UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

LA NTP-ISO/IEC 17799 PARA LA ADMINISTRACIÓN DE RIESGOS DE TI DE LA EMPRESA TELPERU SAC.

Tesis para Optar el título profesional de

INGENIERO DE SISTEMAS

RONALD SAULO, SANTIAGO ALVARADO

Pucallpa - Perú

2024

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° 022-2024

GRADUANDO : SANTIAGO ALVARADO, RONALD SAULO

TEMA : ***"LA NTP ISO/IEC 17799 PARA LA ADMINISTRACIÓN DE RIESGOS DE TI DE LA EMPRESA TELPERU SAC"***

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- APORTE CIENTIFICO Y TECNOLOGICO				
* AL DESARROLLO DE LA COMUNIDAD		X		
* A LA PROFESION		X		

EVALUACION

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

CALIFICACION FINAL:
PUNTAJE : 18 / 30

CONCLUSIONES:
APROBADO POR :
DESAPROBADO POR :

JURADO EVALUADOR

Mg. ARTURO YUPANQUI VILLANUEVA
PRESIDENTE

Mg. OSCAR AMADO RUIZ TORRES
MIEMBRO

Mg. RICHARD PIERO BARDALES LINARES
MIEMBRO

M.SC. CLOTILDE RÍOS HIDALGO DE CERNA
SECRETARIA ACADÉMICA

PUCALLPA, 22 DE NOVIEMBRE DEL 2024

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

COMISIÓN DE GRADOS Y TÍTULOS

"LA NTP-ISO/IEC 17799 PARA LA ADMINISTRACIÓN DE RIESGOS DE TI DE LA EMPRESA TELPERU SAC"

ELABORADO POR: Bach. RONALD SAULO SANTIAGO ALVARADO

APROBADO POR:

Mg. ARTURO YUPANQUI VILLANUEVA
PRESIDENTE

Mg. OSCAR AMADO RUIZ TORRES
MIEMBRO

Mg. RICHARD PIERO BARDALES LINARES
MIEMBRO

M.Sc. EUCLIDES PANDURO PADILLA
ASESOR

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

CONSTANCIA

ORIGINALIDAD DE TRABAJO DE INVESTIGACIÓN

Nº **V/0493-2024**.

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

"**LA NTP-ISO/IEC 17799 PARA LA ADMINISTRACIÓN DE RIESGOS DE TI DE LA EMPRESA TELPERU SAC.**"

Autor(es)	:	**SANTIAGO ALVARADO, RONALD SAULO**
Facultad	:	**INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL**
Escuela	:	**ING. DE SISTEMAS**
Asesor(a)	:	**M.Sc. PANDURO PADILLA, EUCLIDES**

Presenta un **porcentaje de similitud de 5%,** 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: 23/09/2024

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, RONALD SAULO SANTIAGO ALVARADO

Autor de la tesis titulada : "LA NTP-ISO/IEC 17799 PARA LA ADMINISTRACIÓN DE RIESGOS DE TI DE LA EMPRESA TELPERU SAC."

Sustentada el año 2024

Asesor(a): M. Sc. EUCLIDES PANDURO PADILLA

Facultad: INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

Escuela Profesional: INGENIERÍA DE SISTEMAS

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

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: 22 / 11 / 2024

Email: RSAULO28SANTIAGO@GMAIL.COM Firma:

Teléfono: 958938959 DNI: 48025394

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

DEDICATORIA

A mis padres que siempre me dieron el apoyo y confianza que fue fundamental en toda mi vida;

A mi querida hija Stephanie kristie por ser la razón y motivo principal de cumplir con mis metas y objetivos profesional.

AGRADECIMIENTOS

A Dios todo poderoso por tener siempre su compañía, guiándome y cuidándome mi camino.

A la Escuela Profesional de Ingeniería sistemas de la Universidad Nacional de Ucayali, por acogerme en sus aulas el tiempo de mi formación, por compartir sus conocimientos y contribuir con mi formación profesional, por absolver cada uno de mis dudas, con esmero y dedicación en las sesiones de aprendizaje, mi cariño, respeto y admiración por cada uno de ellos.

ÍNDICE GENERAL

Pg.

DEDICATORIA vi

AGRADECIMIENTOS vii

ÍNDICE GENERAL viii

ÍNDICE DE TABLAS xii

ÍNDICE DE FIGURAS xiii

ÍNDICE DE ANEXOS xiv

RESUMEN xv

ABSTRACT xvi

INTRODUCCIÓN xvii

CAPÍTULO I 18

PLANTEAMIENTO DEL PROBLEMA 18

1.1. DESCRIPCIÓN Y FUNDAMENTACION DEL PROBLEMA. 18

1.2. FORMULACIÓN DEL PROBLEMA 19

1.2.1 Problema General 19

1.2.2 Problemas Específicos 19

1.3. OBJETIVOS DE LA INVESTIGACIÓN. 20

1.3.1 Objetivo General 20

1.3.2 Objetivos Específicos 20

1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES. 21

1.4.1 Justificación…… 21

1.4.2 Importancia…… 21

1.4.3 Limitaciones……22

1.5. HIPÓTESIS, VARIABLES DE INVESTIGACIÓN. 22

1.5.1 Hipótesis General……22

1.5.2 Hipótesis Específicas…… 22

1.6. DELIMITACIONES DE LA INVESTIGACIÓN 23

1.6.1 Delimitación Espacial…… 23

1.6.2 Delimitación Social…… 23

1.6.3 Delimitación Temporal……23

1.6.4 Delimitación Conceptual…… 23

1.7. VARIABLES..... 23

1.7.1 Variable independiente:…… 23

1.7.2 Variable dependiente:…… 23

1.7.3 Variable interviniente:…… 24

1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES. 24

1.8.1 Operacionalización de variables…….. 24

CAPÍTULO II 25

MARCO TEÓRICO 25

2.1. ANTECEDENTES DE LA INVESTIGACIÓN 25

2.1.1. Antecedentes Internacionales..... 25

2.1.2. Antecedentes Nacionales. 26

2.2. BASES TEÒRICAS. 27

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS 34

METODOLOGÍA DE LA INVESTIGACIÓN 35

3.1. MÉTODO DE INVESTIGACIÓN. 35

3.2. POBLACIÓN Y MUESTRA. 36

3.3. TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS. . 36

3.4. PROCEDIMIENTO DE RECOLECCIÓN DE DATOS. 37

3.5. TRATAMIENTO DE DATOS. 37

3.6. GRADO DE CONFIABILIDAD DE LOS DATOS. 37

CAPÍTULO IV 38

ADMINISTRACIÓN DE RIEGOS DE TI – TELPERU SAC. 38

4.1. La empresa 38

4.2. Identificación y clasificación de activos de TI 39

4.3. Clasificación de activos por tipo 40

4.4. Criticidad de los activos 40

4.5. Amenazas 41

4.6. Vulnerabilidades de los activos 42

4.7. Valoración del impacto y probabilidad de ocurrencia de amenazas 43

4.8. Métricas para la gestión de riesgos 48

4.9. Propuesta de políticas de seguridad en base a la ISO/IEC 27001 48

4.10. Implementación de medidas de seguridad 49

CAPÍTULO V..... 52

RESULTADOS..... 52

5.1. VARIABLE INDEPENDIENTE: LA NTP/ISO/IEC 17799..... 52

5.2. VARIABLE DEPENDIENTE: ADMINISTRACIÓN DE RIESGOS DE TI 54

5.3. PRUEBA E HIPÓTESIS GENERAL 56

CAPÍTULO VI..... 59

DISCUSIÓN DE RESULTADOS..... 59

CONCLUSIONES 61

RECOMENDACIONES 62

REFERENCIAS BIBLIOGRÁFICAS..... 63

ANEXOS 66

ÍNDICE DE TABLAS

Pg.

Tabla 1: Operacionalización de variable I 24

Tabla 2: Operacionalización de variable II 24

Tabla 3: Población 36

Tabla 4: Inventario de activos 39

Tabla 5: Clasificación de activos por tipo 40

Tabla 6: Criticidad 40

Tabla 7: Amenazas 41

Tabla 8: Vulnerabilidades 42

Tabla 9: Valores del impacto y probabilidad 44

Tabla 10: Riesgos de SI 48

Tabla 11: Políticas a implementar 49

Tabla 12: Medidas de seguridad 49

Tabla 13: Análisis de Frecuencia LA NTP/ISO/IEC 17799 52

Tabla 14: Análisis de Frecuencia LA NTP/ISO/IEC 17799 53

Tabla 15: Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI 54

Tabla 16: Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI 55

Tabla 17: Prueba de Normalidad 57

Tabla 18: Prueba de muestras relacionadas Hipótesis General 58

ÍNDICE DE FIGURAS

Pg.

Figura 1: portal Web de la Institución ……..38

Figura 2: Mapa de ubicación geográfica ……..…39

Figura 3 : Análisis de Frecuencia LA NTP/ISO/IEC 17799 ……...52

Figura 4 : Análisis de Frecuencia LA NTP/ISO/IEC 17799 ……...53

Figura 5 : Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI PRETEST …….55

Figura 6 : Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI POSTEST …….56

ÍNDICE DE ANEXOS

Pg.

Anexo N° 1**:** Matriz de consistencia..... 67

Anexo N° 2**:** Cuestionario de preguntas para la recolección de datos..... 68

Anexo N° 3**:** Validación de Fiabilidad Alpha Cronbach..... 72

RESUMEN

Los procesos de gestión de riegos relacionados a las tecnologías de información y la administración de la continuidad de los procesos organizacionales, representan una acción de tipo imprescindible y estratégica para garantizar la eficacia y efectividad del sistema de Gestión para asegurar la información; representan también herramientas de primer orden que permiten recabar información para el apoyo en las actividades de toma de decisiones. La gestión de riesgos sobre los activos de información de las empresas representa las buenas prácticas y la garantía de la supervivencia de las empresas, permite obtener el documento de gestión de riesgos tecnológicos. En esta investigación se logró demostrar que la implementación de modelo de gestión basado en la NTP 17799 en conjunto con la metodología Magerit, permite alcanzar una mayor efectividad en la determinación de los niveles de riesgos de los activos y el tratamiento adecuado para minimizar o mitigar.

Palabras clave: NTP, Administración, Riesgos, TI

ABSTRACT

Risk management processes related to information technology and the administration of the continuity of organizational processes represent an essential and strategic action to guarantee the efficiency and effectiveness of the management system to ensure information; they also represent first-rate tools that allow gathering information to support decision-making activities. Risk management on information assets of companies represents good practices and the guarantee of the survival of companies, allowing the obtaining of the technological risk management document. In this research it was possible to demonstrate that the implementation of a management model based on NTP 17799 in conjunction with the Magerit methodology allows achieving greater effectiveness in determining the risk levels of assets and the appropriate treatment to minimize or mitigate.

Keywords: NTP, Administration, Risks, IT

INTRODUCCIÓN

La primicia de la tecnología de la mayoría de empresas, se han ejecutado y se continúan ejecutando en algunas o en la mayoría de ocasiones sin el control adecuado propiciando, en la actualidad, que las empresas desconozcan la forma de la estructura del área informática, como también carecen de información sobre la cantidad, características y estados de los distintos activos informático, situación que genera un alto riesgo y posibles eventos desfavorables.

La presente tesis, se sustenta en esa carencia de gestión de activos, proporcionará los lineamientos de una correcta estructura organizativa y un acertado tratamiento de riesgos relacionados a TI, se identificará las vulnerabilidades y amenazas al que están expuesto los activos de TI. Para desarrollar lo precisado se hará uso a través de la implementación de la NTP ISO/IEC 17799.

Esta investigación se encuentra organizada por capítulo los cuales se presentan a continuación: Capítulo I: Con secciones de la Realidad problemática, los Objetivos, Variables de investigación. Capitulo II; C Marco teórico, con los antecedentes, bases y definición de términos. Capitulo III: La Metodológica aplicada de la investigación, el método, tipo, el nivel y diseño de la investigación. Capitulo IV: Implementación de la solución. Capitulo V: Se detalla los Resultados de la investigación. Capítulo VI: Se presentan las Conclusiones y Recomendaciones; Y por último las secciones de Bibliografías y anexos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. DESCRIPCIÓN Y FUNDAMENTACION DEL PROBLEMA.

En aceptado que la tecnología avanza cada vez mejor y de una manera impresionante, la interconectividad entre distintos dispositivos, la manera de buscar información, la forma y los medios de comprar de forma virtual, son algunos ejemplos como el internet ha venido a cambiarnos la vida. La Tecnologías e información es una necesidad urgente para cualquier tipo de negocio debido a que brinda el soporte para una gestión, control y planificación de forma más exacta y precisa.

La información producto del procesamiento de los datos generados por distintos procesos empresariales se ha convertido en uno del activo más importante para una organización y debido a que nos encontramos en un entorno muy interconectado la información se encuentra más expuestas y vulnerables, siendo necesario aplicar medidas para una mayor protección, control y monitoreo constante para asegurar la integridad de la información.

Así como la tecnología mejora los procesos también aparecen personas que de una y otra forma ven la oportunidad de efectuar acciones ilícitas, con la finalidad de aprovecharse y adquirir beneficios, asimismo, en la actualidad, también, existen diversos mecanismos y herramientas, metodologías y buenas prácticas que el soporte para garantizar y mejorar la seguridad de la información.

La empresa presenta una deficiencia en la gestión de seguridad de la información, debido a políticas de seguridad deficientes que impide un exacto y correcto monitoreo de accesos, carece de concientización de los usuarios sobre temas tales como: riesgos, clasificación y control de activos, fidelización de los usuarios con respecto a normativas; también se puede apreciar la falta de integridad que carece la información de los procesos de TI. Luego de una consulta rápida se pudo notar que la mayoría de los empleados no tiene conocimiento de los aspectos de confidencialidad presentes en la firma de sus contratos, desconocen las políticas de seguridad con respecto a los activos de información

De continuar en esta situación problemática, existe una gran probabilidad de sufrir un alto impacto negativo y generaría pérdidas a nivel de costos, credibilidad; por este motivo se busca auxiliar a la empresa a través de la implementación de controles eficientes y eficaces, así como de brindar el conocimiento respecto a seguridad de la información y la necesidad para mantener competitividad, rentabilidad y continuidad del negocio; con las buenas prácticas a través de la aplicación de la NTP ISO/IEC 17799 para la gestión de seguridad de la información.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1 Problema General.

- ¿De qué manera la implementación de la NTP-ISO/IEC 17799 mejorará la administración de riesgos de TI de la empresa TELPERU SAC?

1.2.2 Problemas Específicos.

- ¿De qué forma la identificación y clasificación de activos de TI mejorará la administración de riesgos de TI de la empresa TELPERU SAC?

- ¿Cómo la identificación de las amenazas y vulnerabilidades de los activos de TI mejorará la administración de riesgos de TI de la empresa TELPERU SAC?
- ¿De qué manera la valoración del Impacto y probabilidad de ocurrencia de amenazas mejorará la administración de riesgos de TI de la empresa TELPERU SAC?
- ¿De qué forma la implementación de medidas de seguridad y estrategias mejorará la administración de riesgos de TI de la empresa TELPERU SAC?

1.3. OBJETIVOS DE LA INVESTIGACIÓN.

1.3.1 Objetivo General.

- Implementar la NTP-ISO/IEC 17799 para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.

1.3.2 Objetivos Específicos.

- Identificar y clasificar activos de TI para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.
- Identificar las amenazas y vulnerabilidades de los activos de TI para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.
- Efectuar una valoración del Impacto y probabilidad de ocurrencia de amenazas para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.
- Implementar de medidas de seguridad y estrategias para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.

1.4. JUSTIFICACIÓN, IMPORTANCIA Y LIMITACIONES.

1.4.1 Justificación.

Justificación teórica

Debido a que uno de los propósitos implícitos de esta investigación es aportar acerca del conocimiento de la NTP-ISO/IEC, a partir de la implementación que se propone, como acerca de la Administración de Riesgo, ya que se consideran las concepciones tecnológicas y teóricas necesarias para un adecuado abordaje investigativo de estas variables en la sede de estudio.

Justificación práctica

Debido a que mediante esta investigación se pretende aportar a la solución de las dificultades para la Administración de Riesgo, esto a través de la implementación NTP-ISO/IEC, que servirá de estímulo adecuado para generar confianza en la empresa TELPERU SAC.

Justificación metodológica

Debido a que el abordaje y los procedimientos que se siguen en esta investigación presentan una alternativa a investigaciones de esta índole, por lo que servirá de guía a nuevos investigadores que aborden las variables de este estudio, así también, el instrumento de recolección de datos, podrá ser reutilizado en contextos con características similares al que se aborda en esta investigación.

1.4.2 Importancia.

El desarrollo de NTP-ISO/IEC 17799 en la empresa TELPERU SAC. surge por la importancia determinar los objetivos, procesos y procedimientos

para el establecimiento de políticas y controles de seguridad que ayudarán a gestionar los riesgos en la seguridad de la información.

1.4.3 Limitaciones.

En la ejecución prevista de esta investigación podrían presentarse ciertas limitaciones tales como:

- Escasos trabajos de investigación especializados con las dimensiones de nuestra variable dependiente, en nuestro medio, que nos sirvan como antecedentes.
- La aplicación de los instrumentos de recolección de datos a los estudiantes en cuanto se refiere a la confiabilidad de los resultados, que puedan ser respuestas sesgadas.
- La aplicación de la norma NTP-ISO/IEC 17799 se desarrollará en forma proporcional, de acuerdo a las estrategias de la empresa.

1.5. HIPÓTESIS, VARIABLES DE INVESTIGACIÓN.

1.5.1 Hipótesis General

- La Implementación de la NTP-ISO/IEC 17799 mejora la administración de riesgos de TI de la empresa TELPERU SAC.

1.5.2 Hipótesis Específicas

- La Identificación y clasificación de activos de TI mejoran la administración de riesgos de TI de la empresa TELPERU SAC.
- La Identificación de las amenazas y vulnerabilidades de los activos de TI mejoran la administración de riesgos de TI de la empresa TELPERU SAC.
- La valoración del Impacto y probabilidad de ocurrencia de amenazas mejora la administración de riesgos de TI de la empresa TELPERU SAC.

- La implementación de medidas de seguridad y estrategias mejora la administración de riesgos de TI de la empresa TELPERU SAC.

1.6. DELIMITACIONES DE LA INVESTIGACIÓN

1.6.1 Delimitación Espacial.

Esta investigación se realizará con aplicación práctica en la empresa TELPERU SAC.

1.6.2 Delimitación Social.

El grupo social objeto de estudio son los empleados que laboran en la empresa TELPERU SAC, quienes deberían administrar del modo adecuado la NTP-ISO/IEC 17799.

1.6.3 Delimitación Temporal.

El objeto de la investigación se realizará en el periodo probable desde Abril del 2024 hasta Abril del 2025.

1.6.4 Delimitación Conceptual.

En la presente investigación se hace uso de teorías relacionados a la Administración de Riesgo; “Es identificar, cuantificar y administrar los riesgos relacionados con la seguridad de la información para alcanzar los objetivos de la empresa TELPERU SAC mediante una serie de tareas que requiere del conocimiento del gerente de seguridad de la información sobre la técnica clave de la gestión de riesgos”.

1.7. VARIABLES

1.7.1 Variable independiente:

LA NTP-ISO/IEC 17799

1.7.2 Variable dependiente:

ADMINISTRACIÓN DE RIESGOS DE TI

1.7.3 Variable interviniente:

TELPERU SAC

1.8. SISTEMA DE VARIABLES, DIMENSIONES E INDICADORES.

1.8.1 Operacionalización de variables.

- **Variable**: La NTP-ISO/IEC 17799

Tabla 1: Operacionalización de variable I

Dimensión	Indicadores	Escala
Activos	• Procesos de TI. • Activos de información. • Valoración de activos.	Muy en desacuerdo En desacuerdo Indiferente De acuerdo Muy de acuerdo
Exposición	• Amenazas • Vulnerabilidades. • Tolerancia a riesgo.	
Valoración	• Impacto • Probabilidad de ocurrencia. • Métricas	
Políticas	• Políticas. • Medidas y estrategias de seguridad.	

- **Variable**: **Administración** de riesgos de TI.

Tabla 2: Operacionalización de variable II

Dimensión	Indicadores	Escala
Estructuración de la metodología de análisis y tratamiento de riesgos	• Efectividad en la definición de los riesgos. • Nivel de integración del modelo en la gestión de riesgos • Grado de concientización	Muy en desacuerdo En desacuerdo Indiferente De acuerdo Muy de acuerdo
Gobierno de los riesgos de TI	• Cumplimiento normativo de las variables • Efectividad en la evaluación de los componentes • Efectividad del monitoreo de las actividades • Tiempo de recuperación de incidentes	
Análisis y tratamiento de riesgos	• Nivel de aplicabilidad del proceso implantado • Efectividad los niveles de riesgos inherentes de TI • Efectividad de la implantación de controles y seguimiento.	
Gobierno de los riesgos de TI	• Grado de satisfacción por la información resultante • Grado de satisfacción del modelo para la toma de decisiones	

CAPÍTULO II

MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. Antecedentes Internacionales.

De acuerdo a la investigación de Melano (2019), en cuya investigación procura Identificar una estrategia en el proceso para implementación de un Sistema de Gestión de Seguridad de Información tomando como base la norma ISO 27001 en el área de TI para la empresa Market Mix. Al finalizar alcanzó las siguientes conclusiones: Después haberse seleccionado las herramientas para la evaluación del estado actual de TI, los datos obtenidos se procesaron y se identificó la mejor estrategia a fin de cumplir con los objetivos, el estudio de la estrategia y el monitoreo de labores y responsabilidades asignadas a los integrantes, han permitido identificar riesgos dentro de la organización, así mismo tratarlos y realizar correcciones a fin de hacer mejoras continuas y proteger la información.

Según investigación de Guevara (2019), se planteó la Implementación de la norma de seguridad ISO 27001 para alcanzar mejorar la confidencialidad, disponibilidad e integridad de los SI y comunicación del Departamento de Sistemas de la Cooperativa de Ahorro y Crédito — San Francisco‖ Ltda. Al finalizar se concluyó en: La ISO 27001 está orientado para el tratamiento de seguridad de la información a través la gestión de riesgos, describe la forma de mantener y mejorar la seguridad de activos de información, para lograr garantizar y mejorar la seguridad se ha logrado diseñar un Sistema de Gestión de SI, en donde se ha elegido algunos activos se encuentran desprotegidos, se ha definido controles que aseguren su protección, al implementar un SGSI bajo la norma ISO 27001, se alcanzó contar

con la seguridad máxima sobre la información de la organización, esto significa que se cumplió con los requerimientos y las mejores prácticas y además pueda evolucionar hacia la sofisticación.

2.1.2. Antecedentes Nacionales.

En la investigación realizada por (Oré Crisóstomo, 2018), cuya finalidad fue la de formular políticas de SI para así mejorar la Gestión de Información en la UGEL de Chincha, alcanzo los siguientes resultados: Con la aplicación de la NTP ISO/IEC 17799 se logró formular adecuadamente las políticas para el inventario de activos, se elaboró e implemento un plan de protección, se realizó exitosamente el análisis de riesgos para la Gestión de información.

En la investigación de (Chicoma Gutarra, 2018), el investigador busca determinar el efecto que la ISO/IEC 17799 causa sobre la seguridad de la información sobre las empresas denominada Nuevo mundo viajes, y logro concluir en: Con la implementación de la norma, la cantidad de accesos sin autorización se logró pasar desde un promedio inicial de 13.13% a 5.57 % por los controles implementados; en lo que respecta a la manipulación de datos se logró una mejora significativa en la seguridad al disminuir de un promedio de 7.96% a 3.63%; en lo que respecta al tiempo de disponibilidad del sistema se mejoró desde un promedio de 27.7% de disponibilidad a un promedio de 98.38%; con esta información se concluye que la aplicación de la norma fue positiva para la mejora de la seguridad de la información.

En la investigación de (Donayre Uchuya, 2017), que tuvo como fin el diseño de un modelo de auditoría de SI que se alinee con las políticas de seguridad de la institución, concluyo que: Las personas encuestadas están de acuerdo con el diseño de modelo de auditoría, este diseño permitió la alineación de auditorías

físicas con las políticas de seguridad, también manifestaron su acuerdo sobre la adaptabilidad del nuevo modelo.

2.2. BASES TEÒRICAS.

- **Seguridad de la información.**

Según Microsoft (2024). La seguridad de la información, a menudo abreviada (InfoSec), es un conjunto de procedimientos y herramientas de seguridad que protegen ampliamente la información corporativa sensible del uso indebido, el acceso no autorizado, la destrucción o la destrucción. La seguridad de la información cubre la seguridad física y ambiental, el control de acceso y la seguridad de la red.

Según Tang (2023). La seguridad de la información (InfoSec) es fundamental en el mundo digital actual. A medida que el volumen de información confidencial almacenada y transmitida digitalmente continúa creciendo, el riesgo de filtraciones de datos y delitos cibernéticos continúa aumentando. Tanto los individuos como las empresas deben tomar medidas para proteger los datos confidenciales contra el acceso no autorizado, el robo y el uso indebido.

- **El papel de las medidas de seguridad de la información en las empresas**

Una de las funciones clave de las medidas de seguridad de la información de una empresa es proteger los datos confidenciales. La información confidencial incluye secretos comerciales, información de clientes, información financiera, etc. Al implementar sistemas de prevención de intrusiones, como cifrado de datos, controles de acceso y firewalls, las empresas pueden garantizar que los datos confidenciales estén protegidos contra el acceso no autorizado y el uso indebido.

Las medidas de seguridad de la información también ayudan a las empresas a cumplir con los requisitos reglamentarios. Muchas industrias tienen acuerdos de confidencialidad (NDA) que requieren la protección de información confidencial. El incumplimiento de estas regulaciones puede resultar en responsabilidad legal, multas y daños a la reputación. Al implementar medidas efectivas de seguridad de la información, las empresas pueden garantizar el cumplimiento de estas regulaciones y evitar posibles consecuencias legales y financieras.

- **Tipos de seguridad de la información.**

  - **Seguridad de la aplicación.**

De acuerdo con (Cisco, 2024). Este tipo de seguridad busca proteger los programas informáticos y las interfaces de programación de aplicaciones (API) asegurando que la información que utilizan funcione correctamente de acuerdo con los principios de Confidencialidad, Integridad y Disponibilidad (CIA). Diseñado.

La seguridad de las aplicaciones generalmente son las medidas tomadas para proteger las aplicaciones de software de amenazas y vulnerabilidades que podrían comprometer la confidencialidad, integridad o disponibilidad de los datos y sistemas que ejecutan las aplicaciones de software. Esto incluye considerar la seguridad al diseñar, desarrollar, probar e implementar aplicaciones e implementar controles para detectar y responder a incidentes de seguridad.

La seguridad de las aplicaciones incluye una variedad de tecnologías y prácticas, que incluyen:

- **Autenticación y autorización:** un sistema de prevención de intrusiones que autentica a los usuarios y otorga el nivel adecuado de acceso a los recursos dentro de una aplicación.

- **Validación de entrada:** asegúrese de que todos los datos ingresados en su aplicación estén correctamente desinfectados y validados para evitar ataques de inyección como inyección SQL, secuencias de comandos entre sitios (XSS) y otros ataques similares.
- **Cifrado:** cifre sus datos en reposo y en tránsito para evitar la pérdida de datos.
- **Control de acceso:** implemente políticas de seguridad de datos o gestión de identidad y acceso para controlar quién tiene acceso a qué datos y funcionalidades dentro de su aplicación.
- **Prácticas de codificación segura:** desarrolle aplicaciones utilizando prácticas de codificación segura para reducir el riesgo de vulnerabilidades.
- **Pruebas de seguridad:** realice varios tipos de pruebas de seguridad, como pruebas de penetración, escaneos de vulnerabilidades y revisiones de código para identificar y remediar vulnerabilidades.

➢ **Ventajas de implementar un sistema de clasificación de información en el programa de seguridad de la información de una organización:**

De acuerdo con Geeksforgeeks (2024)**:**

- **Seguridad mejorada:** al identificar y clasificar la información confidencial, las organizaciones pueden proteger mejor sus activos más confidenciales contra el acceso o la divulgación no autorizados.

- **Cumplimiento:** muchas regulaciones y estándares de la industria, como HIPAA y PCI-DSS, requieren que las organizaciones implementen medidas de clasificación de información y protección de datos.

- **Aumente la eficiencia:** al identificar y etiquetar claramente los mensajes, los empleados pueden determinar rápida y fácilmente los requisitos de procesamiento y acceso adecuados para diferentes tipos de datos.

- **Mejor gestión de riesgos:** al comprender el impacto potencial de una violación de datos o una divulgación no autorizada, las organizaciones pueden priorizar los recursos y desarrollar planes de respuesta a incidentes más efectivos.

- **Ahorro de costos:** al implementar controles de seguridad adecuados para diferentes tipos de información, las organizaciones pueden evitar gastos innecesarios en medidas de seguridad que pueden no ser necesarias para datos menos confidenciales.

- **Respuesta mejorada a incidentes:** al comprender claramente la importancia de datos específicos, las organizaciones pueden responder a los incidentes de seguridad de una manera más efectiva y eficiente.

- **La Norma Técnica Peruana 17799.**

Según Pmg-ssi (2015). La norma técnica peruana NTP-ISO/IEC 17799 brinda todas las recomendaciones necesarias para la gestión de un sistema de seguridad de la información (ISS), mientras que la norma internacional ISO 27001 también brinda orientación para ayudar a los responsables de áreas específicas a iniciar, implementar, mantener y gestionar un sistema de seguridad de la información. sistema de seguridad (ISS). Proporciona los requisitos necesarios. Mejore la seguridad de su organización.

La norma ISO/IEC 17799 pretende proporcionar una base común para implementar normas de seguridad dentro de las empresas y para prácticas eficaces de gestión de la seguridad.

La Norma Técnica Peruana ISO/IEC 17799 es una guía práctica para establecer estándares de seguridad para su organización y crear prácticas efectivas en sus procesos de gestión de seguridad de la información. También puede aumentar la confianza al construir relaciones entre diferentes organizaciones. Todas las recomendaciones generadas a partir de esta norma deben utilizarse de conformidad con la legislación aplicable al tema.

La información es un activo muy valioso para su empresa y debe protegerse adecuadamente. Debería considerar mejorar la seguridad dentro de su organización. Como resultado de este crecimiento, la información se ha vuelto más vulnerable a numerosas amenazas y vulnerabilidades.

La información se utiliza de diversas maneras. Esto puede estar en formato papel, almacenarse electrónicamente o transmitirse por correo electrónico, video o conversación cara a cara. Esto requiere proteger adecuadamente su información, independientemente del formato en el que no se pueda encontrar.

Un sistema de seguridad de la información (ISS) protege la información de una variedad de amenazas, asegurando la continuidad del negocio, reduciendo el daño organizacional y maximizando el retorno de la inversión y las oportunidades comerciales.

Los requisitos estándar de ISO/IEC 17799 son específicos de cada terminal, que son los requisitos necesarios para interpretar la especificación y, en última

instancia, todos los terminales se definen basándose en una comprensión básica de:

- **Activo**: Aporta gran valor a la organización.
- **Control**: Incluye política, política, estructura organizacional, administración natural, tecnología jurídica, etc.
- **Pauta**: Explique nuestra situación y comprenda los objetivos de nuestra política de seguridad.
- **Instalación de procesamiento de información:** Localización de sistemas, servicios o infraestructuras de información.
- **Seguridad de la información:** Preservación de la información confidencial, integridad y confidencialidad de la información, y muchas otras medidas de protección para garantizar la seguridad, la confidencialidad y la confidencialidad.
- **Incidente de seguridad de la información:** situación en la que puede ocurrir un problema o situación relacionada con la seguridad en un sistema, servicio o política de seguridad de la información.
- **Incidente de seguridad de la información:** es un incidente separado, no hay una sola persona o autor y existe una alta posibilidad de que se violen las operaciones de transacción y las medidas de seguridad de la información.
- **Política de seguridad**: Documento que establece el propósito de implementar el sistema de seguridad de la información de una organización. Es algo grandioso porque es algo grandioso. Esto es genial.

- **Riesgo:** Es la combinación de la probabilidad de que ocurra un evento y la probabilidad de que ocurra el evento.
- **Análisis:** utiliza información del sistema para identificar situaciones comunes y todos los recursos relevantes.
- **Evaluación:** El proceso general de análisis y evaluación de una evaluación.
- **Resultados de la evaluación**: compare los resultados de la evaluación con los resultados de la evaluación.
- **Gestión:** Dirigir y controlar las actividades de una organización, teniendo en cuenta la gestión de los productores.
- **Tratamiento:** Procedimientos y métodos selectivos para modificar el tratamiento.
- **Tercero:** Una persona independiente que tenga una idea sobre el tema que se está tratando.
- **Causa:** La causa raíz de un incidente es el resultado del sistema organizacional.
- **Vulnerabilidad:** Debilidad debida a una actividad o conjunto de actividades que resulta en alguna actividad destructiva.

2.3. DEFINICIÓN DE TÉRMINOS BÁSICOS

- **NTP-ISO 17799.**

De acuerdo con Esan (2016). Es una compilación de recomendaciones para las prácticas exitosas de seguridad, que toda organización puede aplicar independientemente de su tamaño o sector.

- **Administración.**

De acuerdo con Quiroa (2020). La gestión es el proceso de planificar, organizar, ejecutar y controlar los recursos para utilizarlos de manera más eficiente para lograr los objetivos organizacionales.

- **Gestión**.

Según (Coursera, 2023) .La gestión es la forma en que una empresa organiza y dirige sus procesos comerciales, operaciones y empleados para lograr los objetivos de la empresa.

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. MÉTODO DE INVESTIGACIÓN.

- **Tipo de investigación**

  El tipo de investigación[1] por finalidad empleado es: Aplicada

- **Nivel de investigación**

  Descriptiva (Se mide las variables relevantes) – Pre - Experimental Según Hernández, Fernández y Baptista (2010) la Metodología de la Investigación señala que: "es aquella que obtiene datos a través de la experimentación y los compara con variables constantes, a fin de determinar las causas y/o los efectos de los fenómenos en estudio).

- **Método de investigación**

  El método que utilizaremos es el hipotético-deductivo. Usaremos hipótesis para identificar necesidades o problemas en la empresa TELPERU SAC y deduciremos las posibles consecuencias.

- **Diseño de la investigación**

  El diseño de la tesis es EXPERIMENTAL DE TIPO PRE-EXPERIMENTAL. Esto se debe a que estaremos implementando la norma técnica peruana NTP-ISO/IEC 17799 y evaluando su impacto en la administración de riesgos de TI de la empresa TELPERU SAC. Además de que se carece de grupos de control y de comparación.

[1]Hernández Sampieri, Fernández Collado y Baptista Lucio (2010) – Metodología de la investigación Científica" (p. 115).

3.2. POBLACIÓN Y MUESTRA.

- **Población.**

La población lo conforman los empleados que realizan sus labores en el área de TI los cuales se detalla a continuación:

Tabla 3: Población

Cargo	Cantidad
Jefe	01
Adm. Redes	01
Soporte técnico	03
Asistente	03
Total	**08**

- **Muestra.**

Para la muestra se optó por no aplicar el muestreo probabilístico, y eso debido al número reducido de la población; por lo cual, se aplicará el muestreo por conveniencia, siento el tamaño de la muestra la misma cantidad que la población 08 empleados.

3.3. TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS.

La técnica elegida para obtener los datos a partir de la muestra estadística es la encuesta y el instrumento es el cuestionario de preguntas que tendrá como escala la de Likert aplicando como base las variables de investigación.

3.4. PROCEDIMIENTO DE RECOLECCIÓN DE DATOS.

El procedimiento de recolección de datos será a través de la aplicación de cuestionario a los empleados elegidos como parte de la muestra, estos serán comunicados y capacitados de ser caso, y la aplicación de la encuesta se realizará en dos momentos diferentes.

3.5. TRATAMIENTO DE DATOS.

Para esto será necesario el uso de una herramienta de software estadístico como el SPSS de IBM, herramienta que permitirá obtener información sintetizada a través del tablas y gráficos para su evaluación.

3.6. GRADO DE CONFIABILIDAD DE LOS DATOS.

Será necesario el uso de alfa de Cronbach que viene a ser un coeficiente que se utiliza para medir la fiabilidad de la escala de medida utilizada en el instrumento de recolección de datos.

CAPÍTULO IV

ADMINISTRACIÓN DE RIEGOS DE TI – TELPERU SAC.

4.1. La empresa

Es una empresa con experiencia en el campo de la ingeniería de telecomunicaciones, electricidad, electrónica. Fundada en el año 2006 con RUC 20486407965. Participa en proyectos, diseño de infraestructura, puesta en marcha de soluciones cumpliendo altos estándares de calidad.

WEB: https://telperusac.com/

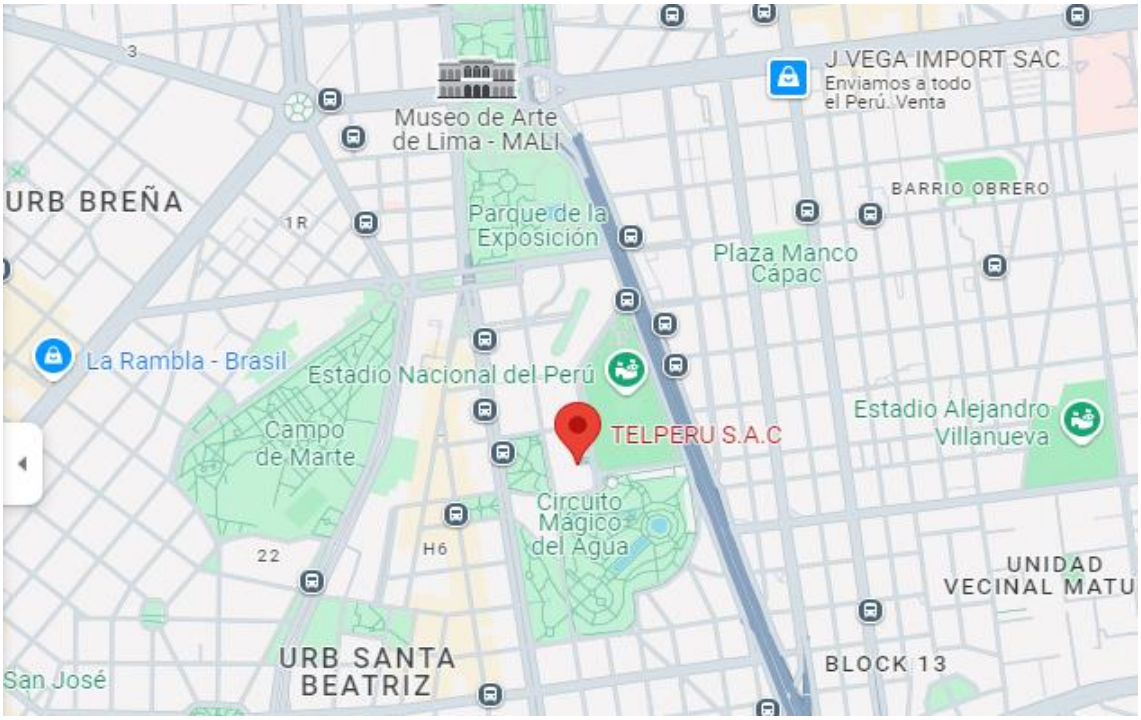
Figura 1: portal Web de la Institución



Ubicación

C. José Díaz 452, Lima 15046

Figura 2: Mapa de ubicación geográfica



4.2. Identificación y clasificación de activos de TI

En esta fase se aplicó la metodología de abajo hacia arriba, bottom-up, producto de reuniones con los involucrados se identificó los siguientes activos:

Tabla 4: Inventario de activos

Ítem	Activo
01	Servidor de dominio y AD
02	Servidor de Aplicaciones y Base de datos
03	Redes de comunicaciones y equipos
04	Base de datos
06	Copias de seguridad
06	Personal de TI
07	Aplicaciones informáticas
08	Correo electrónico
09	Computadoras personales y portátiles
10	Impresoras
11	Archivos- documentación física
12	Equipos UPS

4.3. Clasificación de activos por tipo

Tabla 5: Clasificación de activos por tipo

Ítem	Tipo	Activo
01	Servicio	Servidor de dominio y AD
02	Servicio	Servidor de Aplicaciones y Base de datos
03	Equipos	Redes de comunicaciones y equipos
04	Información	Base de datos
06	Información	Copias de seguridad
06	Personal	Personal de TI
07	Aplicaciones	Aplicaciones informáticas
08	Servicio	Correo electrónico
09	Equipos	Computadoras personales y portátiles
10	Equipos	Impresoras
11	Información	Archivos- documentación física
12	Equipos	Equipos UPS

4.4. Criticidad de los activos

Tabla 6: Criticidad

Ítem	Tipo	Activo.	C. de seguridad			Total	Nivel Criticidad
			C	I	D		
01	Servicio	Servidor de dominio y AD	4	5	5	4	Alto
02	Servicio	Servidor de Aplicaciones y Base de datos	5	5	5	5	Muy Alto
03	Equipos	Redes de comunicaciones y equipos	4	1	5	3	Medio
04	Información	Base de datos	5	5	5	5	Muy Alto
06	Información	Copias de seguridad	5	5	5	5	Muy Alto
06	Personal	Personal de TI	4	1	5	3	Medio
07	Aplicaciones	Aplicaciones informáticas	4	4	5	4	Alto
08	Servicio	Correo electrónico	4	4	5	4	Alto
09	Equipos	Computadoras personales y portátiles	5	5	5	5	Muy Alto
10	Equipos	Impresoras	3	3	3	3	Medio
11	Información	Archivos- documentación física	3	3	5	3	Medio
12	Equipos	Equipos UPS	4	4	4	4	Alto

4.5. Amenazas

Se evaluó cada uno de los activos y se han identificado amenazas que atentan contra la seguridad, los cuales se listan a continuación.

Tabla 7: Amenazas

Ítem	Activo	Amenazas
01	Servidor de dominio y AD	Detenido del proceso, apagado del servidor, paralización del servicio y paralización las actividades de la empresa
02	Servidor de Aplicaciones y Base de datos	Carencia de recursos de Hardware, cortes de fluido eléctrico, falla del equipo
03	Redes de comunicaciones y equipos	Apagado de equipos de comunicación, falla de equipos.
04	Base de datos	Paralización del servicio, perdida de información.
06	Copias de seguridad	Desactualización, información corrupta, información incompleta.
06	Personal de TI	Tardanzas, retraso en atención de servicios, mala gestión, incumplimiento de políticas, inasistencias. Divulgación de información sensible Borrado de información.
07	Aplicaciones informáticas	Fallas de servicio. Ataques de archivos maliciosos.
08	Correo electrónico	Pérdida de acceso a internet.
09	Computadoras personales y portátiles	Obsolescencia tecnológica, fallas de hardware, mal uso.
10	Impresoras	Deterioro, falta de mantenimiento.
11	Archivos- documentación física	Perdida, deterioro, ambiente de resguardo inadequado.
12	Equipos UPS	Obsolescencia, cumplimiento de vida útil de bateristas.

4.6. Vulnerabilidades de los activos

Una vez identificado las amenazas de los activos de TI, se procedió con identificar las vulnerabilidades y se obtuvieron como resultado lo siguiente.

Tabla 8: Vulnerabilidades

Ítem	Activo	Amenazas	Vulnerabilidad
01	Servidor de dominio y AD	Detenido del proceso, apagado del servidor, paralización del servicio y paralización las actividades de la empresa	Cortes de fluido eléctrico por el servicio de Enel Perú. Ataques de programas maliciosos. Carencia de un plan de mantenimiento Carencia de personal especializado. Carencia de actualizaciones de sistemas operativos
02	Servidor de Aplicaciones y Base de datos	Carencia de recursos de Hardware, cortes de fluido eléctrico, falla del equipo	La cuenta con rol de administrador maestro, puede realizar modificaciones. Falta de componentes actualizados Carencia de actualizaciones de sistemas operativos Falta de plan de mantenimiento.
03	Redes de comunicaciones y equipos	Apagado de equipos de comunicación, falla de equipos.	Falla de la línea de conexión a internet. Carencia de documentación técnica. Carencia de un servidor firewall.
04	Base de datos	Paralización del servicio, perdida de información.	Carencia de procedimientos documentados para asignación de roles. Contraseñas fáciles de los usuarios. Modificación sin autorización.
06	Copias de seguridad	Desactualización, información corrupta, información incompleta.	Lugar inadecuado de resguardo. Falla del sistema backup. Carencia de espacio de almacenamiento

			Falta de registro de copias de seguridad.
06	Personal de TI	Tardanzas, retraso en atención de servicios, mala gestión, incumplimiento de políticas, inasistencias. Divulgación de información sensible Borrado de información.	Inadecuada segregación de las funciones. Carencia de un plan de capacitaciones. Personales indisponibles por problemas de enfermedades, accidentes, etc.
07	Aplicaciones informáticas	Fallas de servicio. Ataques de archivos maliciosos.	Mal uso de privilegios Errores de usuarios Falta de conexión a la red Fallas eléctricas Carencia del soporte adecuado.
08	Correo electrónico	Pérdida de acceso a internet.	Problemas de conexión con el servidor No generar backups Contraseñas inseguras
09	Computadoras personales y portátiles	Obsolescencia teológica, fallas de hardware, mal uso.	Mal uso del personal Equipos desfazados Falta de mantenimiento Errores de sistemas operativos
10	Impresoras	Deterioro, falta de mantenimiento.	Condiciones ambientales no adecuadas Falta mantenimiento Falta de consumibles Fallas eléctricas.
11	Archivos-documentación física	Perdida, deterioro, ambiente de resguardo inadecuado.	Mala manipulación Ambientes inadecuados
12	Equipos UPS	Obsolescencia, cumplimiento de vida útil de bateristas.	Fallas de equipos Vida útil completada Falta de mantenimiento

4.7. Valoración del impacto y probabilidad de ocurrencia de amenazas

Se efectúa estas actividades para poder determinar el nivel de riesgo al que se encuentra expuesto el activo; para esto, se realizó la captura de información sobre la evaluación de controles actuales, se realizó entrevistas, observaciones y testeo.

Los resultados de la valoración para impacto y probabilidad de ocurrencia de cada una de las amenazas se detallan en la siguiente tabla.

Tabla 9: Valores del impacto y probabilidad

Ítem	Activo	Amenazas	Vulnerabilidad	Impacto		Probabilidad-amenaza explote la vulnerabilidad		Nivel de Riesgo Intrínseco		
				Nivel	Categoría	Nivel	Categoría	Id Riesgo	Nivel	Categoría
01	Servidor de dominio y AD	Detenido del proceso, apagado del servidor, paralización del servicio y paralización las actividades de la empresa	Cortes de fluido eléctrico por el servicio de Enel Perú.	5	Catastrófico	4	Probable	R1	5	Muy alto
			Ataques de programas maliciosos.	2	Menor	2	Improbable	R2	2	Bajo
			Carencia de un plan de mantenimiento	2	Menor	2	Improbable	R3	2	Bajo
			Carencia de personal especializado.	3	Moderado	3	Posible	R4	3	Medio
			Carencia de actualizaciones de sistemas operativos	3	Moderado	3	Posible	R5	3	Medio
02	Servidor de Aplicaciones y Base de datos	Carencia de recursos de Hardware, cortes de fluido eléctrico, falla del equipo	La cuenta con rol de administrador maestro, puede realizar modificaciones.	4	Mayor	3	Posible	R6	3	Medio
			Falta de componentes actualizados	3	Moderado	3	Posible	R7	3	Medio
			Carencia de actualizaciones de sistemas operativos	2	Menor	2	Improbable	R8	2	Bajo

03	Redes de comunicaciones y equipos	Apagado de equipos de comunicación, falla de equipos.	Falta de plan de mantenimiento.	3	Moderado	3	Posible	R9	3	Medio
			Falla de la línea de conexión a internet.	5	Catastrófico	4	Probable	R10	5	Muy alto
			Carencia de documentación técnica.	3	Moderado	3	Posible	R11	3	Medio
			Carencia de un servidor firewall.	4	Mayor	4	Probable	R12	4	Alto
04	Base de datos	Paralización del servicio, perdida de información.	Carencia de procedimientos documentados para asignación de roles.	4	Mayor	4	Probable	R13	4	Alto
			Contraseñas fáciles de los usuarios.	3	Moderado	3	Posible	R14	3	Medio
			Modificación sin autorización.	4	Mayor	3	Posible	R15	4	Alto
06	Copias de seguridad	Desactualización, información corrupta, información incompleta.	Lugar inadecuado de resguardo.	3	Moderado	3	Posible	R16	3	Medio
			Falla del sistema backup.	3	Moderado	3	Posible	R17	3	Medio
			Carencia de espacio de almacenamiento	3	Moderado	3	Posible	R18	3	Medio
			Falta de registro de copias de seguridad.	4	Mayor	3	Posible	R19	4	Alto
06	Personal de TI	Tardanzas, retraso en atención de servicios,	Inadecuada segregación de las funciones.	5	Catastrófico	4	Probable	R20	5	Muy alto

				Carencia de un plan de capacitaciones.	3	Moderado	3	Posible	R21	3	Medio
				Personales indisponibles por problemas de enfermedades, accidentes, etc.	4	Mayor	3	Posible	R22	4	Alto
				Mal uso de privilegios	4	Mayor	3	Posible	R23	4	Alto
				Errores de usuarios	3	Moderado	3	Posible	R24	3	Medio
07	Aplicaciones informáticas	Fallas de servicio.	Taques de archivos maliciosos.	Falta de conexión a la red	5	Catastrófico	4	Probable	R25	5	Muy alto
				Fallas eléctricas	5	Catastrófico	4	Probable	R26	5	Muy alto
				Carencia del soporte adecuado.	3	Moderado	3	Posible	R27	3	Medio
				Problemas de conexión con el servidor	4	Mayor	4	Probable	R28	4	Alto
08	Correo electrónico	Pérdida de acceso a internet.		No generar backups	3	Moderado	3	Posible	R29	3	Medio
				Contraseñas inseguras	3	Moderado	3	Posible	R30	3	Medio
09	Computadoras	Obsolescencia teológica, fallas de hardware,		Mal uso del personal	4	Mayor	4	Probable	R31	4	Alto

10	Impresoras	Deterioro, falta de mantenimiento.	Equipos desfazados	4	Mayor	4	Probable	R32	4	Alto
			Falta de mantenimiento	3	Moderado	3	Posible	R33	3	Medio
			Errores de sistemas operativos	4	Mayor	4	Probable	R34	4	Alto
			Condiciones ambientales no adecuadas	3	Moderado	3	Posible	R35	3	Medio
			Falta mantenimiento	3	Moderado	3	Posible	R36	3	Medio
			Falta de consumibles	4	Mayor	3	Posible	R37	4	Alto
			Fallas eléctricas.	3	Moderado	3	Posible	R38	3	Medio
11	Archivos- documentación física	Perdida, deterioro, ambiente de resguardo inadecuado.	Mala manipulación	3	Moderado	3	Posible	R38	3	Medio
			Ambientes inadecuados	3	Moderado	3	Posible	R40	3	Medio
12	Equipos UPS	Obsolescencia, cumplimiento de vida útil de bateristas.	Fallas de equipos	3	Moderado	3	Posible	R41	3	Medio
			Vida útil completada	5	Catastrófico	4	Probable	R42	5	Muy alto
			Falta de mantenimiento	4	Mayor	3	Posible	R43	4	Alto

4.8. Métricas para la gestión de riesgos

Para poder determinar la probabilidad de un evento se produzca y a través de las consecuencias impacte negativamente es necesario establecer métricas, los cuales están basados en los indicadores de los riesgos claves (KRI).

Estos indicadores tienen como finalidad, ser de utilidad como alertas tempranas para informar sobre los cambios en los perfiles o valores de los riesgos.

En concordancia con la Asociación de Gestión de Riesgos, existen categorías de las cuales, por el tema de investigación, el siguiente:

- Riesgo de seguridad de la información.

Tabla 10: Riesgos de SI

Indicador.	Fuente.	Frecuencia (medición)
Nro. de personas que trabajan con información sensible de los clientes	Indicadores de los riesgos claves	Cada 03 meses
Nro. de ataques registrados por la seguridad de la información	Indicadores de los riesgos claves	Cada 03 meses
Nro. de fallos con los sistemas de información y los equipos informáticos	Propuesta propia	Cada 03 meses
Nro. de solicitudes de mesa de ayuda	Propuesta propia	Cada mes
Tiempo promedio de los sistemas en estado inactivo	Propuesta propia	Cada mes
Incremento de carga en las transacciones sobre los sistemas	Propuesta propia	Cada mes

4.9. Propuesta de políticas de seguridad en base a la ISO/IEC 27001

La implementación de políticas de seguridad se implementa antes de aplicar los controles que tratan los riesgos, estas políticas están según el marco de la ISO/IEC 27001.

Las políticas a implementar son:

Tabla 11: Políticas a implementar

Clausula.	Categoría	Control	Descripción
Política sobre seguridad	Política de SI	Documentación de la política de SI	La jefatura de la empresa debe aprobar el documento de políticas, publicarlas y hacerle extensible a todos los empleados
		Revisión de la policía de SI	La Políticas de SI deber pasar por una revisión y/o actualización de forma periódica
Organización de la SI	Interna	Compromiso de la jefatura	Los altos directivos deben comprometerse con apoyar las medidas propuestas por las políticas de SI
		Coordinación	Se debe efectuar coordinaciones con las áreas que sean pertinentes a fin de cumplir completamente lo planteado en las políticas de SI
		Confidencialidad	Se debe regular la confidencialidad de la información sobre la no divulgación.
	Externa	Interacción con clientes	Se debe evaluar todos los aspectos de seguridad en caso de proporcionar acceso a la información a los usuarios
Gestión de los activos	Responsabilidad	Inventario	Los activos deben correctamente inventariados.
		Uso aceptable	Se debe regular la forma de uso de los activos
	Clasificación	Lineamientos	Se debe clasificar la información en base a aspectos legales y confidencialidad
		Etiquetado y manipulación	Se debe establecer procedimiento de etiquetado de activos y la forma de manejarlos de acuerdo a su clasificación
Gestión de incidencias	Reportes	Eventos	Los eventos relacionados con la SI deben ser registrados y reportados
		Debilidades	Se debe solicitar a los empleados y terceros informar sobre alguna debilidad u observación sobre la SI
	Gestión de incidentes y mejoras	Responsabilidad	Se deben definir y otorgar responsabilidades y procedimientos para asegurar una rápida respuesta y de forma efectiva
		Aprendizaje	Se debe crear procedimientos para cuantificar y hacer monitoreos de los incidentes y su impacto

4.10. Implementación de medidas de seguridad

Luego la divulgación y/o difusión de las políticas de seguridad de la información, se procedió con definir los controles que sirvieron como mecanismo de tratamiento de riesgos, y son los que se muestran a continuación.

Tabla 12: Medidas de seguridad

NRI		Control			Estrategia
Id Riesgo	Nivel	Categoría	Id control	Descripción	
R1	5	Muy alto	**C1**	Adquisición de un generador para el edificio Adquisición de UPS por piso	Evitar el riesgo

Id Riesgo	Nivel	Categoría	Id Control	Descripción	Estrategia
R2	2	Bajo	**C2**	Contar con equipos firewall, proxy Contar con antivirus	Evitar el riesgo
R3	2	Bajo	**C3**	Elaboración de un plan de mantenimiento de los activos de información de tipo físico	Evitar el riesgo
R4	3	Medio	**C4**	Planear capacitaciones especializadas. Programar charlas informativas	Evitar el riesgo
R5	3	Medio	**C5**	Contar con licencias actualizadas Crear un servidor de actualizaciones tipo WSUS	Evitar el riesgo
R6	3	Medio	**C6**	Elaborar procedimiento de asignación de soles de acceso en base a perfiles evaluados de acuerdo a las funciones desempeñadas.	Evitar el riesgo
R7	3	Medio	**C7**	Inventario de equipos actualizado Gestionar adquisición de componentes	Evitar el riesgo
R8	2	Bajo	**C8**	Contar con licencias actualizadas Crear un servidor de actualizaciones tipo WSUS	Evitar el riesgo
R9	3	Medio	**C9**	Elaborar un plan de mantenimiento preventivo y correctivo	Evitar el riesgo
R10	5	Muy alto	**C10**	Adquirir una línea backup de acceso a internet. Controlar la vida útil de los equipos de comunicación	Evitar el riesgo
R11	3	Medio	**C11**	Elaborar una política y procedimiento, formatos para documentar de forma técnicas los equipos	Evitar el riesgo
R12	4	Alto	**C12**	Adquirir servidor o equipo firewall	Evitar el riesgo
R13	4	Alto	**C13**	Elaboración de documentos para la asignación de roles.	Evitar el riesgo
R14	3	Medio	**C14**	Definir políticas de claves de acceso y difundir a todos los empleados	Evitar el riesgo
R15	4	Alto	**C15**	Definir controles de auditoría, políticas y procedimientos	Evitar el riesgo
R16	3	Medio	**C16**	Gestionar adecuación del ambiento de almacenamiento de archivos físicos Elaborar plan de digitalización	Evitar el riesgo
R17	3	Medio	**C17**	Mantenimiento preventivo Seguimiento permanente	Evitar el riesgo
R18	3	Medio	**C18**	Control y verificación de espacio de almacenamiento en servidores Políticas de respuesta en caso de fallas	Evitar el riesgo

R19	4	Alto	**C19**	Elaborar un registro de control de copias de seguridad.	Evitar el riesgo
R20	5	Muy alto	**C20**	Elaborar procedimiento de segregación de funciones para la atención de servicios	Evitar el riesgo
R21	3	Medio	**C21**	Elaborar un plan de capacitación al personal de Ti	Evitar el riesgo
R22	4	Alto	**C22**	Capacitaciones de funciones entre todo el personal de TI, para suplir falencias	Evitar el riesgo
R23	4	Alto	**C23**	Desarrollar mecanismos de control de trazabilidad de acciones sobre el sistema	Evitar el riesgo
R24	3	Medio	**C24**	Capacitaciones permanentes sobre el uso de equipos y software	Evitar el riesgo
R25	5	Muy alto	**C25**	Adquisición de un sistema alterno cd conexión	Evitar el riesgo
R26	5	Muy alto	**C26**	Adquisición generadora eléctrico y UPS para todo el edificio	Evitar el riesgo
R27	3	Medio	**C27**	Policía de segregación de funciones y elaboración de bitácora de fallas y soluciones	Evitar el riesgo
R28	4	Alto	**C28**	Mantenimiento de equipos de forma permanente	Evitar el riesgo
R29	3	Medio	**C29**	Política y procedimiento de copias de seguridad.	Evitar el riesgo
R30	3	Medio	**C30**	Políticas y capacitación sobre seguridad de contraseñas a los usuarios	Evitar el riesgo
R31	4	Alto	**C31**	Capacitaciones de forma permanente sobre tecnología	Evitar el riesgo
R32	4	Alto	**C32**	Plan de adquisición de equipos	Evitar el riesgo
R33	3	Medio	**C33**	Plan de mantenimiento de equipos informáticos	Evitar el riesgo
R34	4	Alto	**C34**	Mantener actualizado Implementación del WSUS.	Evitar el riesgo
R35	3	Medio	**C35**	Plan de adecuación de ambientes físicos	Evitar el riesgo
R36	3	Medio	**C36**	Plan de mantenimiento	Evitar el riesgo
R37	4	Alto	**C37**	Plan de adquisición de consumibles	Evitar el riesgo
R38	3	Medio	**C38**	Generador eléctrico y mantenimiento de UPS	Evitar el riesgo

CAPÍTULO V

RESULTADOS

5.1. VARIABLE INDEPENDIENTE: LA NTP/ISO/IEC 17799

➢ PRETEST

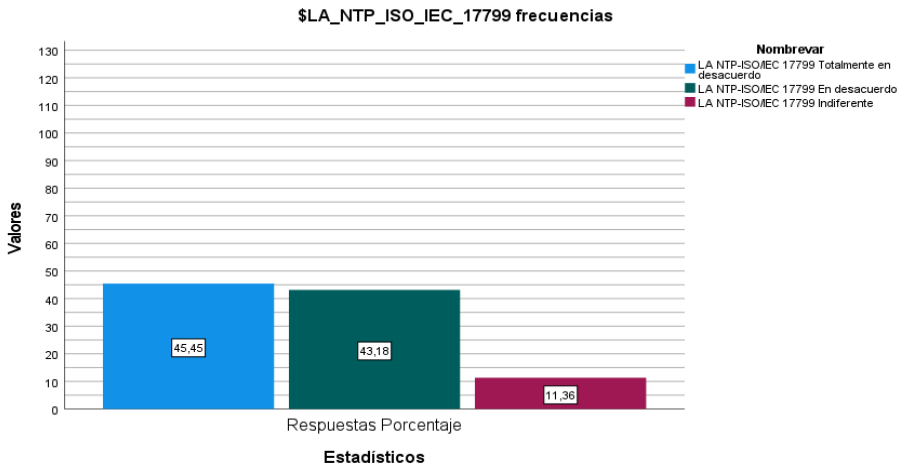
Tabla 13: Análisis de Frecuencia LA NTP/ISO/IEC 17799

Frecuencias				
		Respuestas		Porcentaje de casos
		N	Porcentaje	
LA NTP-ISO/IEC 17799[a]	Totalmente en desacuerdo	40	45,5%	500,0%
	En desacuerdo	38	43,2%	475,0%
	Indiferente	10	11,4%	125,0%
Total		88	100,0%	1100,0%

a. grupo

Fuente: IBM SPSS

Figura 3 : Análisis de Frecuencia LA NTP/ISO/IEC 17799



Interpretación: De acuerdo al análisis realizado se obtiene que, de las 88 respuestas generadas en las 11 preguntas, 40/88 valorado en tasa porcentual equivalente al 45.5% están en indicando una etiqueta de valor <Total Desacuerdo>,

38/88 valorado en tasa porcentual equivalente al 43.2% están en indicando una etiqueta de valor <En Desacuerdo>, 10/88 valorado en tasa porcentual equivalente al 11.4% están en indicando una etiqueta de valor <Indiferente>.

- **POSTEST**

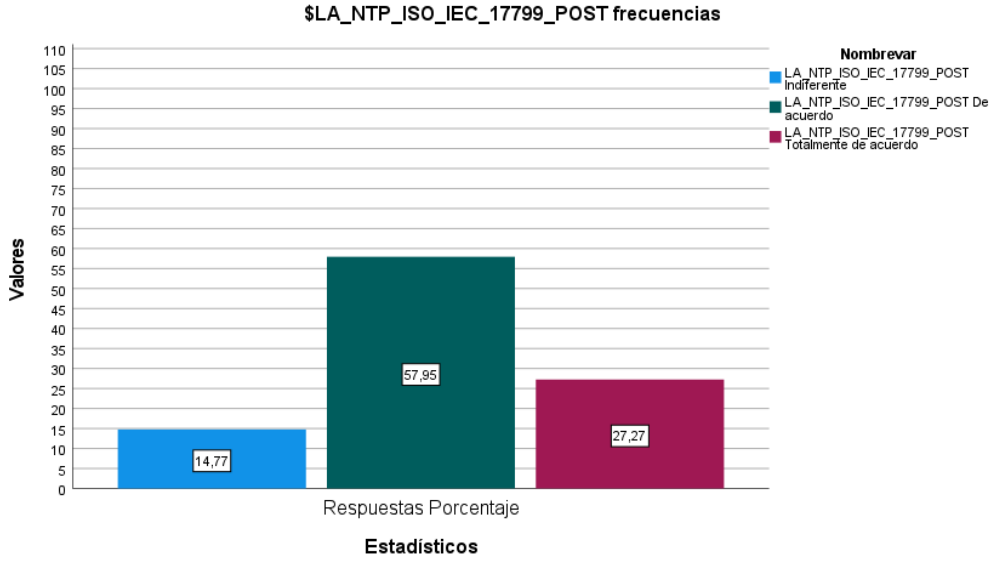
Tabla 14: Análisis de Frecuencia LA NTP/ISO/IEC 17799

LA_NTP_ISO_IEC_17799_POST frecuencias				
		Respuestas		Porcentaje de casos
		N	Porcentaje	
LA_NTP_ISO_IEC_17799_POST[a]	Indiferente	13	14,8%	162,5%
	De acuerdo	51	58,0%	637,5%
	Totalmente de acuerdo	24	27,3%	300,0%
Total		88	100,0%	1100,0%

a. Grupo

Fuente: IBM SPSS

Figura 4 : Análisis de Frecuencia LA NTP/ISO/IEC 17799



Interpretación: De acuerdo al análisis realizado se obtiene que, de las 88 respuestas generadas en las 11 preguntas, 13/88 valorado en tasa porcentual equivalente al 14.8% están en indicando una etiqueta de valor <Indiferente>, 51/88 valorado en tasa porcentual equivalente al 58.0% están en indicando una etiqueta de valor <De acuerdo>, 24/88 valorado en tasa porcentual equivalente al 27.3% están en indicando una etiqueta de valor <Totalmente de Acuerdo>.

5.2. VARIABLE DEPENDIENTE: ADMINISTRACIÓN DE RIESGOS DE TI

- **PRETEST**

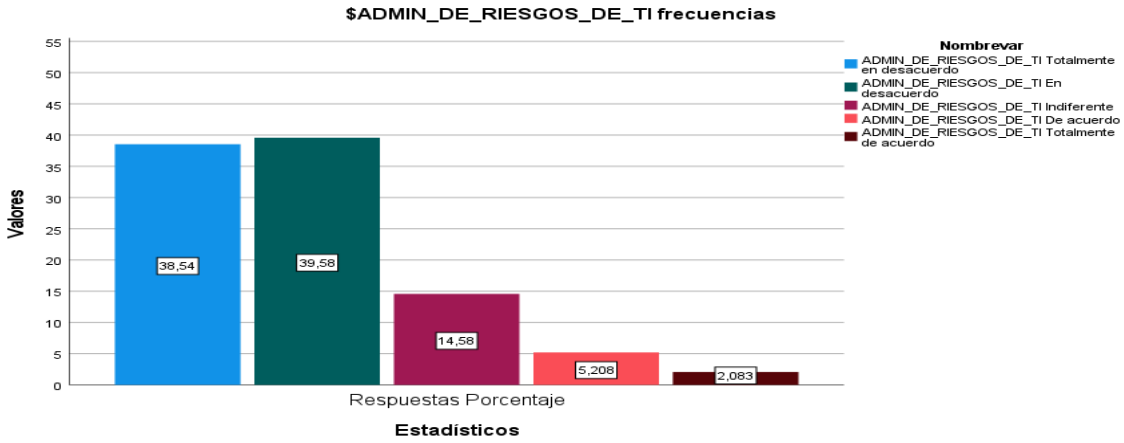
Tabla 15: Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI

ADMIN_DE_RIESGOS_DE_TI frecuencias				
		Respuestas		Porcentaje de casos
		N	Porcentaje	
ADMIN_DE_RIESGOS_DE_TI[a]	Totalmente en desacuerdo	37	38,5%	462,5%
	En desacuerdo	38	39,6%	475,0%
	Indiferente	14	14,6%	175,0%
	De acuerdo	5	5,2%	62,5%
	Totalmente de acuerdo	2	2,1%	25,0%
Total		96	100,0%	1200,0%

a. Grupo

Fuente: IBM SPSS

Figura 5 : Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI PRETEST



Interpretación: De acuerdo al análisis realizado se obtiene que, de las 96 respuestas generadas en las 12 preguntas, 37/96 valorado en tasa porcentual equivalente al 38.5% están en indicando una etiqueta de valor <Total Desacuerdo>, 38/96 valorado en tasa porcentual equivalente al 39.6% están en indicando una etiqueta de valor <En Desacuerdo>, 14/96 valorado en tasa porcentual equivalente al 14.6% están en indicando una etiqueta de valor <Indiferente> y 2/96 valorado en tasa porcentual equivalente al 2.1% están en indicando una etiqueta de valor <Totalmente de acuerdo>.

POSTEST

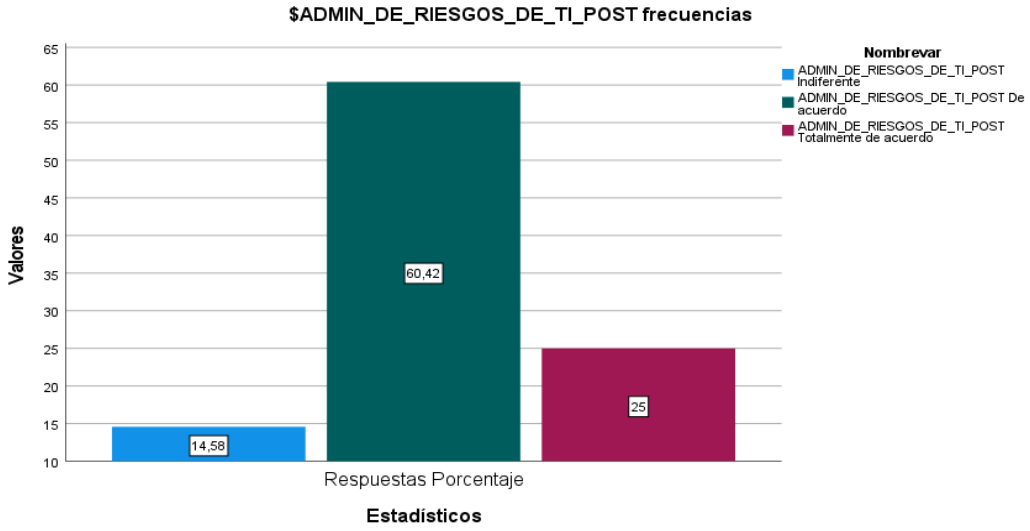
Tabla 16: Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI

ADMIN_DE_RIESGOS_DE_TI_POST Frecuencias				
		Respuestas		Porcentaje de casos
		N	Porcentaje	
ADMIN_DE_RIESGOS_DE_TI_POST[a]	Indiferente	14	14,6%	175,0%
	De acuerdo	58	60,4%	725,0%
	Totalmente de acuerdo	24	25,0%	300,0%
Total		96	100,0%	1200,0%

a. Grupo

Fuente: IBM SPSS

Figura 6 : Análisis de Frecuencia ADMINISTRACIÓN DE RIESGOS DE TI POSTEST



Fuente: IBM SPSS

Interpretación: De acuerdo al análisis realizado se obtiene que, de las 96 respuestas generadas en las 12 preguntas, 14/96 valorado en tasa porcentual equivalente al 14.6% están en indicando una etiqueta de valor <Indiferente>, 58/96 valorado en tasa porcentual equivalente al 60.4% están en indicando una etiqueta de valor <De acuerdo>, 24/96 valorado en tasa porcentual equivalente al 25.0% están en indicando una etiqueta de valor <Totalmente de acuerdo>.

5.3. PRUEBA E HIPÓTESIS GENERAL

Paso 1: Planteamiento de la Hipótesis General

Hipótesis nula ($\boldsymbol{H0}$) = La Implementación de la NTP-ISO/IEC 17799 no mejora la administración de riesgos de TI de la empresa TELPERU SAC

Hipótesis alterna ($\boldsymbol{H1}$) = La Implementación de la NTP-ISO/IEC 17799 si mejora la administración de riesgos de TI de la empresa TELPERU SAC

Paso 2: Especificar el nivel de significancia y muestra

Nivel de significancia (α) = 5% (0.05)

Nivel de confiabilidad (1-α) = 95% (0.95)

Muestra (n) = 8

Paso 3: Prueba de Normalidad

Tabla 17: Prueba de Normalidad

Pruebas de normalidad			
	Shapiro-Wilk		
	Estadístico	gl	Sig.
D_PRE_POSTEST	.941	8	.620

Fuente: Elaboración Propia

Interpretación: p(Sig.) = Usando las diferencias se observa en ambas pruebas que p > 0.05, por lo tanto, los datos de la muestra proceden de una distribución normal.

Paso 4: Criterio de Decisión

Para el cálculo de la función de prueba, se ha empleado el programa estadístico SPSS, insertando los valores promedios de los resultados del cuestionario aplicado:

Si, p(valor) >= 0.05, aceptamos la hipótesis H0 y rechazamos la H1

Si, p(valor) < 0.05, rechazamos la hipótesis H0 y aceptamos la H1

Paso 05: Toma de decisiones:

Tabla 18: Prueba de muestras relacionadas Hipótesis General

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	POSTEST - PRETEST	2,30525	,52216	,18461	1,86872	2,74179	12,487	7	,000

Fuente: Elaboración Propia

Interpretación: Como p(valor) = 0.000 < 0.005, se rechaza la H0 y se acepta la H1, por lo que luego de aplicar cálculos estadísticos, se determina que: La Implementación de la NTP-ISO/IEC 17799 si mejora la administración de riesgos de TI de la empresa TELPERU SAC.

CAPÍTULO VI

DISCUSIÓN DE RESULTADOS

Melano (2019). Que define la ESTRATEGIA PARA IMPLEMENTAR UN SGSI. Con las siguientes conclusiones: El objetivo de este trabajo de grado era identificar una estrategia para la implementación de un Sistema de Gestión de Seguridad de la Información para el área de TI, después de haber elegido las herramientas que permitieron realizar la evaluación del estado actual, los datos permitieron identificara la mejor estrategia paso a paso con el fin de alcanzar con los objetivos de la misma. La implementación de la estrategia y monitoreo constante asignadas a cada uno de los integrantes, permitieron identificar los riesgos, así mismo tratarlos y realizar las acciones de corrección con el fin de lograr las mejoras continuas y así proteger la información.

Guevara (2019). Que trata sobre la NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA. Se concluyo en: La ISO 27001 está orientado al procedimiento de seguridad de la información a través la gestión de riesgos, describe la forma de mantener y mejorar la seguridad de la información, para asi garantizar y mejorar la seguridad de la información en el Departamento de Sistemas de la Cooperativa, se diseñó un SGSI, en donde los activos se encuentran desprotegidos, se ha definido controles para protegerlos, al contar con un SGSI no significa contar con seguridad máxima, sino que la empresa cumple con los requerimientos y las mejores prácticas.

A su vez la presente investigación afirma de acuerdo al análisis realizado en los encuestados, como p(valor) = 0.000 < 0.005, se rechaza la H0 y se acepta la

H1, por lo que luego de aplicar cálculos estadísticos, se determina que: La Implementación de la NTP-ISO/IEC 17799 si mejora la administración de riesgos de TI de la empresa TELPERU SAC; también se afirma de acuerdo al análisis de las diferencias de medias realizado en los encuestados, la Identificación y clasificación de activos de TI mejora en una tasa porcentual del 39.76 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC; La Identificación de las amenazas y vulnerabilidades de los activos de TI mejora en una tasa porcentual de 18.64 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC; La valoración del Impacto y probabilidad de ocurrencia de amenazas mejora en una tasa porcentual de 5.097 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC; La implementación de medidas de seguridad y estrategias mejora en una tasa porcentual de 15.19 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC.

CONCLUSIONES

- Se afirma de acuerdo al análisis realizado en los encuestados, como p(valor) = 0.000 < 0.005, se rechaza la H0 y se acepta la H1, por lo que luego de aplicar cálculos estadísticos, se determina que: La Implementación de la NTP-ISO/IEC 17799 si mejora la administración de riesgos de TI de la empresa TELPERU SAC.
- Se afirma de acuerdo al análisis de las diferencias de medias realizado en los encuestados, la Identificación y clasificación de activos de TI mejora en una tasa porcentual del 39.76 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC.
- Se afirma de acuerdo al análisis de las diferencias de medias realizado en los encuestados, La Identificación de las amenazas y vulnerabilidades de los activos de TI mejora en una tasa porcentual de 18.64 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC.
- Se afirma de acuerdo al análisis de las diferencias de medias realizado en los encuestados, La valoración del Impacto y probabilidad de ocurrencia de amenazas mejora en una tasa porcentual de 5.097 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC.
- Se afirma de acuerdo al análisis de las diferencias de medias realizado en los encuestados, La implementación de medidas de seguridad y estrategias mejora en una tasa porcentual de 15.19 % con referente a la administración de riesgos de TI de la empresa TELPERU SAC.

RECOMENDACIONES

- Realizar capacitaciones y charlas permanentes con todo el personal sobre la seguridad de la información, explicando los controles, políticas, procedimientos, recursos etc.
- Programar evaluaciones sobre el nivel de cumplimiento de implementación de controles que tengan que ver con adquisición de recursos o servicios desde terceros.
- Realizar de forma frecuente la evaluación de los controles implementados para así determinar posibles cambio y ajustes a la gestión de la seguridad de la información.

REFERENCIAS BIBLIOGRÁFICAS

Alteryx. (20 de 12 de 2023). *Alteryx*. Obtenido de https://www.alteryx.com/glossary/business-intelligence

Barrantes. (2008). *Investigacion Cientifica.*

Bhat, A. (21 de 12 de 2023). *Questionpro*. Obtenido de https://www.questionpro.com/blog/business-intelligence/

Bismart. (25 de 12 de 2023). *Bismart*. Obtenido de https://blog.bismart.com/que-es-business-intelligence

Casey, K. (21 de 04 de 2021). *Enterprisersproject*. Obtenido de https://enterprisersproject.com/article/2021/4/how-explain-business-intelligence-bi-plain-english

Chavarría, B. (2021). *Implementación de un modelo de Business Intelligence para mejorar el proceso de toma de decisiones en el área de Trade marketing de la marca Puma, Lima, 2019 .* Lima: Ucss.

Chicoma Gutarra, M. A. (2018). *Implementacion de la ISO 17799 en la Seguridad de Informacion de la empresa Nuevo Mundo.* Lima: UCV.

Cisco. (24 de 01 de 2024). Obtenido de https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

Coursera. (23 de 11 de 2023). Obtenido de https://www.coursera.org/mx/articles/management

Díaz, L. (2021). *Business intelligence y su incidencia en la toma de decisiones en el área comercial en la empresa corporación Canelie sac, Lima - Perú.* Lima: Upn.

Donayre Uchuya, E. A. (2017). *Auditoria de Si y el alineamiento con politicas de seguridad del Hospital San Juan Bautista.* Huacho: UNJFSC.

Esan. (04 de 04 de 2016). Obtenido de https://www.esan.edu.pe/conexion-esan/norma-tecnica-peruana-politicas-procedimientos-seguridad-informacion#:~:text=La%20NTP%2DISO%2017799%20es,de%20su%20tama%C3%B1o%20o%20sector.

Geeksforgeeks. (24 de 01 de 2024). Obtenido de https://www.geeksforgeeks.org/what-is-information-security/

Guevara, D. (2019). *NORMA DE SEGURIDAD INFORMÁTICA ISO 27001 PARA MEJORAR LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD DE LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIÓN EN EL DEPARTAMENTO DE SISTEMAS DE LA COOPERATIVA DE AHORRO Y CRÉDITO SAN FRANCISCO LTDA.* Ambato: UTA.

hpe. (s.f.).

Hpe. (15 de 12 de 2023). *Hpe*. Obtenido de https://www.hpe.com/us/en/what-is/business-intelligence-and-analytics.html

López, R. (2017). *Implementación de business intelligence para mejorar la eficiencia de la toma de decisiones en la gestión de proyectos.* Lima: Usil.

Melano, R. (2019). *ESTRATEGIA PARA IMPLEMENTAR UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 EN EL ÁREA DE TI PARA LA EMPRESA MARKET MIX.* BOGOTÁ: UCC.

Microsoft. (24 de 01 de 2024). Obtenido de https://www.microsoft.com/en/security/business/security-101/what-is-information-security-infosec

Montaño, A. (2018). *Metodología de business intelligence para la toma de decisiones efectivas en las empresas pyme.* Mexico: Upucsa.

Oré Crisóstomo, W. R. (2018). *Formulacion de Politicas sobre Seguridad Inf. Basada en la Norma ISO 17799 para la Gestion de Inf.* Chincha: UAI.

Patiño, S. (s.f.).

Pérez, J., & Fernández, M. (2018). *Revisión bibliográfica: Business Intelligence en la toma dedecisiones para la competitividad.* Medellin: Ua.

Pmg-ssi. (15 de 03 de 2015). Obtenido de https://www.pmg-ssi.com/2015/03/ntp-isoiec-17799-norma-tecnica-peruana/

Quiroa, M. (01 de 01 de 2020). Obtenido de https://economipedia.com/definiciones/administracion.html

Tang, D. (10 de 07 de 2023). Obtenido de https://www.orientsoftware.com/blog/types-of-information-security/

Zevallos, M. (2021). *Implementación de business intelligence para la optimización de toma de decisiones en la gerencia de operaciones en una empresa de instalación de sistemas contra incendios.* Lima: Unms.

ANEXOS

Anexo N° 1**:** Matriz de consistencia.

<table>
<tr>
<th>FORMULACIÓN DEL PROBLEMA</th>
<th>OBJETIVOS</th>
<th>HIPÓTESIS</th>
<th>VARIABLES/DIMENSIONES E INDICADORES</th>
<th>METODOLOGÍA DE LA INVESTIGACIÓN</th>
</tr>
<tr>
<td>¿De qué manera la implementación de la NTP-ISO/IEC 17799 mejorará la administración de riesgos de TI de la empresa TELPERU SAC?</td>
<td>Implementar la NTP-ISO/IEC 17799 para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.</td>
<td>La Implementación de la NTP-ISO/IEC 17799 mejora la administración de riesgos de TI de la empresa TELPERU SAC.</td>
<td rowspan="2">
Variable: La NTP-ISO/IEC 17799
<table>
<tr><th>Dimensión</th><th>Indicadores</th><th>Escala</th></tr>
<tr><td>Activos</td><td>• Procesos de TI.
• Activos de información.
• Valoración de activos.</td><td rowspan="4">Muy en desacuerdo
En desacuerdo
Indiferente
De acuerdo
Muy de acuerdo</td></tr>
<tr><td>Exposición</td><td>• Amenazas
• Vulnerabilidades.
• Tolerancia a riesgo.</td></tr>
<tr><td>Valoración</td><td>• Impacto
• Probabilidad de ocurrencia.
• Métricas</td></tr>
<tr><td>Políticas</td><td>• Políticas.
• Medidas y estrategias de seguridad.</td></tr>
</table>
Variable: Administración de riesgos de TI.
<table>
<tr><th>Dimensión</th><th>Indicadores</th><th>Escala</th></tr>
<tr><td>Estructuración de la metodología de análisis y tratamiento de riesgos</td><td>• Efectividad en la definición de los riesgos.
• Nivel de integración del modelo en la gestión de riesgos
• Grado de concientización</td><td rowspan="4">Muy en desacuerdo
En desacuerdo
Indiferente
De acuerdo
Muy de acuerdo</td></tr>
<tr><td>Gobierno de los riesgos de TI</td><td>• Cumplimiento normativo de las variables
• Efectividad en la evaluación de los componentes
• Efectividad del monitoreo de las actividades
• Tiempo de recuperación de incidentes</td></tr>
<tr><td>Análisis y tratamiento de riesgos</td><td>• Nivel de aplicabilidad del proceso implantado
• Efectividad los niveles de riesgos inherentes de TI
• Efectividad de la implantación de controles y seguimiento.</td></tr>
<tr><td>Gobierno de los riesgos de TI</td><td>• Grado de satisfacción por la información resultante
• Grado de satisfacción del modelo para la toma de decisiones</td></tr>
</table>
</td>
<td rowspan="2">
Tipo de investigación: Aplicada
Nivel de investigación: Descriptivo
Población: Empleados que realizan sus labores en el área de TI (8), con diferentes cargos y funciones.
Muestra: Muestreo por conveniencia
Diseño de la investigación: Experimental De Tipo Pre-Experimental
<table>
<tr><th>Fuentes</th><th>Técnicas</th><th>Instrumentos</th></tr>
<tr><td>Primaria</td><td>Encuesta</td><td>Cuestionarios</td></tr>
<tr><td>Secundaria</td><td>Análisis documental</td><td>Resumen de autores.</td></tr>
</table>
</td>
</tr>
<tr>
<td>• ¿De qué forma la identificación y clasificación de activos de TI mejorará la administración de riesgos de TI de la empresa TELPERU SAC?
• ¿Cómo la identificación de las amenazas y vulnerabilidades de los activos de TI mejorará la administración de riesgos de TI de la empresa TELPERU SAC?
• ¿De qué manera la valoración del Impacto y probabilidad de ocurrencia de amenazas mejorará la administración de riesgos de TI de la empresa TELPERU SAC?
• ¿De qué forma la implementación de medidas de seguridad y estrategias mejorará la administración de riesgos de TI de la empresa TELPERU SAC?</td>
<td>1. Identificar y clasificar activos de TI para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.
2. Identificar las amenazas y vulnerabilidades de los activos de TI para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.
3. Efectuar una valoración del Impacto y probabilidad de ocurrencia de amenazas para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.
4. Implementar de medidas de seguridad y estrategias para mejorar la administración de riesgos de TI de la empresa TELPERU SAC.</td>
<td>• La Identificación y clasificación de activos de TI mejoran la administración de riesgos de TI de la empresa TELPERU SAC.
• La Identificación de las amenazas y vulnerabilidades de los activos de TI mejoran la administración de riesgos de TI de la empresa TELPERU SAC.
• La valoración del Impacto y probabilidad de ocurrencia de amenazas mejora la administración de riesgos de TI de la empresa TELPERU SAC.
• La implementación de medidas de seguridad y estrategias mejora la administración de riesgos de TI de la empresa TELPERU SAC.</td>
</tr>
</table>

Anexo N° 2**:** Cuestionario de preguntas para la recolección de datos

CUESTIONARIO DE PREGUNTAS SOBRE LA INVESTIGACIÓN
"LA NTP-ISO/IEC 17799 PARA LA ADMINISTRACIÓN DE RIESGOS DE TI DE LA EMPRESA TELPERU SAC."

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

Tabla N° 1: Reseña de recolección de datos

Descripción	Valor
Totalmente en desacuerdo	1
En desacuerdo	2
Indiferente	3
De acuerdo	4
Totalmente de acuerdo	5

Preguntas:

Variable Independiente

1. ¿Cuál es su apreciación respecto a los procesos de TI evaluados como parte del estudio para la aplicación de la NTP 177999?
2. ¿Cuál es su apreciación respecto a los activos de información identificados como parte del estudio para la aplicación de la NTP 177999?
3. ¿Cuál es su apreciación a la valoración de los activos de información como parte del estudio para la aplicación de la NTP 177999?

4. ¿Cuál es su apreciación respecto a las amenazas a los que pueden estar expuestos los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
5. ¿Cuál es su apreciación respecto a las vulnerabilidades detectadas en los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
6. ¿Cuál es su apreciación respecto a la tolerancia de riesgo por parte de los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
7. ¿Cuál es su apreciación respecto al nivel de impacto del riesgo de los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
8. ¿Cuál es su apreciación respecto a valor probabilísticos de la ocurrencia de los riesgos que podría afectar a los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
9. ¿Cuál es su apreciación respecto a las métricas propuestas para salvaguardar los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
10. ¿Cuál es su apreciación respecto a las políticas propuestas para salvaguardar los activos de información identificados parte del estudio para la aplicación de la NTP 177999?
11. ¿Cuál es su apreciación respecto a las medidas y estrategias de seguridad propuestas para salvaguardar los activos de información identificados parte del estudio para la aplicación de la NTP 177999?

Variable dependiente

12. ¿Cuál es su apreciación respecto la efectividad en la definición de los riesgos en el proceso de administración de riesgos de TI?
13. ¿Cuál es su apreciación respecto al nivel de integración del modelo en gestión de riesgos de TI?
14. ¿Cuál es su apreciación al grado de concientización del personal como parte del proceso de administración de riesgos de TI?
15. ¿Cuál es su apreciación del cumplimiento normativo de las variables como parte del proceso de administración de riesgos de TI?
16. ¿Cuál es su apreciación respecto a la efectividad en la evaluación de los componentes como parte del proceso de administración de riesgos de TI?
17. ¿Cuál es su apreciación respecto a la efectividad del monitoreo de las actividades como parte del proceso de administración de riesgos de TI?
18. ¿Cuál es su apreciación respecto al tiempo de recuperación de incidentes como parte del proceso de administración de riesgos de TI?
19. ¿Cuál es su apreciación respecto al nivel de aplicabilidad del proceso implantado como parte del proceso de administración de riesgos de TI?
20. ¿Cuál es su apreciación respecto a la efectividad los niveles de riesgos inherentes de TI como parte del proceso de administración de riesgos de TI?
21. ¿Cuál es su apreciación respecto a la efectividad de la implantación de controles y seguimiento como parte del proceso de administración de riesgos de TI?
22. ¿Cuál es su apreciación respecto al grado de satisfacción por la información resultante como parte del proceso de administración de riesgos de TI?

23. ¿Cuál es su apreciación respecto al grado de satisfacción del modelo para la toma de decisiones como parte del proceso de administración de riesgos de TI?

Anexo N° 3**:** Validación de Fiabilidad Alpha Cronbach

Tabla N° 2: Análisis de Fiabilidad – La NTP-ISO/IEC 17799

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,789	11

Fuente: Elaboración Propia

Tasa Porcentual: 78.9% de Fiabilidad, con etiqueta de valor <Alta Correlación>

Tabla N° 3: Análisis de Fiabilidad – Administración de riesgos de TI

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,861	12

Fuente: Elaboración Propia

Tasa Porcentual: 86.1% de Fiabilidad, con etiqueta de valor <Muy Alta Correlación >

Tabla N° 4: Coeficiente de Correlación

Coeficiente de Correlación	**Interpretación**
0	Nula Correlación
De 0.01 a 0.19	Muy Baja Correlación
De 0.20 a 0.39	Baja Correlación
De 0.40 a 0.59	Moderada Correlación
De 0.60 a 0.79	Alta Correlación
De 0.80 a 0.99	Muy Alta Correlación
1	Perfecta Correlación

Fuente: Introducción conceptual al análisis multivariable. Un enfoque informático con los paquetes SPSS[2]

[2] BISQUERRA Alzina, R.; (1989). "Introducción conceptual al análisis multivariable. Un enfoque informático con los paquetes SPSS-X, BMDP", LISREL y SPAD. Barcelona: PPU.

Tabla N° 5: Comparación del resultado de la aplicación del cuestionario, pre y post test

N°	MEDIA HIPO 1 PRE	%	MEDIA HIPO 1 POS	%	x̄ % (Abs)	MEDIA HIPO 2 PRE	%	MEDIA HIPO 2 POS	%	x̄ % (Abs)	MEDIA HIPO 3 PRE	%	MEDIA HIPO 3 POS	%	x̄ % (Abs)	MEDIA HIPO 4 PRE	%	MEDIA HIPO 4 POS	%	x̄ % (Abs)
1	2.3333	20.59%	4.0000	12.00%	8.59%	2.3333	15.56%	4.0000	12.90%	2.65%	1.6667	12.50%	4.3333	12.62%	0.121%	2.3333	15.56%	4.6667	14.29%	1.27%
2	1.6667	14.71%	4.0000	12.00%	2.71%	2.0000	13.33%	4.0000	12.90%	0.43%	1.6667	12.50%	4.3333	12.62%	0.121%	2.0000	13.33%	4.3333	13.27%	0.07%
3	2.3333	20.59%	4.0000	12.00%	8.59%	2.3333	15.56%	3.3333	10.75%	4.80%	1.6667	12.50%	4.0000	11.65%	0.850%	2.3333	15.56%	3.6667	11.22%	4.33%
4	1.0000	8.82%	4.3333	13.00%	4.18%	1.6667	11.11%	3.0000	9.68%	1.43%	1.6667	12.50%	4.6667	13.59%	1.092%	1.6667	11.11%	3.0000	9.18%	1.93%
5	1.0000	8.82%	4.0000	12.00%	3.18%	1.6667	11.11%	4.6667	15.05%	3.94%	1.6667	12.50%	4.6667	13.59%	1.092%	1.6667	11.11%	4.3333	13.27%	2.15%
6	1.0000	8.82%	4.6667	14.00%	5.18%	1.6667	11.11%	4.0000	12.90%	1.79%	1.6667	12.50%	4.0000	11.65%	0.850%	1.6667	11.11%	4.6667	14.29%	3.17%
7	1.0000	8.82%	4.0000	12.00%	3.18%	1.6667	11.11%	4.0000	12.90%	1.79%	1.6667	12.50%	4.0000	11.65%	0.850%	1.6667	11.11%	4.0000	12.24%	1.13%
8	1.0000	8.82%	4.3333	13.00%	4.18%	1.6667	11.11%	4.0000	12.90%	1.79%	1.6667	12.50%	4.3333	12.62%	0.121%	1.6667	11.11%	4.0000	12.24%	1.13%
Total	11.3333	100.00%	33.3333	100.00%	39.76%	15.0000	100.00%	31.0000	100.00%	18.64%	13.3333	100.00%	34.3333	100.00%	5.097%	15.0000	100.00%	32.6667	100%	15.19%

Fuente: Elaboración Propia