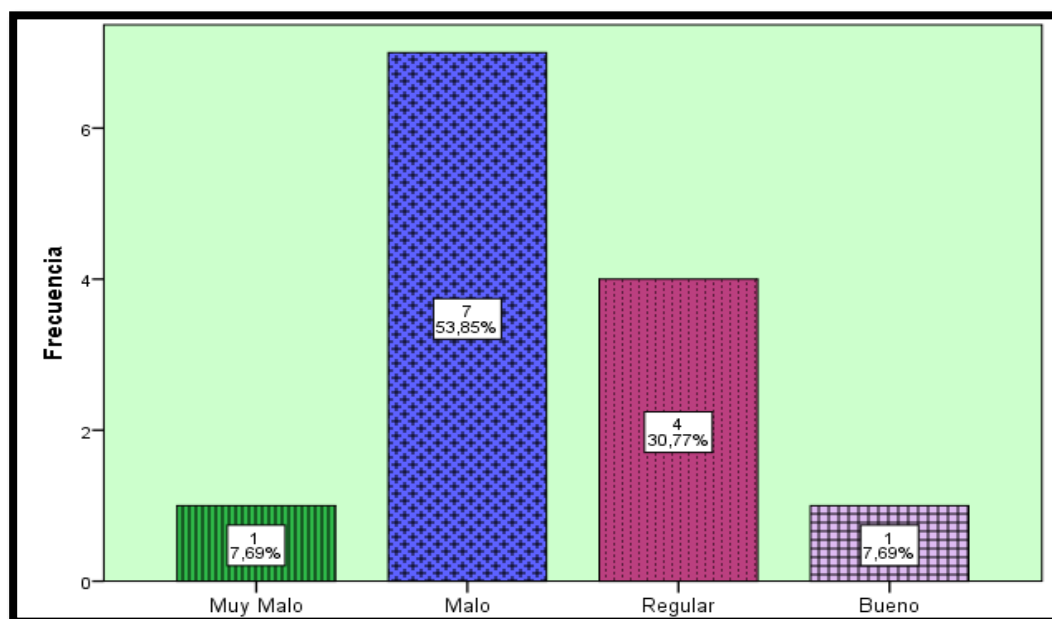
¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Muy Malo	1	7,7	7,7	7,7
Malo	7	53,8	53,8	61,5
Válidos Regular	4	30,8	30,8	92,3
Bueno	1	7,7	7,7	100,0
Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 15

¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?



Fuente: Tabla 14.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 7,69% afirma sobre el tiempo de respuesta a sucesos por la gestión de servicios de la red de datos es muy malo, un 53,85% lo consideran malo, un 30,77% afirma que es regular y por último un 7,69% afirma que es bueno.

Tabla 15

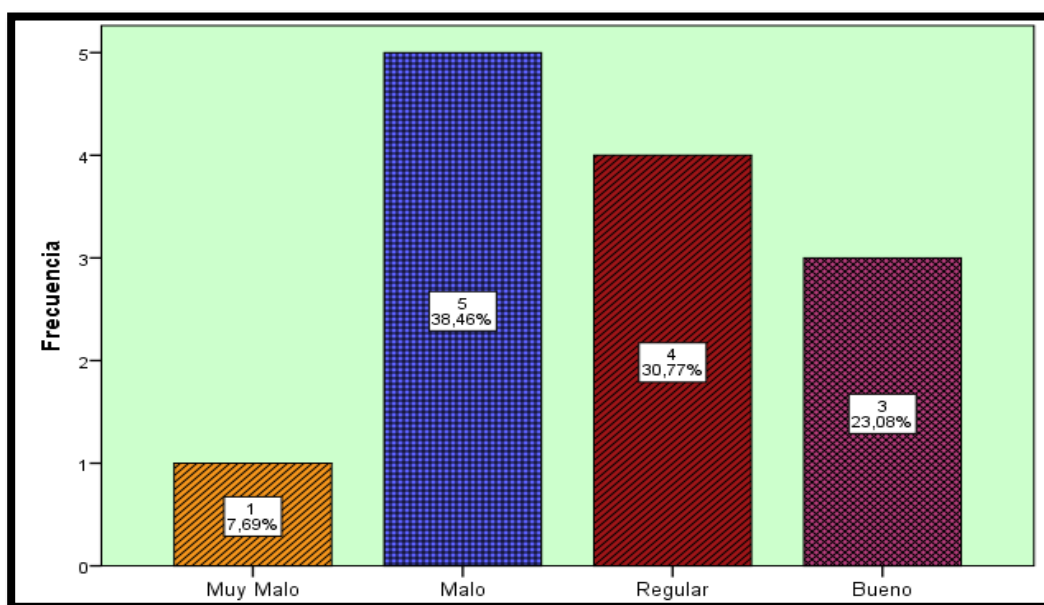
¿Cuál es su punto de vista sobre las actividades de mejora continua empleados en la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	1	7,7	7,7	7,7
	Malo	5	38,5	38,5	46,2
	Regular	4	30,8	30,8	76,9
	Bueno	3	23,1	23,1	100,0
	Total	13	100,0	100,0.	

Fuente: Instrumento aplicado.

Tabla 16

¿Cuál es su punto de vista sobre las actividades de mejora continua empleados en la Gestión de servicios de la red de datos?



Fuente: Tabla 15.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 7,69% afirma sobre las actividades de mejora continua empleados en la gestión de servicios de la red de datos es muy malo, un 38,46% lo consideran malo, un 30,77% afirma que es regular y por último un 23,08% afirma que es bueno.

4.2. RESULTADOS DE LA INVESTIGACIÓN POST-TEST

Tabla 16

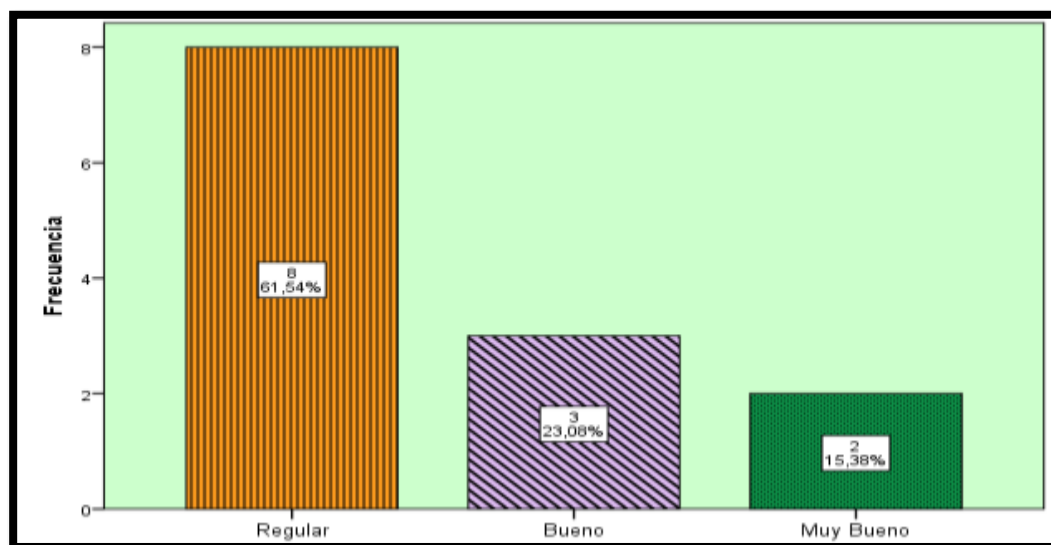
¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	8	61,5	61,5	61,5
	Bueno	3	23,1	23,1	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 17

¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?



Fuente: Tabla 16.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 61,54% afirma sobre los medios utilizados para efectuar una correcta gestión de riesgos es regular, un 23,08% lo consideran bueno, y por último un 15,38% cree que es muy bueno.

Tabla 17

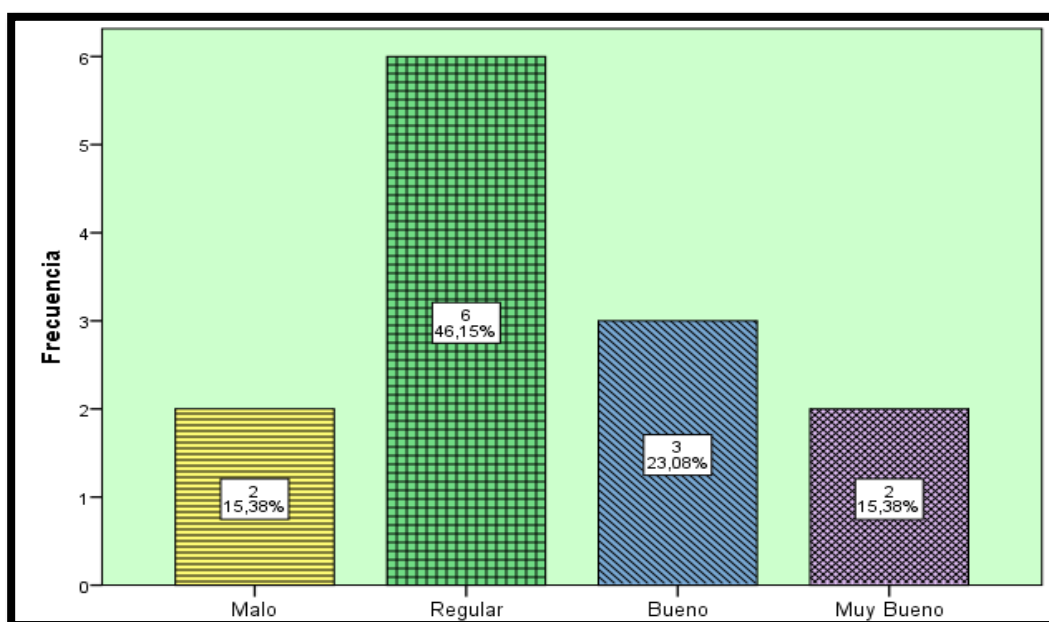
¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Malo	2	15,4	15,4	15,4
Regular	6	46,2	46,2	61,5
Válidos Bueno	3	23,1	23,1	84,6
Muy Bueno	2	15,4	15,4	100,0
Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 18

¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?



Fuente: Tabla 17.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 15,38% considera sobre los métodos utilizados para efectuar una correcta gestión de riesgos es malo, un 46,15% lo consideran regular, un 23,08 afirman que bueno y por último un 15,38% manifiesta que es muy bueno.

Tabla 18

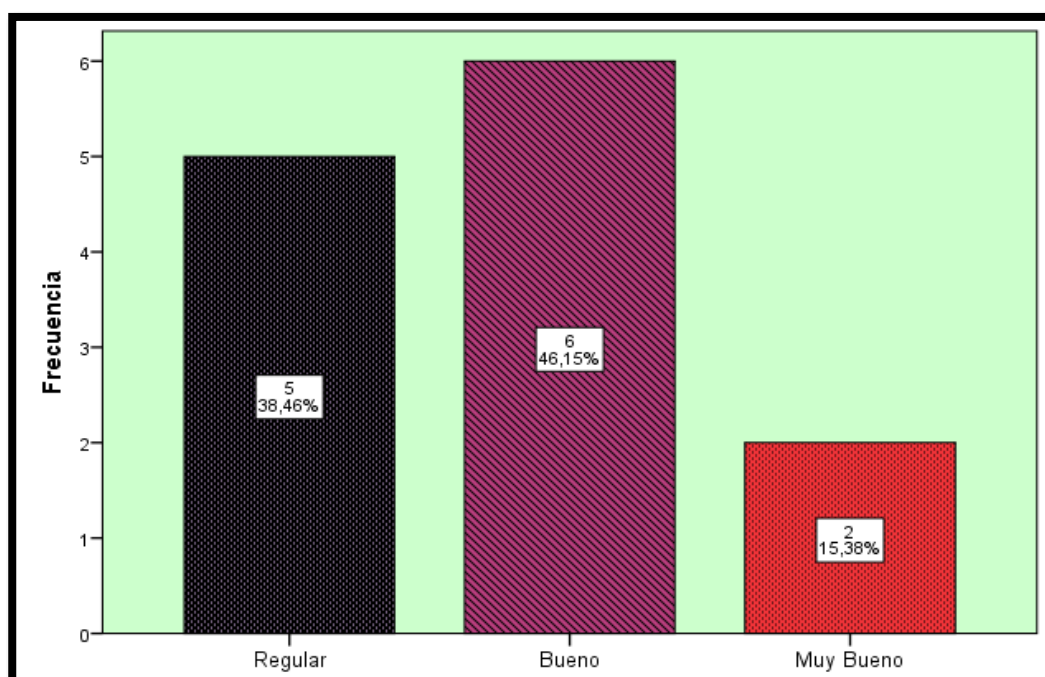
¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	5	38,5	38,5	38,5
	Bueno	6	46,2	46,2	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 19

¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?



Fuente: Tabla 18.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% afirma sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgos son regulares, un 46,15% lo consideran bueno, y por último un 15,38% creen que es muy bueno.

Tabla 19

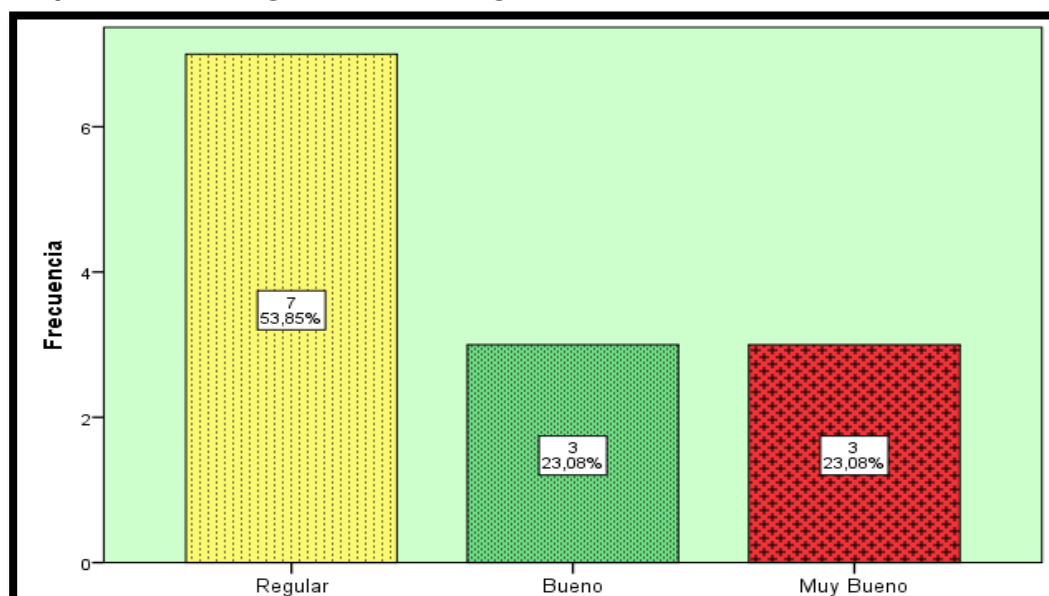
¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	7	53,8	53,8	53,8
	Bueno	3	23,1	23,1	76,9
	Muy Bueno	3	23,1	23,1	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 20

¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?



Fuente: Tabla 19.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 53,85% considera sobre las perspectivas de diagnóstico empleadas en la gestión de riesgos es regular, un 23,08% lo consideran bueno, y por último un 23,08% manifiesta que es muy bueno.

Tabla 20

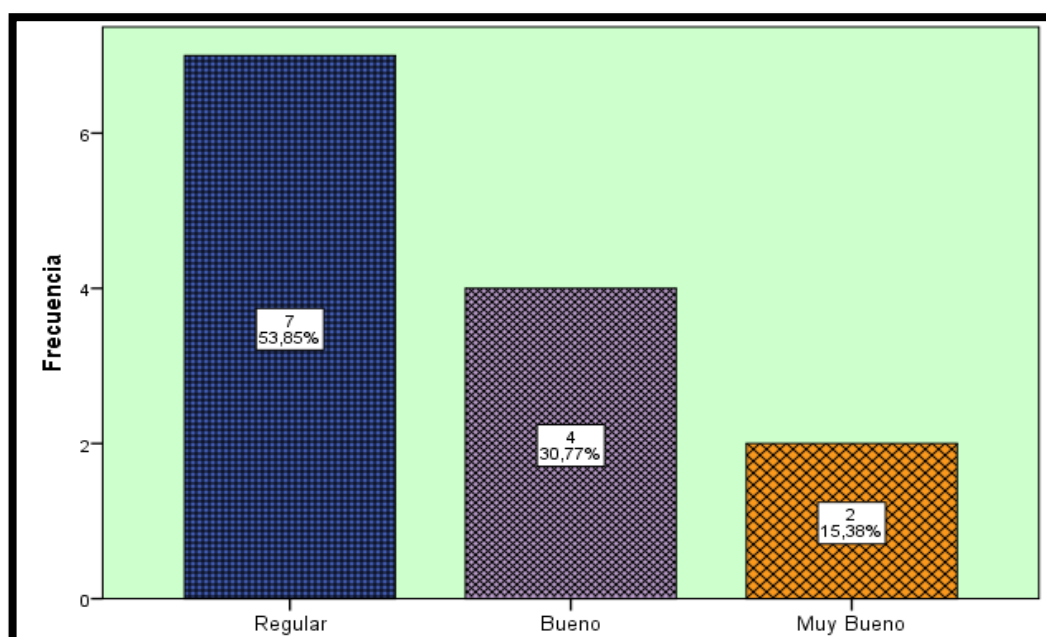
¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	7	53,8	53,8	53,8
	Bueno	4	30,8	30,8	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 21

¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?



Fuente: Tabla 20.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 53,85% afirma sobre el grado de diagnóstico obtenido en la gestión de riesgo que es regular, un 30,77% lo consideran bueno, y por último un 15,38% consideran que es muy bueno.

Tabla 21

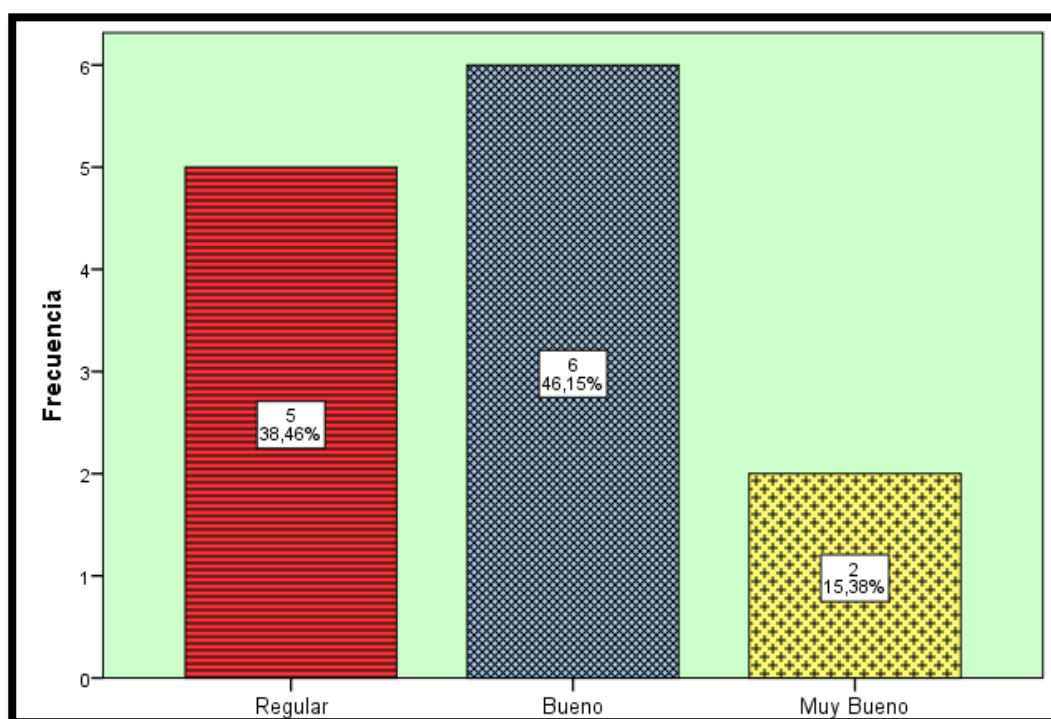
¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	5	38,5	38,5	38,5
	Bueno	6	46,2	46,2	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 22

¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?



Fuente: Tabla 21.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% considera sobre la comparación entre controles de seguridad para la gestión de riesgo que es regular, un 46,15% lo consideran bueno, y en último caso un 15,38% manifiesta que es muy bueno.

Tabla 22

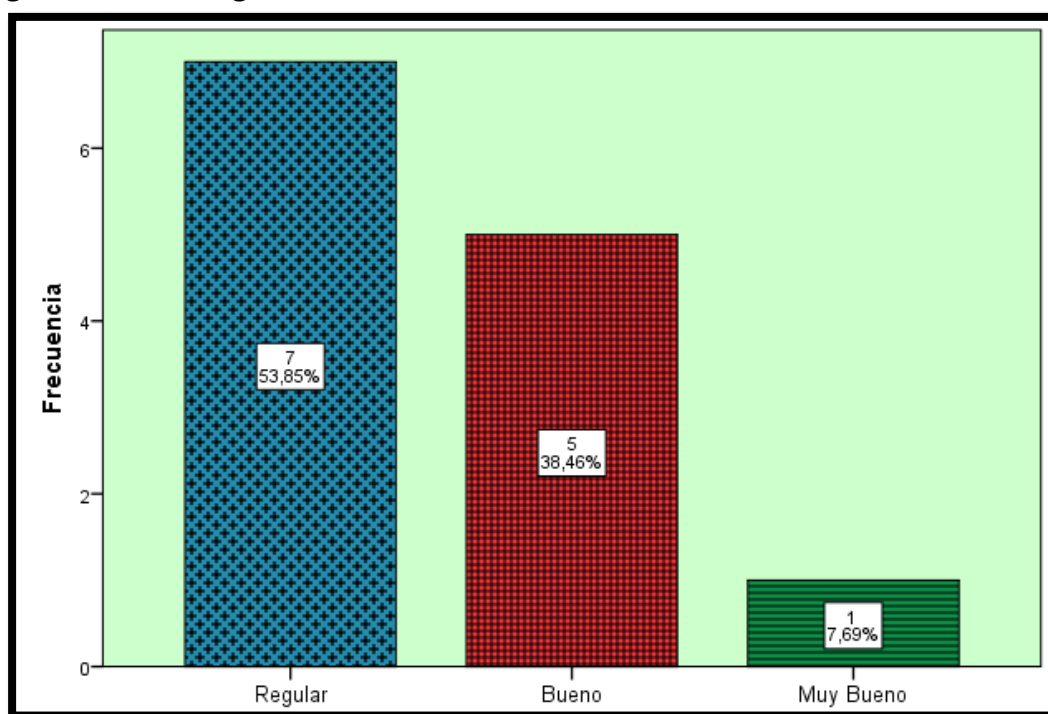
¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	7	53,8	53,8	53,8
	Bueno	5	38,5	38,5	92,3
	Muy Bueno	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 23

¿Cuál es su punto de vista sobre las alternativas identificadas para la gestión de riesgo?



Fuente: Tabla 22.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 53,85% considera sobre las alternativas identificadas para la gestión de riesgo es regular, un 38,46% lo consideran bueno, y por último un 7,69% manifiesta que es muy bueno.

Tabla 23

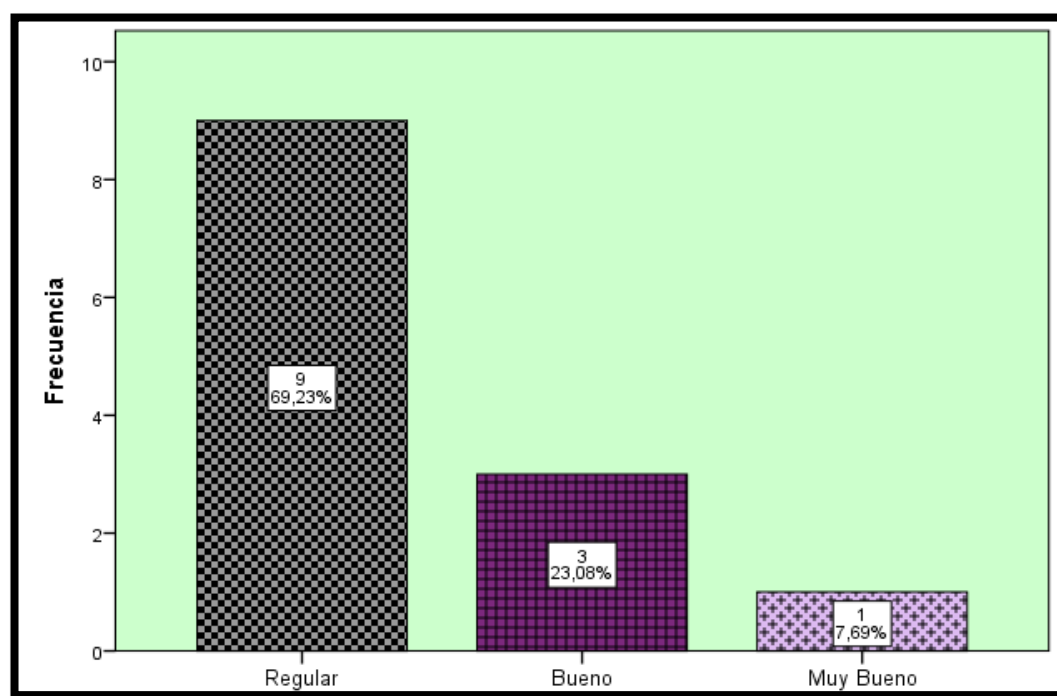
¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	9	69,2	69,2	69,2
	Bueno	3	23,1	23,1	92,3
	Muy Bueno	1	7,7	7,7	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 24

¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?



Fuente: Tabla 23.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 69,23% considera sobre las alternativas seleccionadas para la gestión de riesgo es regular, mientras que un 23,08% lo consideran bueno y por último un 7,69 los consideran muy bueno.

Tabla 24

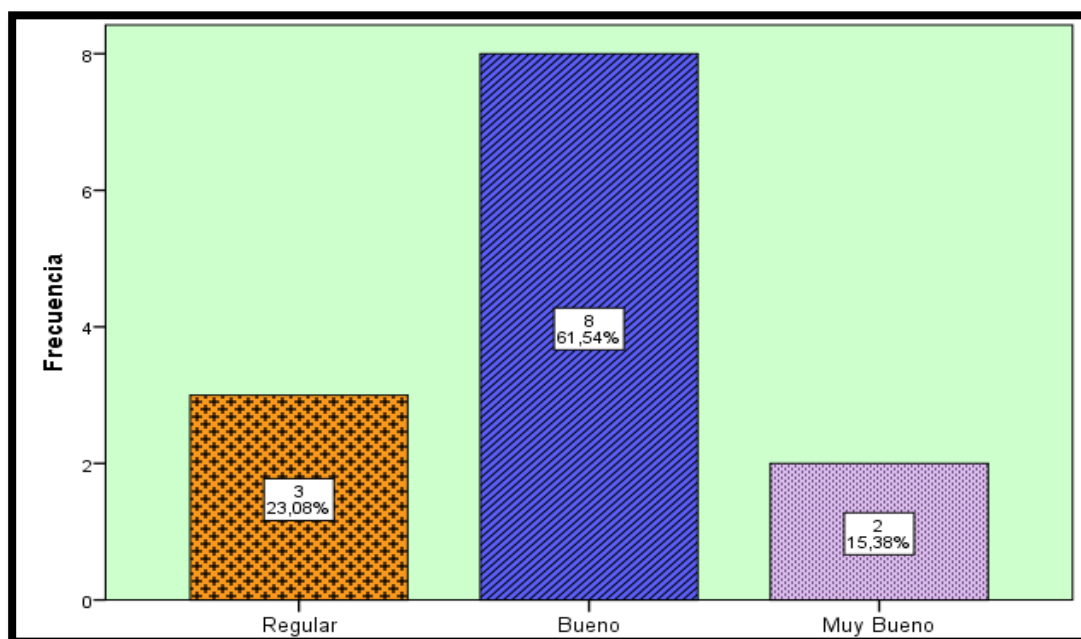
¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	3	23,1	23,1	23,1
	Bueno	8	61,5	61,5	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Tabla 25

¿Cuál es su punto de vista sobre las alternativas seleccionadas para la gestión de riesgo?



Fuente: Tabla 24.

Interpretación: En la tabla y figura mostrado del total de las 13 personas encuestadas, un 23,08% considera sobre el grado de eficiencia empleado para la gestión de servicios de la red datos es regular, mientras que un 61,543% lo consideran bueno y finalmente un 15,38 lo consideran muy bueno.

Tabla 25

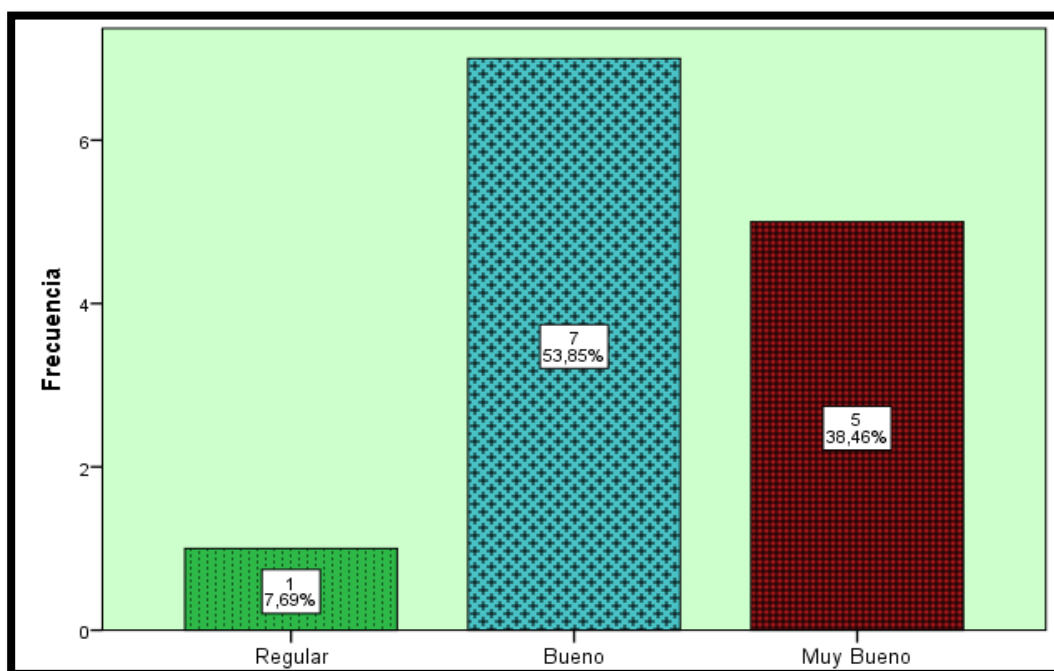
¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	1	7,7	7,7	7,7
	Bueno	7	53,8	53,8	61,5
	Muy Bueno	5	38,5	38,5	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 26

¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?



Fuente: Tabla 25.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 7,69% considera sobre el grado de efectividad empleado para la gestión de servicios de la red de datos es regular, un 53,85% lo consideran bueno, y por último un 38,46% manifiesta que es muy bueno.

Tabla 26

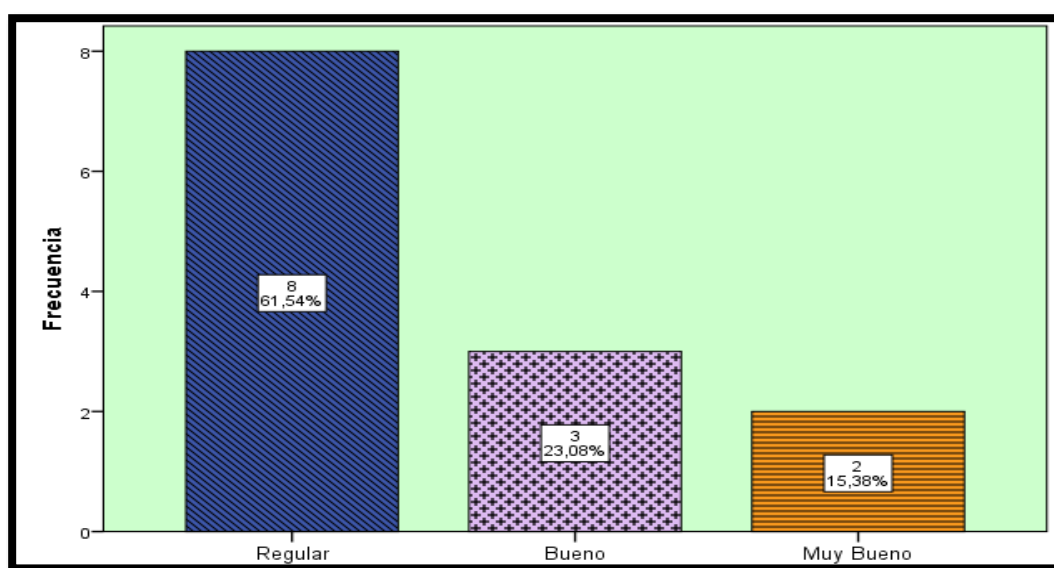
¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	8	61,5	61,5	61,5
	Bueno	3	23,1	23,1	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 27

¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?



Fuente: Tabla 26.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 61,54% afirma sobre el grado de confianza que emiten los controles y/o mecanismos empelados para la gestión de servicios de la red de datos es regular, un 23,08% lo consideran bueno, y por último un 15,38% afirma que es muy bueno.

Tabla 27

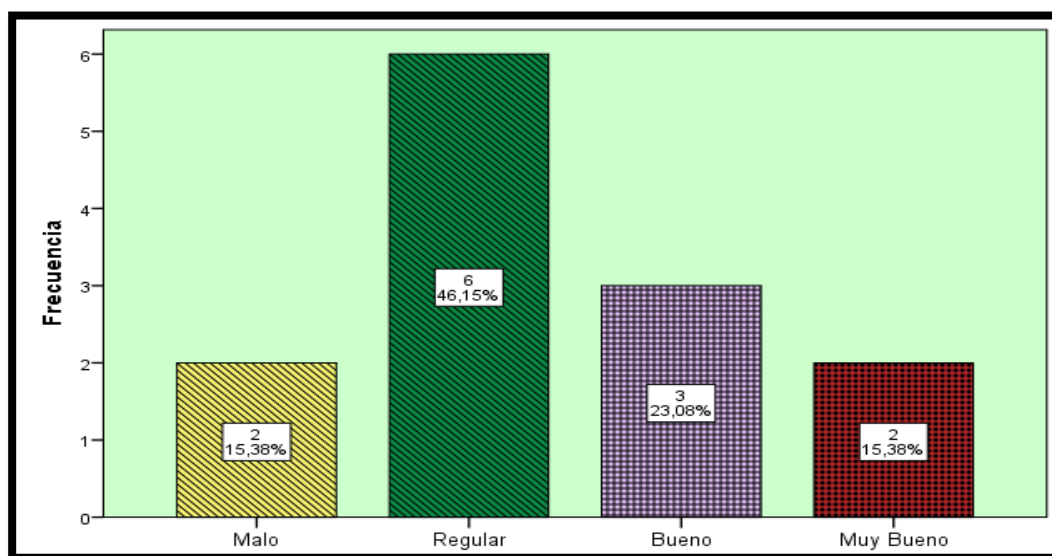
¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Malo	2	15,4	15,4	15,4
Regular	6	46,2	46,2	61,5
Válidos Bueno	3	23,1	23,1	84,6
Muy Bueno	2	15,4	15,4	100,0
Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 28

¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?



Fuente: Tabla 27.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 15,38% considera sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la gestión de servicios de la red de datos es malo, un 46,15% lo consideran regular, un 23,08 lo consideran bueno y por último un 15,38% manifiesta que es muy bueno.

Tabla 28

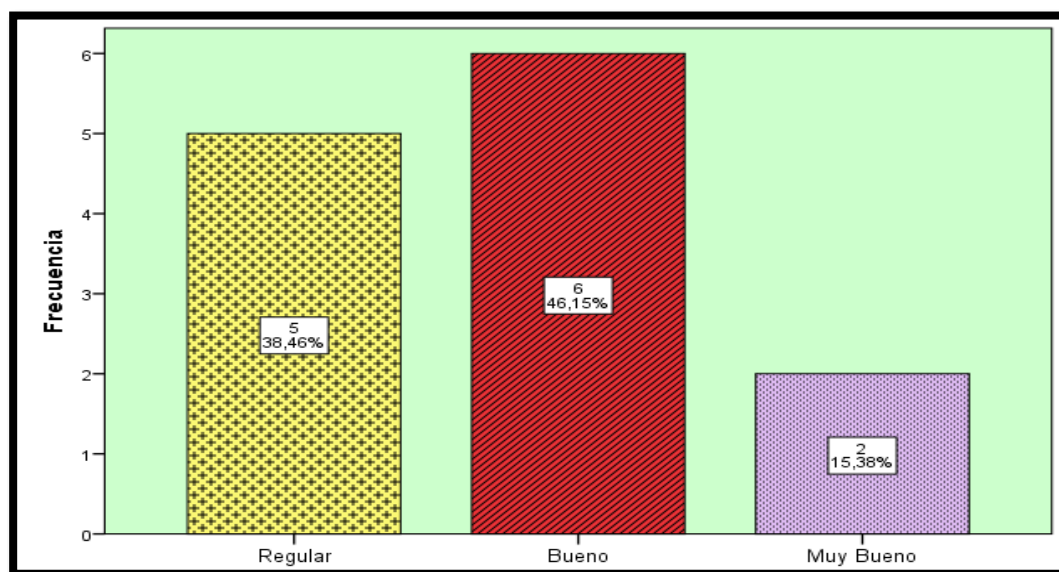
¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	5	38,5	38,5	38,5
	Bueno	6	46,2	46,2	84,6
	Muy Bueno	2	15,4	15,4	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 29

¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?



Fuente: Tabla 28.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 38,46% afirma sobre el tiempo de respuesta a sucesos por la gestión de servicios de la red de datos es regular, un 46,15% lo consideran bueno y por último un 15,38% afirma que es muy bueno.

Tabla 29

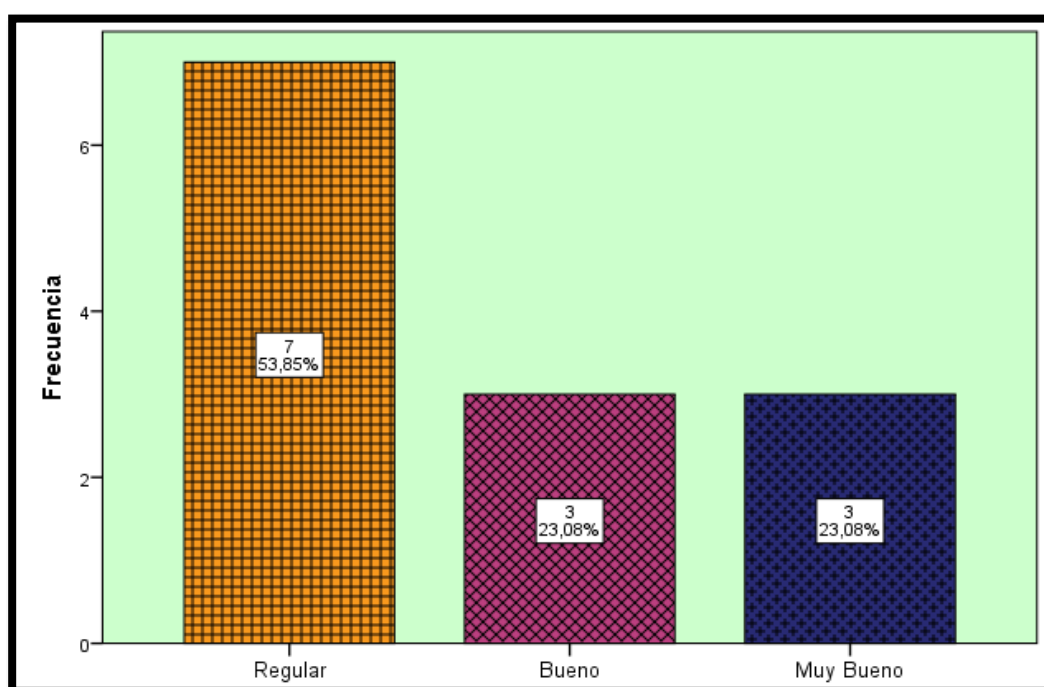
¿Cuál es su punto de vista sobre las actividades de mejora continuad empleados en la Gestión de servicios de la red de datos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	7	53,8	53,8	53,8
	Bueno	3	23,1	23,1	76,9
	Muy Bueno	3	23,1	23,1	100,0
	Total	13	100,0	100,0	

Fuente: Instrumento aplicado.

Figura 30

¿Cuál es su punto de vista sobre las actividades de mejora continuad empleados en la Gestión de servicios de la red de datos?



Fuente: Tabla 29.

Interpretación: En la tabla y figura mostrada del total de las 13 personas encuestadas, un 53,85% afirma sobre las actividades de mejora continua empleados en la gestión de servicios de la red de datos es regular, un 23,08% lo consideran bueno y por último un 23,08% afirman que es muy bueno.

4.3. MEDICIÓN DE NORMALIDAD

Según Reyna (2019) afirma que antes de querer aplicar test estadísticos para comparar las medias, es básico saber si las muestras provienen de una distribución normal (Normalidad) y si presentan en conjunto igualdad de varianzas. De igual forma, también precisa: el test de Shapiro-Wilk se usa para contrastar si un conjunto de datos sigue una distribución normal o no. Para la investigación realizada mediremos la normalidad del instrumento de recolección de datos tanto ante como después de la implementación de la solución utilizando el estadístico de Shapiro-Wilk y porque además nuestra muestra es menor de 50, aplicando el software SPSS.

Para ello utilizamos los siguientes niveles:

- Nivel de confianza = 95%
- Desviación estándar $Z = < -1,96$ o $> +1,96$
- Nivel de significancia = 0.05.

H0: La variable esta normalmente distribuida.

H1: La variable **NO** está normalmente distribuida.

Rechazamos la H_0 si nuestro p valor es menor de 0.05 (nivel de significancia).

Tabla 30

Pruebas de normalidad

	Kolmogórov-Smirnov			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Gestión de Riesgos	,373	13	,000	,709	13	,001
Gestión de servicios de la red de datos	,392	13	,000	,628	13	,000

a. Corrección de la significación de Lilliefors.

Se observa en la gráfica los resultados de la prueba para la variable Gestión de Riesgos se obtuvo un valor de 0,001 menor a 0,05 por lo cual se determina que tiene una distribución no normal. Asimismo, para la variable Gestión de servicios de la red datos se obtuvo un valor de 0,000 menor a 0,05, por lo cual también se determina que tiene una distribución no normal.

Entonces como nuestras variables no están normalmente distribuidas se realizaron las pruebas no paramétricas de un estudio longitudinal de muestras relacionadas ya que usaremos una sola muestra en dos tiempos distintos, teniendo así dos medidas para lo cual se aplicó el estadístico de Wilcoxon porque la medida es ordinal ya que se utilizó la escala de Likert de 1-5, siendo 1 el máximo valor negativo y 5 el máximo valor positivo.

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

4.4. PRUEBA DE HIPÓTESIS

4.4.1. Prueba de hipótesis general

- **H0:** La implementación de la gestión de riesgo **NO** mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.
- **H1:** La implementación de la gestión de riesgo mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

Tabla 31

Prueba de los rangos con signo de Wilcoxon - HG

		N	Rango promedio	Suma de rangos
	Rangos negativos	0 ^a	,00	,00
V1V2POST – VIV2PRE	Rangos positivos	13 ^b	7,00	91,00
	Empates	0 ^c		
	Total	13		

a. V1V2POST < VIV2PRE

b. V1V2POST > VIV2PRE

c. V1V2POST = VIV2PRE

Tabla 32

Estadística de Wilcoxon - HG

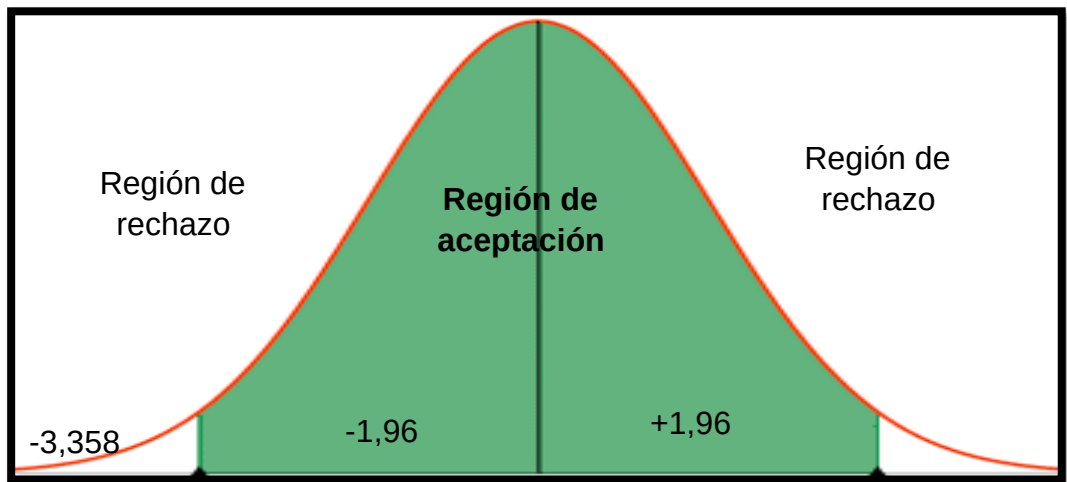
	V1V2POST - VIV2PRE
Z.	-3,358 ^b
Sig. asintót. (bilateral)	,001

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Figura 31

Curva de distribución normal estándar en una prueba de hipótesis bilateral



Después de realizar el análisis de Wilcoxon el resultado de la significación asintótica bilateral ($p=0.01$) es menor a 0.05 (α). Como al trabajar a un nivel del 95% se tiene un valor de ± 1.96 para los límites de la región de aceptación, como el valor de $Z = -3.358$, se ubica en la zona de rechazo.

Por lo tanto, se rechaza H_0 y se acepta H_1 en base a lo explicado se concluye que la implementación de la gestión de riesgo mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

4.4.2. Prueba de hipótesis específicas

Hipótesis específica 1

- **H0:** Las condiciones la confiabilidad del servicio de red **NO** mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.
- **H1:** Las condiciones la confiabilidad del servicio de red mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

Tabla 33

Prueba de los rangos con signo de Wilcoxon – HE1

		N	Rango promedio	Suma de rangos
POST_H1 - PRE_H1	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	10 ^b	5,50	55,00
	Empates	3 ^c		
	Total	13		

a. POST_H1 < PRE_H1

b. POST_H1 > PRE_H1

c. POST_H1 = PRE_H1

Tabla 34

Estadística de Wilcoxon – HE1

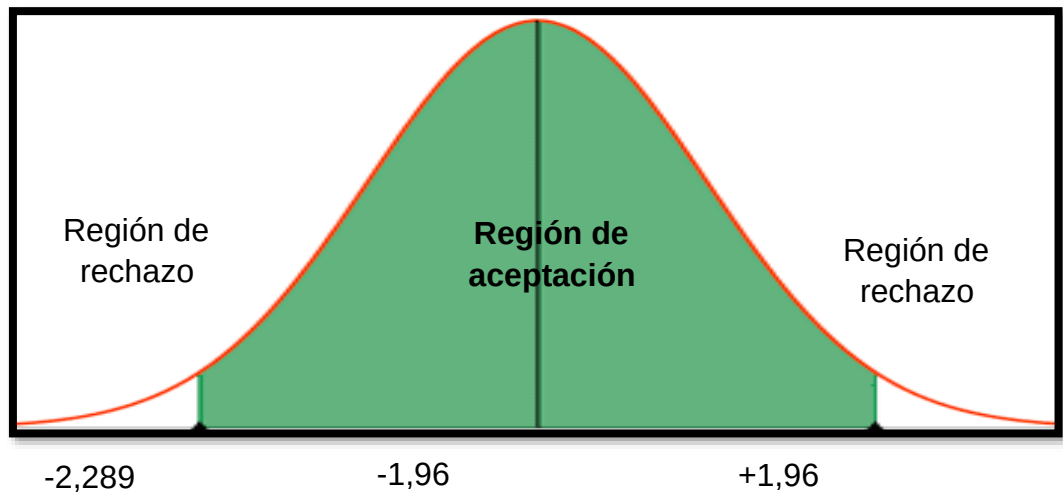
	POST_H1 - PRE_H1
Z	-2,889 ^b
Sig. asintót. (bilateral)	,004

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Figura 32

Curva de distribución normal con regiones de rechazo y de aceptación en una prueba de hipótesis bilateral – HE1



Después de realizar el análisis de Wilcoxon el resultado de la significación asintótica bilateral ($p=0.004$) es menos a 0.05 (α). Como al trabajar a un nivel del 95% se tiene un valor de ± 1.96 para los límites de la región de aceptación, como el valor de $Z = -2,889$, se ubica en la zona de rechazo.

Por lo tanto, se rechaza H_0 y se acepta H_1 en base a lo explicado se concluye que las condiciones la confiabilidad del servicio de red mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

Hipótesis específica 2

- **H₀:** Las características del aseguramiento de la información identificadas **NO** mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

- **H1:** Las características del aseguramiento de la información identificadas mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

Tabla 35

Prueba de los rangos con signo de Wilcoxon – HE2

		N	Rango promedio	Suma de rangos
POST_H2 - PRE_H2	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	13 ^b	7,00	91,00
	Empates	0 ^c		
	Total	13		

a. POST_H2 < PRE_H2

b. POST_H2 > PRE_H2

c. POST_H2 = PRE_H2

Tabla 36

Estadística de Wilcoxon – HE2

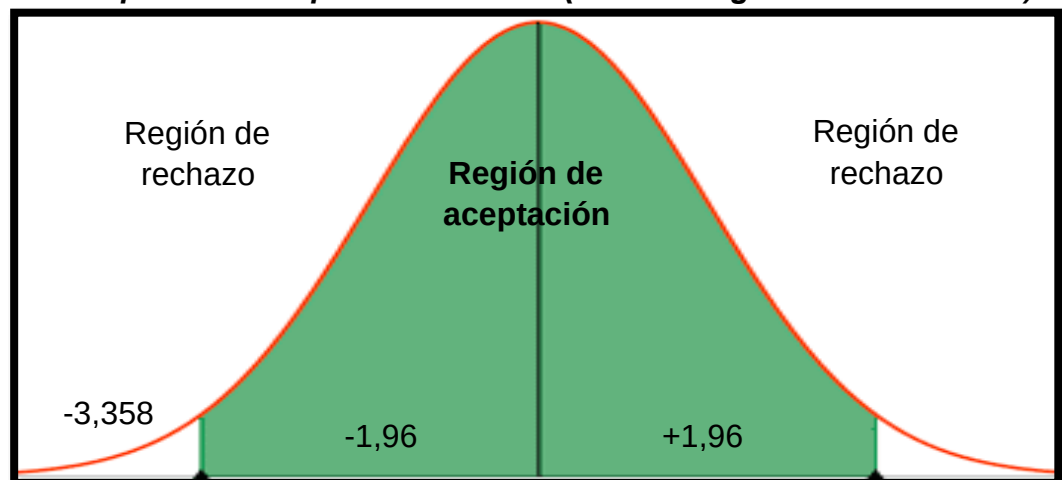
	POST_H2 - PRE_H2
Z	-3,358 ^b
Sig. asintót. (bilateral)	,001

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Figura 33

Curva de distribución normal con regiones de aceptación y rechazo en una prueba de hipótesis bilateral (nivel de significancia $\alpha = 0.05$)



Después de realizar el análisis de Wilcoxon el resultado de la significación asintótica bilateral ($p=0.001$) es menos a 0.05 (α). Como al trabajar a un nivel del 95% se tiene un valor de ± 1.96 para los límites de la región de aceptación, como el valor de $Z = -3,358$, se ubica en la zona de rechazo.

Por lo tanto, se rechaza H_0 y se acepta H_1 en base a lo explicado se concluye que las características del aseguramiento de la información identificadas mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

Hipótesis específica 3

- **H0:** La optimización de la capacidad de respuesta de los servicios de red **NO** mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.
- **H1:** La optimización de la capacidad de respuesta de los servicios de red mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

Tabla 37

Prueba de los rangos con signo de Wilcoxon – HE3

		N	Rango promedio	Suma de rangos
POST_H3 - PRE_H3	Rangos negativos	0 ^a	,00	,00
	Rangos positivos	11 ^b	6,00	66,00
	Empates	2 ^c		
	Total	13		

a. POST_H3 < PRE_H3

b. POST_H3 > PRE_H3

c. POST_H3 = PRE_H3

Tabla 38

Estadística de Wilcoxon – HE3

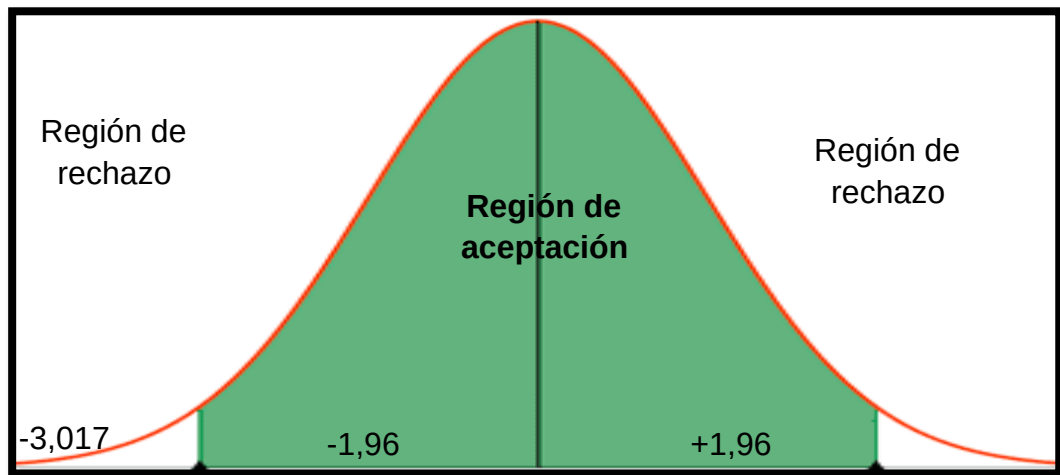
	POST_H3 - PRE_H3
Z	-3,017^b
Sig. asintót. (bilateral)	,003

a. Prueba de los rangos con signo de Wilcoxon

b. Basado en los rangos negativos.

Figura 34

Curva de distribución normal estándar con regiones de aceptación y rechazo para una prueba de hipótesis bilateral



Después de realizar el análisis de Wilcoxon el resultado de la significación asintótica bilateral ($p=0.003$) es menos a 0.05 (α). Como al trabajar a un nivel del 95% se tiene un valor de ± 1.96 para los límites de la región de aceptación, como el valor de $Z = -3.017$, se ubica en la zona de rechazo.

Por lo tanto, se rechaza H_0 y se acepta H_1 en base a lo explicado se concluye que la optimización de la capacidad de respuesta de los servicios de red mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.

CONCLUSIONES

En el presente trabajo de investigación aplicada después del levantamiento de información que se recopilaron por medio de las entrevistas a nuestra muestra y las encuestas realizadas se llegaron a las siguientes conclusiones:

- En relación con el objetivo general, los resultados obtenidos evidencian que la implementación de la gestión de riesgo impacta positivamente en la mejora de la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A. Esta afirmación se sustenta en los valores estadísticos obtenidos ($p = 0.001 < 0.05$ y $Z = -3.358$), los cuales permiten rechazar la hipótesis nula y aceptar la alternativa, confirmando así la eficacia del enfoque propuesto.
- Respecto al primer objetivo específico, se concluye que las condiciones de confiabilidad del servicio de red influyen significativamente en la gestión de los servicios de datos, toda vez que el análisis estadístico ($p = 0.004 < 0.05$ y $Z = -2.889$) demuestra una mejora notable tras la evaluación e implementación de medidas orientadas a fortalecer la estabilidad y continuidad del servicio.
- En cuanto al segundo objetivo específico, los hallazgos indican que las características del aseguramiento de la información, tales como la integridad, confidencialidad y disponibilidad, contribuyen sustancialmente al fortalecimiento de la gestión de servicios de red. Los datos estadísticos obtenidos ($p = 0.001 < 0.05$ y $Z = -3.358$) respaldan esta conclusión,

validando la importancia de aplicar mecanismos de seguridad adecuados para garantizar la protección de la información en la infraestructura de red.

- Finalmente, en referencia al tercer objetivo específico, se concluye que la optimización de la capacidad de respuesta ante incidentes o fallas en la red genera una mejora directa en la gestión de servicios, lo cual se corrobora mediante la significancia estadística del análisis realizado ($p = 0.003 < 0.05$ y $Z = -3.017$). Este resultado subraya la necesidad de contar con procesos ágiles y protocolos eficientes que permitan actuar oportunamente frente a eventos críticos en la red.

RECOMENDACIONES

- Es de vital importancia que el sistema de gestión de la seguridad de la información en la empresa acoja a todos los procesos, no solamente para la seguridad de la red de datos, sino en su conjunto para cubrir todas las necesidades a que están expuestos la información de la empresa.
- Se recomienda capacitaciones constantes en temas relacionados a la seguridad de la información, sobre todo a los nuevos trabajadores que a futuro ingresen a laborar, para poder garantizar la seguridad de la información y activos de la empresa de forma permanente.
- Se recomienda registrar siempre las incidencias que se podrían presentar para poder manejarlas adecuadamente en futuras problemas que se podrían presentar.

REFERENCIAS BIBLIOGRÁFICAS

- Barrantes Echavarría, R. (2002). *Investigación: Un camino al conocimiento, un enfoque cualitativo y cuantitativo. primera edición. San José, C. R.: EUNED, 280 p. 27 ct.*
- Cáceres Perez, F. (2018). *La gestión de riesgos y su impacto en la rentabilidad de las empresas de telecomunicaciones ubicadas en Lima Metropolitana 2012-2015.*
- Cárdenas Cruz, J. (2019). *Análisis de riesgos de seguridad de la información para la empresa pijaos telecomunicaciones del municipio de Cajamarca en el departamento del Tolima.*
- CFI. (2024). *Administración de Riesgos.*
- Compartamos. (2024). *Misión y Visión.*
- Hernández, S., Fernandez, C., & Baptista, L. (2014). *Metodología de la Investigación. sexta edición. McGrawHill.*
- Hpe. (2024). *Administración de la red.* Obtenido de:
<https://www.hpe.com/lamerica/es/what-is/network-management.html>
- Huaurea Mere, M. (2019). *Gestión de riesgos de seguridad de la información para empresas del sector telecomunicaciones.*
- Ibm. (2024). *Administración de Riesgo.* Obtenido de: <https://www.ibm.com/mx-es/topics/risk-management>
- Implika. (2024). *Qué son las redes informáticas y cómo funcionan.* Obtenido de:
<https://www.implika.es/blog/que-son-redes-informaticas>

- Maquera Mamani, G. (2022). *Sistema de gestión de seguridad de la información y su relación con la calidad de servicio de las redes lan en la municipalidad distrital de Ilabaya*.
- Molina Alcocer, J. (2018). *Diseño de una política para la clasificación y etiquetado de la información basada en riesgos para instituciones públicas en el Ecuador*.
- Oviedo, H. C., & Campo-Arias, A. (2005). Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría*, 34(4), 572–580.
- Parodi, R. (2020). *Administración de la Gestión de Riesgos*.
- Reyna, J. (2019). *Estadística aplicada a la investigación científica con SPSS*. Lima: Editorial San Marcos.
- Rosero Álvarez, E. O. (2019). *Análisis de riesgos de la seguridad de la red de área local (Lan) de la matriz de la contraloría general del estado*.
- SafetyCulture. (2024). Gestión de riesgos.
- Sánchez Galán, J. (2024). Servicio: Qué es, características y ejemplos. *Economipedia*. Obtenido de:
https://economipedia.com/definiciones/servicio.html#google_vignette.
- Santos, D. (2024). *Análisis de riesgos*. Hubspot.
- Suárez, E. (2024). *Método inductivo y deductivo*.
- Valverde Flores, D. (2022). *Implementación de una gestión de riesgos de TI para mejorar la seguridad de la información de una empresa de agencia publicitaria - 2021*.

ANEXOS

ANEXO 1

EVALUACIÓN DE CONFIABILIDAD DEL INSTRUMENTO

Según Oviedo y Campo (2005) comenta: El valor mínimo aceptable para el coeficiente alfa de Cronbach es 0,70; por debajo de ese valor la consistencia interna de la escala utilizada es baja. Por su parte, el valor máximo esperado es 0,90; por encima de este valor se considera que hay redundancia o duplicación. Varios ítems están midiendo exactamente el mismo elemento de un constructo; por lo tanto, los ítems redundantes deben eliminarse. Usualmente, se prefieren valores de alfa entre 0,80 y 0,90.

Interpretación del valor de confiabilidad de la escala de Cronbach.

Alpha	Nivel de Fiabilidad
Mayor de 0.9	Excelente
Entre 0.8 y 0.9	Muy Bueno
Entre 0.7 y 0.8	Bueno
Entre 0.6 y 0.7	Aceptable (solo para estudios exploratorios)
Entre 0.5 y 0.6	Pobre
Menor de 0.5	Inaceptable

Comprobación Pre-Test

Alfa de Cronbach	N de elementos
,918	14

El coeficiente Alfa de Cronbach aplicado a los ítems del cuestionario se calculó a través del software SPSS y su resultado es de 0.918, por lo tanto, se concluye que la consistencia interna del instrumento utilizado es aceptable y se puede aplicar.

Comprobación Post-Test

Alfa de Cronbach	N de elementos
,923	14

El coeficiente Alfa de Cronbach aplicado a los ítems del cuestionario se calculó a través del software SPSS y su resultado es de 0.923, por lo tanto, se concluye que la consistencia interna del instrumento utilizado es aceptable y se puede aplicar

ANEXO 2

MATRIZ DE CONSISTENCIA

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES/DIMENSIONES E INDICADORES	METODOLOGÍA DE LA INVESTIGACIÓN												
¿La implementación de la gestión de riesgo mejora la gestión de servicios de la red de datos de la empresa, Compartamos Financiera S.A.?	Implementar la gestión de riesgo para mejorar, la gestión de servicios de la red de datos de la empresa, Compartamos Financiera S.A.	La implementación de la gestión, de riesgo mejora la gestión de servicios de la red, de datos de la empresa Compartamos Financiera S.A.	Variable I <table><tr><th>Dimensión</th><th>Indicador</th><th>Escala</th></tr><tr><td>Prevención</td><td> - Medios - Métodos - Factores </td><td> - Malo - Regular - Normal </td></tr><tr><td>Diagnostico</td><td> - Perspectiva - Grado </td><td> - Bueno - Muy bueno </td></tr><tr><td>Valoración</td><td> - Comparación - Alternativas </td><td></td></tr></table>	Dimensión	Indicador	Escala	Prevención	- Medios - Métodos - Factores	- Malo - Regular - Normal	Diagnostico	- Perspectiva - Grado	- Bueno - Muy bueno	Valoración	- Comparación - Alternativas		Tipo de investigación: Aplicada Nivel de investigación: Descriptiva. Población: La población está representada por todos los individuos relacionados con el estudio, siendo estos el personal del Área de Informática que conformar un total de 13 empleados. Muestra: La muestra en una parte representativa de la población de estudio, pero al notar que la población está conformada por un número pequeño, no es necesario emplear el método probabilístico, y siendo el más adecuado la elección por conveniencia, debido a ello el total de la muestra será la misma cantidad de la población siendo estos 13 empleados Diseño, de la investigación: Experimental de tipo pre experimental. Ge: Y1 ---- X ----Y2 Donde: Ge: Grupo, experimental Y1: Pretest Y2: Postest X: Gestión de Riesgo
Dimensión	Indicador	Escala														
Prevención	- Medios - Métodos - Factores	- Malo - Regular - Normal														
Diagnostico	- Perspectiva - Grado	- Bueno - Muy bueno														
Valoración	- Comparación - Alternativas															
¿De qué manera las condiciones de la confiabilidad mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?	Determinar las condiciones de la confiabilidad del servicio de red para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.	Las condiciones la confiabilidad del servicio de red mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.	Variable D <table><tr><th>Dimensión</th><th>Indicador</th><th>Escala</th></tr><tr><td>Confiabilidad</td><td> - Eficiencia - Efectividad </td><td> - Malo - Regular - Normal </td></tr><tr><td>Aseguramiento</td><td> - Confianza - Credibilidad </td><td> - Bueno - Muy bueno </td></tr><tr><td>Capacidad de respuesta</td><td> - Tiempo de respuesta. - Mejora continua </td><td></td></tr></table>	Dimensión	Indicador	Escala	Confiabilidad	- Eficiencia - Efectividad	- Malo - Regular - Normal	Aseguramiento	- Confianza - Credibilidad	- Bueno - Muy bueno	Capacidad de respuesta	- Tiempo de respuesta. - Mejora continua		
Dimensión	Indicador	Escala														
Confiabilidad	- Eficiencia - Efectividad	- Malo - Regular - Normal														
Aseguramiento	- Confianza - Credibilidad	- Bueno - Muy bueno														
Capacidad de respuesta	- Tiempo de respuesta. - Mejora continua															
¿Cuáles son las características del aseguramiento de la información para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?	Identificar las características del aseguramiento de la información para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.	Las características, del aseguramiento de la información, identificadas mejoran la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.														
¿Cómo la, capacidad de respuesta de los servicios de red mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.?	Optimizar la capacidad de respuestas de los servicios de red para mejorar la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.	La optimización, de la capacidad de respuesta de los servicios, de red mejora la gestión de servicios de la red de datos de la empresa Compartamos Financiera S.A.														

Fuentes	Técnicas	Instrumentos
Primaria	Encuesta	Cuestionarios
Secundaria	Análisis documental	Resumen de autores

ANEXO 3

CUESTIONARIO DE PREGUNTAS SOBRE LA INVESTIGACIÓN

“GESTIÓN DE RIESGO PARA MEJORAR LA GESTIÓN DE SERVICIOS DE LA RED DE DATOS EN LA EMPRESA COMPARTAMOS FINANCIERA S.A”

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

N° PREG	PREGUNTAS	1	2	3	4	5
VARIABLE INDEPENDIENTE: Gestión de Riesgos						
Dimensión: Prevención						
1	¿Cuál es su punto de vista sobre los medios utilizados para efectuar una correcta gestión de riesgo?					
2	¿Cuál es su punto de vista sobre los métodos utilizados para efectuar una correcta gestión de riesgo?					
3	¿Cuál es su punto de vista sobre los factores de evaluación utilizados para efectuar una correcta gestión de riesgo?					
Dimensión: Diagnóstico						
4	¿Cuál es su punto de vista sobre las perspectivas de diagnóstico empleadas en la gestión de riesgo?					
5	¿Cuál es su punto de vista sobre el grado de diagnóstico obtenido en la gestión de riesgo?					
Dimensión: Valoración						
6	¿Cuál es su punto de vista sobre la comparación entre controles de seguridad para la gestión de riesgo?					
7	¿Cuál es su punto de vista sobre el las alternativas identificadas para la gestión de riesgo?					
8	¿Cuál es su punto de vista sobre el las alternativas seleccionadas para la gestión de riesgo?					
VARIABLE DEPENDIENTE: Gestión de servicios de la red de datos						
Dimensión: Confiabilidad						

9	¿Cuál es su punto de vista sobre el grado de eficiencia empleado para la Gestión de servicios de la red de datos?					
10	¿Cuál es su punto de vista sobre el grado de efectividad empleado para la Gestión de servicios de la red de datos?					
Dimensión: Aseguramiento						
11	¿Cuál es su punto de vista sobre el grado de confianza que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?					
12	¿Cuál es su punto de vista sobre el grado de credibilidad que emiten los controles y/o mecanismos empleados para la Gestión de servicios de la red de datos?					
Dimensión: Capacidad de respuesta						
13	¿Cuál es su punto de vista sobre el tiempo de respuesta a sucesos por la Gestión de servicios de la red de datos?					
14	¿Cuál es su punto de vista sobre las actividades de mejora continuad empleados en la Gestión de servicios de la red de datos?					

ANEXO 4

FORMATO DE VALIDACIÓN DE LOS INSTRUMENTOS POR EXPERTOS

I. DATOS PERSONALES

- 1.1. APELLIDO Y NOMBRE DEL INFORMANTE:
- 1.2. GRADO ACADÉMICO:
- 1.3. INSTITUCIÓN DONDE LABORA:
- 1.4. TÍTULO DE LA INVESTIGACIÓN:
- 1.5. AUTOR DEL INSTRUMENTO:
- 1.6. NOMBRE DEL INSTRUMENTO:

II. ASPECTO A EVALUAR: (CALIFICACIÓN CUANTITATIVA)

INDICADORES DEL INSTRUMENTO DE EVALUACIÓN	CRITERIOS CUALITATIVOS CUANTITATIVOS	Deficiente (01-09)	Regular (10-13)	Bueno (14-16)	Muy bueno (17-18)	Excelente (19-20)
01. CLARIDAD	Está formulado con lenguaje apropiado.					
02. OBJETIVIDAD	Está expresado con conductas observables.					
03. ACTUALIDAD	Adecuado al avance de la ciencia y calidad.					
04. ORGANIZACIÓN	Existe una organización lógica del instrumento.					
05. SUFICIENCIA	Valora los aspectos en cantidad y calidad.					
06. INTENCIONALIDAD	Adecuado para cumplir con los objetivos.					
07. CONSISTENCIA	Basado en el aspecto teórico científico del tema de estudios.					
08. COHERENCIA	Entre las hipótesis, dimensiones e indicadores.					
09. METODOLOGÍA	Las estrategias responden al propósito del estudio.					
10. OPORTUNIDAD	Genera nuevas pautas para la investigación y construcción de teorías.					
Sub Total						
TOTAL						

Valoración cuantitativa (total x0.4)

Valoración cualitativa

Valoración de aplicabilidad

Leyenda:
 01-13 Importante
 14-16 Aceptable con recomendación
 17-20 Aceptable

Lugar y Fecha:

Firma y Post – Firma del Experto:

DNI:

ANEXO 5

FICHA DE EXPERTOS



UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE INGENIERIA DE SISTEMAS



I. DATOS GENERALES

- 1.1. APELLIDOS Y NOMBRES: AGURTO CHERRE CESAR AUGUSTO
- 1.2. GRADO ACADÉMICO: MAGISTER
- 1.3. INSTITUCIÓN QUE LABORA: UNIVERSIDAD NACIONAL DE UCAYALI
- 1.4. TÍTULO DE LA INVESTIGACIÓN: Gestión de riesgo para mejorar la gestión de servicios de la red de datos en la empresa Compartamos Financiera S.A
- 1.5. AUTOR DEL INSTRUMENTO: DÁVILA RÍOS JORGE MICHAEL JUNIOR
- 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)
(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)

II. ASPECTOS A EVALUAR

INDICADORES DE EVALUACIÓN DEL INSTRUMENTO	CRITERIOS CUALITATIVOS - CUANTITATIVOS	Deficiente (01 - 09)	Regular (10 - 12)	Buena (13 - 15)	Muy buena (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. SUFFICIENCIA	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. CONCORDANCIA	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
VALORACIÓN CUALITATIVA
OPINIÓN DE APLICABILIDAD

: 19
: EXCELENTE
: APLICABLE

Lugar y Fecha: 02/09/2024.



UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE INGENIERIA DE SISTEMAS



I. DATOS GENERALES

- 1.1. APELLIDOS Y NOMBRES: PINEDO COBOS ALDO IVAN
- 1.2. GRADO ACADÉMICO: INGENIERO DE SISTEMAS
- 1.3. INSTITUCIÓN QUE LABORA: GERENCIA REGIONAL FORESTAL DE FLORA Y FAUNA SILVESTRE
- 1.4. TÍTULO DE LA INVESTIGACIÓN: Gestión de riesgo para mejorar la gestión de servicios de la red de datos en la empresa Compartamos Financiera S.A
- 1.5. AUTOR DEL INSTRUMENTO: DAVILA RIOS JORGE MICHAEL JUNIOR
- 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)

(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)

III. 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 técnico 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 pistas para la investigación y construcción de teorías					19
SUB TOTAL						19
TOTAL						19

VALORACION CUANTITATIVA : 19
 VALORACION CUALITATIVA : EXCELENTE
 OPINION DE APLICABILIDAD : APLICABLE

Lugar y Fecha: 02/09/2024

ANEXO 6

RESUMEN DE VALIDACIÓN POR EXPERTOS

INDICADORES	AGURTO CHERRE, CESAR AUGUSTO	PINEDO COBOS ALDO IVAN	$\bar{X}$
1. CALIDAD	19	19	19
2. OBJETIVIDAD	19	19	19
3. ACTUALIDAD	19	19	19
4. ORGANIZACIÓN	19	19	19
5. SUFICIENCIA	19	19	19
6. INTENSIONALIDAD	19	19	19
7. CONSISTENCIA	19	19	19
8. COHERENCIA	19	19	19
9. METODOLOGÍA	19	19	19
10. OPORTUNIDAD	19	19	19
$\bar{X}$	19	19	19

Conclusión:

Según la valoración de 02 expertos se obtuvo cuantitativamente 19 puntos; el cual significa que el instrumento es cualitativamente EXCELENTE, concluyéndose que el instrumento es APLICABLE.

ANEXO 7

SISTEMA DE GESTIÓN DE RIESGOS

1. Diagnóstico Inicial

En esta fase de diagnóstico situacional de la Red LAN de la EMPRESA COMPARTAMOS FINANCIERA S.A, se desarrollaron actividades para recabar información. Se coordinó con el encargado del área de informática y comunicaciones, para lograr una evaluación de los distintos puntos del SGSI y cuya información se muestra en la siguiente tabla:

Tabla 1A
Diagnóstico Inicial

Requerimiento según ISO 27001:2014	Estado	Evidencia	Sugerencia
Contexto	No cuenta	La empresa carece de un SGSI	Implementar un SGSI tomando en cuentas aspectos internos y externos
Funcionalidad	Parcial	Cuenta con documento como: Plan Operativo Informático, Plan estratégico de Información	Ninguna
Compresión de la necesidad organizacional	No cuenta	Ninguna	Realizar un estudio minucioso de las para comprendes las necesidades y expectativas con respecto al SGSI
Alcance	No cuenta	Ninguna	Realizar un estudio para determinar el nivel de alcance del SGSI relacionado a la RED LAN
SGSI	No cuenta		Implementar mecanismos en el proceso del SGSI
Políticas	No cuenta		Elaborar políticas de Seguridad de la información.

2. Preparación del Sistema de Gestión de Seguridad de la Información

En esta fase se detallará el proceso para subsanar los riesgos, controlar amenazas, y vulnerabilidades.

2.1. Contexto de la empresa

El SGSI como requisitos esenciales debe estar estrechamente relacionado y alineado a las estrategias y la cultura organizacional de la empresa.

Propósito



Nuestro Propósito

Impulsamos los sueños de nuestros clientes atendiendo sus necesidades financieras con sentido humano. Desde hace más de 30 años, trabajamos para llevar oportunidades que promuevan su desarrollo y el de sus comunidades.

Generamos VALOR TOTAL:

- Valor social: Ofreciéndote oportunidades de inclusión financiera en el menor tiempo posible y compartiendo los beneficios obtenidos con las comunidades donde trabajamos.
- Valor económico: Construyendo modelos comerciales innovadores, eficientes y rentables con los que te puedas beneficiar.
- Valor humano: Confiando en ti y en tu crecimiento y que a través de la educación financiera utilices soluciones financieras a tu favor.

Fuente: Compartamos (2024).

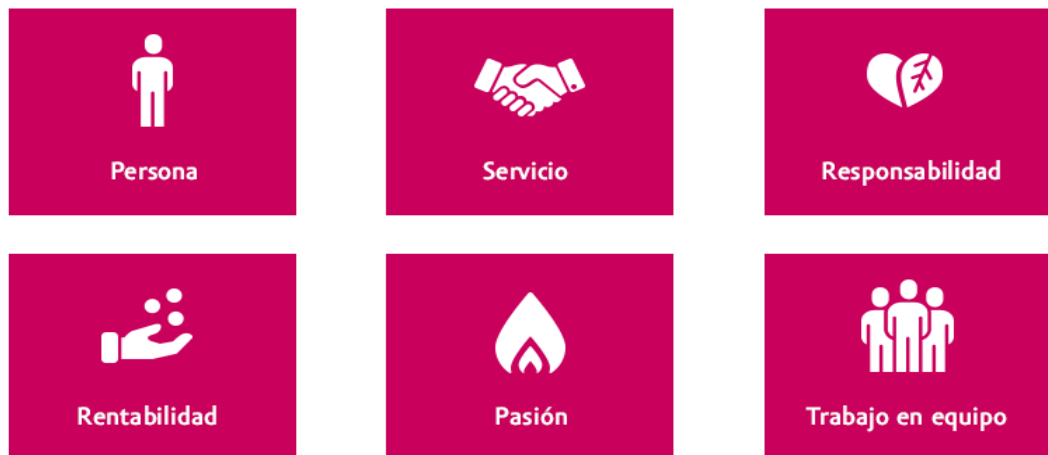
Visión



Fuente: Compartamos (2024).

Valores

Nuestros Valores



Fuente: Compartamos (2024).

2.1.1. SGSI Actual y funcionalidad

La empresa COMPARTAMOS FINANCIERA S.A, actualmente no cuenta con un SGSI, lo que significa que se viene realizando una inadecuada administración y organización de los activos de información.

La forma de mitigar las amenazas y/o riesgos se produce de forma verbal a través de llamadas telefónicas al personal de informática, quienes acuden a la solicitud de soporte. Asimismo, luego de la solución de los incidentes no se lleva un control o registro de las actividades realizadas.

Los archivos digitales que se clasifican como activos de información, son trabajados en las computadoras personales de los empleados. No se cuenta con un servicio de red que centralice estos activos, permaneciendo así en un estado vulnerable ya sea por ataque de tipo personales, o informáticos a través de programas maliciosos como lo virus, troyanos, etc.

Con el fin de proceder con la implementación de SGSI, se procedió con efectuar un análisis de los riesgos y para ello se aplicó MAGERIT, procedimientos que a continuación se detallan:

○ **Necesidades del negocio.**

Lista de Componentes, son los siguientes:

- Hardware: Son equipos físicos como servidores, equipos de comunicación, computadoras personales, laptops, etc.
- Software: Son los programas informáticos utilizados en el desarrollo de las actividades.
- Seguridad: Son los componentes utilizados para mejorar la protección y seguridad la información.
- Persona: Es el capital humano, los colaboradores relacionados pro el proceso de SGSI.
- Continuidad de servicios: Son mecanismo y procedimientos utilizados para garantizar la continuidad del negocio.

Identificación de las amenazas y vulnerabilidad, esto se realiza por niveles de probabilidad – NP, para ello se definió una escala:

- Nivel 1: Improbable y no cuenta con evidencia histórica de su presencia.

- Nivel 2: Probable, puede ocurrir 01 vez cada 02 años.
- Nivel 3: Muy Probable, puede producirse 01 vez cada 3 meses.

A continuación, se muestra información de la clasificación de las amenazas:

Tabla 2A

Clasificación de amenazas

Componente	Amenaza	Vulnerabilidad	NP
Hardware	A1: Daños al servidor	V1: Tiempo de uso, factores eléctricos, mal uso.	1
	A2: Carencia de soporte	V2: No se cuenta con personal adecuado	2
Software	A3: Configuraciones	V3: Mala configuración	1
	A4: Carácter legal	V4: Carencia de licencias	1
Seguridad	A5: Perfil de acceso	V5: Asignación de perfiles inadecuados	1
	A6: Información no disponible	V6: Carencia de plan de pruebas	1
Personal	A7: Personal no calificado	V7: Personal con carencia total o parcial de conocimientos requeridos.	1
Continuidad	A8: Paralización de continuidad del servicio	V8: Carencia de herramientas, procedimientos y/o mecanismo que garanticen la continuidad del negocio	1

Es necesario definir la valoración del impacto con el fin de clasificar las amenazas en caso de que estas se materialicen, esta valoración se muestra a continuación:

Tabla 3A**Valoración de impacto**

Valor	Denominación	Descripción
1	Insignificante	Con consecuencias y/o efectos mínimos.
2	Menor	De bajo impacto o efectos bajos.
3	Moderado	Consecuencia mediana o efectos medianos
4	Mayor	Consecuencias o efectos altos
5	Catastrófico	Consecuencia o efectos desastrosos.

También se definió un mapa de color con el fin de ubicar zonas de riesgo derivados del producto de los valores de probabilidad e impacto, esta información se muestra a continuación:

Tabla 4A**Mapa de color evaluación de impacto**

Prob.	Impacto				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15

Donde:

- Zona de riesgo baja, acción: Asumir el riesgo.
- Zona moderada, acción: Asumir riesgo, reducirlo.
- Zona alta: Reducir riesgo, evitarlo, compartirlo o transferirlo.
- Zona extrema: Reducir, evitarlo, compartirlo o transferirlo.

A continuación, se efectuó la clasificación de Amenazas y calcular el riesgo potencial, información que se muestra a continuación:

Tabla 5A

Clasificación de amenazas y cálculo de riesgo

Comp.	Amenaza	Vulnerabilidad	NP	Impacto	Riesgo Potencial
Hardware	A1: Daños al servidor	V1: Tiempo de uso, factores eléctricos, mal uso.	1	3	3
	A2: Carencia de soporte	V2: No se cuenta con personal adecuado	2	3	6
Software	A3: Configuraciones	V3: Mala configuración	1	3	3
	A4: Carácter legal	V4: Carencia de licencias	1	3	3
Seguridad	A5: Perfil de acceso	V5: Asignación de perfiles inadecuados	1	2	2
	A6: Información no disponible	V6: Carencia de plan de pruebas	1	3	3
Personal	A7: Personal no calificado	V7: Personal con carencia total o parcial de conocimientos requeridos.	1	2	2
Continuidad	A8: Paralización de continuidad del servicio	V8: Carencia de herramientas, procedimientos y/o mecanismo que garanticen la continuidad del negocio	1	3	3

Como se puede apreciar existen 08 amenazas, y posterior a la evaluación de acuerdo a su nivel de riesgo potencial se concluye: 01 de ellas se encuentra en el nivel de amenazas moderadas; por lo tanto, se debe definir estrategias para reducir el riesgo; por otra parte, 07 de los riesgos resultaron en el nivel de potencialmente bajo; por lo que, estos riesgos se podrían asumir.

También, las amenazas traen consigo riesgos los cuales se definen a continuación:

Tabla 6A

Riesgos por amenazas

Comp.	Amenaza	Vulnerabilidad	Riesgo	Descripción
Hardware	A1: Daños al servidor	V1: Tiempo de uso, factores eléctricos, mal uso.	R1	Cambio o alteración de la disponibilidad de los servidores No se cuente o la ausencia del personal o carencia de contratos de soporte por terceros
	A2: Carencia de soporte	V2: No se cuenta con personal adecuado	R2	Falla de configuración de los programas del servidor
Software	A3: Configuraciones	V3: Mala configuración	R3	No se cuenta con licencias en los programas de pago
	A4: Carácter legal	V4: Carencia de licencias	R4	Acceso indebido a acciones
Seguridad	A5: Perfil de acceso	V5: Asignación de perfiles inadecuados	R5	Falta de testeo de niveles de acceso a la información.
	A6: Información no disponible	V6: Carencia de plan de pruebas	R6	Carencia de personal con las capacidades requeridas
Personal	A7: Personal no calificado	V7: Personal con carencia total o parcial de conocimientos requeridos.	R7	Caída de servicio de forma general.
	A8: Paralización de continuidad del servicio	V8: Carencia de herramientas, procedimientos y/o mecanismo que garanticen continuidad del negocio	R8	

A continuación, se detalla información del riesgo potencial sobre la infraestructura del servidor (causas y efectos).

Tabla 7A

Causas y efectos

Causa	Efecto
Deterioro de los componentes por el tiempo de uso	Falla y perdida dificultad de conseguir componentes por desface tecnológico
Falta de contratos de servicio especializado	Infraestructura comprometida por ausencia de servicio especializado.
Mantenimiento preventivo no efectuado	Falla en los componentes físicos del servidor, paralización del servicio parcial o total, temporal o permanente
Poco o Nada de presupuesto	Uso de software sin licencia, incumplimiento legal.
Falta de gestión en la asignación de roles y perfiles	Mal manejo de servicios por personal no autorizado, paralización total o parcial del servicio, perdida de información.
Persona sin competencias adecuadas	Falta de capacidades, consumo alto de tiempo en aprendizaje, afecta otros servicios.
Falta de herramientas y mecanismos para mantener la alta disponibilidad	Paralización de servicios del negocio.

Salvaguarda – controles existentes

Con la visión previa del impacto potencial y los potenciales riesgos, se realizó con la verificación de cada uno de los riesgos y se creó una matriz con la finalidad de definir controles y de esta manera mitigar el riesgo.

Para poder encontrar el nivel de efectividad de los controles se elaboró la siguiente evaluación para los niveles de efectividad.

- Nivel 3: Control funciona de forma eficaz frente a las amenazas.
- Nivel 2: Es parcialmente eficaz, el control de las amenazas se procede con mucha en la mayoría de los casos.
- Nivel 1: Control poco efectivo, carece de eficacia para mitigar las amenazas.

Impacto residual

Posterior a la definición de controles existentes en el área de informática de procedió con el cálculo del impacto residual que se obtiene a partir del cálculo de los valores del impacto potencia sobre el nivel de eficacia del control.

Riesgo residual

Viene a ser la identificación del riesgo residual, para ello se utiliza el valor del impacto residual multiplicado por la probabilidad de ocurrencia.

Tabla 8A

Riesgos residuales

Comp.	Amenaza	Vulnerabilidad	Riesgo	Descripción
Hardware	A1: Daños al servidor	V1: Tiempo de uso, factores eléctricos, mal uso.	R1	Cambio o alteración de la disponibilidad de los servidores
	A2: Carencia de soporte	V2: No se cuenta con personal adecuado	R2	No se cuenta o la ausencia del personal o carencia de contratos de soporte por terceros
Software	A3: Configuraciones	V3: Mala configuración	R3	Falla de configuración de los programas del servidor
	A4: Carácter legal	V4: Carencia de licencias	R4	No se cuenta con licencias en los programas de pago
Seguridad	A5: Perfil de acceso	V5: Asignación de perfiles inadecuados	R5	Acceso indebido a acciones
	A6: Información no disponible	V6: Carencia de plan de pruebas	R6	Falta de testeo de niveles de acceso a la información.
Personal	A7: Personal no calificado	V7: Personal con carencia total o parcial de conocimientos requeridos.	R7	Carencia de personal con las capacidades requeridas
Continuidad	A8: Paralización de continuidad del servicio	V8: Carencia de herramientas, procedimientos y/o mecanismo que garanticen la continuidad del negocio	R8	Caída de servicio de forma general.

Matriz de impacto residual y riesgo residual de la infraestructura del servidor.

Tabla 9A

Matriz de impacto residuales

Controles	Tipo	Eficacia	Impacto Potencial	Impacto residual	Probabilidad	Riesgo Residual
Adquisición de nuevo servidor	Minimizar	3	3	1	1	1
Migración a nuevo servidor	Minimizar	3	3	1	2	2
Elaboración de formatos para control de revisiones del servidor	Minimizar	3	3	1	1	1
Adquisición e instalación de licencias	Minimizar	3	3	1	1	1
Personal capacitado	Minimizar	3	2	0.67	1	0.67
Servidor de respaldo	Minimizar	3	3	1	1	1

2.2. Procedimientos

A continuación, se muestra un ejemplo del procedimiento de mantenimiento:

PROCEDIMIENTO DE MANTENIMIENTO PREVENTIVO, CORRECTIVO Y SOPORTE TÉCNICO DE LA INFRAESTRUCTURA TECNOLÓGICA

OBJETIVO Garantizar la disponibilidad de la infraestructura tecnológica de la Entidad.

RESPONSABLE Jefe del área de informática.

ALCANCE Recursos de TI como Software, Hardware almacenamiento, redes LAN, entre otros.

DEFINICIONES

- **Mantenimiento Preventivo:** Acciones de verificación y ajustes programados para reducir la probabilidad de falla de algún componente de la infraestructura tecnológica.
- **Soporte Técnico:** Actividad para recibir, diagnosticar y resolver solicitud de los usuarios sobre funcionalidades o errores de operación de algún componente de la infraestructura tecnológica.
- **Mantenimiento Correctivo:** Es el resultado de un diagnóstico que requiere reinstalación de software o reemplazo parcial o total de algún componente de la infraestructura tecnológica

CONDICIONES GENERALES

Mantener la disponibilidad de la infraestructura y de los servicios. Se debe agendar o programar el mantenimiento de forma periódica con el fin de reducir la frecuencia y el impacto de fallas.

La infraestructura tecnológica está constituida por los siguientes elementos entre otros:

- Equipos de cómputo personales, de procesamiento y servidores, de comunicaciones
- Equipos de control ambiental, etc.

Procedimiento

1. ¿Es mantenimiento preventivo? Si la respuesta es afirmativa, continúe con la actividad 1, de lo contrario, remítase a la actividad 6.
2. ¿Es mantenimiento del laboratorio forense? Si la respuesta es afirmativa, continúe con la actividad 9, de lo contrario, remítase a la actividad 14.
3. Mantener inventario de infraestructura tecnológica. Consecución de la lista de activos por tipo de activo.
4. Generar el plan de mantenimiento preventivo, correctivo y soporte técnico.
5. Ejecutar el plan mantenimiento.
6. Actualizar del Plan de mantenimiento preventivo y soporte técnico.
7. Monitorear y controlar el plan de mantenimiento Plataforma tecnológica.
8. Ejecutar Mantenimiento Correctivo.

9. Registrar el Mantenimiento Correctivo como incidente.
10. Actualizar el Mantenimiento Correctivo.
11. Mantener inventario de infraestructura del laboratorio.
12. Generar el plan de mantenimiento preventivo, correctivo y soporte técnico.
13. Ejecutar el plan mantenimiento.
14. Actualizar del Plan de mantenimiento preventivo y soporte técnico.
15. Monitorear y controlar el plan de mantenimiento de plataforma
16. Ejecutar Mantenimiento Correctivo.
17. Registrar el Mantenimiento Correctivo como incidente.
18. Actualizar el Mantenimiento Correctivo.
19. FIN.

2.3. Control y seguimiento continuo

A continuación, se muestra un archivo de gestión de riesgos aplicando hoja de cálculo Excel para la empresa COMPARTAMOS FINANCIERA S.A, el cual fue diseñado e implantado como soporte al proceso.

Figura 1A

Formatos análisis de riesgo

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1					ANÁLISIS DE RIESGOS									
2					INSTRUCCIONES									
3														
4														
5														
6	1ª DESCRIPCIÓN DE LA APLICACIÓN:													
7	La presente aplicación ha sido diseñada como herramienta para facilitar el análisis de riesgos solicitado en la actividad final del curso.													
8	A continuación se procederá a describir el contenido de cada hoja de la aplicación:													
9	• Hoja «Ejemplo de análisis»: contiene un ejemplo de análisis de riesgos que podrás utilizar como referencia para realizar la actividad.													
10	• Hoja «Tablas AR»: incluye unas tablas orientativas para realizar las valoraciones de la probabilidad y el impacto según una escala de tres valores.													
12	• Hoja «Catálogo amenazas»: refleja las principales amenazas a considerar en el ámbito de un análisis de riesgos.													
13	• Hoja «Activos»: contiene un listado con los activos definidos para cada uno de los modelos de empresa propuestos en las instrucciones de la actividad final.													
14	• Hoja «Cruces Activo-Amenaza»: se utilizará para especificar las amenazas que afectan a los activos del modelo elegido.													
15	• Hoja «Análisis de Riesgos»: se utilizará para realizar el análisis de riesgos. Se debe indicar la probabilidad y el impacto de cada amenaza sobre cada uno de los activos.													
17	2ª FUNCIONAMIENTO DE LA APLICACIÓN:													
18	• Paso 1: en la hoja «Activos», existe una columna llamada «aplicación». Esta columna contiene una lista de dos opciones (SI/NO). Hay que rellenar con «SI» los activos que se apliquen dependiendo del modelo de empresa elegido (el resto se dejarán en blanco o se rellenarán con «NO»).													
19	• Paso 2: en la hoja «Cruces Activo-Amenaza», se muestra en la primera columna todas las amenazas y en la primera fila los indicadores de activos (que se corresponden con los de la hoja «Activos»). El objetivo de esta hoja es incluir un «SI» (igual que en el paso 1) en los cruces entre activo y amenaza para que después se muestren automáticamente en la hoja «Análisis de Riesgos».													
20	• Paso 3: en la hoja «Análisis de Riesgos», se debe pulsar el botón «Mostrar activos» (en la esquina superior izquierda). Este botón mostrará automáticamente todos los activos elegidos, con cada una de las amenazas asociadas a dichos activos.													
21	• Paso 4: en la hoja «Análisis de Riesgos», se debe elegir la probabilidad y el impacto de cada amenaza sobre cada activo (se trata otra vez de una lista, pero con tres posibilidades (Bajo(1), Medio(2), Alto(3)). Una vez seleccionados se mostrará en la columna riesgos un número que representa el riesgo acorde a la tabla de la hoja «Tablas AR» y el fondo de la casilla del color correspondiente.													
Recomendaciones de accesibilidad encontradas. Haga clic aquí para investigar.														
Catálogo amenazas Activos Cruces Activo-A ... + - ...														

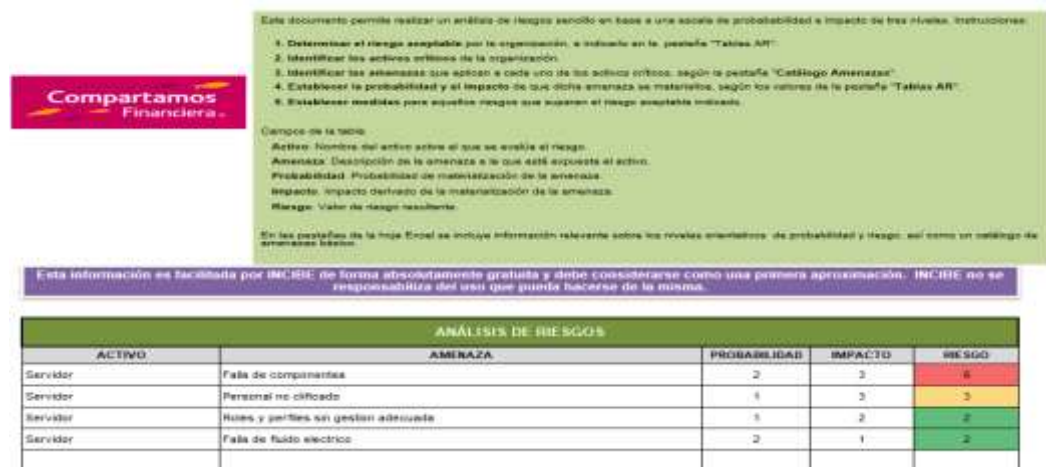


Figura 2A
Formatos activos

	A	B	C	D
		Identificador	Activo	Aplicación
1				
2				
3	Modelo A	A1	ordenador(es)	
4		A2	móvil(es) principalmente para telefonía	
5		A3	conexión a Internet e incluso wifi	
6	Modelo B	B1	ordenadores y conexión a Internet (con wifi)	
7		B2	dispositivos móviles para telefonía y datos	
8			soluciones tecnológicas gratuitas para la gestión empresarial como correo electrónico, CRM e incluso herramientas colaborativas o de almacenamiento cloud	
9		B3	una página web sencilla alojada y gestionada por un proveedor externo	
10	Modelo C	C1	ordenadores e incluso algún servidor (web, correo electrónico,...)	
11		C2	conexión a Internet con wifi	
12		C3	dispositivos móviles con datos y apps para su trabajo	
13		C4	herramienta(s) comercial(es) de gestión de negocio (CRM y ERP)	
14		C5	página web / tienda online y redes sociales que gestionan desde la empresa	
15		C6	herramientas para empresas en la nube	
16		C7	e-administración para su relación con las AAPP	

Figura 3A
Formatos amenazas

	A	B	C	D	E	F	G	H	I	J	K	L
	Amenaza/Activo	A1	A2	A3	B1	B2	B3	B4	C1	C2	C3	C4
1												
2	Fuego											
3	Daños por agua											
4	Desastres naturales											
5	Fuga de información											
6	Introducción de falsa información											
7	Alteración de la información											
8	Corrupción de la información											
9	Destrucción de información											
10	Intercepción de información (escucha)											
11	Corte del suministro eléctrico											
12	Condiciones inadecuadas de temperatura o humedad											
13	Fallo de servicios de comunicaciones											
14	Interrupción de otros servicios y suministros esenciales											
15	Desastres industriales											
16	Degradación de los soportes de almacenamiento de la información											
17	Difusión de software dañino											
18	Errores de mantenimiento / actualización de programas (software)											
19	Errores de mantenimiento / actualización de equipos (hardware)											
20	Calda del sistema por sobrecarga											
21	Pérdida de equipos											
22	Indisponibilidad del personal											
23	Abuso de privilegios de acceso											
24	Acceso no autorizado											
25	Errores de los usuarios											
26	Errores del administrador											
27	Errores de configuración											
28	Denegación de servicio											
29	Robo											
30	Indisponibilidad del personal											
31	Extorsión											
32	Ingeniería social											
33												
34												

Figura 4A

Formatos análisis de RAPI

	A	B	D	E	G	I
1	Mostrar Activos	ANÁLISIS DE RIESGOS				
2		Activo	Amenaza	Probabilidad	Impacto	Riesgo
3						
4						
5						
6						
7						
8						
9						