UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE UNA SOLUCIÓN DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE UCAYALI CONTAMANA

Tesis para optar el título profesional de

INGENIERO DE SISTEMAS

JOEL, MELÉNDEZ HIDALGO

LINDER, SANDI RENGIFO

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° 07-2025

GRADUANDO : SANDI RENGIFO, Linder
MELENDEZ HIDALGO, Joel

TEMA : ***"IMPLEMENTACIÓN DE UNA SOLUCIÓN DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE UCAYALI CONTAMANA"***

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 : 16 / 30

CONCLUSIONES:
APROBADO POR : **MAYORIA**
DESAPROBADO POR :

JURADO EVALUADOR

Dr. NILTON CESAR AYRA APAC
PRESIDENTE

MG. ARTURO YUPANQUI VILLANUEVA
MIEMBRO

M.Sc. Richard Piero BARDALES LINARES
MIEMBRO

M.SC. CLOTILDE RÍOS HIDALGO DE CERNA
SECRETARIA ACADÉMICA

PUCALLPA, 30 DE ENERO DEL 2025

UNIVERSIDAD NACIONAL DE UCAYALI

FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

COMISIÓN DE GRADOS Y TÍTULOS

TESIS TITULADA : "IMPLEMENTACIÓN DE UNA SOLUCIÓN DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE UCAYALI CONTAMANA"

ELABORADA POR : Bach. JOEL MELÉNDEZ HIDALGO
Bach. LINDER SANDI RENGIFO.

APROBADA POR :

DR. NILTON CÉSAR AYRA APAC
PRESIDENTE

MG. ARTURO YUPANQUI VILLANUEVA
MIEMBRO

M.SC. 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/0250-2024**.

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

"IMPLEMENTACIÓN DE UNA SOLUCIÓN DE TI PARA PARA LA SEGURIDAD,DE,LA,INFORMACIÓN DE LA MUNICIPALIDAD,PROVINCIAL,DE UCAYALI CONTAMANA."

Autor(es)	:	**MELÉNDEZ HIDALGO, JOEL**
		SANDI RENGIFO, LINDER
Facultad	:	**INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL**
Escuela	:	**ING. DE SISTEMAS**
Asesor(a)	:	**M.Sc. PANDURO PADILLA, EUCLIDES**

Presenta un **porcentaje de similitud de 2%,** 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: 28/05/2024

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, JOEL MELENDEZ HIDALGO

Autor de la tesis titulada : IMPLEMENTACION DE UNA SOLUCION DE TI PARA LA SEGURIDAD DE LA INFORMACION DE LA MUNICIPALIDAD PROVINCIAL DE UCAYALI CONTAMANA

Sustentada el año: 2025

Asesor(a): MG. EUCLIDES PANDURO PADILLA

Facultad: FISEIC

Escuela Profesional: INGENIERIA DE SISTEMAS

Autorizo la publicación:

PARCIAL [ ] TOTAL [X]

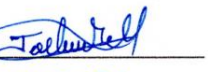
De mi trabajo de investigación en el Repositorio Institucional de la Universidad Nacional de Ucayali (www.repositorio.unu.edu.pe), bajo los siguientes términos:

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: 15 / 09 / 2025

Email: ING.MELENDEZ14@GMAIL.COM Firma: 

Teléfono: 938680624 DNI: 46947899

UNIVERSIDAD NACIONAL DE UCAYALI

DIRECCIÓN DE PRODUCCIÓN INTELECTUAL

AUTORIZACIÓN DE PUBLICACIÓN

Repositorio de la Universidad Nacional de Ucayali

Yo, LINDER SANDI RENGIFO

Autor de la tesis titulada: "IMPLEMENTACIÓN DE UNA SOLUCIÓN DE TI PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE UCAYALI CONTAMANA"

Sustentada el año: 2025

Asesor(a): MG. EUCLIDES PANDURO PADILLA

Facultad: FISEIC

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: 15 / 09 / 2025

Email: sandilsr20@gmail.com Firma:

Teléfono: 945473402 DNI: 70224408

DEDICATORIA

A Dios, por guiarnos con sabiduría, fortaleza y esperanza en cada etapa de este camino académico. Su presencia constante nos dio la serenidad y la motivación necesarias para superar los desafíos y alcanzar esta meta.

A nuestros padres y familias, por su amor incondicional, comprensión y apoyo permanente. Gracias por creer en nosotros, por alentarnos a seguir adelante y por ser fuente de inspiración en cada paso de nuestra formación.

A nuestros docentes y mentores, quienes con su ejemplo nos inculcaron el valor del conocimiento, la disciplina y la ética profesional.

Finalmente, a todos aquellos que confían en que la tecnología puede ser una herramienta poderosa para mejorar las instituciones públicas y contribuir al desarrollo de nuestra región.

AGRADECIMIENTO

Expresamos nuestro más sincero y profundo agradecimiento a Dios, por concedernos la salud, la constancia y la sabiduría necesarias para culminar satisfactoriamente esta investigación.

A la Municipalidad Provincial de Ucayali – Contamana, por brindarnos las facilidades y el espacio institucional para el desarrollo de esta investigación, el cual busca aportar a la mejora de la seguridad de la información y a la gestión tecnológica de la entidad.

A nuestro asesor(a) de tesis, por su orientación académica, sus observaciones oportunas y su dedicación durante el proceso investigativo, que enriquecieron significativamente la calidad de este estudio.

Y, de manera especial, a nuestras familias, por su comprensión, aliento y confianza en nosotros, elementos indispensables que hicieron posible la culminación de esta meta.

RESUMEN

En esta investigación se tratan temas referidos a procesos de evaluación de forma integrar de los recursos de Tecnología de la Información en la Municipalidad Provincial de Ucayali Contamana, este estudio tiene su origen tomando como base la oficina de Informática y Estadística, posteriormente se amplía la evaluación a las demás partes de la organización que cuentan con TI, para luego efectuar una análisis detallado, diseñar un planteamiento adecuado e implementar una solución de TI con el fin de lograr una mejora. Asimismo, el estudio realizado y la solución de TI implementada cumple con las exigencias de una investigación científica, a partir de la definición de la situación problemática, definición de objetivos, hipótesis, el uso de un instrumento de recopilación de información para luego proceder con su evaluación y cumplir con la etapa de contratación de hipótesis, entre otras actividades, y determinar el logro obtenido

Palabras claves: TI, Recursos, Servicios.

ABSTRACT

This research deals with issues related to evaluation processes in an integrated way of Information Technology resources in the Municipality Provincial of Ucayali Contamana, this study has its origin based on the office of Informatics and Statistics, then the evaluation is extended to other parts of the organization that have IT, and then perform a detailed analysis, design an appropriate approach and implement an IT solution in order to achieve an improvement. Likewise, the study conducted and the IT solution implemented complies with the requirements of a scientific research, starting with the definition of the problematic situation, definition of objectives, hypotheses, the use of an information gathering instrument to then proceed with its evaluation and comply with the hypothesis contracting stage, among other activities, and determine the achievement obtained.

Keywords: IT, Resources, Services.

ÍNDICE GENERAL

DEDICATORIA vii

AGRADECIMIENTO viii

RESUMEN ix

ABSTRACT x

INDICE GENERAL xi

ÍNDICE DE TABLAS xv

ÍNDICE DE FIGURAS xvi

INTRODUCCIÓN xvii

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA 18

1.1. Antecedentes del problema 18

1.2. Formulación del problema 19

1.2.1. Problema General 19

1.2.2. Problemas Específicos 20

1.3. Objetivos 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 22

1.4.3. Limitaciones 22

1.5. Hipótesis y/o sistemas de hipótesis 22

1.5.1. Hipótesis General 22

1.5.2. Hipótesis específicas 23

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 24
1.7. Variables 24
1.7.1. Variable independiente 24
1.7.2. Variable dependiente 24
1.7.3. Variable interviniente 24
1.8. Sistema de variables, dimensiones e indicadores 24
1.8.1. Operacionalización de variables 24
CAPÍTULO II: MARCO TEÓRICO 26
2.1. Antecedentes de la investigación 26
2.1.1. Antecedentes internacionales 26
2.1.2. Antecedentes nacionales 32
2.2. Bases teóricas 37
2.3. Definición de términos básicos 45
CAPÍTULO III: METODOLOGÍA DE LA INVESTIGACIÓN 47
3.1. Metodología y técnicas utilizadas 47
3.1.1. Tipo de investigación 47
3.1.2. Nivel de investigación 47
3.1.3. Método de investigación 47
3.1.4. Diseño de la investigación 47
3.2. Población y muestra 48
3.3. Instrumentos de recolección de datos 48
3.4. Procedimiento de recolección de datos 48

3.5. Tratamiento de datos 49

3.6. Grado de confiabilidad de los datos 49

CAPÍTULO IV: SOLUCIÓN 50

4.1. La Municipalidad Provincial de Ucayali – Contamana 50

4.2. Diagnostico situacional 50

4.2.1. Diagnóstico de Data Center 51

4.2.2. Diagnóstico de Servidores 53

4.2.3. Diagnóstico Aplicaciones SIAF, SIGA 57

4.2.4. Diagnóstico de Dominio y Alojamiento 58

4.2.5. Diagnóstico de la Red LAN y Recursos 60

4.2.6. Diagnóstico del Sistema de Video Vigilancia 62

4.3. Soluciones y/o mejoras 63

4.3.1. De Data Center 63

4.3.2. De servidores 64

4.3.3. SIAF, SIGA 64

4.3.4. Dominio y Alojamiento 65

4.3.5. Sistema de Video Vigilancia 65

4.4. Implementación de soluciones 65

4.4.1. Instalación y configuración de software monitor de servidor 66

4.4.2. Instalación y configuración de Antivirus 68

4.4.3. Servidor para SIAF y SIGA 69

4.4.4. Video de cámara vigilancia 72

4.4.5. Procedimiento de seguridad 75

CAPÍTULO V: RESULTADOS 80

5.1. Resultados de la investigación Pre-Test 80

5.2. Resultados de la investigación Post-Test 100

5.3. Prueba de hipótesis 119

5.3.1. Prueba de Normalidad 119

5.3.2. Establecer nivel de significancia 121

5.3.3. Prueba de Hipótesis General 122

5.3.4. Prueba de Hipótesis Específicas 123

CONCLUSIONES 129

RECOMENDACIONES 131

REFERENCIAS BIBLIOGRÁFICAS 132

ANEXOS 136

Anexo 1: Evaluación de confiabilidad del instrumento 137

Anexo 2: Matriz de consistencia 140

Anexo 3: Cuestionario de preguntas para la recolección de datos 141

Anexo 4: Validación de los instrumentos por expertos 141

ÍNDICE DE TABLAS

Tabla N° 1: Operacionalización de variable I 24

Tabla N° 2: Operacionalización de variable II 25

Tabla N° 3: Características técnicas del servidor 54

ÍNDICE DE FIGURAS

Figura 1: Switch Data Center 51

Figura 2: Gabinete de comunicaciones 52

Figura 3: Gabinete de comunicaciones – oficinas 53

Figura 4: Servidores 56

Figura 5: Aires acondicionados 56

Figura 6: Sistema de envío/recepción SIAF 57

Figura 7: Servidor de aplicaciones 58

Figura 8: Portal WEB de la MPU 59

Figura 9: Switch 326-24G 61

Figura 10: Receptor emisor de internet 61

Figura 11: Torre receptora / emisora de internet de 50 megas 62

Figura 12: Cableado de red desordenado 62

Figura 13: Propuesta de Data Center 64

Figura 14: Grabadores de video 72

Figura 15: Gabinete de grabación 73

Figura 16: Plano de ubicación de cámara 1er nivel 73

Figura 17: Plano de ubicación de cámara 2do nivel 74

Figura 18: Cámaras de video vigilancia de la MPU 74

Figura 19: Pantalla central de video 75

INTRODUCCIÓN

Esta Investigación fue realizado en la Municipalidad Provincial de Ucayali Contamana, la cual cuenta con procesos propios de sus funciones, distribuido en áreas, entre las que se encuentra la Oficina de Informática y Estadística, cuya función principal es la gestión de recursos y servicios de TI, ya sea de carácter interno o externo.

Se realizó, posterior a un análisis detallado, la implementación de soluciones de carácter de TI, así como presentación de propuestas relacionadas a la presente investigación, pero que por motivos presupuestales y de tiempo no fue posible su implementación.

Esta investigación, cumple con los capítulos solicitados por las directivas de la Oficina de Grados y Titulo de la Facultad de Ingeniería de sistemas e ingeniería civil, capítulos que a continuación se resumen:

Capítulo I: Donde se presenta información de la Realidad problemática, los Objetivos general y específicos, Operacionalización de las Variables de investigación.

Capitulo II: Donde se detallas información del Marco teórico, antecedentes relacionados a la investigación, bases teóricas y definición de términos básicos.

Capitulo III: Donde se detalla información de la Metodológica de investigación utilizada de la investigación, tales como el método de investigación, tipo - nivel y diseño de la investigación.

Capitulo IV: Se detalla la implementación de la solución.

Capitulo V: Se presentan información de los Resultados obtenidos de la investigación, las Conclusiones y Recomendaciones;

En la última sección se presentan las referencias bibliográficas y los anexos.

CAPÍTULO I

PLANTEAMIENTO DEL PROBLEMA

1.1. Antecedentes del problema

Según Geneva (2021). El Índice Mundial de Innovación 2021 muestra que los gobiernos y las empresas de todo el mundo han aumentado su inversión en innovación frente a las enormes pérdidas económicas y humanas causadas por la pandemia de COVID-19. Esto refleja la creciente afirmación de la importancia de las nuevas iniciativas para superar la pandemia y de esta forma garantizar el crecimiento de la economía.

Según Esteban (2025), la tecnología es un sector de alto crecimiento debido al factor innovación que comentábamos unas líneas más arriba. Una empresa tecnológica que no destine recursos a innovación pronto puede verse obsoleta.

Según lacamara (2022), el Perú es uno de los países donde las organizaciones invierten más en tecnologías de la información: el tercero en Latinoamérica con un 9%, según el informe "Internet de las Cosas: La tecnología como aliada de la sostenibilidad. como aliada de la sostenibilidad" de EAE Business School, Perú ocupa el tercer lugar en Latinoamérica con un 9%.

Según larepublica (2022), en la respecta a la inversión pública, el informe, denominado Prospección del Mercado de Tecnologías de la Información (TI), prevé que entre 2020 y 2024, a pesar de la crisis económica, la inversión en el sector alcanzará los 3.355 millones de dólares. Perú también está considerado líder mundial en la creación de un mejor ambiente para las microfinanzas, lo que presumiría una oportunidad para la sección de las TIC.

Municipalidad Provincial de Ucayali Contamana, como entidad pública, en su rol de entidad pública, ha invertido en TI, pero esta inversión es progresiva, a demanda

y sin un criterio integrador, y eso se puede notar claramente en las quejas del personal que hace uso de los recursos y servicios de TI, debido a ello se determinó realizar un trabajo de indagación para determinar cuáles son las quejas más resaltantes que se vienen presentando, relacionados a TI, quejas que se presentan a continuación: malestar por el tiempo de atención de los servicio de TI, quejas por la paralización de los servicios, quejas por no contar con las facilidades de atender información de seguridad cuando se requería, quejas por la falta de seguridad de los recursos de TI, malestar por la el servicio de red e internet, entre otros.

Luego de recabar las quejas presentadas se prosiguió con la determinación de los factores causante logrando encontrar los siguiente: Equipos con recursos de hardware insuficientes, carencia de equipos de seguridad de ambientes, personal y equipos, demora en la atención de servicios por carencia de recursos de TI adecuados, demora por la atención de requerimiento a nivel de la red LAN e internet, falta de equipos de ventilación, carencia de manuales y procedimiento de servicios y gestión de TI.

Tal como se detalló, a nivel de TI, la Municipalidad Provincial de Ucayali Contamana, cuenta con una situación problemática, que debe ser atendida de forma inmediata, ya que de permanecer estas condiciones peligra la integridad de la información.

1.2. Formulación del problema

1.2.1. Problema General

- ¿De qué manera análisis el diseño e implementación de una solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali - Contamana?

1.2.2. Problemas Específicos

- ¿De qué manera el análisis actual de los servicios y recursos de TI mejora la seguridad de la información correspondiente Municipalidad Provincial de Ucayali - Contamana?
- ¿Cuál es el diseño de los recursos y servicios de TI que mejoran la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana?
- ¿La implementación de recursos y servicios de TI mejoran la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana?
- ¿La evaluación de la conformidad de las implementaciones efectuadas mejoran la seguridad de la información de la Municipalidad Provincial de Ucayali - Contamana?

1.3. Objetivos

1.3.1. Objetivo General

- Analizar, diseñar e implementar una solución de TI para mejorar la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

1.3.2. Objetivos Específicos

- Realizar el análisis actual de los servicios y recursos de TI para mejorar la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.
- Diseñar los recursos y servicios de TI para mejorar la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.

- Implementar los recursos - servicios de TI para mejorar la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.
- Evaluar la conformidad de las implementaciones efectuadas para determinar la mejora de la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.

1.4. Justificación, importancia y limitaciones

1.4.1. Justificación

Justificación teórica

Para mantener protegida la información, tres son los pilares que cumplen con este propósito a saber: integridad, confidencialidad y disponibilidad, razón por lo cual esta investigación busca implementar aplicando una solución de TI, para reducir los riesgos de pérdida de información, mal uso de ella, uso adecuado de los equipos informáticos, etc. Mediante la aplicación de esta solución de TI buscamos la identificación de los riesgos y amenazas que pudieran comprometer la integridad de los datos, para establecer medidas de prevención que nos ayuden a reducirlos a nivel aceptable para la Municipalidad.

Justificación práctica

Debido a que la Municipalidad Provincial de Ucayali Contamana no cuenta con sistema de seguridad que proteja su información, de igual manera carece no cuenta con procesos adecuados que se puedan seguir para disminuir los riesgos de la vulnerabilidad de la información, se hace necesario implementar una solución de TI que nos permita reducir estos riesgos para asegurar que nuestros usuarios y clientes de la municipalidad estén seguros con la información proporcionada.

Justificación metodológica.

La presente investigación sigue los lineamientos del proceso de investigación la cual está conformada por la formulación del problema, objetivos e hipótesis, de tal forma que se establezcan los factores que influyen en la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

1.4.2. Importancia

La importancia de esta investigación será de un gran apoyo a los usuarios y clientes de la Municipalidad Provincial de Ucayali Contamana porque nos permitirá reducir los riesgos de perdida, modificación, disponibilidad de la información y además optimizar la información lo cual nos permitirá ahorrar tiempo para nuestros clientes.

1.4.3. Limitaciones

La principal limitación que presentó es la posibilidad que entre el personal encargado existan algunos que se resistan al cambio del uso de las nuevas herramientas tecnológicas y seguir con la práctica de los métodos convencionales.

1.5. Hipótesis y/o sistemas de hipótesis

1.5.1. Hipótesis General

- El análisis, diseño e implementación de una solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

1.5.2. Hipótesis específicas

- El análisis actual de los servicios y recursos de TI mejora la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.
- El diseño de los recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali - Contamana.
- La implementación de recursos y servicios de TI mejora la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.
- La evaluación de la conformidad de las implementaciones efectuadas indica la mejora de la seguridad de la información correspondiente a la Municipalidad Provincial de Ucayali - Contamana.

1.6. Delimitaciones de la investigación

1.6.1. Delimitación Espacial

La delimitación espacial de la presente investigación está centrado a mejorar la seguridad actual de la Municipalidad Provincial de Ucayali Contamana.

1.6.2. Delimitación Social

Esta investigación involucra a usuarios y clientes de la Municipalidad Provincial de Ucayali Contamana que utilizarán el sistema para beneficio de usuarios y clientes de la municipalidad.

1.6.3. Delimitación Temporal

La delimitación temporal de la investigación, como para la implementación, se realizará entre julio del 2023 hasta febrero del 2024.

1.6.4. Delimitación Conceptual

Esta investigación comprende la aplicación de los conceptos de una solución de TI en la Municipalidad Provincial de Ucayali Contamana, con la finalidad de desarrollar el proyecto de manera rápida y sobre todo segura para mejorar la experiencia del usuario y el cliente de nuestra municipalidad que lo manipulará en la gestión de trámites documentales.

1.7. Variables

1.7.1. Variable independiente

Solución de TI.

1.7.2. Variable dependiente

Seguridad de la Información.

1.7.3. Variable interviniente

Municipalidad Provincial de Ucayali Contamana

1.8. Sistema de variables, dimensiones e indicadores

1.8.1. Operacionalización de variables

Variable: Solución de TI

Tabla 1

Operacionalización de variable

Dimensión	Indicador	Escala
Análisis	Servicios de TI Actuales	
	Recursos de TI actuales.	
	Personal de TI.	Malo
Diseño	Servicios de TI propuestos.	Regular
	Recursos de TI propuestos.	Normal
	Recursos de TI implementados y proyectados.	Bueno
Implementación		Muy bueno
	Servicios de TI implementados y proyectados.	

Conformidad	Áreas atendidas. % de conformidad de los servicios TI implementados y proyectados. % de conformidad de los recursos de TI implementados y proyectados.

Fuente: Elaboración propia.

Variable: Seguridad de la Información.

Tabla 2

Operacionalización de variable II

Dimensión	Indicador	Escala
Confidencialidad	Controles generales.	Malo
	Autorizaciones.	Regular
Integridad	Controles de seguridad en comunicaciones.	Normal
	Controles de seguridad en procedimientos.	Bueno
Disponibilidad	Tiempo de acceso a los servicios o recursos.	Muy bueno

Fuente: Elaboración propia.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

De acuerdo con la tesis de Suarez (2021)**,** SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA NORMA ISO/IEC 27001:2015 - EN LA EMPRESA MAGDANIEL LTDA. EN EL DISTRITO ESPECIAL, TURÍSTICO Y CULTURAL DE RIOHACHA, con los objetivos: Analizar el SGSI de Magdaniel Ltda, ubicada en la Zona Especial Turística y Cultural de Riohacha, según la norma ISO/IEC 27001:2015. Definir la política de seguridad de la información de Magdaniel Ltda de acuerdo con la norma ISO/IEC 27001:2015. Magdaniel Ltda define su entorno de seguridad física y de información de acuerdo con la norma ISO/IEC 27001:2015. Identificación de activos de información de acuerdo con ISO/IEC 27001:2015 Magdaniel Ltda. Propuesta de orientación estratégica para el SGSI de Magdaniel Ltda basado en ISO7/IEC 27001:2015, ubicado en la zona especial turística y cultural de Riohacha. Las conclusiones son las siguientes: Las siguientes conclusiones se extraen de una comparación de los resultados y el marco teórico del estudio, que se basa en una síntesis de las consideraciones más importantes que surgen del análisis. Datos que sustentan las premisas propuestas y argumentos para alcanzar los objetivos que guían este trabajo. Según el primer objetivo específico, se determina una estrategia de seguridad. Es evidente que las actividades relacionadas con la consecución del objetivo se llevan a cabo dentro de la empresa, brindando así las garantías necesarias para la seguridad y gestión de la información de los empleados. logrando la protección y recursos

proporcionados por la dirección de la empresa. Asimismo, se reconoce la importancia de los roles y responsabilidades asignadas en el procesamiento de la información utilizando los recursos proporcionados por el entorno, definidos en los niveles operativos y de gestión. Así, la reacción de los empleados de Magdaniel tiene en cuenta la importancia de un sistema de seguridad que ayude a minimizar cualquier tipo de riesgo, especialmente la seguridad de la información, protegiendo así el contenido de la base de datos. organizativo. Por lo tanto, la perspectiva de cada empleado les permite determinar la importancia de las políticas de seguridad de la información mientras se esfuerzan por mantener en los niveles adecuados la confidencialidad de los datos, integridad de la información y disponibilidad de la misma en un grado significativo. En cuanto al segundo objetivo específico, a saber, la determinación de la seguridad física y ambiental, es evidente que la empresa carece de sistemas de gestión y protección de la investigación financiera para evaluar los riesgos sobre los activos de la empresa, a pesar de que en ocasiones está vinculado a ellos; Existían procedimientos apropiados, pero también había deficiencias en la definición de áreas de seguridad y falta de conocimiento sobre los procesos de seguridad de la información. Así, teniendo en cuenta el punto de vista del empleado, la evaluación de riesgos de una empresa impulsa en ocasiones a examinar los peligros que dañan los activos de la organización, así como al establecimiento de medidas y controles para determinar opciones de tratamiento, realizando diagnósticos, garantizando la seguridad del proceso. Respecto al tercer objetivo específico, es decir, la identificación de los activos de información, la empresa cuenta con procesos para describir la propiedad de los activos existentes, lo que se ve facilitado por la evaluación realizada por la

gestión de recursos, en la que se analizan todos los aspectos relacionados con la información. El sistema participa en la realización de análisis de actividad durante el proceso. Por lo tanto, según los empleados, los inventarios de activos realizados internamente cumplen con las expectativas necesarias para llevar a cabo medidas adecuadas para proteger elementos importantes de la organización, principalmente la información, siempre y cuando dichos procesos les permitan pasar por procesos técnicos. lo que conduce a la toma de decisiones en el entorno para identificar riesgos. Al mismo tiempo, debido a la importancia de la seguridad y la gestión continua, trate de identificar que en ocasiones no se siguen procedimientos para comprender y manejar los activos de la empresa.

De acuerdo con la tesis de Molano (2020), 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. Con los objetivos: Determinar las mejores estrategias para que las empresas del portafolio del mercado implementen sistemas de gestión de seguridad de la información basados en las normas ISO 27001 en el sector TI. Diagnosticar la situación actual de seguridad de la información en el sector TI de la empresa mediante una matriz de estrategia. Estructura del mercado. Aplicar herramientas de evaluación (encuestas, entrevistas) al campo de TI en una muestra preseleccionada para comprender los conceptos o prácticas de gestión de seguridad de la información de la empresa. Determinar el método apropiado para implementar ISO 27001 basándose en evaluaciones de TI previas para comprender las estrategias que se pueden seguir para lograr la seguridad de la información. Compruebe si la estrategia elegida representa una solución adecuada para proteger la

información TI de las empresas de la cartera. Conclusión: El propósito de esta tesis es determinar estrategias para implementar sistemas de gestión de seguridad de la información luego de seleccionar herramientas para evaluar el estado actual de los SGSIs en el sector TI de las empresas del portafolio del mercado. La mejor estrategia debe desarrollarse paso a paso para alcanzar tus objetivos. Aplicar esta estrategia y monitorear constantemente las tareas y responsabilidades asignadas a cada miembro permitirá identificar los riesgos que enfrenta en la organización, así como atacarlos y realizar las correcciones oportunas para asegurar mejoras. Mantener y proteger las comunicaciones para que la empresa no se vea comprometida.

De acuerdo con la tesis de Mora (2022). ANALISIS Y DISEÑO DE UN MODELO PARA ESTABLECER UN SISTEMA DE GESTION DE LA SEGURIDAD DE LA INFORMACION DENTRO DE UN AMBIENTE CLOUD COMPUTING, APLICANDO LA NORMA ISO 27001. EN LA EMPRESA DATA-FIBER, con los objetivos: Desarrollar un modelo para la creación de un procedimiento de gestión de seguridad de información en un entorno de computación en la nube basado en el estándar ISO 270001 para que los clientes de DATA-FIBER puedan acceder a sus datos de manera fácil y segura. - Evaluar el contexto actual de seguridad de datos para identificar los puntos de vulnerabilidad más bajos de DATA-FIBER presentados en nuestro tema. Evaluar y definir indicadores (medidas) cuantitativos como base para el proceso de evaluación de la seguridad de la computación en la nube para los clientes. ISO 270001 define componentes técnicos y de otro tipo para determinar las causas que deben evaluarse en el componente de disponibilidad de datos. Elaborar una propuesta de un SGSI en un entorno de computación en la nube

para que los clientes puedan acceder fácilmente al mismo. La conclusión es que cada vez más organizaciones públicas y privadas eligen los servicios que proporciona la tecnología de computación en la nube. Sin embargo, para utilizar los recursos de manera eficaz, los usuarios involucrados deben estar capacitados y ser conscientes de los beneficios y riesgos que ofrece la tecnología de computación en la nube. Todos los procesos de seguridad en un entorno de computación en la nube deben realizarse conjuntamente entre el proveedor de servicios en la nube y el cliente, ya que esto genera responsabilidad. La pérdida de seguridad e integridad de los datos, así como el control o la disponibilidad de la información, es un problema potencial para las organizaciones que buscan pasar de entornos tradicionales a la computación en la nube, ya que esta última afecta directamente la ejecución. Actividades propias de la organización. En un entorno de computación tradicional o en la nube, los procesos y responsabilidades deben estar claramente definidos, y la confidencialidad, integridad y disponibilidad de la información deben ser una preocupación constante. Tomar medidas preventivas ayudará a las organizaciones a proteger su activo más importante: la información, ya que la pérdida o fuga de información puede paralizar una o más de las operaciones de la empresa, lo que resulta en pérdidas financieras significativas. ISO 27001 brinda a los proveedores la capacidad de controlar los recursos sin filtrar información. Por tanto, la aplicación de la norma ISO 27001:2013 al respecto es bastante factible.

De acuerdo con la tesis de Ramiro (2020) SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DISTRITO 8D01 DE

EDUCACIÓN", con los objetivos: Implementar un sistema de gestión de seguridad de la información según los parámetros de la norma ISO/IEC 27001 para mejorar la seguridad de la información en el Distrito Educativo 18D01. Evaluar los mecanismos actuales de procesamiento de información y control de vulnerabilidades. Desarrollar sistemas de gestión de seguridad de la información basados en los parámetros de la norma ISO/IEC 27001 para reducir la probabilidad y ocurrencia de amenazas. Establecer prácticas de gestión y mejorar continuamente el SGSI para asegurar el adecuado procesamiento de la información. Conclusión: El Distrito Educativo 18D01 actualmente no cuenta con procedimientos relacionados con la seguridad de la información. Varios procesos en ejecución no se ejecutan de acuerdo con la política establecida; El simple uso de ciertas reglas de gestión de la información no es suficiente para garantizar la seguridad de la información. Sin un sistema proactivo para gestionar adecuadamente la información, todas las acciones tomadas por la agencia para asegurarla fueron de naturaleza correctiva, lo que resultó en un desperdicio de recursos del distrito. Es evidente que los activos informáticos no se gestionan adecuadamente y por tanto la información procesada a través de ellos es altamente susceptible a amenazas y vulnerabilidades. En términos de protección física y ambiental, existen algunos procedimientos que se llevan a cabo a través de un diseño de planta centralizado, pero se centran en ciertos aspectos como la ubicación y protección de los equipos, mientras que partes como el mantenimiento de los equipos y el perímetro se ignoran en gran medida. La seguridad física, el control de acceso físico, etc. comprometen la integridad de los equipos y del personal. En lo que respecta a la gestión de comunicaciones y operaciones, esta es la parte de gestión. Debido a diversas restricciones y

configuraciones de seguridad de los sistemas de la organización, los archivos y documentos se mantienen y documentan adecuadamente. El problema es que las redes internas no son seguras y son blancos fáciles de ataques informáticos. Gestión de control de acceso insuficiente. Por un lado, las contraseñas de usuario proporcionadas por el departamento de sistemas no se cambian periódicamente y, por otro lado, no hay forma de comprobar si las contraseñas personales administradas por los mismos funcionarios son lo suficientemente seguras y sólidas para administrar los sistemas de la agencia.

2.1.2. Antecedentes nacionales

De acuerdo con la tesis de Rojas (2021), SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO/IEC27001 PARA MEJORAR LA SEGURIDAD DEL ÁREA DE OPERACIONES Y TECNOLOGÍA DE GLOBAL BPO CENTER ALLUS CHICLAYO, con objetivos: Desarrollé un Sistema de Gestión de Seguridad de la Información (SGSI) basado en el estándar ISO/IEC27001 para mejorar la seguridad en las áreas operativas y técnicas del centro global BPO de Allus Chiclayo. OE1: Diagnóstico del proceso de negocio de seguridad de la información del centro global BPO Allus Chiclayo. SO2: Evaluar los activos de información en las áreas operativas y técnicas a través de encuestas y entrevistas. OE3: Identificar riesgos aplicando el estándar de sistemas de información ISO/IEC27001 del Centro Global BPO Allus Chiclayo para gestionar o eliminar riesgos. OE4: Definir controles de seguridad de la información basados en ISO 27001 para el centro global BPO Allus Chiclayo Operaciones y Tecnología. SO5: Definir políticas, estándares y procedimientos de seguridad para responder la integridad, confidencialidad y la disponibilidad de la información. El uso de

la herramienta Magerit identifica procesos de negocio con los siguientes elementos: activos, amenazas, vulnerabilidades, impactos, riesgos, controles de seguridad, lo que nos permite determinar cómo definir nuestros sistemas de control. Utilizando la norma ISO/IEC 27001 para identificar activos de información, se encontró que un total de 29 (Tabla 1) eran de alto valor en términos de su criticidad, y estos activos se tuvieron en cuenta en el desarrollo del SGSI. La evaluación de riesgos utilizando ISO/IEC 27001 comienza con riesgos de alta criticidad y considera vulnerabilidades y amenazas, que se mitigan mediante planes de tratamiento de riesgos. Se seleccionaron un total de 13 controles de ISO/IEC 207001 para abordar los riesgos más críticos en las áreas operativas y técnicas de los centros de BPO en todo el mundo. La definición y estructura de las políticas, estándares y procedimientos de seguridad requeridos por ISO7IEC 27001 son los siguientes: alcance del SGSI, política y objetivos de seguridad de la información, métodos de evaluación y tratamiento de riesgos, declaración de idoneidad, plan de tratamiento de riesgos, lista de activos, control de acceso. La estrategia, los procedimientos de gestión de incidentes y los procedimientos de continuidad del negocio garantizan la confidencialidad, integridad y disponibilidad de la información.

De acuerdo con la tesis de Cruz (2020), DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ SAC, con los objetivos: Reducir los riesgos a los activos de información de MEDCAM Perú S.A.C. clínica. Implementar un SGSI basado en ISO/IEC 27001, implementar una política de seguridad de la información y establecer controles de

procesamiento de datos. Identificar riesgos según ISO/IEC 27002 y aumentar la conciencia de la empresa sobre los problemas de seguridad de la información. Conclusión: 1. Al identificar, desarrollar e implementar controles dirigidos a los riesgos más críticos, se redujeron los riesgos que enfrentan los activos de información de la clínica. Implementar un SGSI es fundamental para lograr objetivos clave. Esto se logra mediante el desarrollo e implementación de estrategias efectivas de control de acceso a la información, tratando de asegurar la integridad, confidencialidad y disponibilidad de los activos de información, minimizando así los riesgos de seguridad de la información. Desarrollar e implementar una política de seguridad de la información es importante porque demuestra el compromiso del gobierno con la seguridad de la información. Además de asignar roles y responsabilidades, establece pautas para la gestión de la empresa y recomendaciones que los empleados deben seguir en su trabajo diario. Luego de nuestra evaluación, llegamos a la conclusión de que establecer controles diseñados en base a variables como el costo de implementación y la efectividad de la mitigación de riesgos es el enfoque ideal de gestión de riesgos para MEDCAM Perú. Identificar y realizar un análisis costo-beneficio. Es vital aumentar la conciencia de los empleados sobre los problemas de seguridad para que se pueda implementar y posteriormente mejorar un SGSI dentro de la organización. El personal de la clínica ahora comprende que la información con la que trabajan es confidencial y deben garantizar su total integridad. Una mayor conciencia sobre los problemas de seguridad de la información puede fortalecer los sistemas implementados y permitir mejoras continuas. Esto también simplifica la implementación del SGSI.

De acuerdo con la tesis de Méndez (2020), DESARROLLO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN ESTÁNDARES PARA EMPRESA DE SEGUROS CASO DE ESTUDIO: EMPRESA DE SEGUROS, con los siguientes objetivos: Desplegar un plan de SI de las compañías de seguros basado en estándares internacionales que incremente la disponibilidad, integridad, confidencialidad de la información de las compañías de seguros. Valorar el estado actual de los estándares de la SI. Identificar amenazas y vulnerabilidades en áreas del sistema. Para beneficio de las compañías de seguros, los planes de seguridad de la información se desarrollan de acuerdo con los estándares internacionales en el campo de las tecnologías de la información. Conclusión: Se valoró la situación actual de la SI de las compañías de seguros de acuerdo con las exigencias de la norma ISO27001:2013, se identificaron las deficiencias existentes, se determinó el nivel actual de seguridad y se propusieron medidas de control para mejorar el nivel de seguridad de la información. Debido a la presencia de una serie de violaciones a la política de seguridad de la información actual, la empresa ha propuesto amenazas y vulnerabilidades a la seguridad de la información que pueden generar riesgos de seguridad de la información y requerir una gestión adecuada de la información. La implementación de los controles especificados en el Anexo A de la norma de seguridad de la información ISO 27001:2013 contribuye significativamente a la protección de los activos de una empresa. El programa de seguridad de la información se desarrolla de acuerdo con la norma ISO 27001:2013, la cual permite a una empresa implementar los controles especificados en el Anexo A priorizando sus necesidades para eliminar y/o reducir las amenazas y vulnerabilidades que enfrenta.

De acuerdo con la tesis de Porras (2019), SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA LA GESTIÓN DE RIESGOS EN ACTIVOS DE INFORMACIÓN, con objetivos: Establecer el impacto de la ejecución de un SGSI en la gestión de riesgos de activos de información en el contact center Digitex de Lima BPO. Establecer el impacto de la ejecución de un SGSI en los controles administrativos de seguridad en Digitex Contact Center, empresa BPO de Lima. Determinar el impacto de la ejecución de un SGSI en los controles lógicos de seguridad del Contact Center Digitex de Lima BPO. Determinar el impacto de la culminación de un SGSI en los controles de seguridad física del Contact Center Digitex, empresa BPO de Lima. Conclusión: Los objetivos identificados en el estudio se lograron al determinar que la ejecución de un sistema de gestión de seguridad tiene un impacto significativo en la gestión de riesgos de los activos de información de Lima BPO Contac Center Digitex. Al considerar el aumento significativo en los valores previos y posteriores a la prueba, finalmente se identificó la hipótesis de que "la ejecución de un sistema de gestión de seguridad tiene implicaciones para la gestión de riesgos de los activos de información del centro de contacto de una empresa de BPO". Se acepta Digitex de Lima y se rechaza la hipótesis nula. Para futuros estudios sería útil ampliar la muestra poblacional para poder analizar nuevos resultados y compararlos con los obtenidos en el estudio. También es posible combinar métodos para analizar si hay algún cambio en los resultados. Se concluyó que el trabajo de investigación logró resultados positivos, indicando que los métodos y recomendaciones fundamentados teóricamente son confiables y pueden ser aplicados en futuras investigaciones. Finalmente se puede concluir que con base en los resultados obtenidos se puede determinar que el valor

promedio de la gestión de riesgos en los activos de información aumentó de 3.65 a 5.22, es decir, aumentó su nivel de madurez, alcanzando el estatus de determinar/administrar. SGSI con activos de información Relación clara entre gestión de riesgos.

2.2. Bases teóricas

2.2.1. Solución de TI

De acuerdo con Bigelow (2023). Una solución de tecnología de la información (TI) es un conjunto de programas de software y/o servicios relacionados que se venden como un solo paquete. Los vendedores de TI, los proveedores de servicios y los revendedores de valor añadido (VAR) agrupan sus paquetes de software y servicios y los venden bajo la etiqueta de "solución" para promover la idea de que la compra del producto ayudará al cliente a resolver con éxito un problema o manejar una situación compleja. Muchos vendedores, especialmente los desarrolladores de software, se refieren a todos sus productos como soluciones de software. Por ejemplo, un vendedor puede referirse a su software antivirus como una solución porque ayuda a resolver un problema concreto. Sin embargo, en un sentido más estricto, una solución informática es un conjunto de productos y servicios, no un producto único e independiente. Por lo tanto, el software antivirus debe ir acompañado de productos relacionados, como filtros antispam o servicios de copia de seguridad, para que se le pueda llamar solución. La distinción entre productos y soluciones se remonta a los años 70, cuando los VAR estaban en auge. En aquella época, el auge de los microordenadores hizo que la informática saliera de la casa de cristal y entrara en otros sectores, como la fabricación y la ingeniería. En respuesta, los VAR agruparon paquetes de software propios o de terceros con

plataformas de hardware específicas y los vendieron como soluciones llave en mano diseñadas para casos de uso específicos. Estas soluciones de hardware y software suelen dirigirse a clientes de nichos de mercado verticales.

Tipo de soluciones de TI

De acuerdo con Servicenow (2023). Tecnología de la información (TI) es un término extremadamente amplio que engloba prácticamente todas las tecnologías digitales relevantes para el desarrollo de la actividad empresarial. Del mismo modo, las soluciones de TI son amplias e inclusivas, y consisten en una variedad de software diseñado para satisfacer necesidades específicas. Dicho esto, la mayoría de las soluciones informáticas entran en al menos una de las siguientes categorías:

Telecomunicaciones

Según Otgroup (2022). Las empresas modernas atienden ahora a un público mundial gracias a las ilimitadas opciones de comunicación que ofrece Internet. Al mismo tiempo, la pandemia de COVID-19 ha obligado a muchas organizaciones a recurrir al teletrabajo. En ambos casos, la necesidad de una tecnología de telecomunicaciones fiable es crítica. Las soluciones de TI pueden ayudar a las empresas a gestionar eficazmente los servicios de telecomunicaciones tanto dentro como fuera de la organización, incluyendo videoconferencia, correo electrónico, SMS, VoIP, Voz sobre Protocolo de Internet (VoiP), chatbots, e incluso redes sociales. Las soluciones de TI también se pueden utilizar para crear soluciones de comunicación a medida.

Soporte Técnico

Según (Moreno, 2023). Como forma fundamental de solución informática, el soporte técnico está diseñado para garantizar que las

organizaciones tengan acceso a asesoramiento experto y opciones fiables en caso de problemas técnicos. El soporte técnico puede prestarse a través de un departamento de TI interno o de una empresa externa de externalización de TI. A menudo, los proveedores de tecnología ofrecen sus propias opciones de soporte técnico, lo que permite a los usuarios ponerse en contacto con el Centro de Soporte y enviar un ticket para obtener una solución rápida a cualquier problema que puedan estar experimentando.

Seguridad en la Red

Según Oviedo (2010). El creciente uso de la tecnología ha abierto nuevas vías para atender a los clientes y mejorar la eficiencia y productividad de las empresas. Por desgracia, esta dependencia de la tecnología también ha creado un nuevo peligro, la amenaza de la ciberdelincuencia. Los ataques digitales son un peligro relativamente nuevo y en evolución para las empresas de todos los sectores. Las soluciones informáticas diseñadas para proteger a las organizaciones de diversas amenazas son una inversión necesaria, tanto para proteger los datos confidenciales como para crear un entorno seguro y productivo para los empleados.

Gestión de Redes e Infraestructuras

Según Internationalit (2022). En lugar de construir un sistema mezcolanza de redes y dispositivos de uno en uno, las organizaciones pueden recurrir a la contratación y gestión de infraestructuras de TI. Las empresas de contratación de redes e infraestructuras de TI ofrecen los servicios necesarios de gestión y mantenimiento del hardware, el software y la conectividad asociados, y reúnen una solución completa que, de otro modo, proporcionarían proveedores de servicios de TI independientes.

Computación en Nube

Según Cisco (2023). La computación en nube permite a las organizaciones externalizar y acceder a recursos informáticos a través de Internet. Estos recursos pueden incluir análisis, almacenamiento de datos, servidores, software e inteligencia. Hay tres tipos de modelos de servicios basados en la nube: La infraestructura de tipo como servicio (IaaS), o plataforma como servicio (PaaS) y por último software como servicio (SaaS). La computación en nube suele ofrecerse en un modelo de "pago por uso", lo que permite a los clientes escalar eficientemente al tiempo que mantienen un estricto control de sus presupuestos.

Administración de Infraestructura de TI.

Según Indeed (2023). Esta solución informática consiste en planificar, adquirir, instalar y gestionar la infraestructura informática de una empresa. El objetivo principal de una empresa que utiliza esta solución es garantizar la flexibilidad, fiabilidad y seguridad de los sistemas que son críticos para el éxito de sus operaciones. La infraestructura de TI consta de dos componentes principales:

Hardware. Incluye dispositivos como ordenadores de sobremesa y portátiles, así como la red formada por servidores, routers y otros dispositivos relacionados. Las instalaciones de la empresa o el espacio que proporciona también entran en este apartado.

Software. Esta parte suele incluir servidores web y sistemas operativos. También incluye sistemas de software como la planificación de recursos empresariales (ERP), la gestión de relaciones con los clientes (CRM) y los sistemas de gestión de contenidos (CMS).

Según Careerexplorer (2023). La infraestructura de TI puede ser tradicional o estar basada en la nube. La infraestructura tradicional se refiere a los componentes de software y hardware que una empresa o usuario suele utilizar in situ. Una infraestructura en nube, en cambio, consta de componentes similares a los que pueden acceder los usuarios finales o los clientes a través de Internet. Esto se consigue mediante la virtualización, que permite disponer de recursos informáticos sin necesidad de instalar los componentes necesarios in situ. Como la infraestructura informática consta de numerosos elementos, los proveedores de servicios suelen ofrecer soluciones separadas, cada una de ellas centrada en áreas específicas, entre ellas:

Administración de Bases de Datos. Supervisar las bases de datos de los clientes para minimizar el riesgo de fallos que puedan afectar al negocio, mantener las bases de datos y proporcionar soporte técnico.

Adquisición de TI. Identificar, abastecer y adquirir el producto o servicio informático ideal para satisfacer las necesidades del cliente.

Gestión de redes: Gestiona, opera y mantiene la red informática de un cliente, a menudo con la ayuda de un sistema de gestión de redes.

Gestión de la Seguridad. Proteger las operaciones informáticas y los activos digitales de los clientes supervisando su infraestructura informática, garantizando el cumplimiento de las políticas de seguridad e implantando y actualizando las tecnologías pertinentes.

Gestión de Servidores. Mantiene los servidores de los clientes, eliminando o minimizando el tiempo de inactividad y las ralentizaciones, garantizando un rendimiento óptimo y gestionando los componentes de hardware y software del servidor.

Soluciones de Virtualización. Ayuda a los clientes con todos los tipos de virtualización, incluida la virtualización de aplicaciones, escritorios, redes, servidores y almacenamiento.

2.2.2. Seguridad de la Información

Según Imperva (2023). La Seguridad de la Información (a veces llamada InfoSec) abarca las herramientas y procesos que utilizan las empresas para proteger la información. Incluye la configuración de políticas que impiden a personas no autorizadas acceder a información empresarial o personal. La seguridad de la información es un campo en crecimiento y evolución, que abarca una amplia gama de áreas, desde la seguridad de redes e infraestructuras hasta las pruebas y auditorías. La seguridad de la información protege la información sensible de actividades no autorizadas, incluidas la inspección, modificación, grabación y cualquier interferencia o destrucción. El objetivo es garantizar la seguridad y privacidad de datos críticos como información sobre cuentas de clientes, datos financieros o propiedad intelectual. Las consecuencias de un incidente de seguridad incluyen el robo de información privada, la manipulación de datos y su eliminación. Los ataques pueden interrumpir el flujo de trabajo y dañar la reputación de una empresa, además de acarrear costes tangibles. Las organizaciones deben asignar fondos a la seguridad y asegurarse de que están preparadas para detectar, responder y prevenir proactivamente ataques como el phishing, el malware, los virus, los intrusos malintencionados y el ransomware.

Principios de la Seguridad de la Información.

Según Unir (2023). Los principios fundamentales de la seguridad de la información son disponibilidad, la confidencialidad e integridad. Cada uno de los elementos de un sistema de seguridad de la información debe de aplicar

desde uno o varios de estos elementos. Juntos, estos principios se conocen como los tres principios CIA.

Confidencialidad

Son medidas que están diseñadas para impedir la divulgación no acreditada de información. El objetivo es mantener la privacidad de la información del personal y garantizar que sólo la vean y accedan a ella quienes la posean o la necesiten para desempeñar funciones organizativas.

Integridad

La coherencia consiste en impedir cambios no autorizados (adiciones, supresiones, manipulaciones, etc.) en los datos. El principio de integridad garantiza que los datos son exactos y fiables y no pueden ser alterados de forma incorrecta, ni de forma accidental, ni de forma malintencionada.

Disponibilidad

La disponibilidad es la capacidad de un sistema de protección para que los sistemas informáticos y los datos estén totalmente disponibles cuando los usuarios los necesiten (o en un momento determinado). El objetivo de la disponibilidad es que la infraestructura técnica, las aplicaciones y los datos estén disponibles cuando los necesiten los procesos organizativos o los clientes de la organización.

¿Qué son los activos de información?

Según Sumologic (2023). Casi todas las organizaciones tienen información que no desean compartir ni hacer pública. Tanto si estos datos se conservan en formato digital como físico, la gestión de la seguridad de la información es esencial para protegerla de accesos no autorizados o robos

Considere si su organización tiene y desea proteger los siguientes tipos de activos de información:

Documentos Estratégicos. Las empresas y organizaciones de TI desarrollan y documentan objetivos estratégicos a largo plazo y objetivos tácticos a corto plazo para definir sus metas y su visión de futuro. Estos valiosos documentos internos contienen secretos y conocimientos que los competidores podrían desear obtener.

Información sobre Productos y Servicios. La información crítica sobre productos y servicios, incluidos los proporcionados por la empresa y las TI, debe protegerse mediante la gestión de la seguridad de la información. Esto incluye el código fuente de las aplicaciones desarrolladas internamente, así como cualquier producto de datos o información vendido a los clientes. Si su empresa vende productos digitales, necesitará seguridad de la información para garantizar que los piratas informáticos no puedan robar sus productos y distribuirlos sin su consentimiento o conocimiento.

Propiedad Intelectual/Patentes. Si su empresa genera propiedad intelectual, incluido software de desarrollo, puede necesitar controles de seguridad de la información para protegerla. Sus competidores pueden querer robarle el código fuente y utilizarlo para aplicar ingeniería inversa a sus productos y competir con los suyos. En algunos países no se aplican las leyes sobre derechos de autor o propiedad intelectual, por lo que es posible que no tenga ningún recurso si esto ocurre.

Conocimientos Patentados/Secretos Comerciales. todas las organizaciones generan conocimientos patentados en el transcurso de su actividad empresarial. En el caso de las organizaciones de TI, estos conocimientos pueden almacenarse

en depósitos de conocimientos internos a los que pueden acceder los operadores de TI y el personal de apoyo. Los secretos comerciales son conocimientos únicos que proporcionan a una organización una ventaja competitiva. Si no está dispuesto a compartir públicamente esta información con sus competidores, debe utilizar controles de gestión de la seguridad de la información para proteger los secretos comerciales y los conocimientos patentados.

Documentación del proyecto en curso. La documentación del proyecto en curso incluye los detalles de la documentación del producto o servicio que se está lanzando. Si sus competidores se enteran de lo que está haciendo, pueden intentar lanzar productos o funciones competidoras más rápido de lo previsto, e incluso pueden establecer puntos de referencia con su nuevo producto para expulsarle del mercado.

Datos de los empleados. Recursos Humanos recopila y conserva datos sobre los empleados, incluyendo evaluaciones de rendimiento, historial laboral, nóminas y otra información. Estos registros pueden contener información confidencial que los ciber atacantes podrían utilizar para chantajear a sus empleados. Las organizaciones rivales pueden utilizar estos datos para identificar objetivos antes de intentar hacerse con sus empleados.

2.3. Definición de términos básicos

- **Solución de TI**

De acuerdo con Gartner (2023). “Una solución es la implementación de personas, procesos, información y tecnología en un sistema único para apoyar un conjunto de capacidades empresariales o técnicas para resolver uno o más problemas empresariales”.

- **Seguridad de TI.**

  De acuerdo con Crowdstrike (2021). “La seguridad informática es el término genérico utilizado para describir el conjunto de políticas, métodos, soluciones y herramientas empleadas para proteger la confidencialidad, integridad y disponibilidad de los datos y activos digitales de una organización.”

- **Tecnología de la Información.**

  Según Mitchell (2020). “Los términos "tecnología de la información" e "informática" están muy extendidos en el ámbito empresarial e informático. La gente utiliza estos términos de forma genérica para referirse a diversas actividades relacionadas con la informática, confundiendo a veces su significado.”

CAPÍTULO III

METODOLOGÍA DE LA INVESTIGACIÓN

3.1. Metodología y técnicas utilizadas

3.1.1. Tipo de investigación

La investigación es del tipo aplicada, los investigadores de este campo tratan de encontrar soluciones inmediatas a los problemas a los que se enfrenta la sociedad o una organización industrial o empresarial. El enfoque es mucho más útil, ya que se esfuerza por encontrar información que influya directamente en la práctica.

3.1.2. Nivel de investigación

El nivel será del tipo descriptivo**,** se refiere al tipo de pregunta de investigación, diseño y análisis de datos que se aplicará a un tema determinado. La estadística descriptiva cuenta lo que es.

3.1.3. Método de investigación

El método será Deductivo – Inductivo que de acuerdo a Robles (s.f.) el método deductivo trabaja desde lo general hacia lo específico. Debido a eso se comienza pensando en las teorías sobre el tema una solución de TI, y luego se reducen a las hipótesis que se quieren probar.

El método de investigación también es inductivo porque la información recolectada de los cuestionarios se va a procesar y analizar en tablas estadísticas (Hernández, Fernández, y Baptista, 2014).

3.1.4. Diseño de la investigación

La investigación es experimental de tipo preexperimental, se manipulará la variable independiente y determinar su efecto sobre sobre la variable

dependiente, se utilizará un grupo experimental al cual se realizará a una prueba de pre test y post test.

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

Población

La población lo conforman los empleados que laboran en las oficinas de la Municipalidad Provincial de Ucayali Contamana, que se encuentran estrechamente relaciono con el uso de Tecnologías de la información, siendo un total de 120 empleados.

Muestra

La muestra se determinó de forma no probabilística, se optó la elección por conveniencia; por lo cual, se utilizará el total de la población, en este caso los 120 empleados.

3.3. Instrumentos de recolección de datos

Se utilizó el cuestionario que es un instrumento de investigación consistente en una serie de preguntas diseñadas para recabar información de los encuestados. Un cuestionario puede considerarse una entrevista escrita. Los cuestionarios pueden administrarse cara a cara, por teléfono, por ordenador o por correo.

3.4. Procedimiento de recolección de datos

Las técnicas de recogida de datos son un conjunto variado de herramientas que permiten recopilar información de forma hábil y eficaz para la investigación y el

análisis. En la presente investigación los datos de recolección serán a través de la aplicación del cuestionado aplicándolo a la muestra.

3.5. Tratamiento de datos

Una vez obtenidos los datos, hay que procesarlos para darles sentido. El tratamiento de la información depende de los requisitos, el tipo de datos recogidos, el tiempo disponible para procesar los datos y muchos otros factores. Se trata de uno de los componentes más críticos del proceso de investigación y en para ellos nos agenciaremos del software estadístico denominado SPSS.

3.6. Grado de confiabilidad de los datos

El alfa de Cronbach es una medida de la coherencia interna, es decir, del grado de relación entre un conjunto de ítems como grupo. Se considera una medida de fiabilidad de la escala. Un valor "alto" de alfa no implica que la medida sea unidimensional. Si, además de medir la consistencia interna, se desea aportar pruebas de que la escala en cuestión es unidimensional, se pueden realizar análisis adicionales (Oarc, 2023).

CAPÍTULO IV

SOLUCIÓN

4.1. La Municipalidad Provincial de Ucayali – Contamana

Misión

La Municipalidad Provincial de Ucayali, es el órgano de Gobierno Local que representa y gestiona los intereses de los vecinos en la jurisdicción, promueve una firme gobernabilidad democrática, asegurando la mayor participación ciudadana en la formulación de las políticas locales, impulsando al máximo sus capacidades administrativas para brindar bienes y servicios de calidad y convertirse en una provincia competitiva y económicamente sostenible, para mejorar la calidad de vida de la población (Muniucayali, 2024)

Visión

Mejorar la calidad de vida de la población en general, con inversión dirigida a impulsar la agricultura y el turismo, cómo ejes principales, para generar el acceso homogéneo a los servicios de educación y salud con calidad.

La provincia Ucayali tendrá un desarrollo sustentable basada en el sector turismo, resaltando las costumbres e identidad que caracteriza a nuestras comunidades, y en el sector agricultura la definición de las líneas de producción y la tecnificación para un mejor aprovechamiento en la producción de la tierra, mediante una gestión municipal democrática, transparente y eficiente, con plena participación ciudadana, equidad de género e igualdad de oportunidades. (Muniucayali, 2024).

4.2. Diagnostico situacional

En ese punto, se procederá a diagnosticar la situación actual de TI de la municipalidad como son: Diagnóstico del Data Center, Diagnóstico de los Servidores, Diagnóstico de aplicaciones principales (SIAF, SIGA), Diagnóstico del dominio y

alojamiento WEB, Diagnóstico de la Red LAN y los recursos, Diagnóstico del Sistema de Video vigilancia.

La elección de los recursos fue en coordinación con el Área de TI de la municipalidad, se seleccionaron tomando en cuenta el nivel de importancia según el personal de TI.

4.2.1. Diagnóstico de Data Center

Cuarto de Telecomunicaciones o Data Center – TR

La municipalidad no cuenta con un Data Center. La Sala de Telecomunicaciones es un espacio único centralizado donde se encuentran armarios y equipos de telecomunicaciones conectados.

El ambiente de equipos que posee la edificación de 5 pisos es:

- Un gabinete mediano donde se encuentra algunos equipos de comunicación;
- 3 extensiones;
- 3 switch de 48 puertos TL-SF1048.

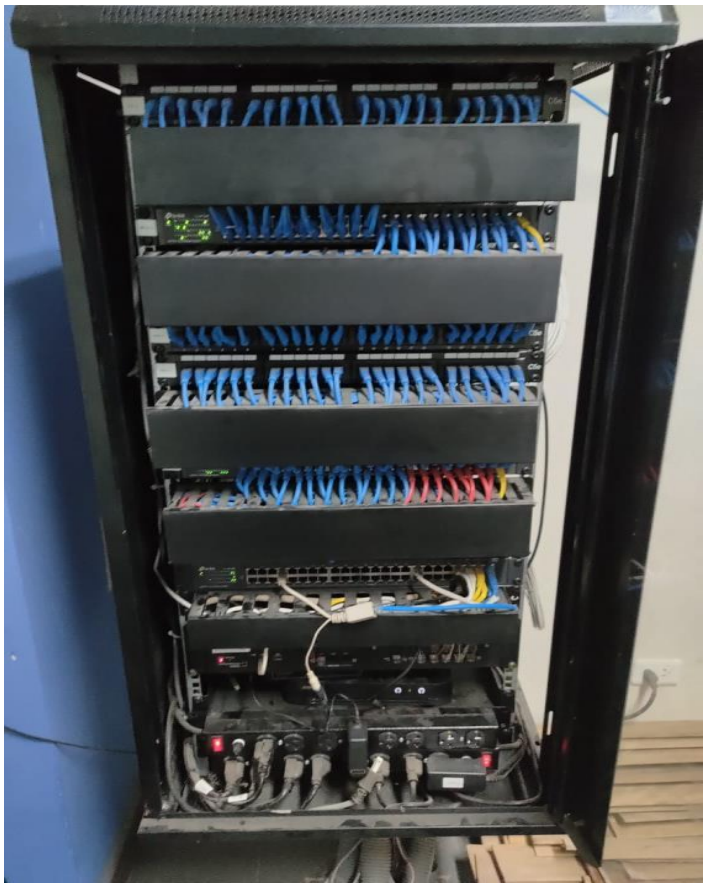
Figura 1

Switch Data center



Figura 2

Gabinete de comunicaciones



El ambiente de equipos que contiene la sede de la MPU de 2 pisos:

- 1 gabinete mediano donde se encuentra algunos equipos de comunicación;
- 1 Servidor Hewlett Packard Enterprise;
- 1 MikroTik Routerboard Rb1100AHx4;
- 2 Cloud Router Switch 326-24G-2S+RM,800 MHz CPU;
- 1 Switch 24 Puertos Trendnet Teg-S24G;
- 1 Switch TP-Link TL-SG1024D;
- 1 Switch 8 Puertos Tp-link Tl-sg1008p;
- 1 UPS Satra horizontal;
- 1 UPS Forza Nt-1012u

Figura 3

Gabinete de comunicaciones - oficinas



Carencias del Data Center

A continuación, se detallan las carencias encontradas en el centro de datos:

- Carencias de climatización adecuada para los equipos.
- No posee área de mantenimiento de red.
- No cuenta con falso piso o piso técnico.
- No posee el sistema de alimentación de energía interrumpida
- Carece de control de incendios y equipos como extintores.
- No posee el control de acceso mediante un biométrico.
- No cuenta con cámaras internas de seguridad en la Data center
- Carencia de un Sistema de alarmas.
- Carencia de equipos de contingencia.

4.2.2. Diagnóstico de Servidores

Los servidores son equipos informáticos utilizados para almacenar, procesar y desplegar información a los usuarios finales. El modelo distribuido

corresponde al tipo Cliente - Servidor. Los usuarios finales hacen uso de los servicios a través de computadoras clientes, laptop, etc. Los servidores deben permanecer en funcionamiento 24/7, deben contar con un nivel de seguridad adecuada para salvaguardar la información de la organización.

Características Técnicas del Servidor

Tabla 3

Características técnicas del servidor

Característica	Descripción
Marca:	Hewlett Packard Enterprise
Modelo	8032
Zócalo:	LGA 1155
Fabricante de Procesador: Intel®	Intel®
Numero de núcleos:	16
Velocidad de Procesador:	2.1GHz
Tipo de Procesador:	Xeon silver
Modelo del procesador:	4110
Ram:	16 GB
Sistemas instalados:	Windows server 2016 estándar 64 bits
Numero de discos duros:	1
Capacidad del Disco duro (HDD):	1TB

Identificación de Riesgos

Esta etapa comprende de las siguientes actividades:

1. Identificación y clasificación de activos: Bienes todos los elementos tangibles utilizados por la empresa para atender los servicios y se clasifican en:

   Recursos: Comprende el hardware y software como son: Servidores, laptops, equipos personales, programas, Equipos de comunicación, Equipos de protección.

   Personal: Son las personas o colaborares que haces uso de los recursos, siendo los siguientes: Informática/soporte Interno, Soporte Técnico Externo, cliente/Personal de la MPC que usa los programas cliente/ciudadano que requiere los servicios, Otras Instituciones externas.

   Datos e información: Vienen a ser los datos e información producto de las actividades de la organización y a través del uso de equipos informáticos, entre los que están: Bases de datos internos, Respaldos Infraestructura (Planes, Documentación, etc.), Informática (programas, código fuente, etc.), Sistemas de autenticación LDAP (Protocolo de Acceso Liviano al Directorio), Sistemas de información no institucionales Navegación en Internet.

2. Vulnerabilidades y Amenazas sobre activos tipo servidor.

   Amenazas Lógica: Se evidenciaron vulnerabilidades en casa uno de los servidores como: ataques de malwares, virus, troyanos, ocasionando síntomas como: ralentizar su computadora, hace funcionar a un nivel máximo durante mucho tiempo puede dañar su dispositivo y aumentar su

desgasto. Lanzamiento de programas ejecutables los archivos ejecutables pueden cambiar configuraciones en su ordenador o servidor y dañarlos.

Amenazas físicas: Condiciones físicas inadecuadas como se muestra en la siguiente imagen:

Figura 4

Servidores



Climatización Inadecuada

Se cuenta con aire acondicionado de tipo confort, siendo este tipo de equipo inadecuado para los servidores, debido a la humedad que puedan generar y corroer los dispositivos electrónicos.

Figura 5

Aires acondicionados



4.2.3. Diagnóstico Aplicaciones SIAF, SIGA

Los programas SIAF y SIGA son instrumentos de gestión que permiten la organización de las actividades e información de los ingresos y gastos de la municipalidad. El SIAF SP, el SIGA y el SEACE son programas de carácter obligatorio establecido por el Estado Peruano.

La municipalidad cuenta con los sistemas de gestión: SIAF, SIGA y Sistema de agua potable (Rentas).

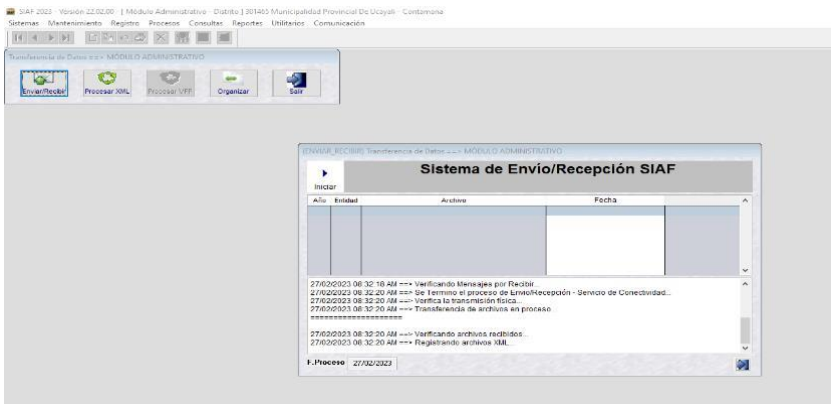
Carencias de las Aplicaciones SIAF, SIGA

A continuación, se detallan las carencias encontradas en las Aplicaciones SIAF, SIGA

- Falta de registro de compromiso que es donde se ven comprometidos los lineamientos que optimizan los procesos correspondientes a las certificaciones del crédito presupuestario y del compromiso de los administradores luego de autorizar y registrar los datos y validarlos haciendo uso de una clave dinámica.
- Se encontró que las transmisiones son en forma manual y no automático.

Figura 6

Sistema de envío/recepción SIAF



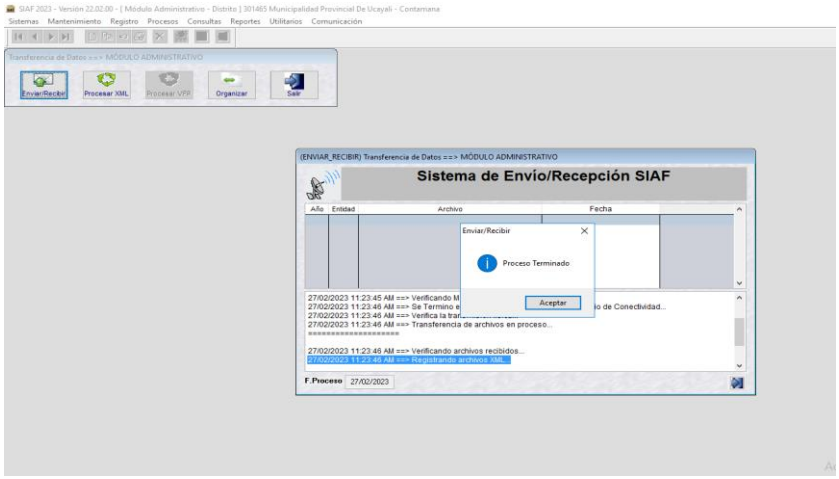
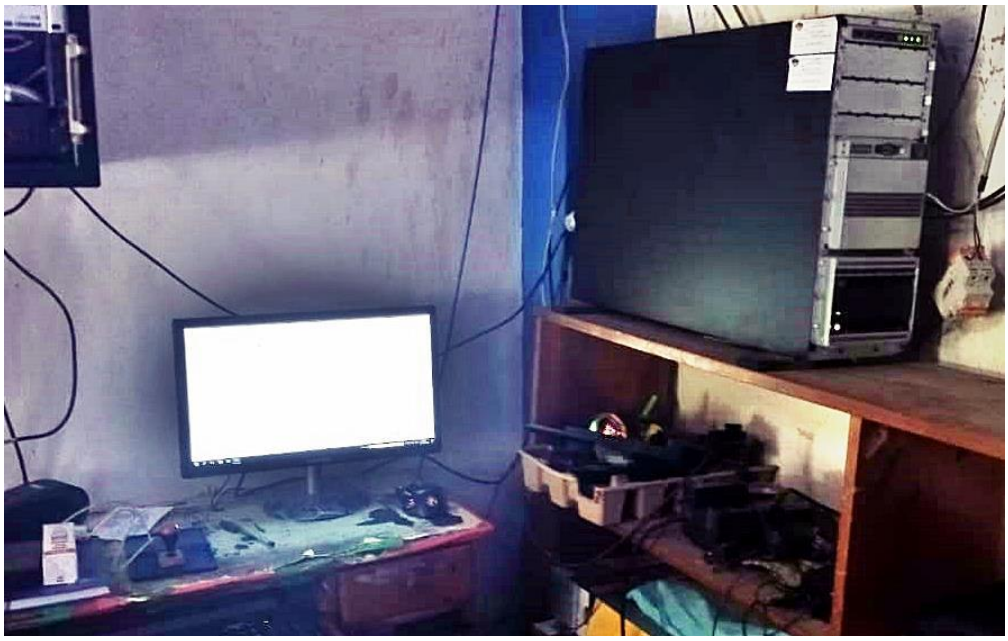


Figura 7

Servidor de aplicaciones



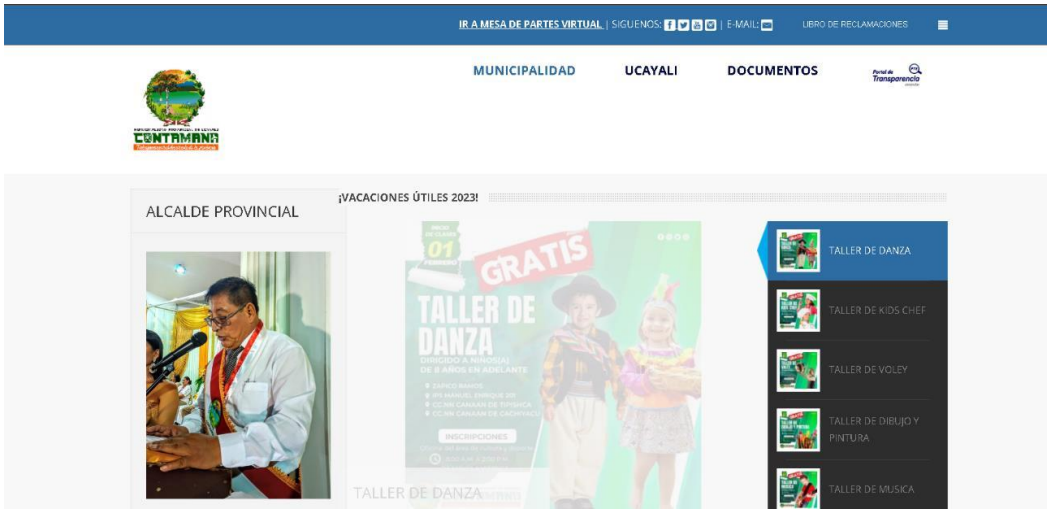
4.2.4. Diagnóstico de Dominio y Alojamiento

Los sistemas de la municipalidad son: Portal web, Gob.pe, Portal Transparencia y Web mail (Correos institucionales)

Página Web (Portal web): https://www.muniucayali.gob.pe/

Figura 8

Portal WEB de la Municipalidad Provincial de Ucayali Contamana



Características

- Plataforma: Web
- Tecnologías: PHP, HTML, JS
- CMS: Joomla
- Versión de PHP: PHP 7.4.33
- Motor de procesamiento de interpretación y cifrado: Zend Engine v3.4.0
- Velocidad: Zend OPcache v7.4.33
- Codificador propietario: ionCube PHP Loader + ionCube24 v10.4.5
- Situación: La página web agregar más secciones, actualizar y crear vistas más interactivas para el usuario final.
- Versión: Anterior fallas en compatibilidad de versión
- Diseño: Antiguo
- Responsive: Regular
- Adaptivo: No en algunas secciones
- Estado: Activo

Carencias del Dominio y Alojamiento

A continuación, se detallan las carencias encontradas en el Dominio y Alojamiento.

La municipalidad no ha incorporado sus canales digitales a la Plataforma Digital Única del Estado Peruano para orientación al ciudadano - GOB.PE, esto afecta negativamente a los ciudadanos y personas en general.

El portal de transparencia esta desactualizado con poca información y las secciones y vistas con poco contenido actualizado

4.2.5. Diagnóstico de la Red LAN y Recursos

Se puede diagnosticar protocolos generales, Volumen de tráfico, Velocidad de transmisión de datos y uso del ancho de banda de la red, así como los errores y problemas reportados por los usuarios. Realizar un diagnóstico de la situación de la red y cables de la Municipalidad.

La Municipalidad cuenta con una red cableada la expansión de redes y diversas zonas de la empresa, actualmente posee 110 equipos de cómputo, 15 impresoras y 26 equipos de telecomunicaciones.

Carencias de la Red LAN

A continuación, se detallan las carencias encontradas en la red LAN.

- Las telecomunicaciones actúan como conmutadores y enrutadores que se conectan a la red el número de puntos de la red no se encontraron el mapa de la red. La red está alimentada por Internet de 50 Mbps a través de una antena repetidora Wi-Fi de 30 Mbps para uso principal y de emergencia. El router principal la cual recibe el internet cableado de proveedor de internet es un MikroTik Routerboard Rb1100AHx4 y conectado con 2 Cloud Router Switch

326-24G-2S+RM,800 MHz CPU,1 Switch 24 Puertos Trendnet TEG-S24G y1 Switch TP-Link TL-SG1024D.

Figura 9

Switch 326-24G



- El número de usuarios de la red es de aproximadamente 120 integrados a través de un cableado estructurado UTP diversas categorías, de topología no identificada, de cobertura LAN y una velocidad teórica máxima de 50 Mbps.
- La red LAN no se encuentra segmentada en subredes ni a nivel lógico (por direcciones IP) ni a nivel virtual (a través de Vlans), lo cual origina en primera instancia gran cantidad de tráfico broadcast que en las horas pico asciende y se produce una red lenta. Adicionalmente, la no segmentación de la red se constituye en un factor de inseguridad ya que en caso de un acceso no autorizado o violento a la red LAN, dicho infractor podría introducirse ar toda la red.

Figura 10

Receptor emisor de internet



Figura 11

Torre receptora/ emisora de internet de 50 megas



- Cableado de red y eléctrico inadecuado, propenso a accidente.

Figura 12

Cableado de red desordenado



4.2.6. Diagnóstico del Sistema de Video Vigilancia

No se cuenta con un sistema de control con video de vigilancia.

4.3. Soluciones y/o mejoras

En esta fase, se realizan la propuesta de solución a cada uno de los recursos evaluados en el punto anterior, esta fase únicamente es para informar las alternativas de solución de la situación problemática, que posteriormente podrían ser implementados por los tesistas y/o el personal de TI del Área de informática de la Municipalidad.

4.3.1. De Data Center

En el diseño y la ubicación de la sala de equipos, debe ser el adecuado espacio sin infiltración del agua.

Dado que los equipos de telecomunicaciones en esta sala por lo general son de gran tamaño, la accesibilidad de entrada debe ser una consideración.

La ubicación ideal de la DATA CENTER debe estar situada cerca de la vía troncal principal para permitir la fácil conexión a dicha vía troncal.

Equipos comunes, incluidos los PBXs de la central telefónica deben de ser con tecnología IP ya que no existe una troncal en la MPU.

Los equipos de telecomunicaciones deben estar conectados a unos ups y a un trasformador de energía eléctrica para estabilizar dicha energía para evitar descargas eléctricas de dichos dispositivos y su deterioro.

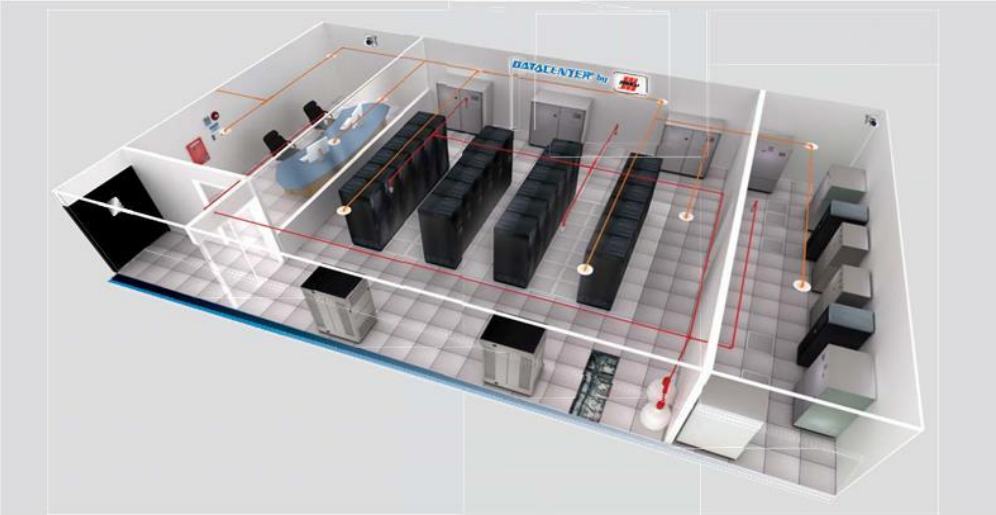
Adquirir ups y transformadores para estabilizar la fuente de energía de los equipos de telecomunicaciones y no se deterioren a causa de una descarga eléctrica por sobrevoltaje.

Se recomienda controlar el DVR con un monitor ya que funciona fluidamente dicho DVR con algunas cámaras en mal estado.

Falta de activar y configuración e instalación de la central telefónica ya sea analógicamente o por IPs ya que se cuenta con dicho recurso.

Figura 13

Propuesta de Data Center



4.3.2. De servidores

- Adquisición de servidores para aplicaciones de gestión como el SIAF, SIGA y otras aplicaciones.
- Elaborar el plan de contingencia de los diferentes dispositivos.
- Adquisición e instalación urgente de una antivirus.
- Instalar en los servidores las herramientas de gestión y en las PCs de las demás áreas solo adicionar como espejo de tal manera que los datos se guarden en el servidor sin acceso de las áreas de manipular la DATA.
- Instalar y/o arreglar el aire acondicionado en la data center para que trabaja a una temperatura ideal de 15°C a 24°C los servidores.
- Implementar ambientes adecuados los servidores acondicionados con la temperatura ideal sin filtro de agua y pintados con pinturas especiales para mantener la temperatura.

4.3.3. SIAF, SIGA

- Incrementar el nivel de seguridad el acceso al aplicativo informático.

- Permitir el registro de identificación del funcionario con su código de usuarios, nombres y apellidos vinculados al servidor para no generar la trazabilidad del registro de información en el SIAF-RP y el control en el proceso de ejecución del gasto público.
- Realizar auditorías de la seguridad de la herramienta de gestión en el servidor.
- Hacer uso de las claves dinámicas en vez de claves estáticas.
- Elaborar un plan para autorizar y comprometer con responsabilidad en el uso adecuado de las contraseñas por los funcionarios.

4.3.4. Dominio y Alojamiento

- Elaborar un plan de trabajo para mantener actualizado la página web, portal gob.pe y portal transparencia actualizados y en funcionamiento.
- Dotar con personal que se dedica exclusivamente a las actividades de análisis y soporte.
- Capacitar al personal en los sistemas de transparencia y portales institucionales.

4.3.5. Sistema de Video Vigilancia

- Implementar un sistema de video vigilancia.

4.4. Implementación de soluciones

A continuación, se detallará las implementaciones que fueron posibles realizar, esto debido a que dependen, en gran medida, de la capacidad y facilidad de acceso a los recursos.

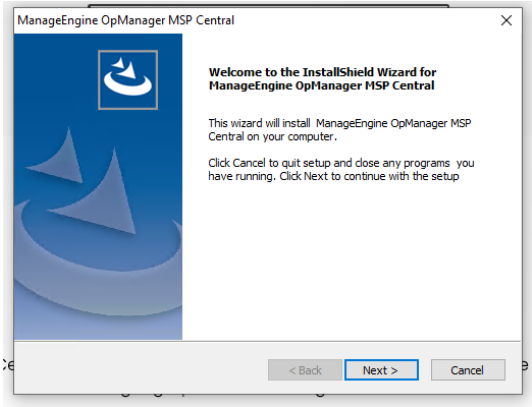
4.4.1. Instalación y configuración de software monitor de servidor

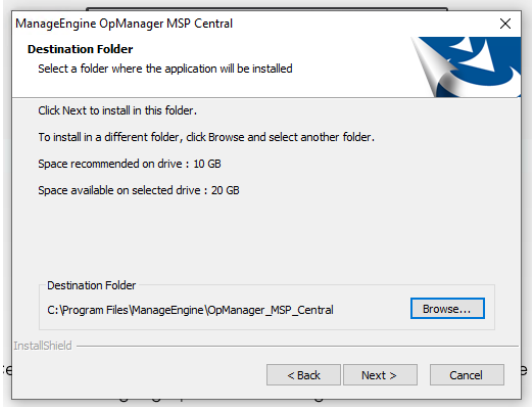
Instalación de OpManager MSP en Windows

Paso 1: Descargar OpManager_MSP_Central.exe desde este enlace: Descargar Central Server | ManageEngine OpManager

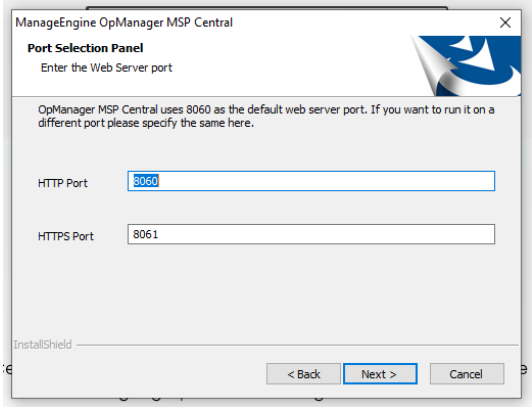
Ejecutar el exe con permiso de 'administrador'

Paso 2: Clic en 'Siguiente'.

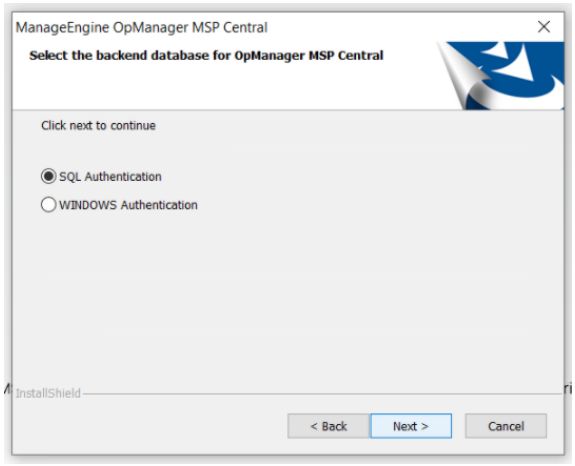


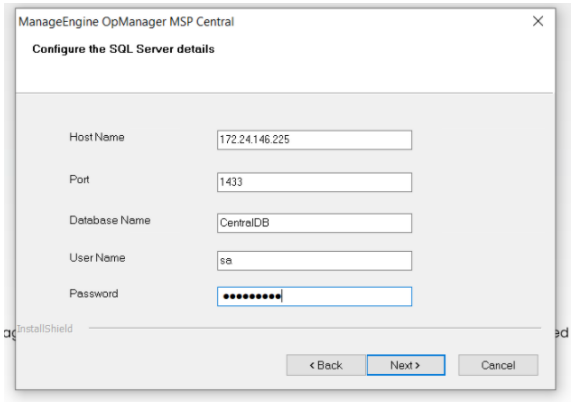


Haga clic en 'Siguiente'.

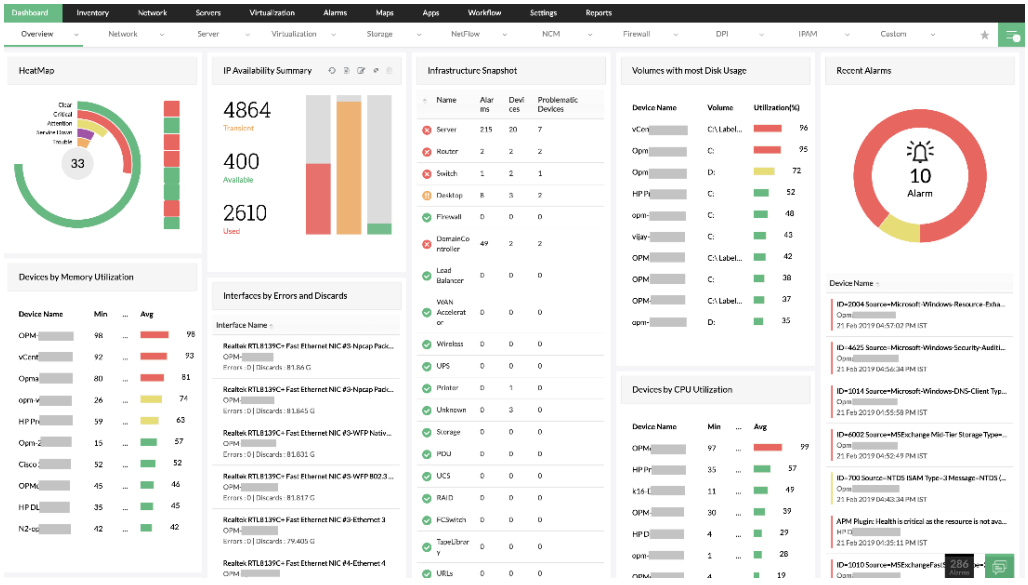


Seleccionar Autenticación de SQL, precise el Nombre de host, Puerto, Nombre de la base de datos. Haga clic en 'Siguiente' para continuar.



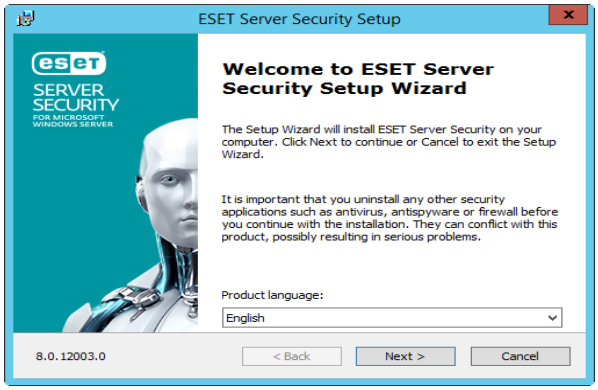


Monitor central

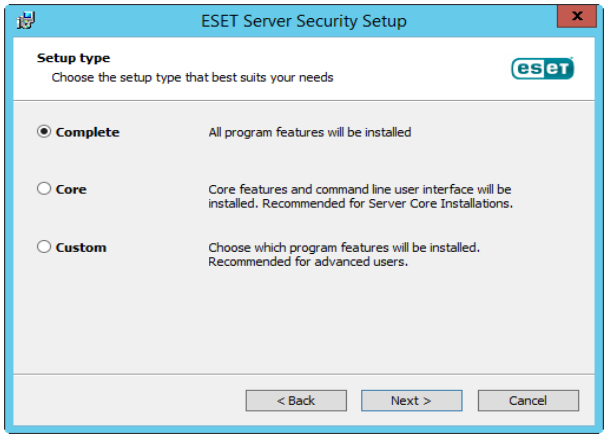


4.4.2. Instalación y configuración de Antivirus

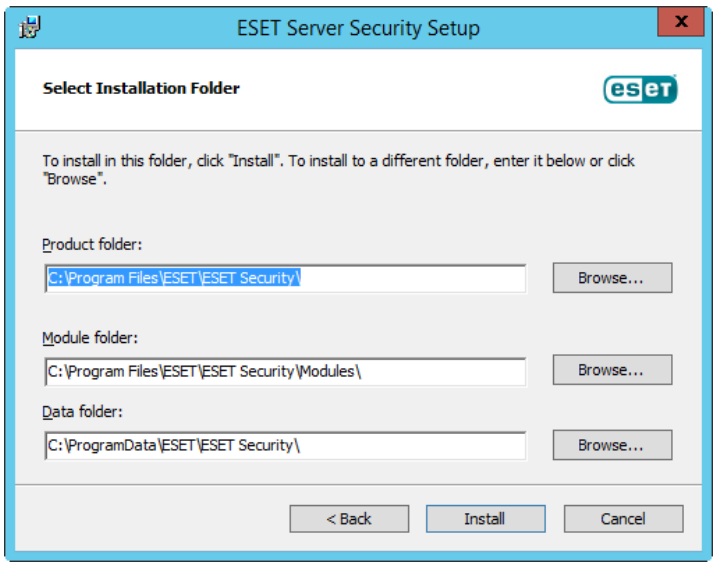
Instalación de ESET Server Security



Completa**:** Cuando se requiere todas las funciones, también llamada instalación integral de seguridad. Recomendable para Windows Server 2012 hasta 2019.



Seleccione la ubicación de instalación.



4.4.3. Servidor para SIAF y SIGA

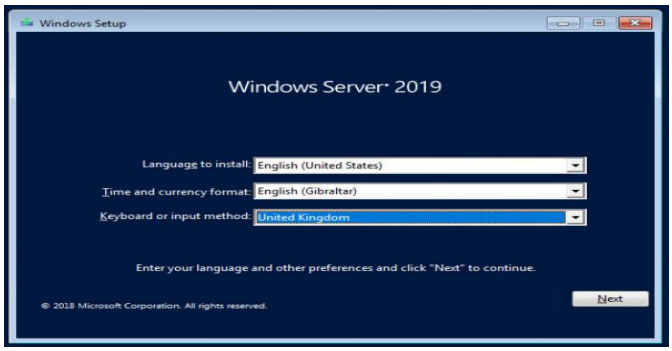
Características del Servidor

Marca	IBM
N° de Parte	XLS9ZPE
Formato	Torre
Procesador	Intel Xeon E3-1220 (3.1GHz, 8MB Cache L2)
Soporte de Procesador	Soporta hasta 1 procesador
Memoria RAM / Expansión	4GB, máximo 32GB con 1333MHz (DDR-3), (UDIMM), 04 ranuras Dual (DIMM)
Slot de expansión	Cuatro ranuras PCIe Gen 2(x16, x8, x4, x1)
Discos incluidos	Disco Duro 1 TB / DVD-ROM 48X
Capacidad de discos	12 TB SATA / (SATA)
Controlador de disco / RAID	ServeRAID-C100 para soportar RAID -0, -1 integrado; actualización a ServeRAID-C100, RAID-5 opcional; soporta RAID-0, -1, -5 por hardware
Controlador de red	(GbE) dual integrado

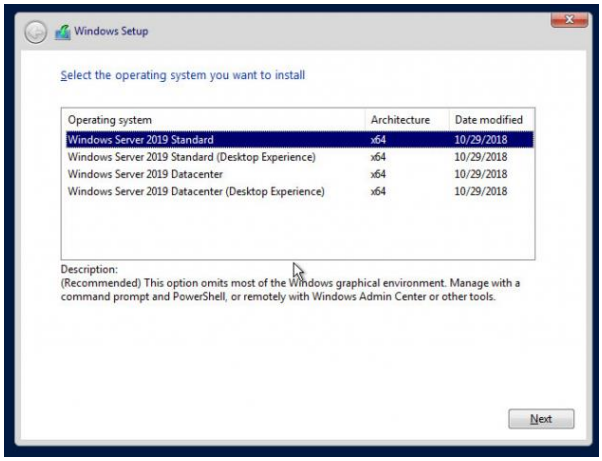


Instalación del Sistema Operativo

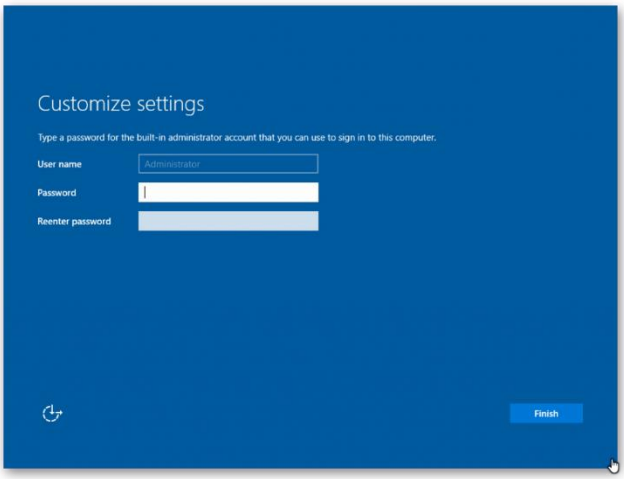
Bootear desde memoria externa, y seleccionar idioma



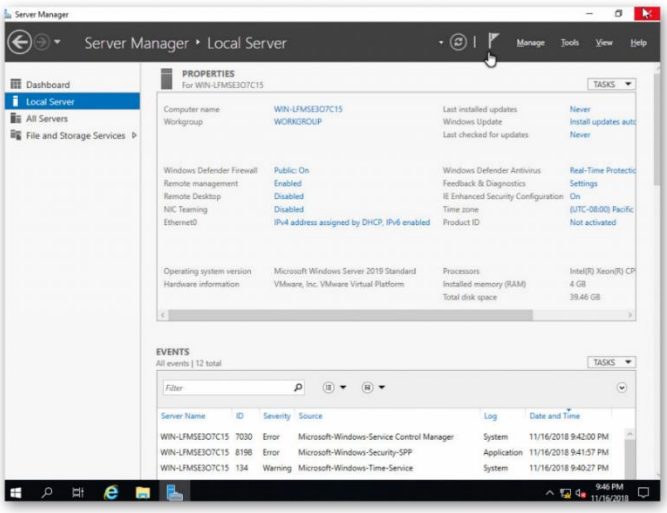
Instalar la versión Estándar



Configurara credenciales

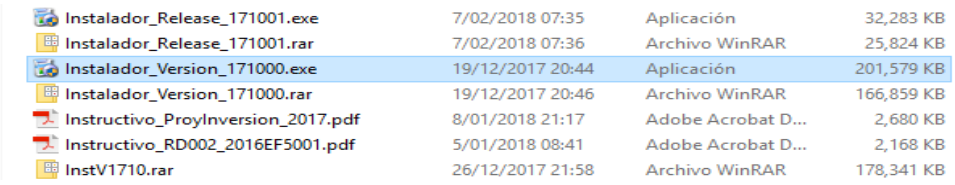


Pantalla inicial de SO

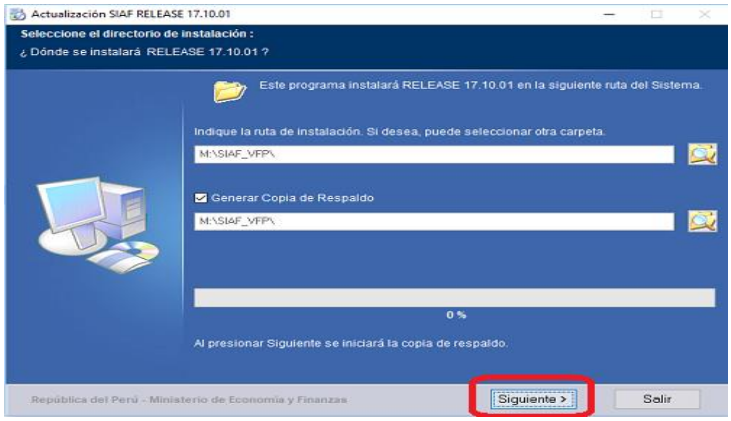


Instalación del SIAF

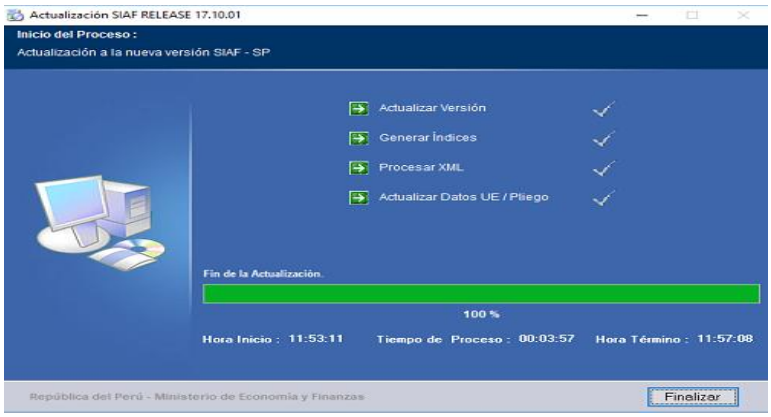
Ubicar el Instalador o Release vigente



Gobiernos Nacional o Regional M:\SIAF_V



Instalación finalizada





4.4.4. Video de cámara vigilancia

Esto fue posible a la adquisición oportuna de los bienes requeridos y se procedió con su implementación e instalación, cuya evidencia se detalla a continuación:

El sistema de video vigilancia consta de 16 cámaras con su respectivo DVR, ubicado en el data center que se encuentran instalados en las edificaciones nuevas de la municipalidad. También tiene en los ambientes antiguos con 8 cámaras y con su respectivo DVR Dahua que está en el despacho de alcaldía.

Equipos

- 2 grabadores digitales de vídeo (1 en la data center y otro en el despacho de alcaldía).
- 1 monitor (1 ubicado en el despacho de alcaldía).
- 2 Mouse.
- 2 cables VGA, HDMI.

Figura 14

Grabadores de video



Figura 15

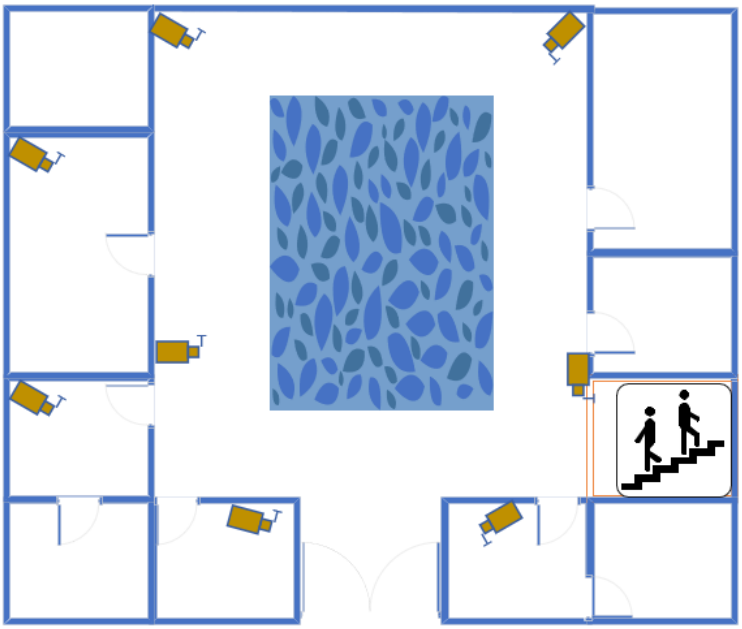
Gabinete de grabación



Ubicación de Cámaras de Video Vigilancia y Configuraciones

Figura 16

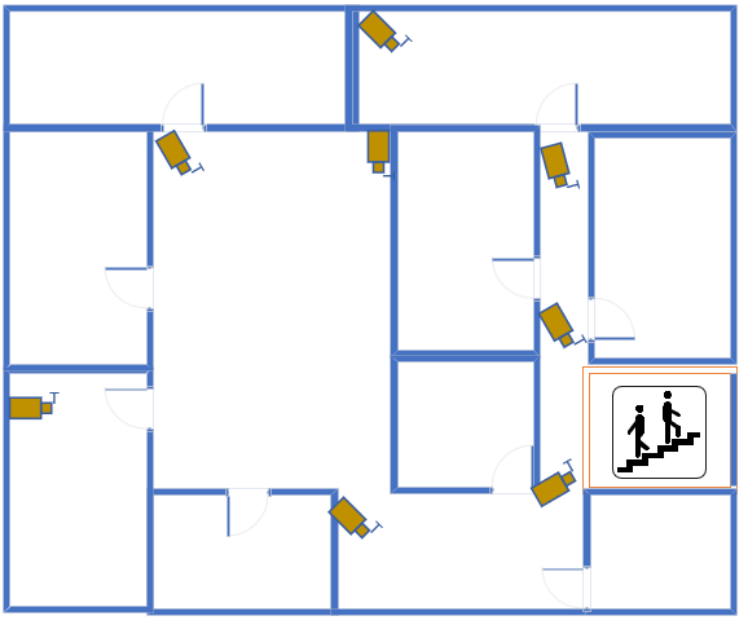
Plano de ubicación de cámaras 1er nivel



Fuente: Elaboración propia

Figura 17

Plano de ubicación de cámaras 2do nivel



Fuente: Elaboración propia

Figura 18

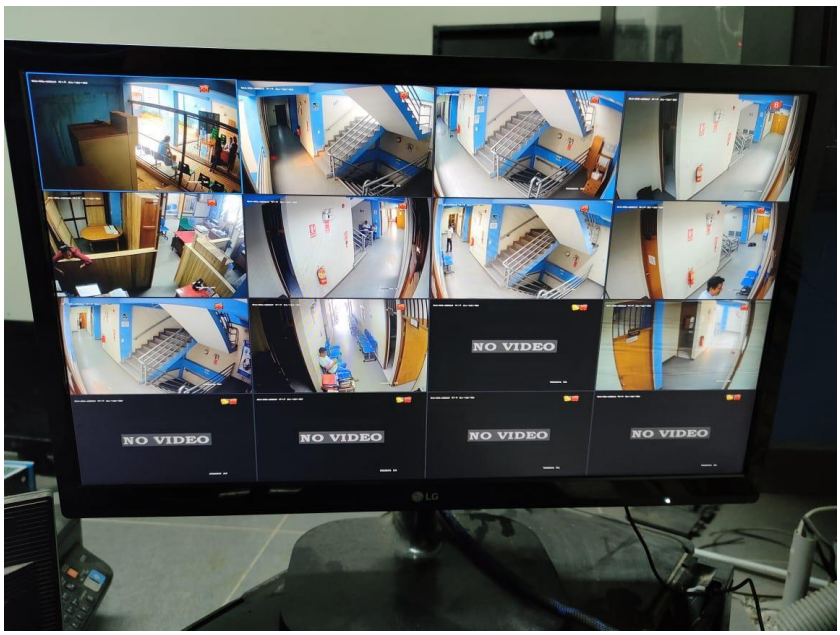
Cámaras de videovigilancia de la MPU





Figura 19

Pantalla central de video



4.4.5. Procedimiento de seguridad

Procedimiento Ante Ataque de la Plataforma Web

Se detallará los procedimientos a seguir para prevenir y atender ataques de 1 y 2:

Ataque Tipo 1: Ataque de Superficie

- Interrumpir servicios o acceder sin autorización.
- Ataques como: DDoS, fuerza bruta, phishing, explotación de vulnerabilidades conocidas.

Ataque Tipo 2: Ataque Avanzado/Persistente

- Robo de datos, mantenimiento de acceso prolongado.
- Como: APT (Amenazas Persistentes Avanzadas), inyección SQL avanzada, backdoors, rootkits.

Procedimiento de respuesta ataque tipo 1

- **Responsable:** Asisten de TI.
- **Herramientas:**

  Detección: SIEM (Splunk, ELK).

  Contención: Firewalls (iptables).

  Análisis Forense: Autopsy.

- **Actividades**

Fase	Acciones
Fase 1: Detección y Clasificación	Monitorear logs de acceso, firewalls, IDS/IPS, SIEM. Analizar alertas de seguridad (ej.: tráfico anómalo, intentos de login fallidos). Clasificar el ataque
Fase 2: Contención Inmediata	Bloquear IPs maliciosas (vía firewall/WAF). Limitar tasa de acceso (rate limiting). Deshabilitar servicios afectados temporalmente.
Fase 3: Erradicación	Parchear vulnerabilidades explotadas. Actualizar reglas WAF/IDS
Fase 4: Recuperación	Parchear vulnerabilidades explotadas. Actualizar reglas WAF/IDS

Procedimiento de respuesta ataque tipo 2

- **Responsable:** Asisten de TI.
- **Herramientas:**

  Detección: SIEM (Splunk, ELK).

  Contención: Firewalls (iptables).

  Análisis Forense: Autopsy.

- **Actividades**

Fase	Acciones
Fase 1: Detección y Clasificación	Monitorear logs de acceso, firewalls, IDS/IPS, SIEM. Analizar alertas de seguridad (ej.: tráfico anómalo, intentos de login fallidos). Clasificar el ataque
Fase 2: Contención Inmediata	Aislar servidores comprometidos de la red. Cambiar credenciales de acceso (SSH, FTP, BD). Revocar certificados TLS comprometidos.
Fase 3: Erradicación	Realizar análisis forense (buscar rootkits, backdoors). Restaurar desde backups limpios (si es necesario). Revisar integridad de bases de datos y archivos
Fase 4: Recuperación	Restaurar servicios gradualmente. Monitorear comportamiento post-ataque. Validar que no queden vectores de ataque activos

Procedimiento Copia de Seguridad SIAF y SIGA

Este procedimiento establece las directrices para realizar copias de seguridad de los sistemas SIAF (Sistema Integrado de Administración Financiera) y SIGA (Sistema Integrado de Gestión Administrativa), garantizando la disponibilidad, integridad y recuperación de la información en caso de fallos, desastres o ataques cibernéticos.

Objetivo

- Asegurar la disponibilidad de los datos críticos de SIAF y SIGA.
- Minimizar el riesgo de pérdida de información por fallos técnicos, errores humanos o ciberataques.
- Cumplir con normativas legales y políticas institucionales de respaldo de datos.

Alcance

- Aplicable a las bases de datos, archivos de configuración y registros transaccionales de SIAF y SIGA.
- Cubre servidores principales, servidores de respaldo y almacenamiento externo seguro.

Responsables

- Administrador de Bases de Datos y Equipo de TI/Soporte

Procedimiento de Backup

Preparación

- Verificar que los servidores de SIAF/SIGA estén operativos.
- Confirmar espacio disponible en medios de almacenamiento.
- Asegurar que no haya procesos críticos en ejecución durante el backup.

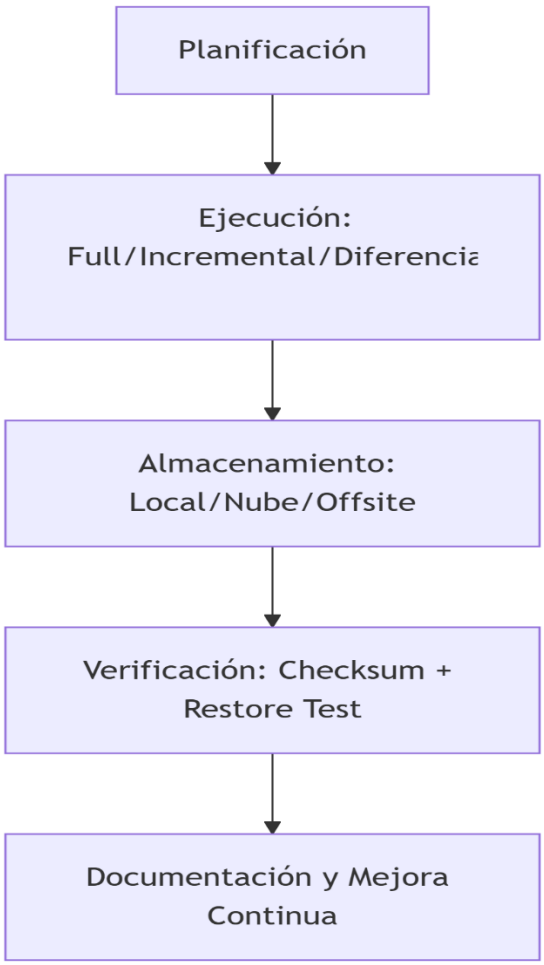
Almacenamiento Seguro

- Local: Guardar en discos externo

Verificación del Backup

- Realizar pruebas de restauración parcial mensualmente.

Etapas generales



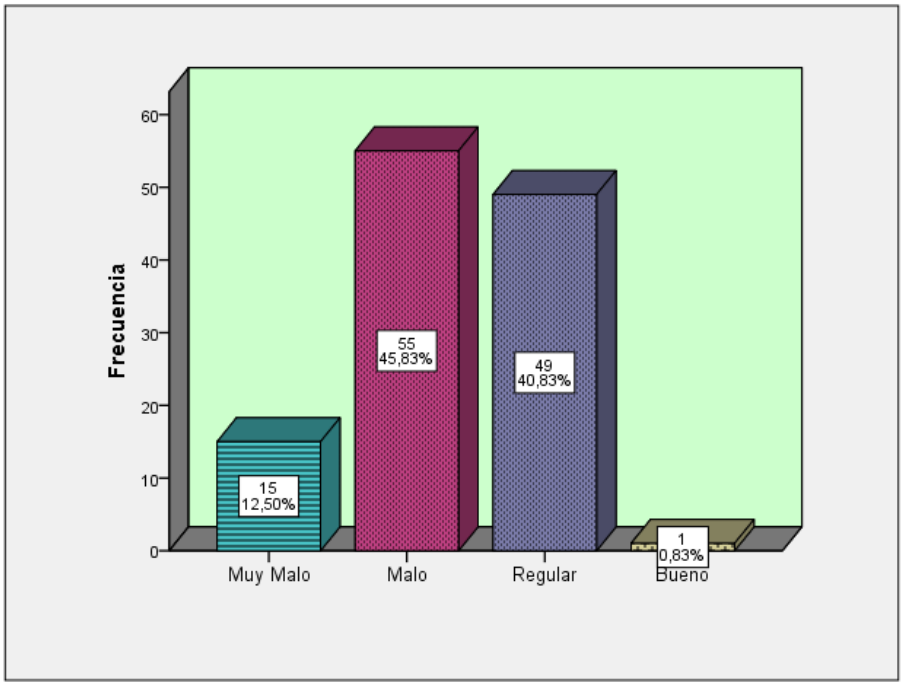
CAPÍTULO V

RESULTADOS

5.1. Resultados de la investigación Pre-Test

P1. ¿Cómo calificaría la el nivel de disponibilidad de los datos e información en el sistema en la actualidad?

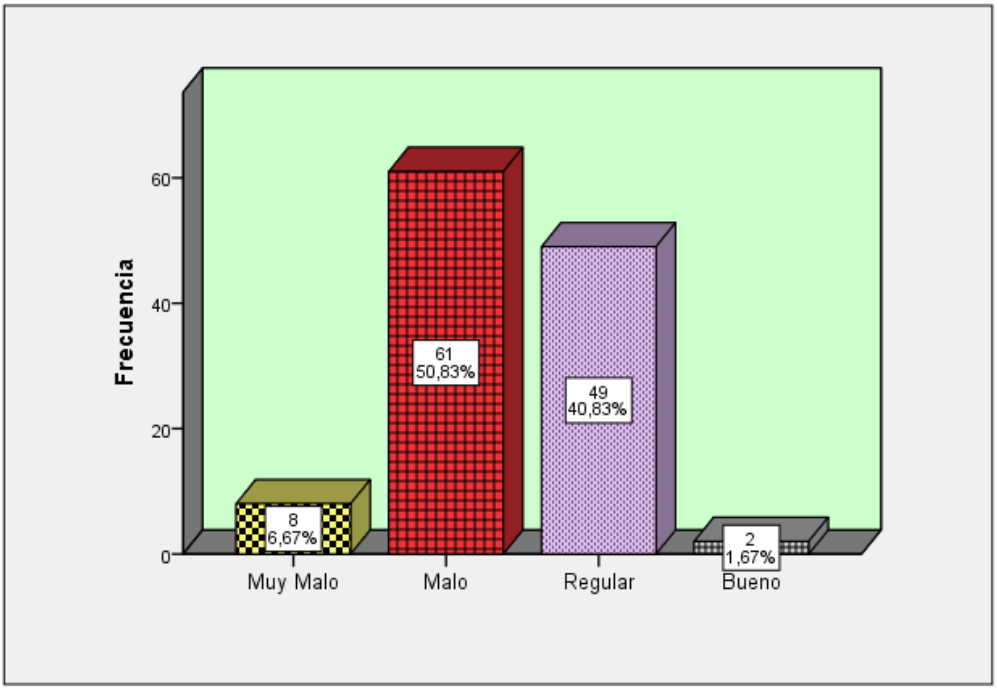
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	15	12,5	12,5	12,5
	Malo	55	45,8	45,8	58,3
	Regular	49	40,8	40,8	99,2
	Bueno	1	,8	,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 12,50% de las personas encuestadas menciona que es muy malo, mientras que el 45,83% es malo, el 40,83% es regular, y el 0,83% que consideran bueno la disponibilidad de la información en el sistema actual.

P2. ¿Cómo calificaría el desempeño, funcionalidad del sistema informático que se está aplicando para los procesos administrativos de atención al público?

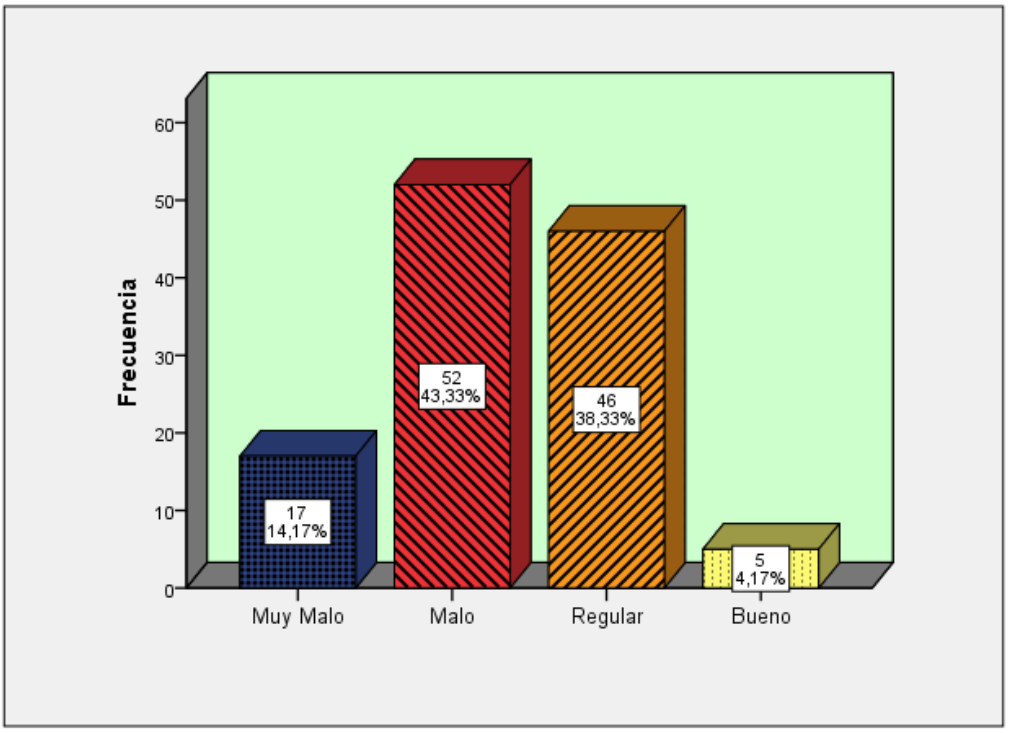
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	8	6,7	6,7	6,7
	Malo	61	50,8	50,8	57,5
	Regular	49	40,8	40,8	98,3
	Bueno	2	1,7	1,7	100,0
	Total	120	100,0	100,0	



Interpretación: El 6,67% de las personas encuestadas menciona que es muy malo, mientras que el 50,83% es malo, el 40,83% es regular, y el 1,67% que consideran bueno el actual desempeño y funcionalidad del sistema.

P3. ¿Cómo califica la forma como el personal de la Municipalidad accede a la información de sus servidores?

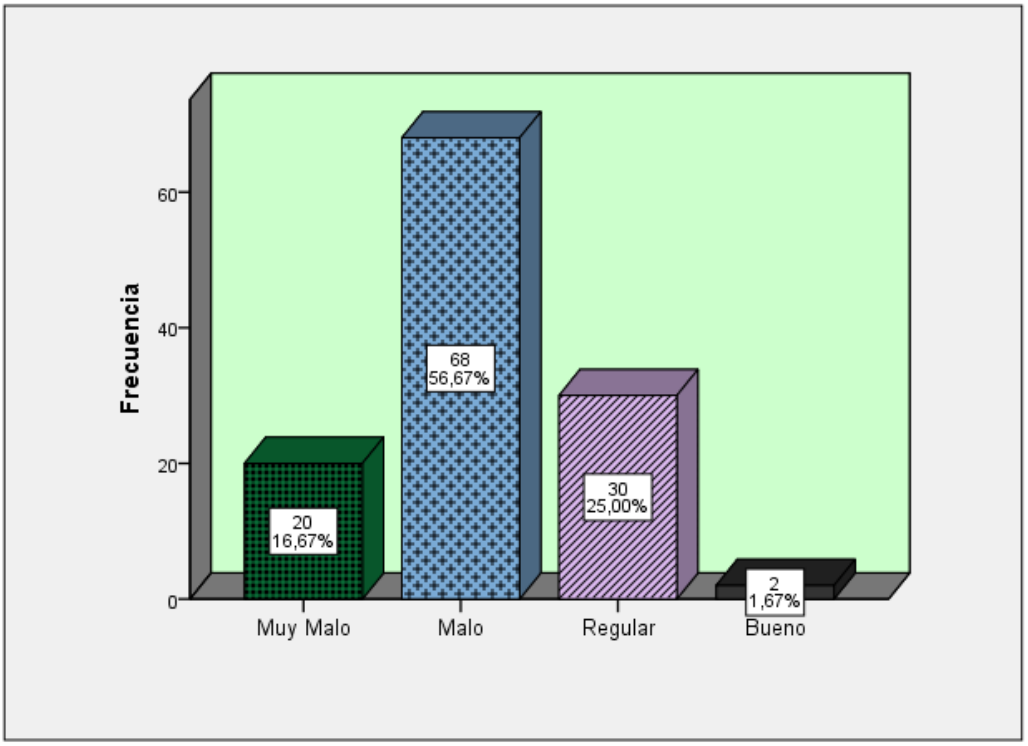
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	17	14,2	14,2	14,2
	Malo	52	43,3	43,3	57,5
	Regular	46	38,3	38,3	95,8
	Bueno	5	4,2	4,2	100,0
	Total	120	100,0	100,0	



Interpretación: El 14,17% de las personas encuestadas menciona que es muy malo, mientras que el 43,33% es malo, el 38,83% es regular, y el 4,17% que consideran bueno la forma como el personal de la municipalidad accede a la información de sus servidores.

P4. ¿Como calificaría el nivel de frecuencia con la que solicita la revisión de su PC frente a cualquier inconveniente?

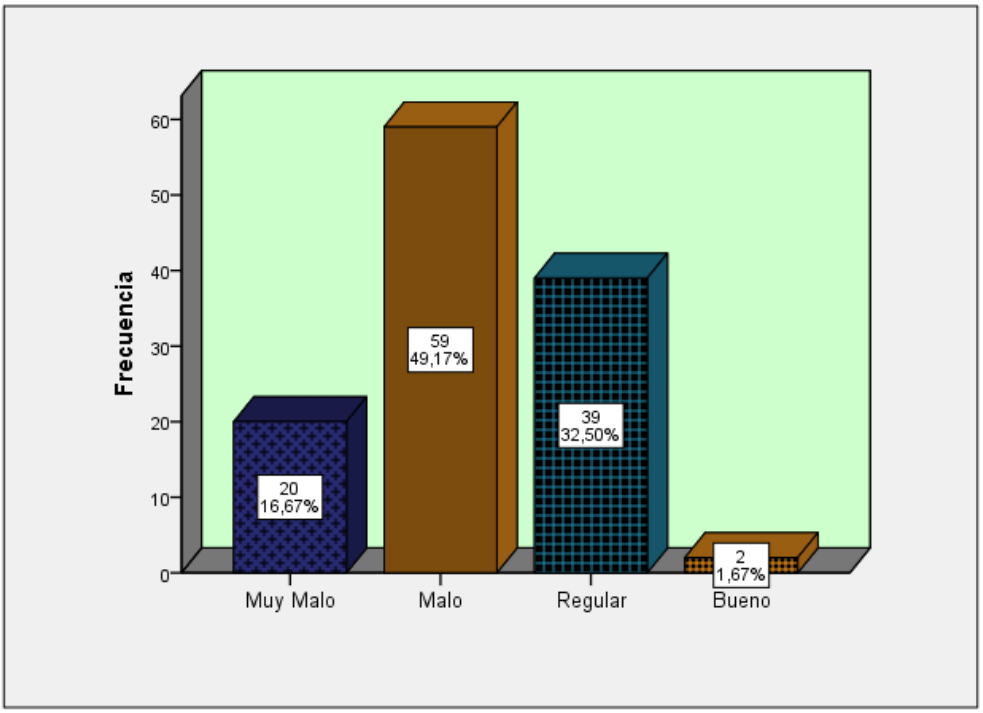
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	20	16,7	16,7	16,7
	Malo	68	56,7	56,7	73,3
	Regular	30	25,0	25,0	98,3
	Bueno	2	1,7	1,7	100,0
	Total	120	100,0	100,0	



Interpretación: El 16,67% de las personas encuestadas menciona que es muy malo, mientras que el 56,67% es malo, el 25,00% es regular, y el 1,67% que consideran bueno la solicitud de frecuencia que le revisen su PC frente a cualquier falla.

P5. ¿Cómo califica el tipo de servicio recibido por los usuarios al consultar por una solicitud?

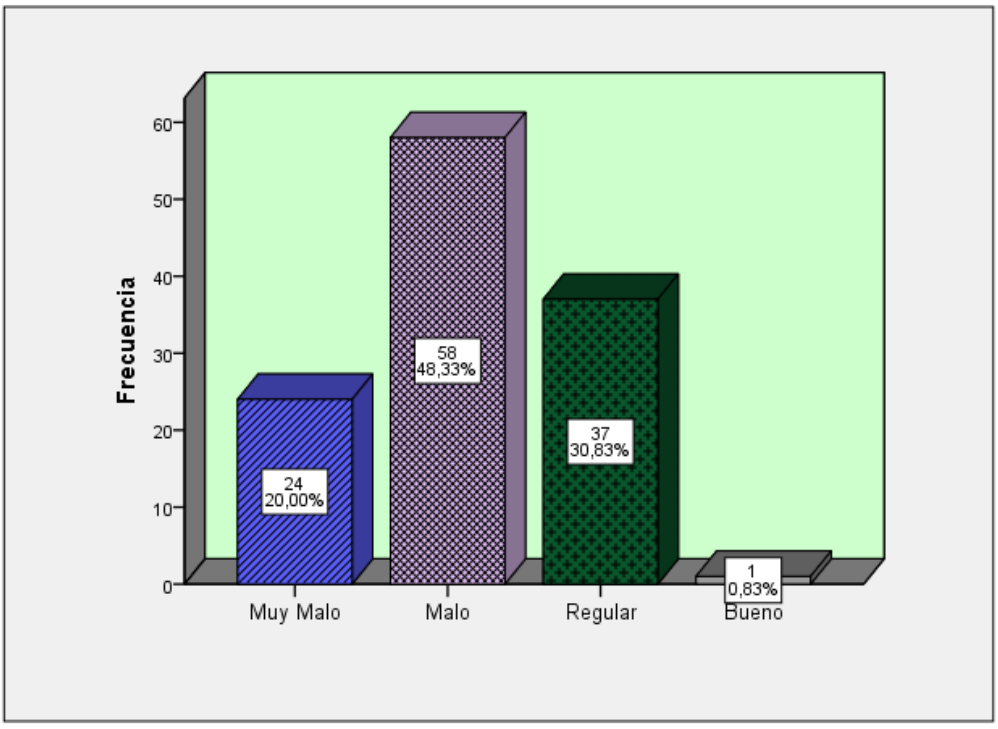
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	20	16,7	16,7	16,7
	Malo	59	49,2	49,2	65,8
	Regular	39	32,5	32,5	98,3
	Bueno	2	1,7	1,7	100,0
	Total	120	100,0	100,0	



Interpretación: El 16,67% de las personas encuestadas menciona que es muy malo, mientras que el 49,17% es malo, el 32,50% es regular, y el 1,67% que consideran bueno el tipo de servicio que reciben usuarios al realizar una consulta respecto a su solicitud.

P6. ¿Cómo calificaría si la municipalidad cumple con los objetivos de seguridad de información?

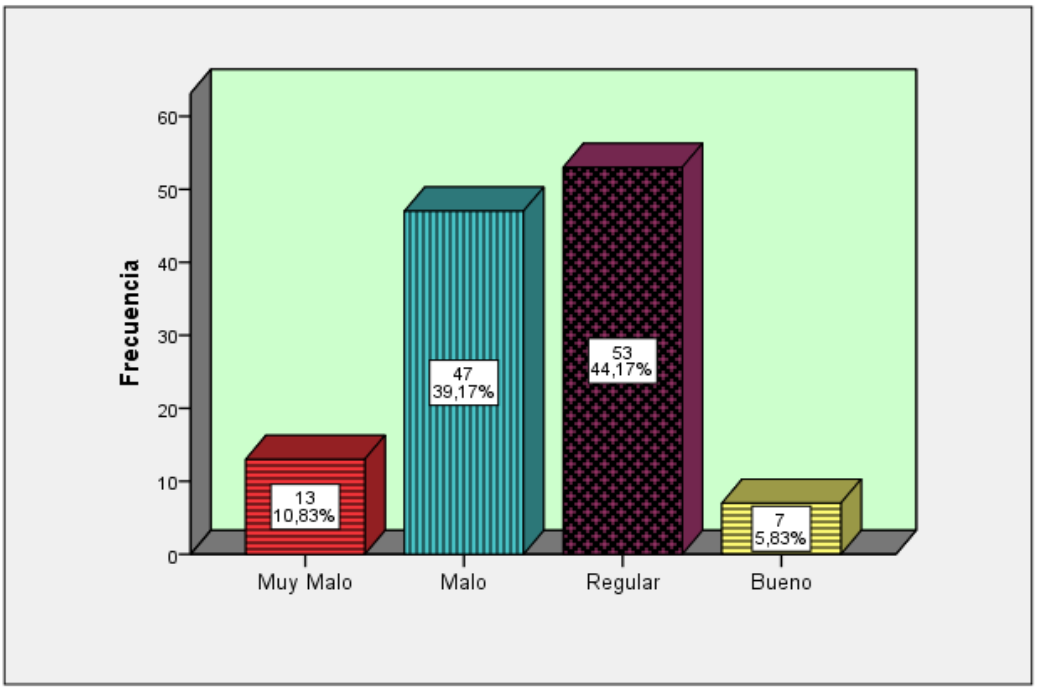
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	24	20,0	20,0	20,0
	Malo	58	48,3	48,3	68,3
	Regular	37	30,8	30,8	99,2
	Bueno	1	,8	,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 20,00% de las personas encuestadas menciona que es muy malo, mientras que el 48,33% es malo, el 30,83% es regular, y el 0,83% que consideran bueno como cumple la municipalidad con los objetivos de seguridad de la información.

P7. ¿Como calificaría a las herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identificación de los riesgos en la municipalidad?

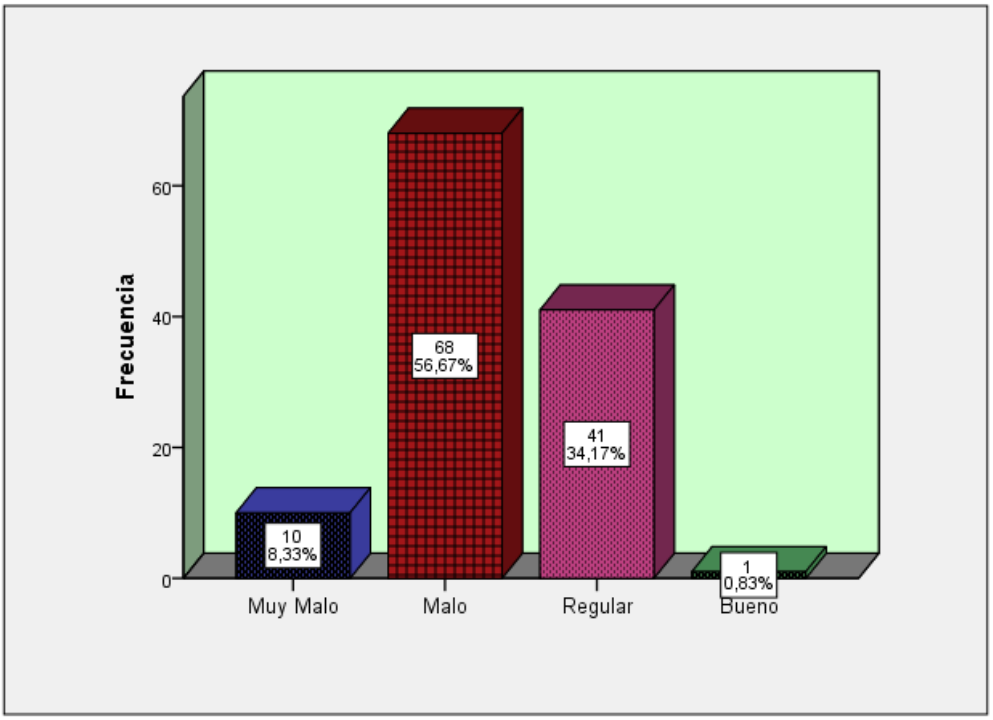
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	13	10,8	10,8	10,8
	Malo	47	39,2	39,2	50,0
	Regular	53	44,2	44,2	94,2
	Bueno	7	5,8	5,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 10,83% de las personas encuestadas menciona que es muy malo, mientras que el 39,17% es malo, el 44,17% es regular, y el 5,83% que consideran bueno las herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identificación de los riesgos de la municipalidad.

P8. ¿Cómo calificaría Ud. el proceso de seguimiento de los trámites que se presentan y se generan durante una consulta de los usuarios?

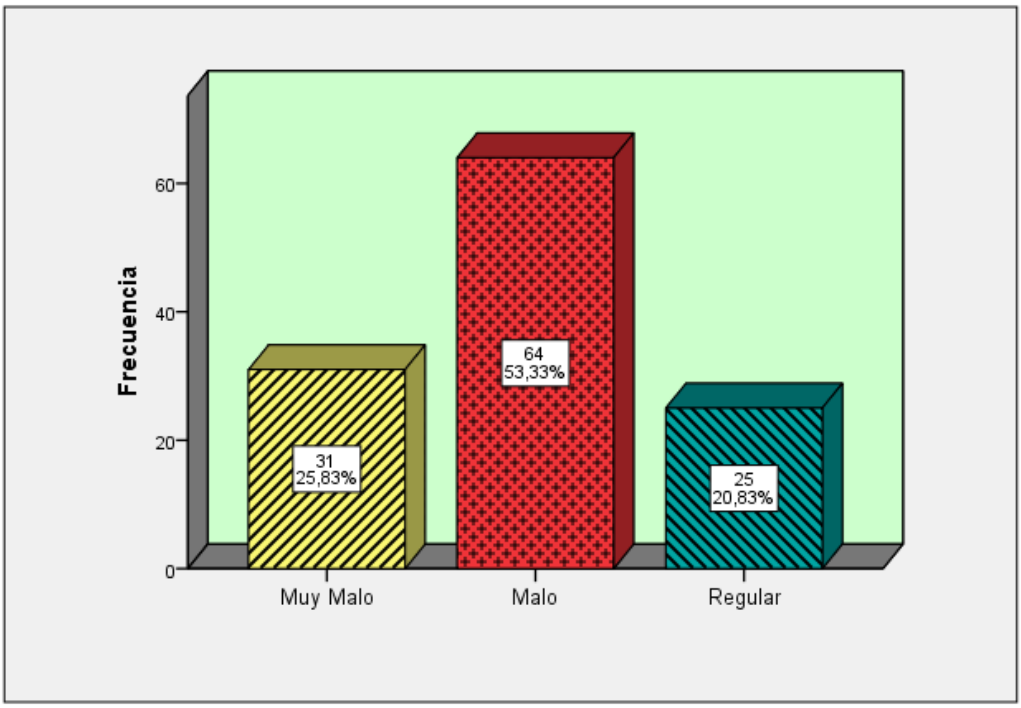
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	10	8,3	8,3	8,3
	Malo	68	56,7	56,7	65,0
	Regular	41	34,2	34,2	99,2
	Bueno	1	,8	,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 8,33% de las personas encuestadas menciona que es muy malo, mientras que el 56,67% es malo, el 34,17% es regular, y el 0,83% que consideran bueno el proceso de seguimiento de los tramites que se presentan y se generan durante una consulta de los usuarios.

P9. ¿Cómo calificaría al actual desempeño, funcionalidad del sistema informático que se aplica en los procesos administrativos de la municipalidad?

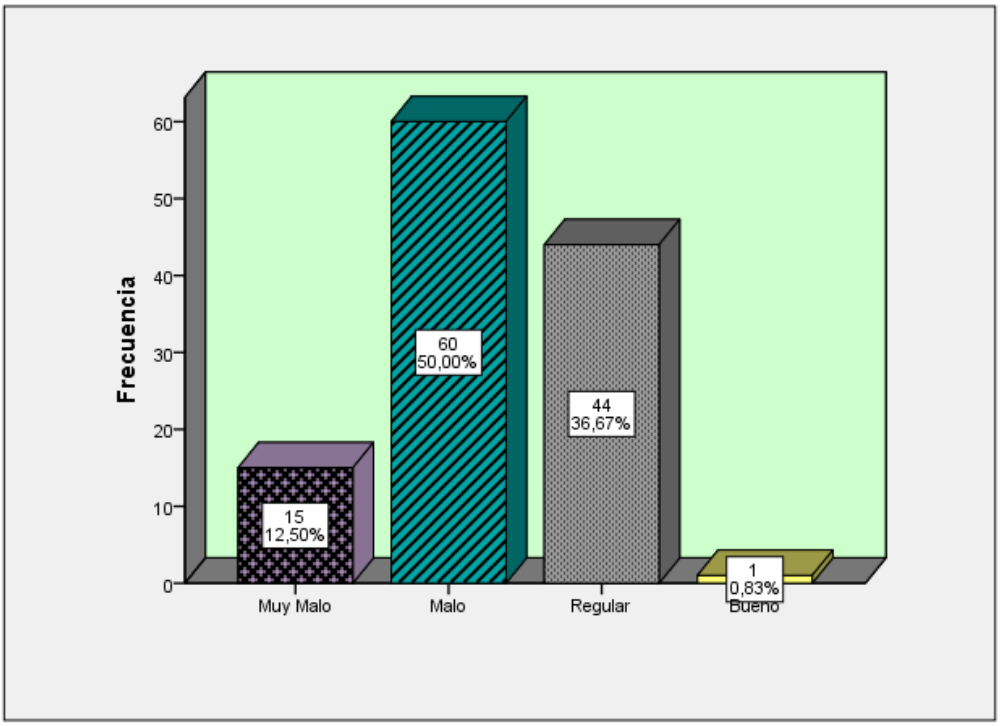
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	31	25,8	25,8	25,8
	Malo	64	53,3	53,3	79,2
	Regular	25	20,8	20,8	100,0
	Bueno				
	Total	120	100,0	100,0	



Interpretación: El 25,83% de las personas encuestas menciona que es muy malo, mientras que el 53,33% es muy malo y el 20,83% lo consideran regular al desempeño actual y la funcionalidad determinada del sistema informático que se aplica en los procesos administrativos de la municipalidad.

P10. ¿Cómo calificaría las respuestas del sistema a tiempo cuando se detecta alguna amenaza contra la seguridad de la información en la municipalidad?

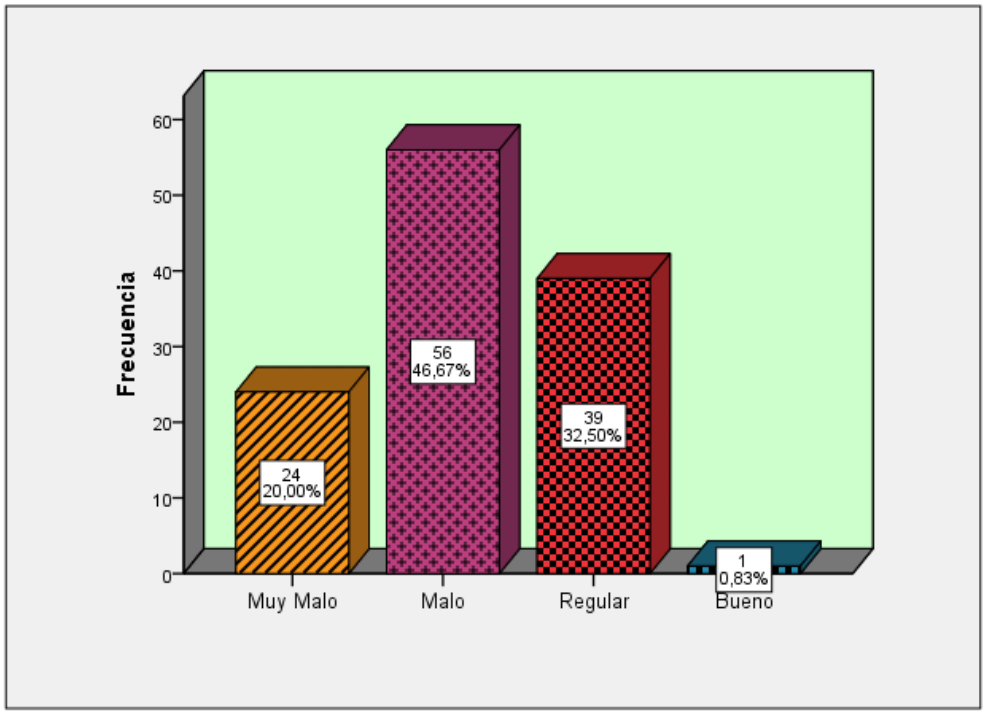
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	15	12,5	12,5	12,5
	Malo	60	50,0	50,0	62,5
	Regular	44	36,7	36,7	99,2
	Bueno	1	,8	,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 12,50% de las personas encuestadas menciona que es muy malo, mientras que el 50,00% es malo, el 36,67% es regular, y el 0,83% que consideran bueno las respuestas del sistema a tiempo cuando se detecta alguna amenaza contra la seguridad de la información en la municipalidad.

P11. ¿Cómo calificaría el hecho que solo el personal de la municipalidad debe contar con la autorización necesaria para acceder a sus datos personales?

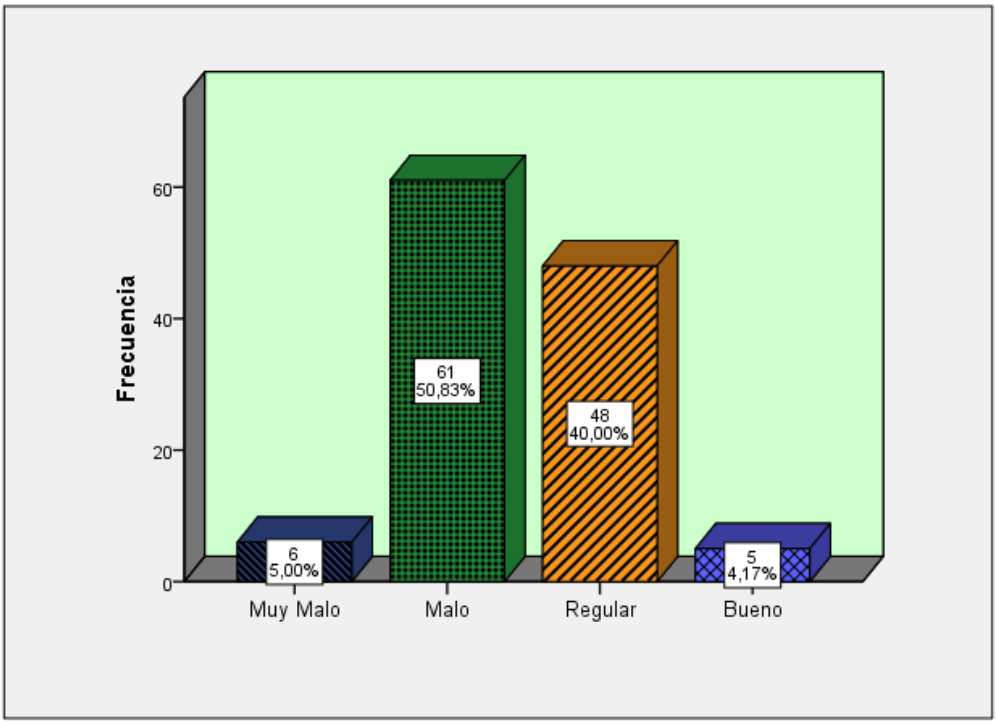
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	24	20,0	20,0	20,0
	Malo	56	46,7	46,7	66,7
	Regular	39	32,5	32,5	99,2
	Bueno	1	,8	,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 20,00% de las personas encuestadas menciona que es muy malo, mientras que el 46,67% es malo, el 32,50% es regular, y el 0,83% que consideran bueno el hecho que solo el personal de la municipalidad deba contar con la autorización necesaria para acceder a sus datos personales.

P12. ¿Cómo calificaría la frecuencia en el transito virtual de sus datos personales en la municipalidad?

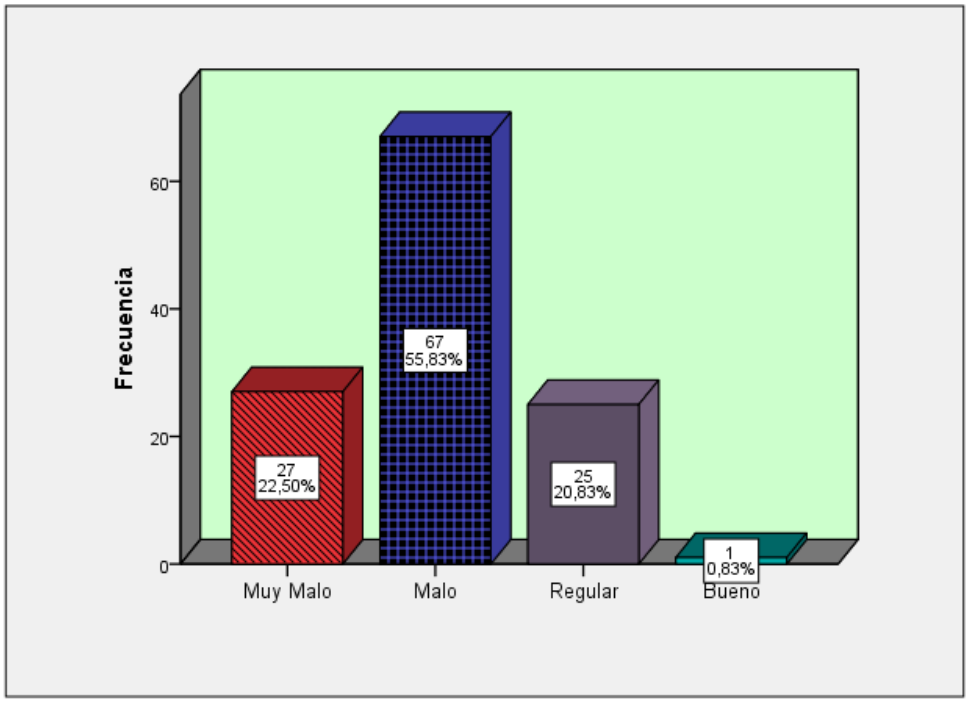
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	6	5,0	5,0	5,0
	Malo	61	50,8	50,8	55,8
	Regular	48	40,0	40,0	95,8
	Bueno	5	4,2	4,2	100,0
	Total	120	100,0	100,0	



Interpretación: El 5,00% de las personas encuestadas menciona que es muy malo, mientras que el 50,83% es malo, el 40,00% es regular, y el 4,17% que consideran bueno la frecuencia en el transito virtual de sus datos personales en la municipalidad.

P13. ¿Cómo calificaría el hecho que solo el personal autorizado pueda acceder a su información personal?

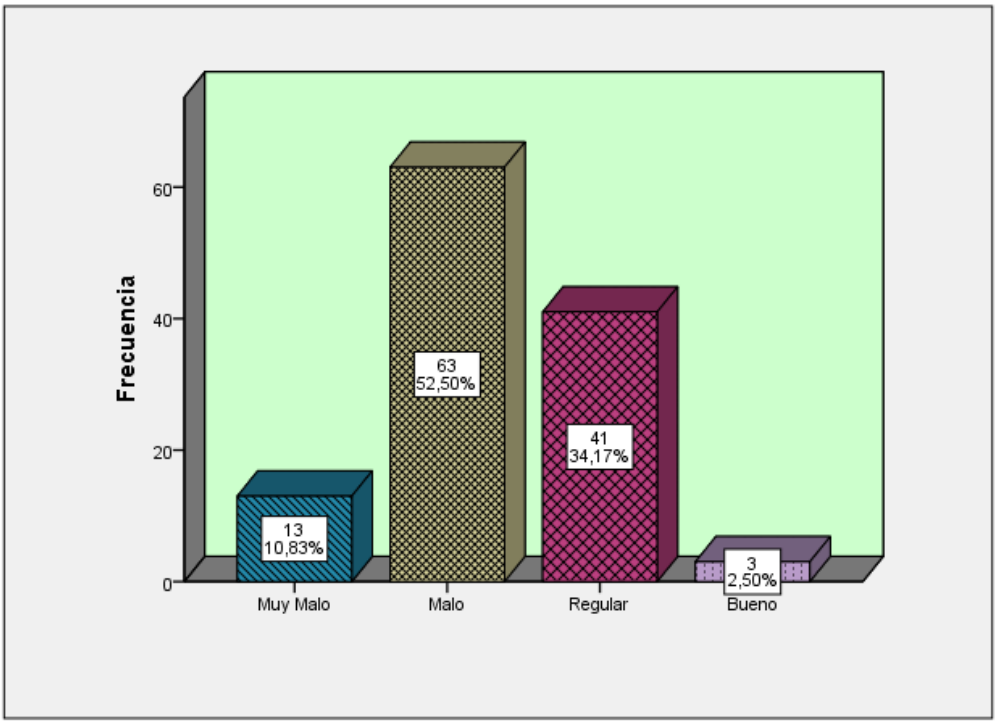
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	27	22,5	22,5	22,5
	Malo	67	55,8	55,8	78,3
	Regular	25	20,8	20,8	99,2
	Bueno	1	,8	,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 22,50% de las personas encuestadas menciona que es muy malo, mientras que el 55,83% es malo, el 20,83% es regular, y el 0,83% que consideran bueno el hecho que solo el personal autorizado pueda acceder a su información personal.

P14. ¿Cómo calificaría la seguridad en el tránsito virtual de sus datos personales en la municipalidad?

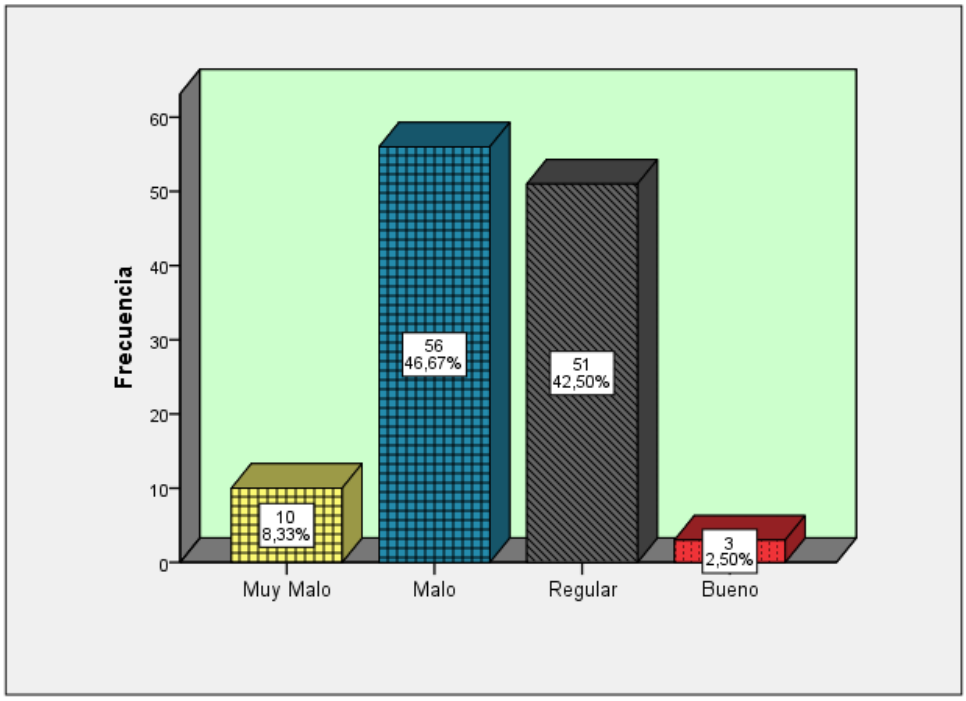
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	13	10,8	10,8	10,8
	Malo	63	52,5	52,5	63,3
	Regular	41	34,2	34,2	97,5
	Bueno	3	2,5	2,5	100,0
	Total	120	100,0	100,0	



Interpretación: El 10,83% de las personas encuestadas menciona que es muy malo, mientras que el 52,50% es malo, el 34,17% es regular, y el 2,50% que consideran bueno la seguridad en el transito virtual de sus datos personales de la municipalidad.

P15. ¿Cómo calificaría la precisión de sus datos personales que ofrece la municipalidad?

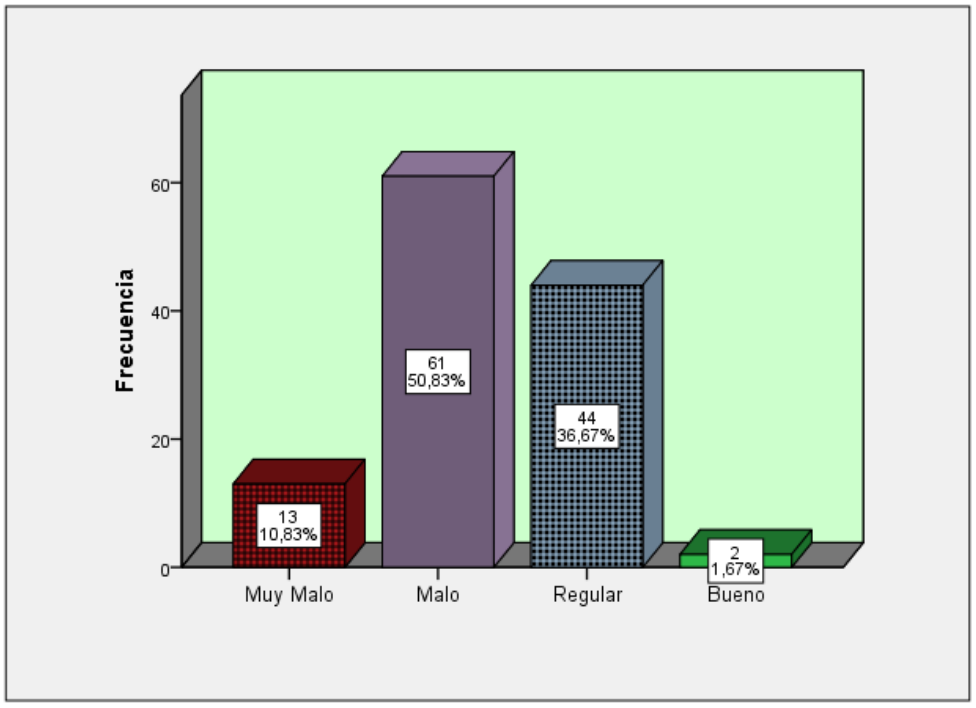
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	10	8,3	8,3	8,3
	Malo	56	46,7	46,7	55,0
	Regular	51	42,5	42,5	97,5
	Bueno	3	2,5	2,5	100,0
	Total	120	100,0	100,0	



Interpretación: El 8,33% de las personas encuestadas menciona que es muy malo, mientras que el 46,67% es malo, el 44,50% es regular, y el 2,50% que consideran bueno la precisión de sus datos personales que ofrece la municipalidad.

P16. ¿Cómo calificaría la precisión de sus datos a través del tiempo ofrecidos por la municipalidad?

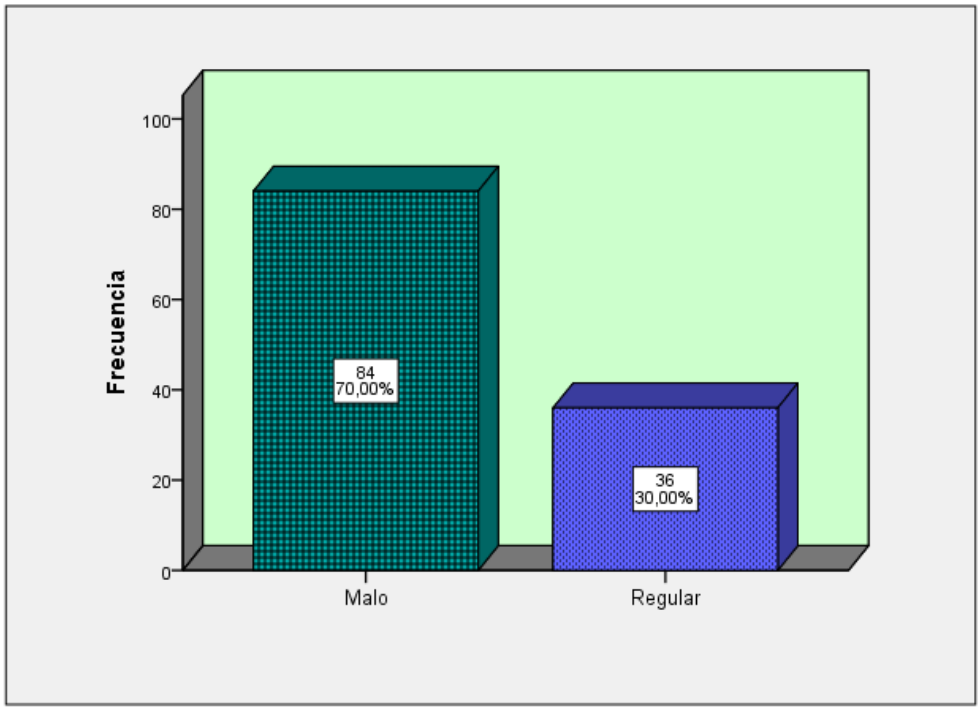
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	13	10,8	10,8	10,8
	Malo	61	50,8	50,8	61,7
	Regular	44	36,7	36,7	98,3
	Bueno	2	1,7	1,7	100,0
	Total	120	100,0	100,0	



Interpretación: El 10,83% de las personas encuestadas menciona que es muy malo, mientras que el 50,83% es malo, el 36,67% es regular, y el 1,67% que consideran bueno la precisión de sus datos a través del tiempo ofrecidos por la municipalidad.

P17. ¿Cómo calificaría los permisos de los usuarios con respecto a su limitación para acceder a su información?

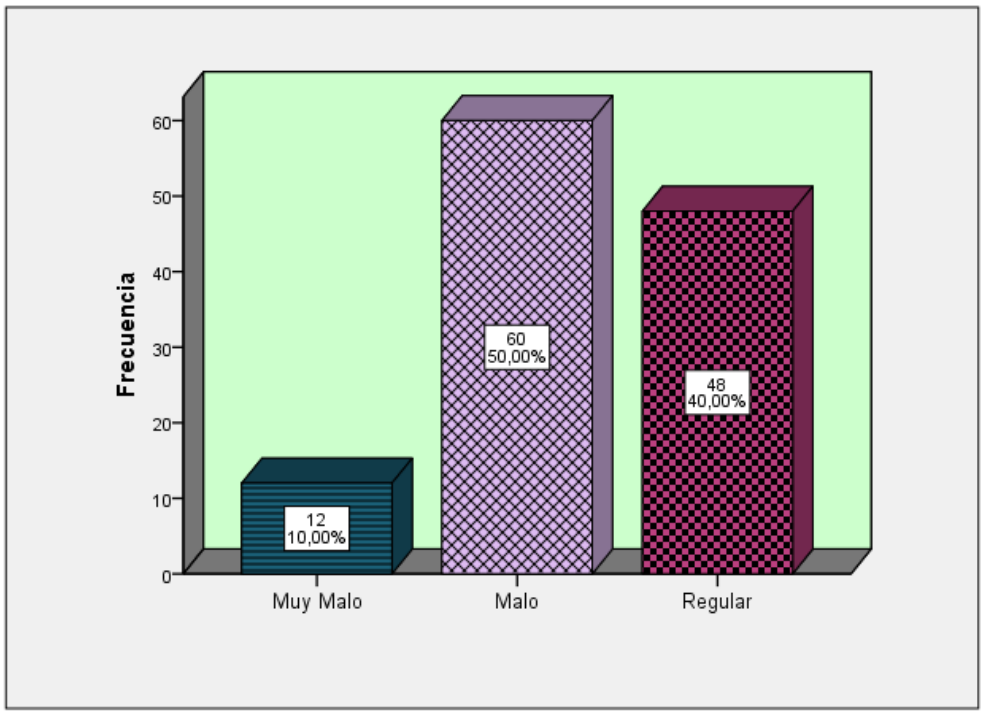
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo				
	Malo	84	70,0	70,0	70,0
	Regular	36	30,0	30,0	100,0
	Bueno				
	Total	120	100,0	100,0	



Interpretación: El 70,00% de las personas encuestadas menciona que es malo, mientras que el 30,00% consideran regular los permisos de los usuarios con respecto a su limitación para acceder a su información.

P18. ¿Cómo calificaría la Gestión de cambios para asegurar la integridad de los procesos en la municipalidad?

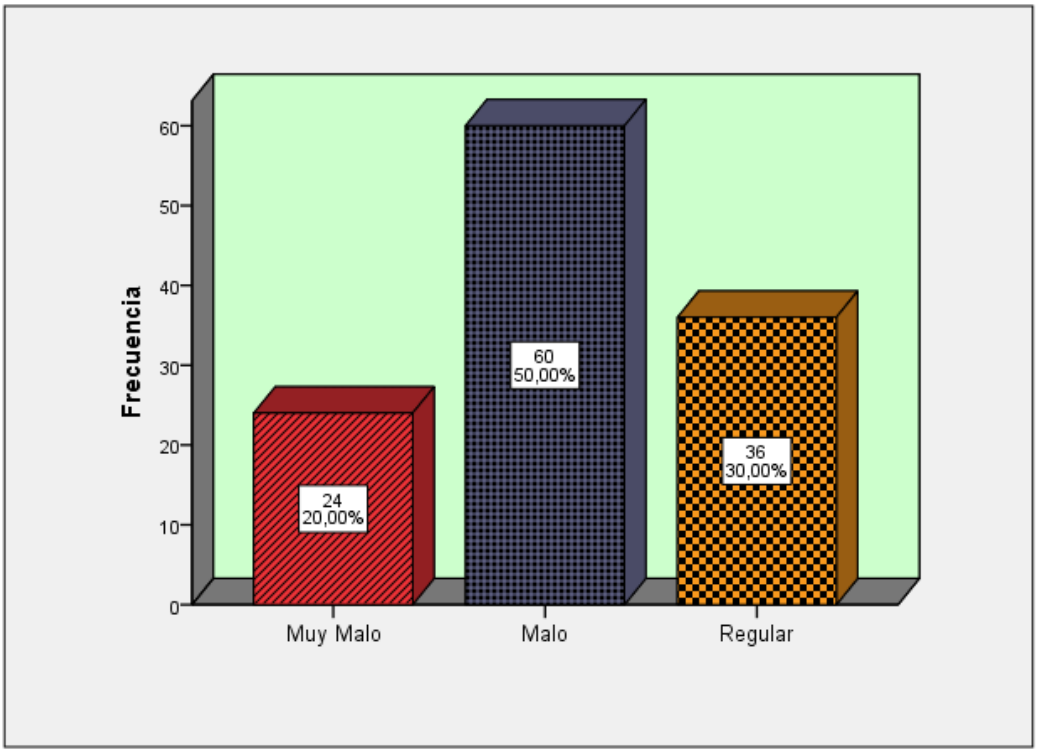
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	12	10,0	10,0	10,0
	Malo	60	50,0	50,0	60,0
	Regular	48	40,0	40,0	100,0
	Bueno				
	Total	120	100,0	100,0	



Interpretación: El 10,00% de las personas encuestas menciona que es muy malo, mientras que el 50,00% es muy malo y el 40,00% lo consideran regular la gestión de cambios para asegurar la integridad de los procesos en la municipalidad.

P19. ¿Cómo calificaría la funcionalidad de los dispositivos de red, equipos de TI y nuestras aplicaciones para acceder a la información de la municipalidad?

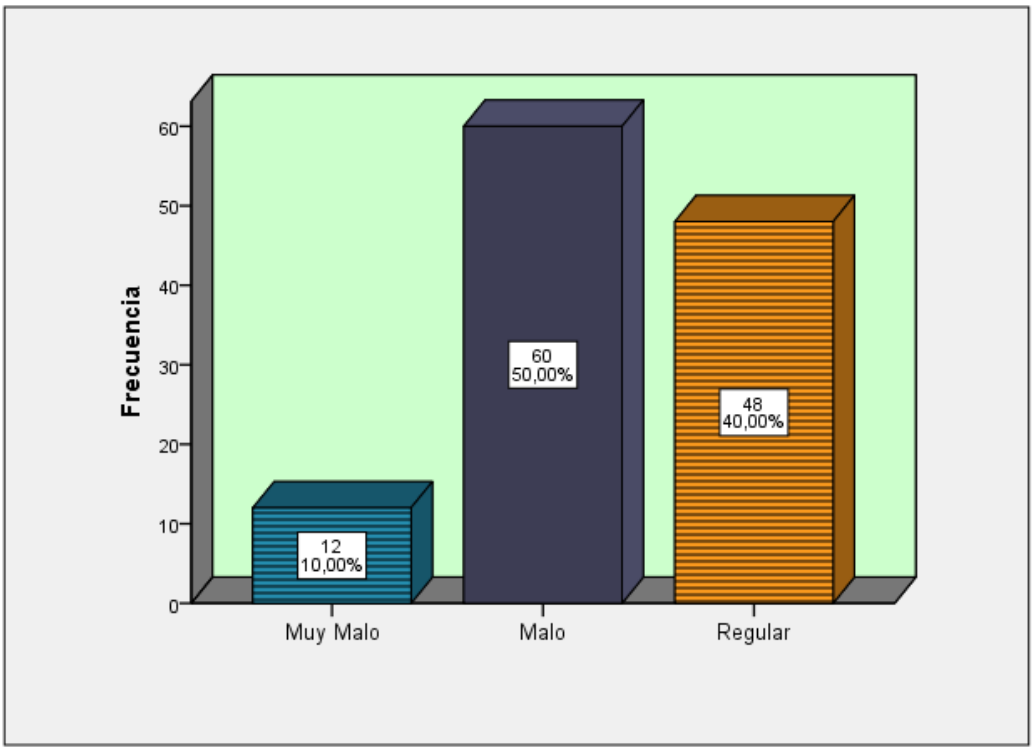
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	24	20,0	20,0	20,0
	Malo	60	50,0	50,0	70,0
	Regular	36	30,0	30,0	100,0
	Bueno				
	Total	120	100,0	100,0	



Interpretación: El 20,00% de las personas encuestas menciona que es muy malo, mientras que el 50,00% es muy malo y el 30,00% lo consideran regular la funcionalidad de los dispositivos de red, equipos de TI y nuestras aplicaciones para acceder a la información de la municipalidad.

P20. ¿Cómo calificaría la rapidez en el proceso de actualización de sus datos personales que les ofrece la municipalidad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Muy Malo	12	10,0	10,0	10,0
	Malo	60	50,0	50,0	60,0
	Regular	48	40,0	40,0	100,0
	Bueno				
	Total	120	100,0	100,0	

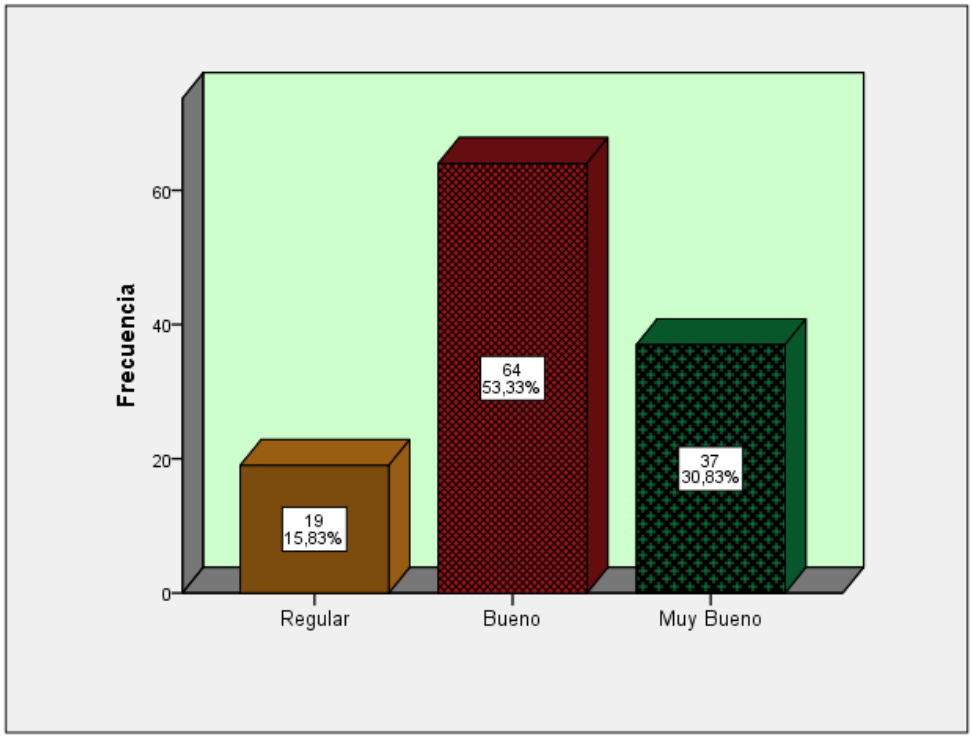


Interpretación: El 10,00% de las personas encuestas menciona que es muy malo, mientras que el 50,00% es muy malo y el 40,00% lo consideran regular la rapidez en el proceso de actualización de sus datos personales que les ofrece la municipalidad.

5.2. Resultados de la investigación Post-Test

P1. ¿Cómo calificaría la el nivel de disponibilidad de los datos e información en el sistema en la actualidad?

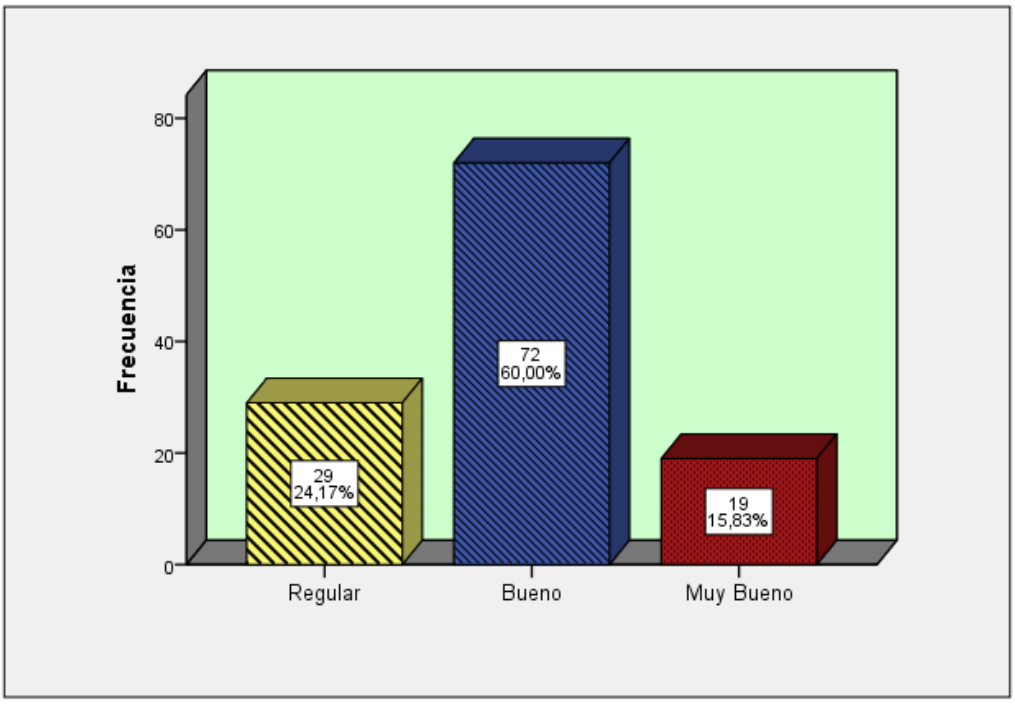
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	19	15,8	15,8	15,8
	Bueno	64	53,3	53,3	69,2
	Muy Bueno	37	30,8	30,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 15,83% de las personas encuestadas menciona que es regular, mientras que el 53,33% es bueno, y el 30,83% que consideran muy bueno la disponibilidad de la información en el sistema actual.

P2. ¿Cómo **calificaría el desempeño, funcionalidad del sistema informático que se está aplicando para los procesos administrativos de atención al público??**

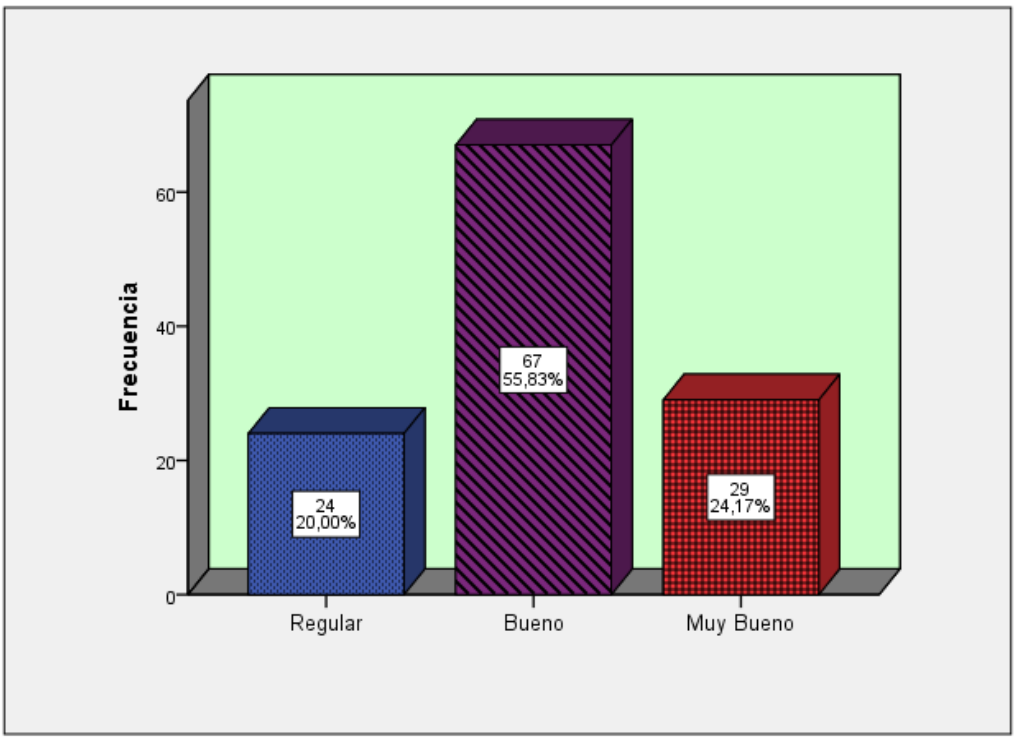
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	29	24,2	24,2	24,2
	Bueno	72	60,0	60,0	84,2
	Muy Bueno	19	15,8	15,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 24,17% de las personas encuestadas menciona que es regular, mientras que el 60,00% es bueno, y el 15,83% que consideran muy bueno el actual desempeño y funcionalidad del sistema.

P3. ¿Cómo califica la forma como el personal de la Municipalidad accede a la información de sus servidores?

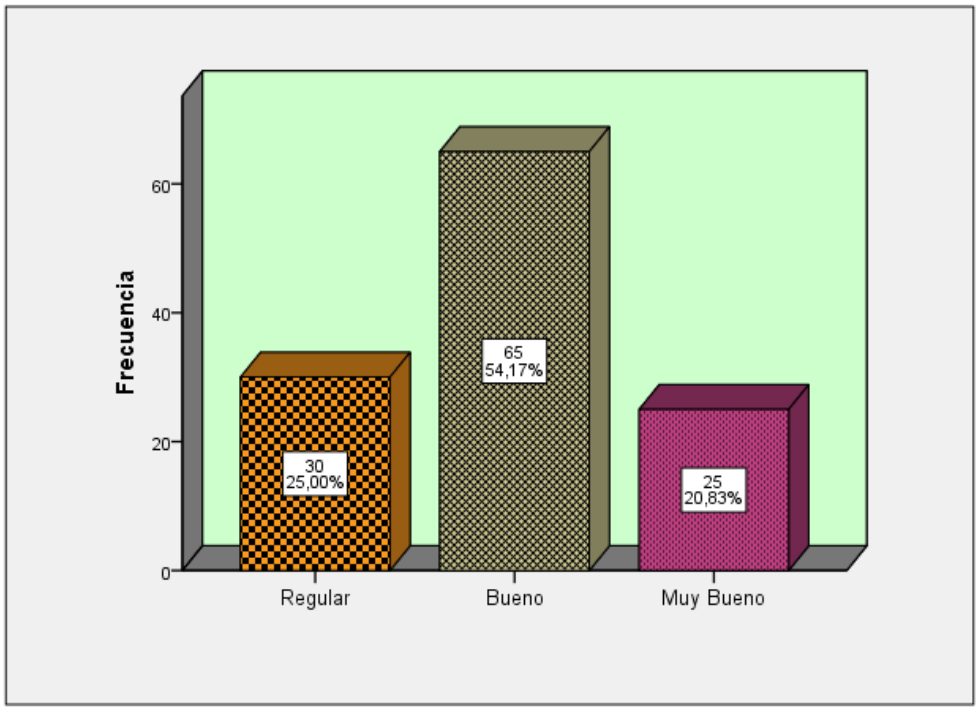
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	24	20,0	20,0	20,0
	Bueno	67	55,8	55,8	75,8
	Muy Bueno	29	24,2	24,2	100,0
	Total	120	100,0	100,0	



Interpretación: El 20,00% de las personas encuestadas menciona que es regular, mientras que el 55,83% es bueno, y el 24,17% que consideran muy bueno la forma como el personal de la municipalidad accede a la información de sus servidores

P4. ¿Cómo calificaría el nivel de frecuencia con la que solicita la revisión de su PC frente a cualquier inconveniente?

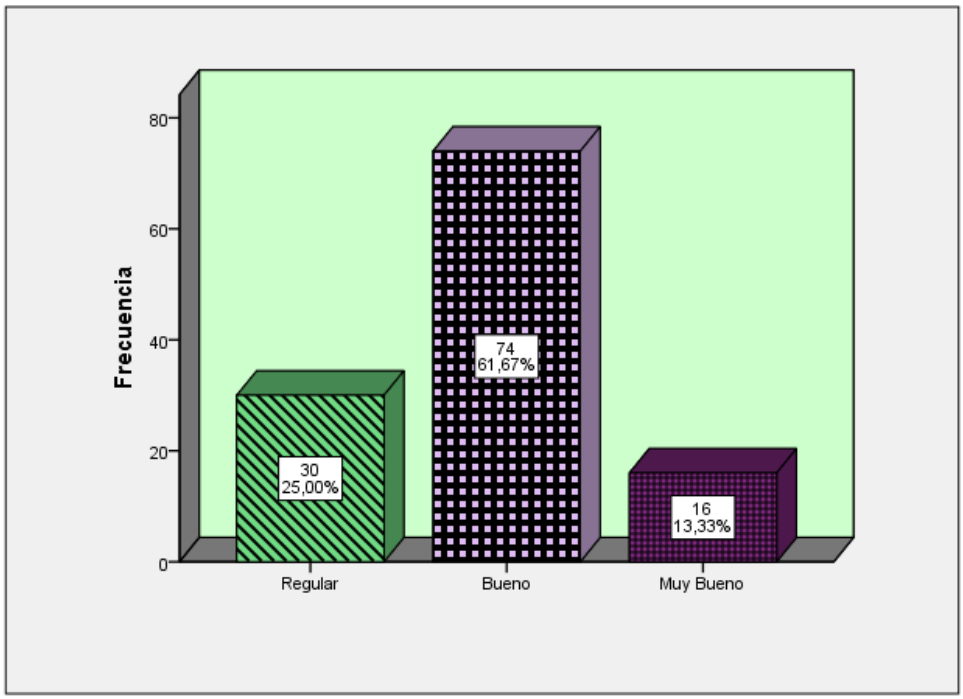
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	30	25,0	25,0	25,0
	Bueno	65	54,2	54,2	79,2
	Muy Bueno	25	20,8	20,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 25,00% de las personas encuestadas menciona que es regular, mientras que el 54,17% es bueno, y el 20,83% que consideran muy bueno la solicitud de frecuencia que le revisen su PC frente a cualquier falla.

P5. ¿Cómo califica el tipo de servicio recibido por los usuarios al consultar por una solicitud?

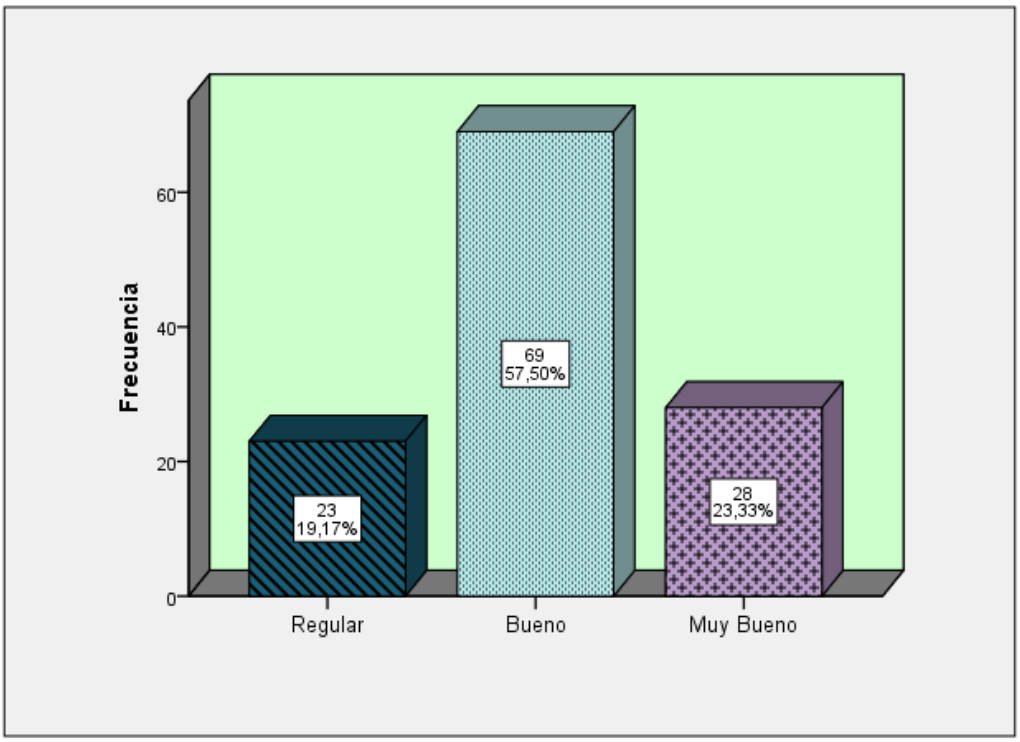
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	30	25,0	25,0	25,0
	Bueno	74	61,7	61,7	86,7
	Muy Bueno	16	13,3	13,3	100,0
	Total	120	100,0	100,0	



Interpretación: El 25,00% de las personas encuestadas menciona que es regular, mientras que el 61,67% es bueno, y el 13,33% que consideran muy bueno el tipo de servicio que reciben usuarios al realizar una consulta respecto a su solicitud.

P6. ¿Cómo calificaría si la municipalidad cumple con los objetivos de seguridad de información?

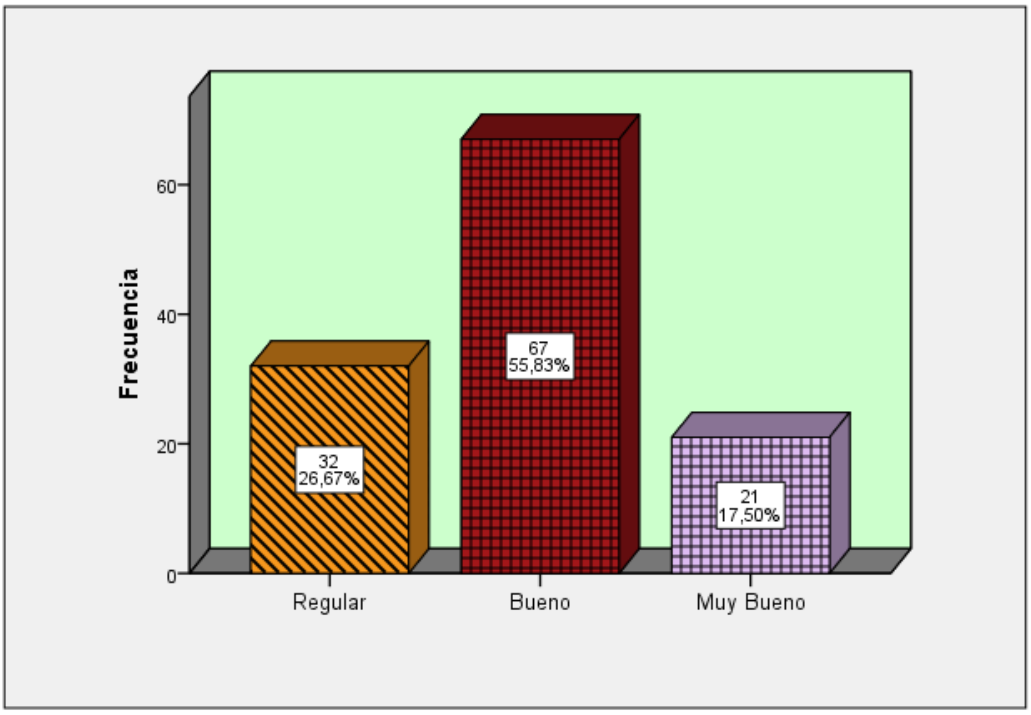
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	23	19,2	19,2	19,2
	Bueno	69	57,5	57,5	76,7
	Muy Bueno	28	23,3	23,3	100,0
	Total	120	100,0	100,0	



Interpretación: El 19,17% de las personas encuestadas menciona que es regular, mientras que el 57,50% es bueno, y el 23,33% que consideran muy bueno como cumple la municipalidad con los objetivos de seguridad de la información.

P7. ¿Como calificaría a las herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identificación de los riesgos en la municipalidad?

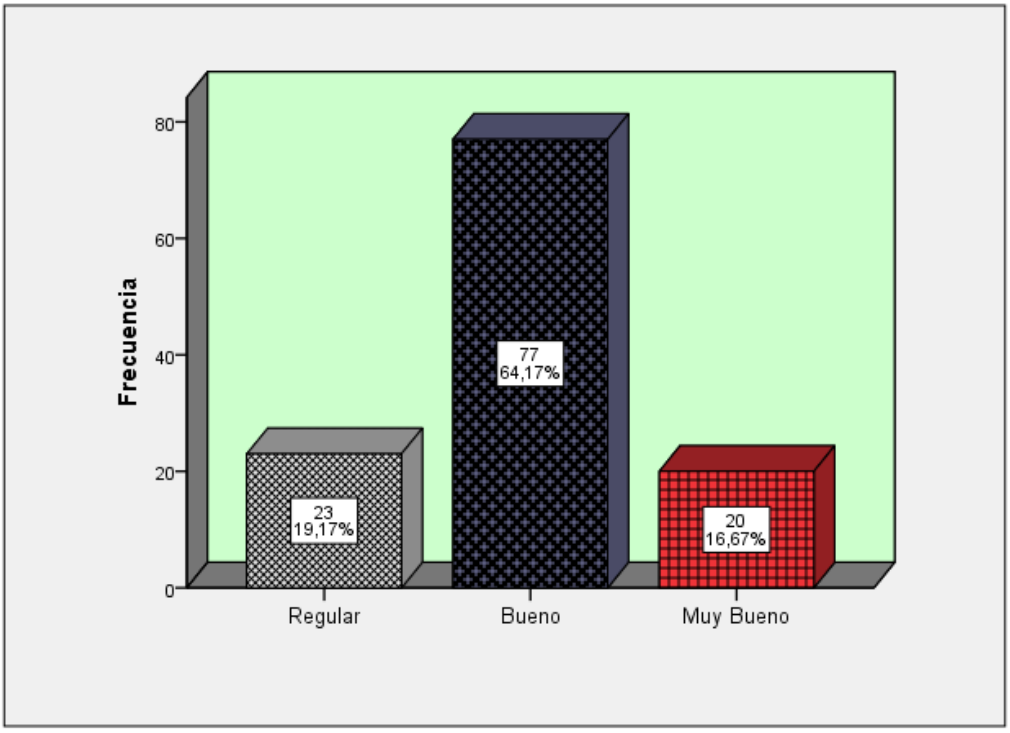
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	32	26,7	26,7	26,7
	Bueno	67	55,8	55,8	82,5
	Muy Bueno	21	17,5	17,5	100,0
	Total	120	100,0	100,0	



Interpretación: El 26,67% de las personas encuestadas menciona que es regular, mientras que el 55,83% es bueno, y el 17,50% que consideran muy bueno las herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identificación de los riesgos de la municipalidad.

P8. ¿Cómo calificaría Ud. el proceso de seguimiento de los trámites que se presentan y se generan durante una consulta de los usuarios?

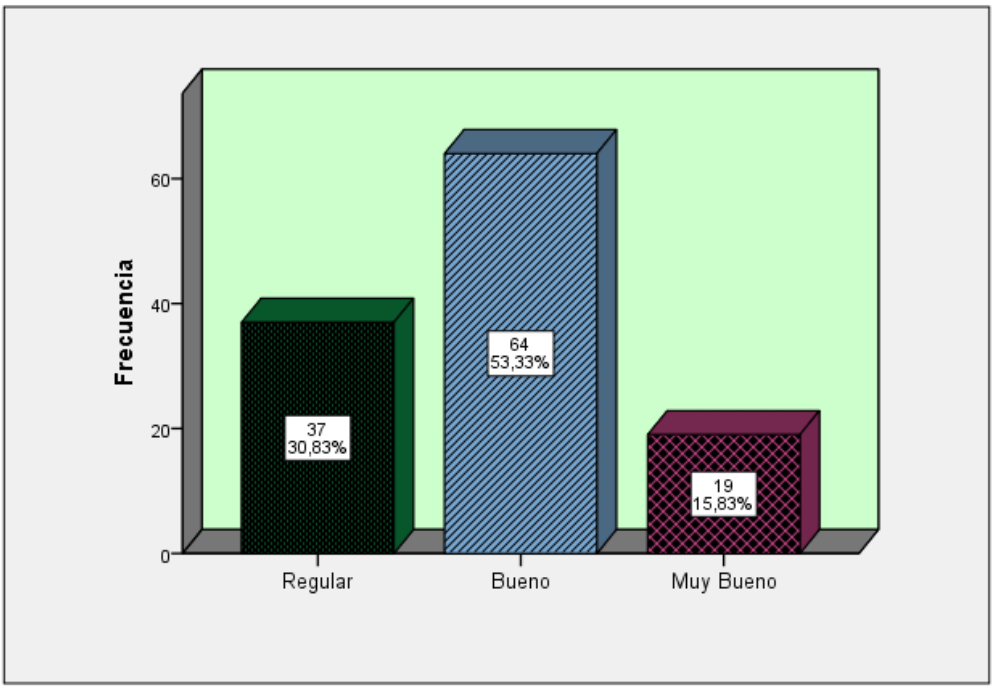
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	23	19,2	19,2	19,2
	Bueno	77	64,2	64,2	83,3
	Muy Bueno	20	16,7	16,7	100,0
	Total	120	100,0	100,0	



Interpretación: El 19,17% de las personas encuestadas menciona que es regular, mientras que el 64,17% es bueno, y el 16,67% que consideran muy bueno el proceso de seguimiento de los tramites que se presentan y se generan durante una consulta de los usuarios.

P9. ¿Cómo calificaría al actual desempeño, funcionalidad del sistema informático que se aplica en los procesos administrativos de la municipalidad?

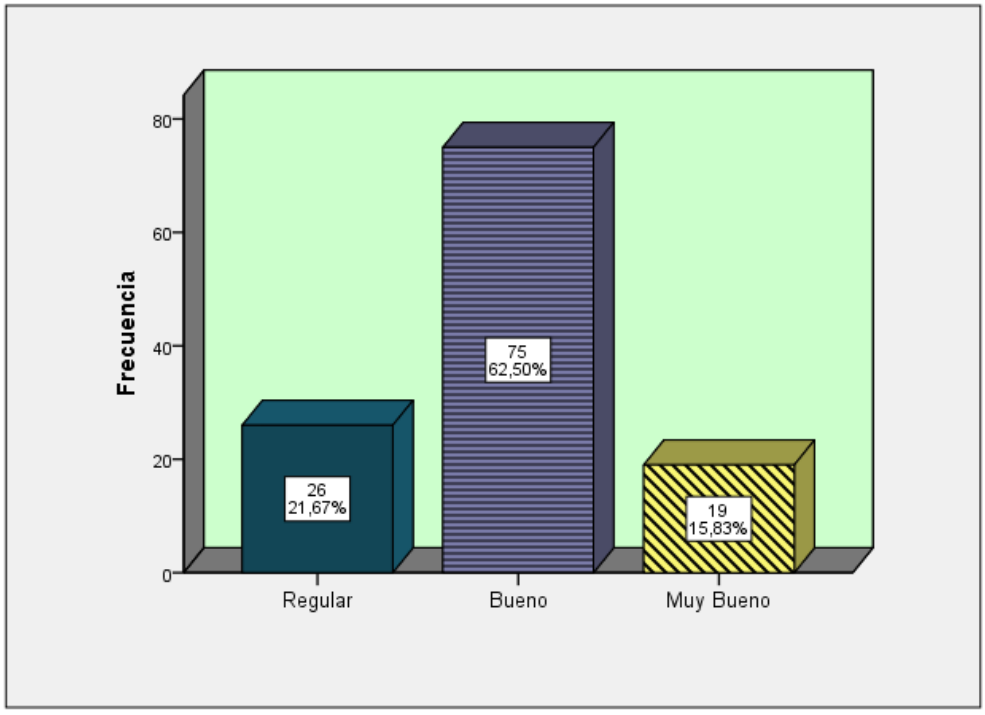
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	37	30,8	30,8	30,8
	Bueno	64	53,3	53,3	84,2
	Muy Bueno	19	15,8	15,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 30,83% de las personas encuestas menciona que es regular, mientras que el 53,33% es bueno y el 15,83% lo consideran muy bueno al actual desempeño y funcionalidad del sistema de trabajo o sistema informático que se aplica en los procesos administrativos de la municipalidad.

P10. ¿Cómo calificaría las respuestas del sistema a tiempo cuando se detecta alguna amenaza contra la seguridad de la información en la municipalidad?

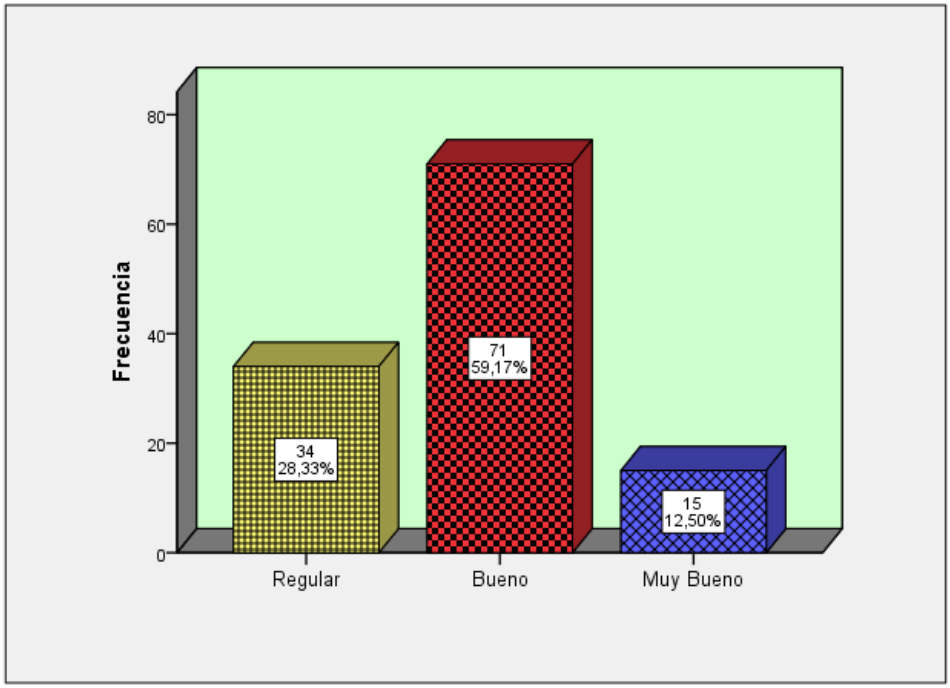
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	26	21,7	21,7	21,7
	Bueno	75	62,5	62,5	84,2
	Muy Bueno	19	15,8	15,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 21,67% de las personas encuestadas menciona que es regular, mientras que el 62,50% es bueno, y el 15,83% que consideran muy bueno las respuestas del sistema a tiempo cuando se detecta alguna amenaza contra la seguridad de la información en la municipalidad.

P11. ¿Cómo calificaría el hecho que solo el personal de la municipalidad debe contar con la autorización necesaria para acceder a sus datos personales?

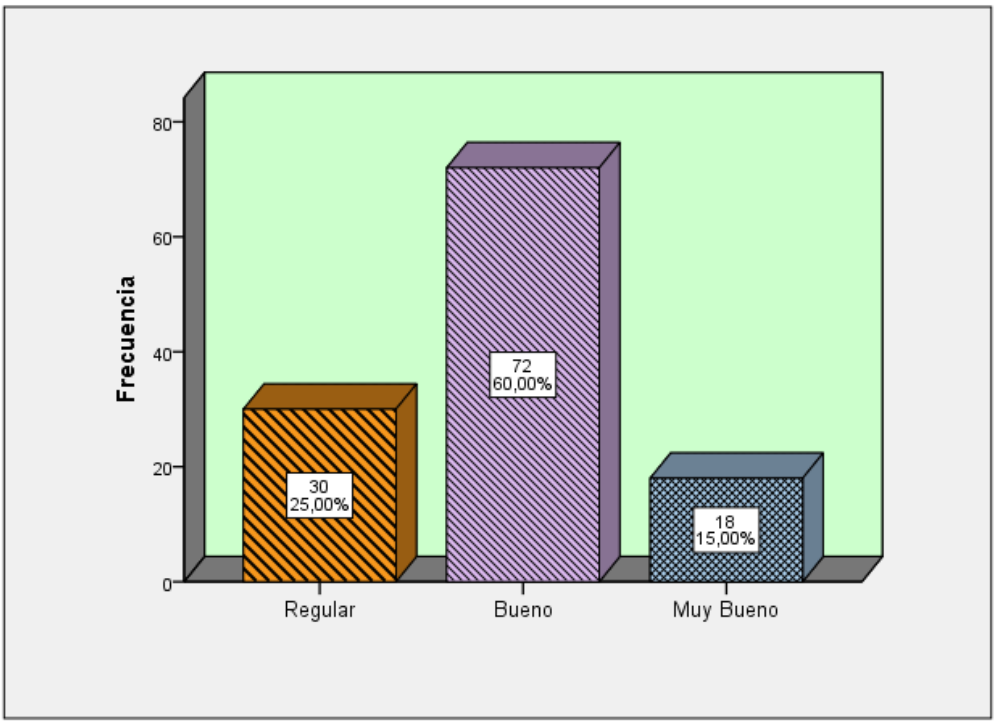
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	34	28,3	28,3	28,3
	Bueno	71	59,2	59,2	87,5
	Muy Bueno	15	12,5	12,5	100,0
	Total	120	100,0	100,0	



Interpretación: El 28,33% de las personas encuestadas menciona que es regular, mientras que el 59,17% es bueno, y el 12,50% que consideran muy bueno el hecho que solo el personal de la municipalidad deba contar con la autorización necesaria para acceder a sus datos personales.

P12. ¿Cómo calificaría la frecuencia en el transito virtual de sus datos personales en la municipalidad?

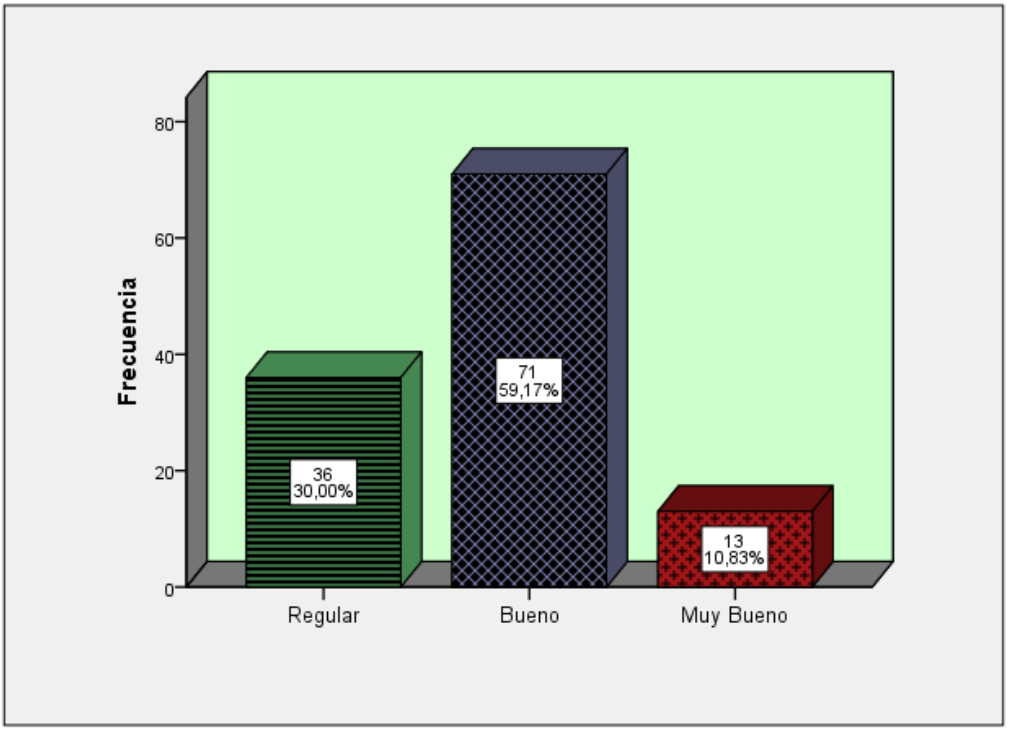
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	30	25,0	25,0	25,0
	Bueno	72	60,0	60,0	85,0
	Muy Bueno	18	15,0	15,0	100,0
	Total	120	100,0	100,0	



Interpretación: El 25,00% de las personas encuestadas menciona que es regular, mientras que el 60,00% es bueno, y el 15,00% que consideran muy bueno la frecuencia en el transito virtual de sus datos personales en la municipalidad.

P13. ¿Cómo calificaría el hecho que solo el personal autorizado pueda acceder a su información personal?

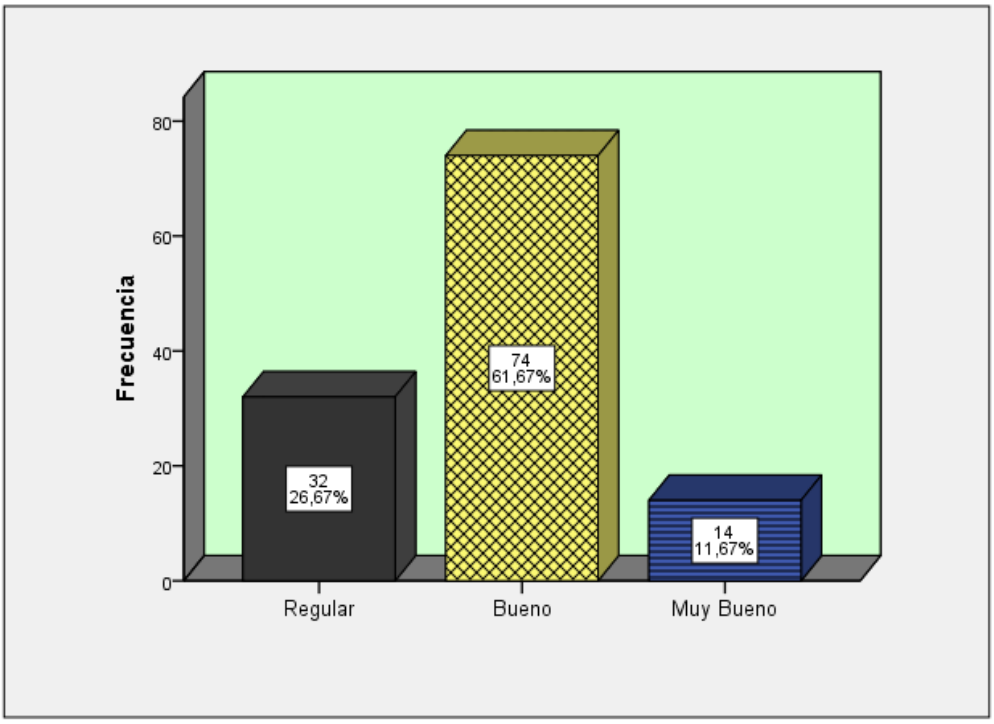
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	36	30,0	30,0	30,0
	Bueno	71	59,2	59,2	89,2
	Muy Bueno	13	10,8	10,8	100,0
	Total	120	100,0	100,0	



Interpretación: El 30,00% de las personas encuestadas menciona que es regular, mientras que el 59,17% es bueno, y el 10,83% que consideran muy bueno el hecho que solo el personal autorizado pueda acceder a su información personal.

P14. ¿Cómo calificaría la seguridad en el tránsito virtual de sus datos personales en la municipalidad?

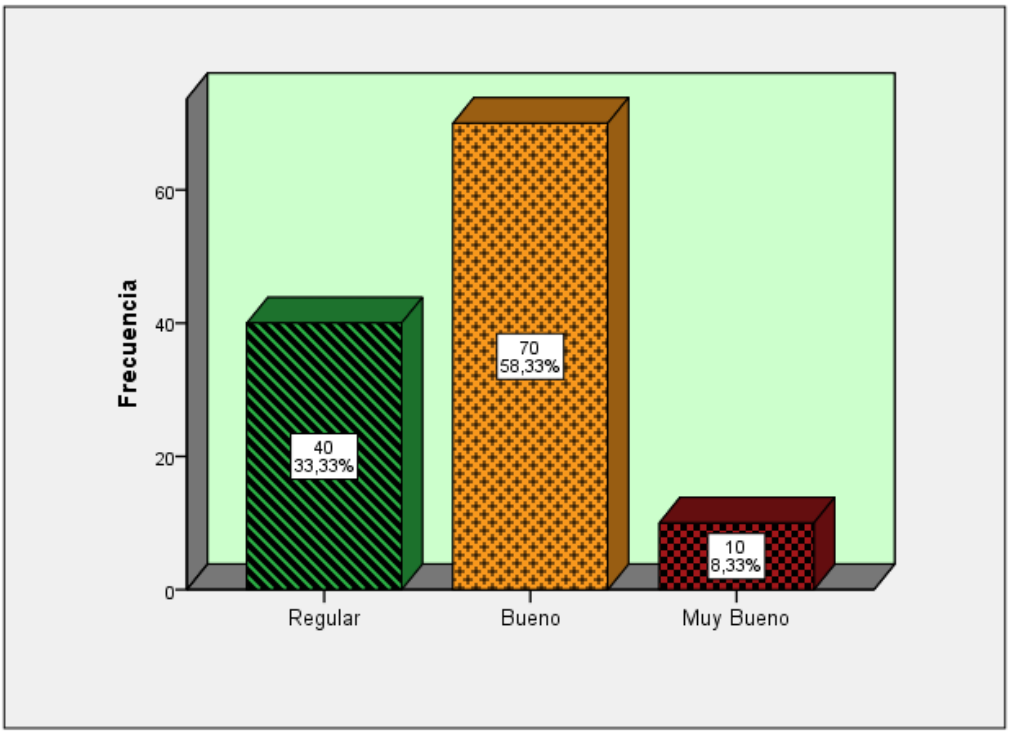
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	32	26,7	26,7	26,7
	Bueno	74	61,7	61,7	88,3
	Muy Bueno	14	11,7	11,7	100,0
	Total	120	100,0	100,0	



Interpretación: El 26,67% de las personas encuestadas menciona que es regular, mientras que el 61,67% es bueno, y el 11,67% que consideran muy bueno la seguridad en el transito virtual de sus datos personales de la municipalidad.

P15. ¿Cómo calificaría la precisión de sus datos personales que ofrece la municipalidad?

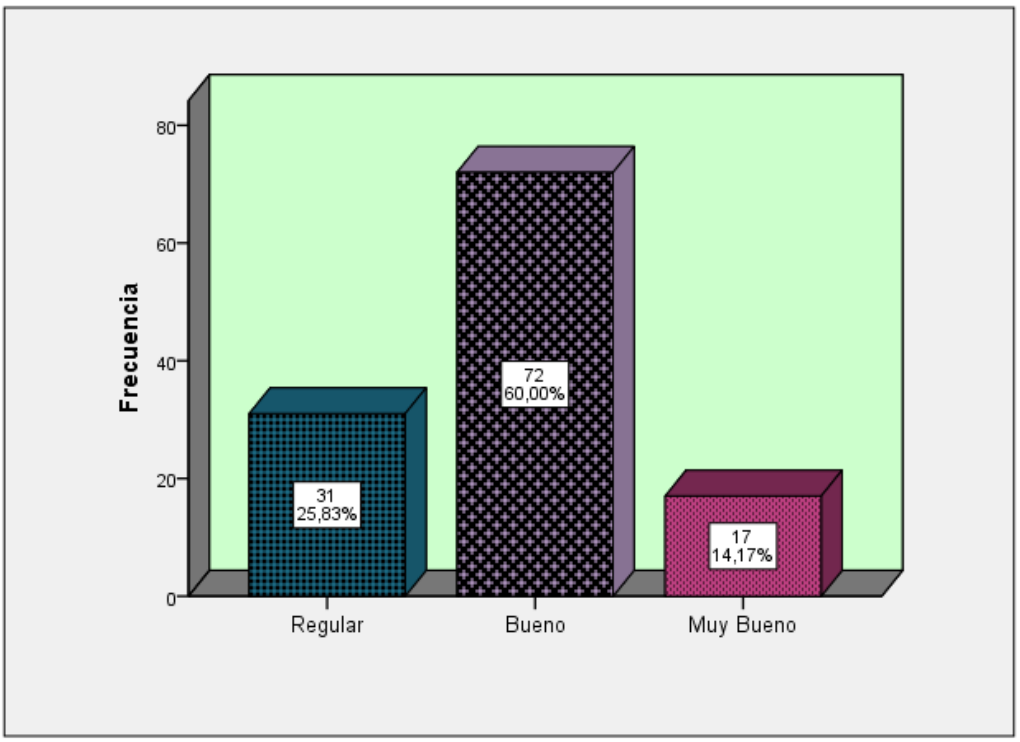
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	40	33,3	33,3	33,3
	Bueno	70	58,3	58,3	91,7
	Muy Bueno	10	8,3	8,3	100,0
	Total	120	100,0	100,0	



Interpretación: El 33,33% de las personas encuestadas menciona que es regular, mientras que el 58,33% es bueno, y el 8,33% que consideran muy bueno la precisión de sus datos personales que ofrece la municipalidad.

P16. ¿Cómo calificaría la precisión de sus datos a través del tiempo ofrecidos por la municipalidad?

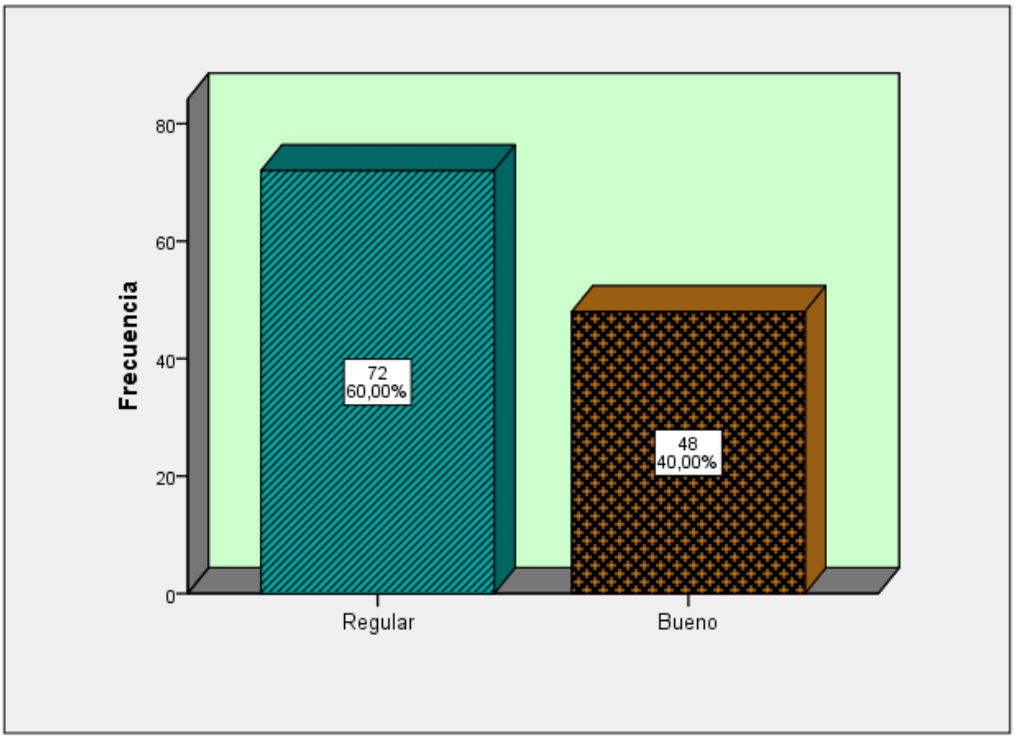
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	31	25,8	25,8	25,8
	Bueno	72	60,0	60,0	85,8
	Muy Bueno	17	14,2	14,2	100,0
	Total	120	100,0	100,0	



Interpretación: El 25,83% de las personas encuestadas menciona que es regular, mientras que el 60,00% es bueno, y el 14,17% que consideran muy bueno la precisión de sus datos a través del tiempo ofrecidos por la municipalidad.

P17. ¿Cómo calificaría los permisos de los usuarios con respecto a su limitación para acceder a su información?

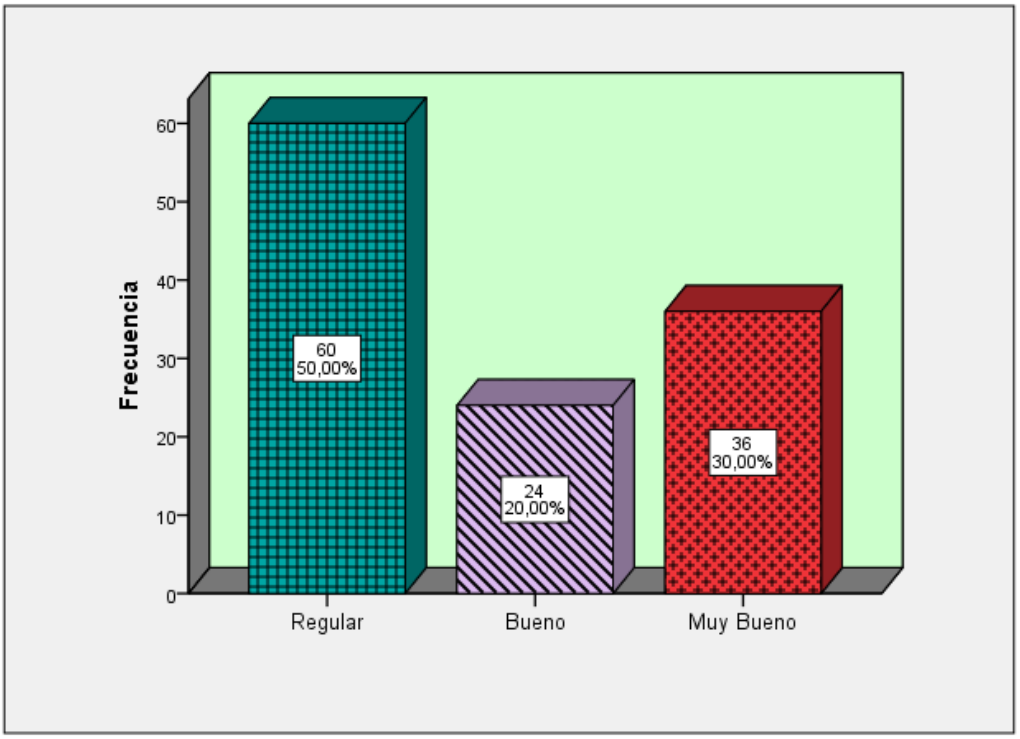
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	72	60,0	60,0	60,0
	Bueno	48	40,0	40,0	100,0
	Total	120	100,0	100,0	



Interpretación: El 60,00% de las personas encuestadas menciona que es regular, mientras que el 40,00% consideran bueno los permisos de los usuarios con respecto a su limitación para acceder a su información.

P18. ¿Cómo calificaría la Gestión de cambios para asegurar la integridad de los procesos en la municipalidad?

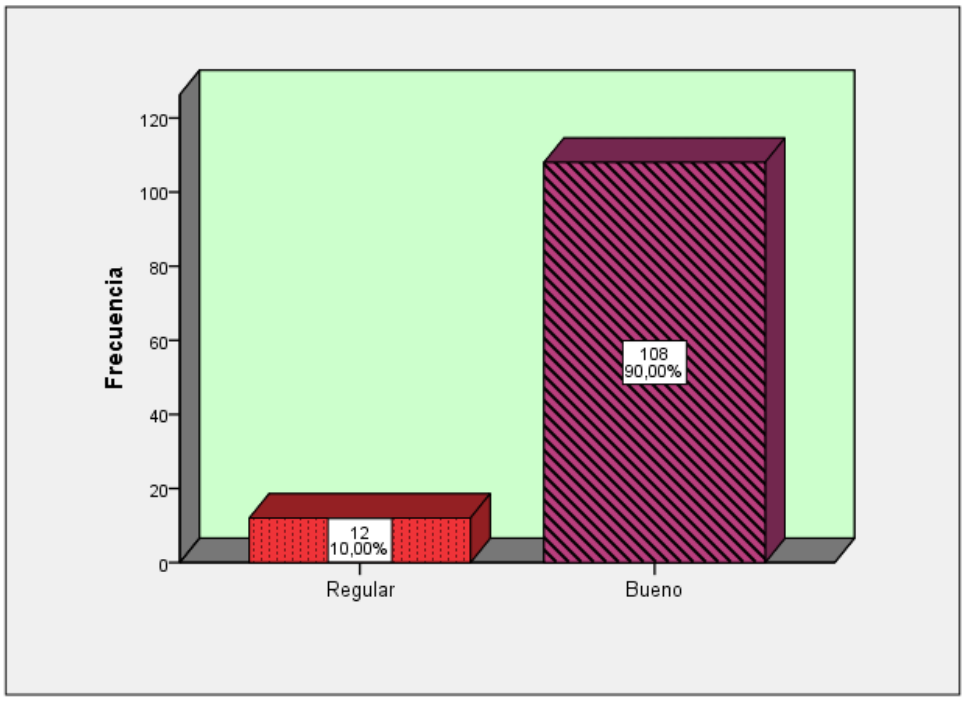
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	60	50,0	50,0	50,0
	Bueno	24	20,0	20,0	70,0
	Muy Bueno	36	30,0	30,0	100,0
	Total	120	100,0	100,0	



Interpretación: El 50,00% de las personas encuestas menciona que es regular, mientras que el 20,00% es bueno y el 30,00% lo consideran muy bueno la gestión de cambios para asegurar la integridad de los procesos en la municipalidad.

P19. ¿Cómo calificaría la funcionalidad de los dispositivos de red, equipos de TI y nuestras aplicaciones para acceder a la información de la municipalidad?

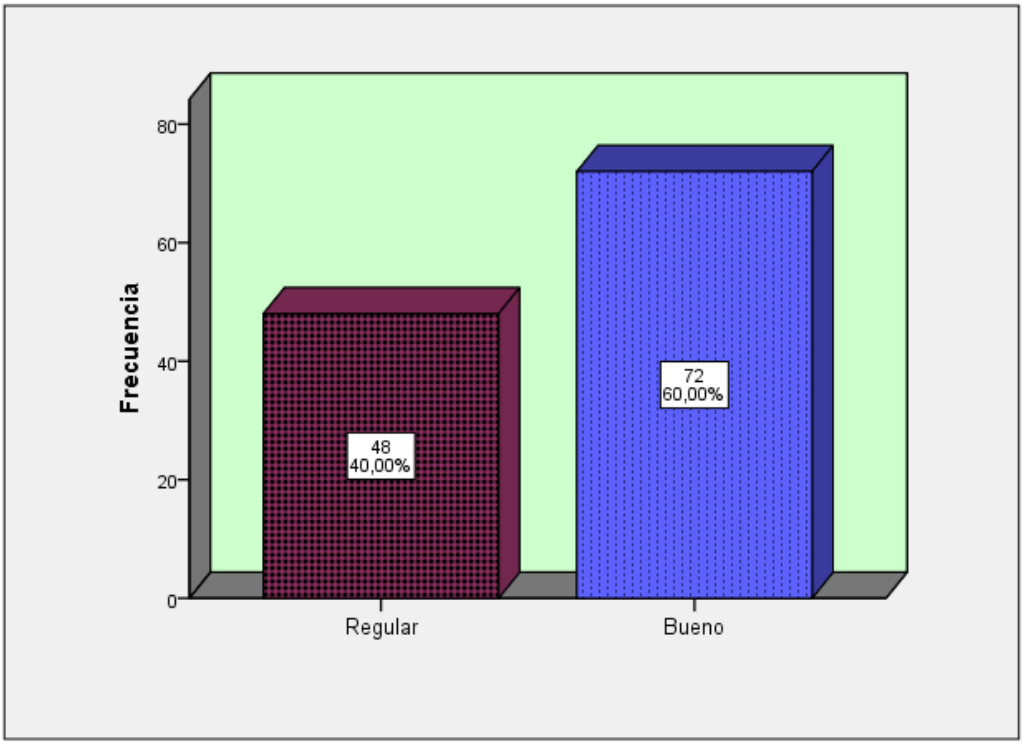
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	12	10,0	10,0	10,0
	Bueno	108	90,0	90,0	100,0
	Total	120	100,0	100,0	



Interpretación: El 10,00% de las personas encuestas menciona que es regular, y el 90,00% lo consideran bueno la funcionalidad de los dispositivos de red, equipos de TI y nuestras aplicaciones para acceder a la información de la municipalidad.

P20. ¿Cómo calificaría la rapidez en el proceso de actualización de sus datos personales que les ofrece la municipalidad?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válidos	Regular	48	40,0	40,0	40,0
	Bueno	72	60,0	60,0	100,0
	Total	120	100,0	100,0	



Interpretación: El 40,00% de las personas encuestas menciona que es regular, y el 60,00% lo consideran bueno la rapidez en el proceso de actualización de sus datos personales que les ofrece la municipalidad.

5.3. Prueba de hipótesis

5.3.1. Prueba de Normalidad

De acuerdo a la información y al ser la muestra una cantidad mayor que 50, aplicaremos **Kolmogorov-Smirnov** para comprobar el cumplimiento con la prueba de normalidad nuestras variables en estudio.

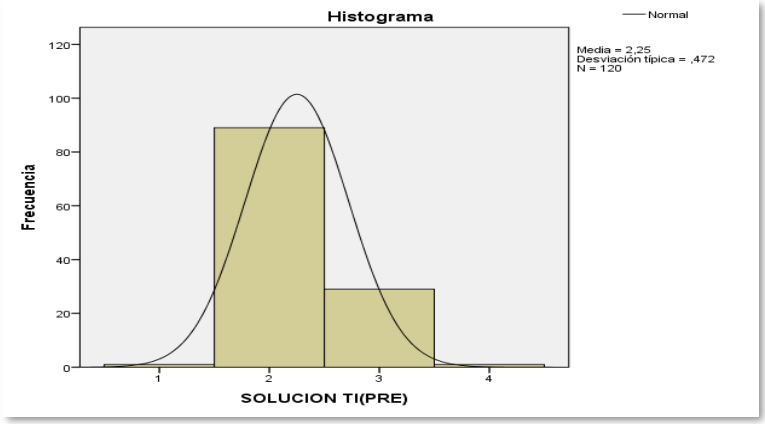
Resumen del procesamiento de los casos

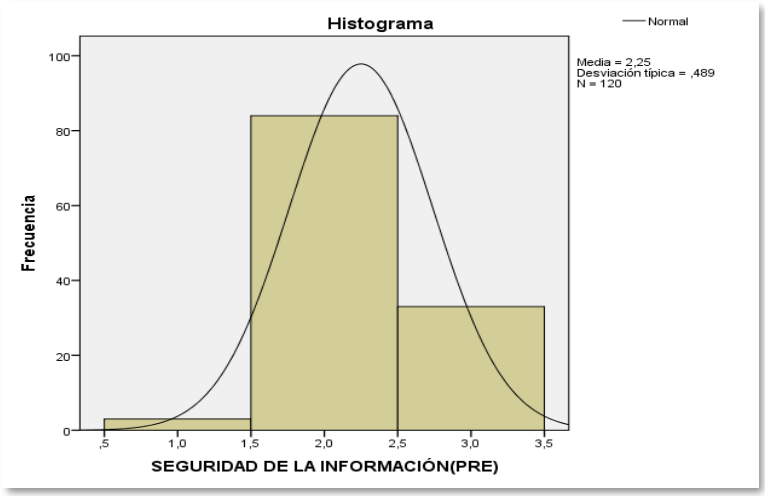
	Casos					
	Válidos		Perdidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
Solución TI (pre)	120	100,0%	0	0,0%	120	100,0%
Seguridad de la información (Pre)	120	100,0%	0	0,0%	120	100,0%

Pruebas de normalidad

	Kolmogorov, Smirnov[a]			Shapiro Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
Solución TI(Pre)	,452	120	,000	,601	120	,000
Seguridad de la Información (Pre)	,420	120	,000	,648	120	,000

a. Corrección de la significación de Lilliefors





Como podemos observar la gráfica de la Prueba de Normalidad el Sig. en ambos casos es < 0,05, por lo que podemos afirmar que nuestras variables de estudio no están normalmente distribuidas; por lo que, se debe aplicar una prueba no paramétrica en el desarrollo del de la investigación.

Para las pruebas de verificación de las hipótesis aplicaremos la prueba estadística de Wilcoxon, debido a que los resultados de la prueba de normalidad corresponden al tipo no paramétricos y las muestras de estudio se presentan relacionadas, ya que buscamos determinar que la Solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

5.3.2. Establecer nivel de significancia

En nivel de confianza de 95%, hallaremos el valor de "Z" con el que vamos a trabajar. Para el valor de 95% se puede representar también como 0.95, por lo que, para determinad el valor de Alfa (α) se hace lo siguiente:

$\alpha=1 - 0.95$

$\alpha=0.05$

Una vez obtenido el valor de Alfa (α), continuamos con efectuar el cálculo de "Z" usando su fórmula:

$$Z = 1 - \frac{\propto}{2}$$

$$Z = 1 - \frac{0.05}{2}$$

$$Z = 0.975$$

Posterior de efectuar el cálculo de "Z", se ubicó el valor en la tabla estadística correspondiente a la distribución normal, obteniéndose como

resultado 1.96, por lo que se hará uso de este valor para encontrar las zonas de rechazo y aceptación.

5.3.3. Prueba de Hipótesis General

Hipótesis Nula

- H0: El análisis, diseño e implementación de una solución de TI NO mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Hipótesis Alterna

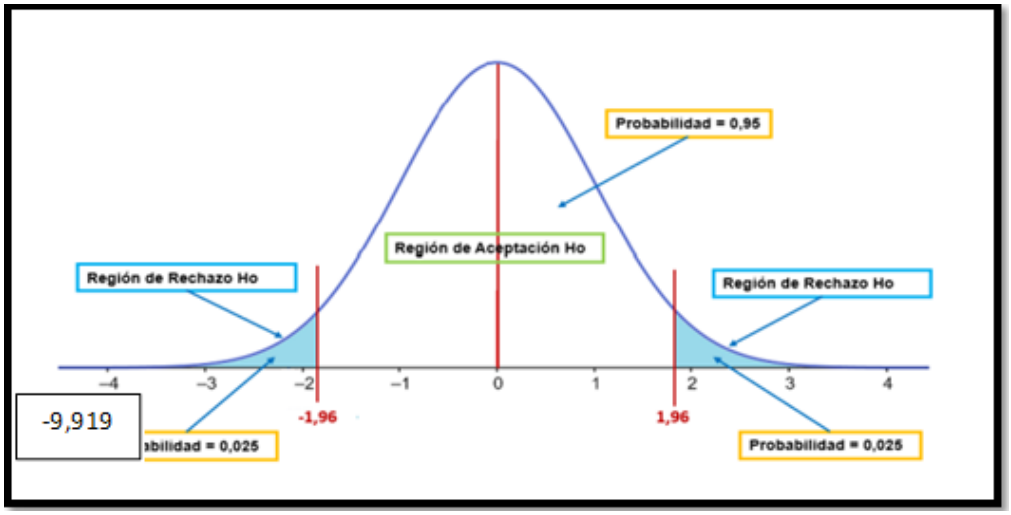
- H1: El análisis, diseño e implementación de una solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Estadísticos de contraste[a]

	POST_PRO.V1V2 - PRE_PRO.V1V2
Z	-9,919[b]
Sig. Asintóti. (bilateral)	,000

a. Prueba de los rangos realizado con signo de Wilcoxon

b. Basado en rangos negativos.



Interpretación: Como se observa, el valor de Sig. asintót. (bilateral) es 0.000 lo cual cumple con la condición de la prueba de Wilcoxon 0.000 < 0.05, así mismo en la campana de Gauss se observa que el valor Z es -9.919 encontrándose en la región de rechazo. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, afirmando que el análisis, diseño e implementación de una solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

5.3.4. Prueba de Hipótesis específicas

Hipótesis Específica 1

H0: El análisis actual de los servicios y recursos de TI NO mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

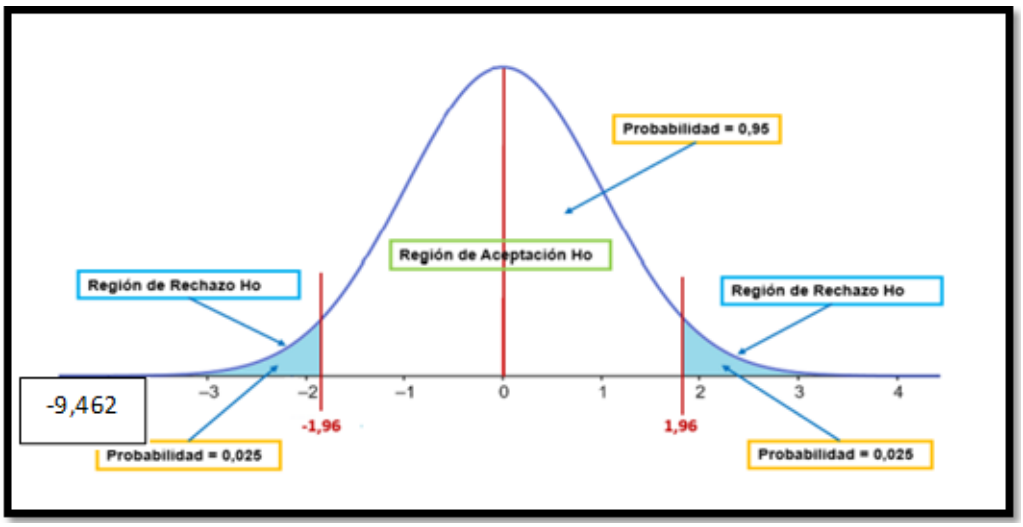
H1: El análisis actual, de los servicios y recursos, de TI mejora la seguridad de la información de la Municipalidad, Provincial de Ucayali Contamana.

Estadísticos de contraste[a]

	POST_PRO.V1D1 - PRE_PRO.V1D1
Z	-9,462[b]
Sig. Asintóti. (bilateral)	,000

a. Prueba de los rangos realizado con signo de Wilcoxon

b. Basado en rangos negativos.



Interpretación: Como se observa, el valor de Sig. asintót. (bilateral) es 0.000 lo cual cumple con la condición de la prueba de Wilcoxon 0.000 < 0.05, así mismo en la campana de Gauss se observa que el valor Z es -9.462 encontrándose en la región de rechazo. Por lo tanto, se rechazar la hipótesis nula y se aceptar la hipótesis alternativa, afirmando que el análisis actual de los servicios y recursos de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Hipótesis Específica 2

H0: El diseño de los recursos y servicios de TI NO mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

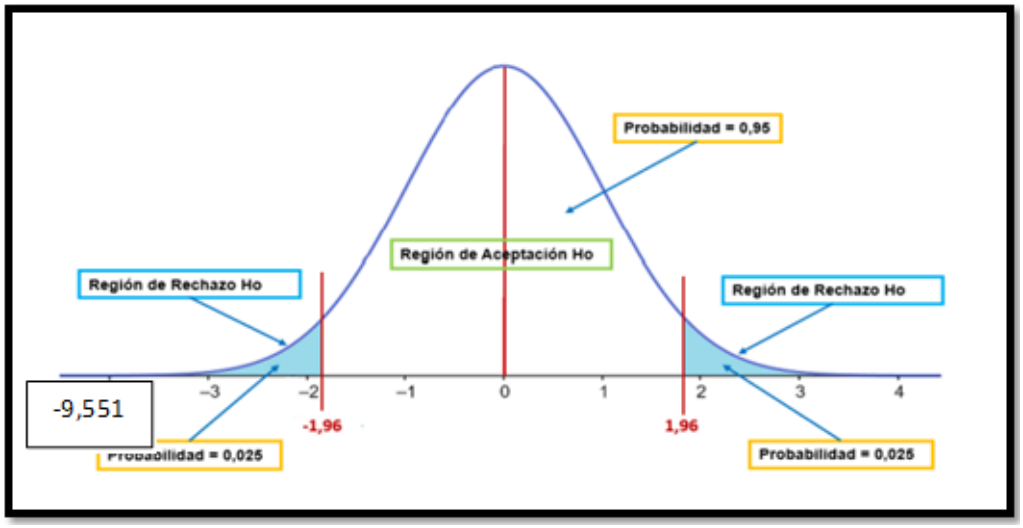
H1: El diseño de los recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Estadísticos de contraste[a]

	POST_PRO.V1D2 - PRE_PRO.V1D2
Z	-9,551[b]
Sig. Asintóti. (bilateral)	,000

a. Prueba de los rangos realizado con signo de Wilcoxon

b. Basado en rangos negativos.



Interpretación: Como se observa, el valor de Sig. asintót. (bilateral) es 0.000 lo cual cumple con la condición de la prueba de Wilcoxon 0.000 < 0.05, así mismo en la campana de Gauss se observa que el valor Z es -9.551 encontrándose en la región de rechazo. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, afirmando que el diseño de los recursos y

servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Hipótesis Específica 3

H0: La implementación de recursos y servicios de TI **NO** mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana

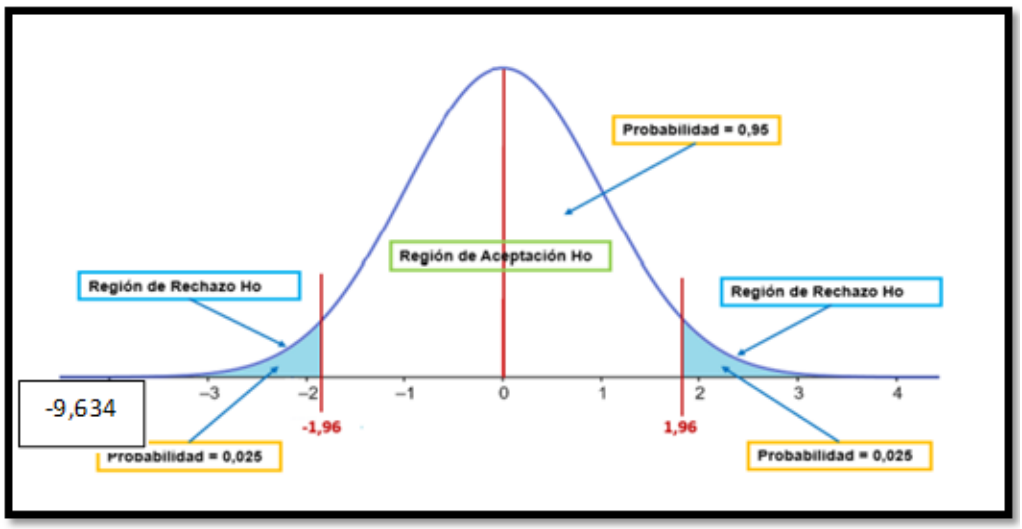
H1: La implementación de recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Estadísticos de contraste[a]

	POST_PRO.V1D3 - PRE_PRO.V1D3
Z	-9,634[b]
Sig. Asintóti. (bilateral)	,000

a. Prueba de los rangos realizado con signo de Wilcoxon

b. Basado en rangos negativos.



Interpretación: Como se observa, el valor de Sig. asintót. (bilateral) es 0.000 lo cual cumple con la condición de la prueba de Wilcoxon 0.000 < 0.05, así mismo en la campana de Gauss se observa que el valor Z es -9.634 encontrándose en la región de rechazo. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, afirmando que la implementación de recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Hipótesis Específica 4

H0: La evaluación de la conformidad de las implementaciones efectuadas indica la **NO** mejora seguridad de la información de la Municipalidad Provincial de Ucayali Contamana

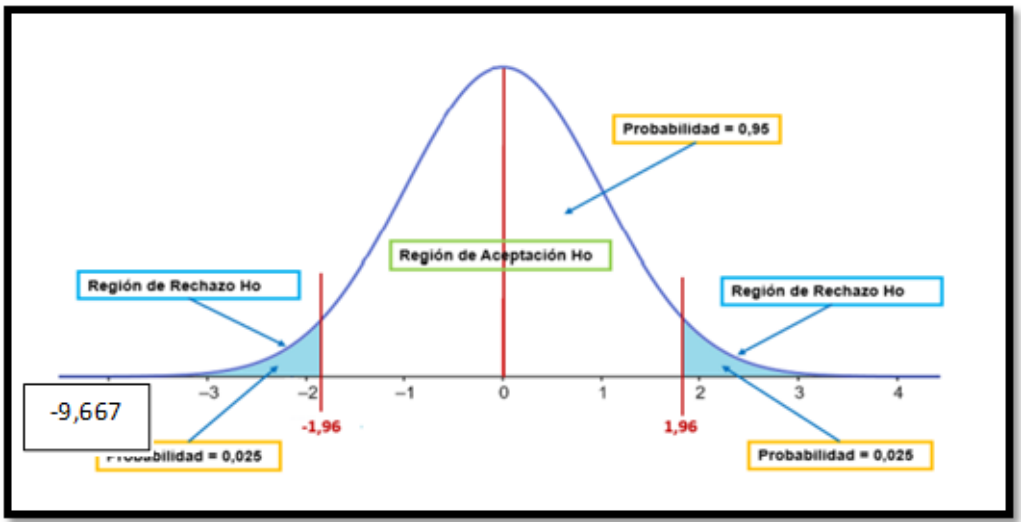
H1: La evaluación de la conformidad de las implementaciones efectuadas indica la mejora de la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

Estadísticos de contraste[a]

	POST_PRO.V1D4 - PRE_PRO.V1D4
Z	-9,667[b]
Sig. Asintóti. (bilateral)	,000

a. Prueba de los rangos realizado con signo de Wilcoxon

b. Basado en rangos negativos.



Interpretación: Como se observa, el valor de Sig. asintót. (bilateral) es 0.000 lo cual cumple con la condición de la prueba de Wilcoxon 0.000 < 0.05, así mismo en la campana de Gauss se observa que el valor Z es -9.667 encontrándose en la región de rechazo. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alternativa, afirmando que la evaluación de la conformidad de las implementaciones efectuadas indica la mejora de la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

CONCLUSIONES

Al término de la investigación se ha llegado a las siguientes conclusiones:

- El resultado de la variable independiente la solución de TI obtuvo un Sig. (Bilateral) de 0.000 en la prueba de Wilcoxon, cumpliendo así la condición de 0.000<0.05, además se pudo observar en nuestra campana de Gauss que el valor de "Z" es igual a -9,919, cayendo así en la región de rechazo, como consecuencia se rechaza la hipótesis nula, y, comprobándose así de esta manera la hipótesis general. Afirmando que el análisis, diseño e implementación de una solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
- El resultado de la dimensión análisis actual de los servicios y recursos de TI obtuvo un Sig. (Bilateral) de 0.000 en la prueba de Wilcoxon, cumpliendo así la condición de 0.000<0.05, además se pudo observar en nuestra campana de Gauss que el valor de "Z" es igual a -9,462, cayendo así en la región de rechazo, como consecuencia se rechaza la hipótesis nula, y, comprobándose así de esta manera la primera hipótesis específica. Afirmando que el análisis actual de los servicios y recursos de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
- El resultado de la dimensión el diseño de los recursos y servicios de TI obtuvo un Sig. (Bilateral) de 0.000 en la prueba de Wilcoxon, cumpliendo así la condición de 0.000<0.05, además se pudo observar en nuestra campana de Gauss que el valor de "Z" es igual a -9,551, cayendo así en la región de rechazo, como consecuencia se rechaza la hipótesis nula, y, comprobándose así de esta manera la segunda hipótesis específica. Afirmando que el diseño de los recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
- El resultado de la dimensión la implementación de recursos y servicios de TI obtuvo un Sig. (Bilateral) de 0.000 en la prueba de Wilcoxon, cumpliendo así la condición de

0.000<0.05, además se pudo observar en nuestra campana de Gauss que el valor de “Z” es igual a -9,634, cayendo así en la región de rechazo, como consecuencia se rechaza la hipótesis nula, y, comprobándose así de esta manera la tercera hipótesis específica. Afirmando que la implementación de recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

- El resultado de la dimensión de la evaluación de la conformidad de las implementaciones efectuadas obtuvo un Sig. (Bilateral) de 0.000 en la prueba de Wilcoxon, cumpliendo así la condición de 0.000<0.05, además se pudo observar en nuestra campana de Gauss que el valor de “Z” es igual a -9,667, cayendo así en la región de rechazo, como consecuencia se rechaza la hipótesis nula, y, comprobándose así de esta manera la cuarta hipótesis específica. Afirmando que la evaluación de la conformidad de las implementaciones efectuadas indica la mejora de la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

RECOMENDACIONES

- Realizar capacitaciones constantes para el personal de la municipalidad respecto a la seguridad de la información, para que de esta manera todos los trabajadores tomen conciencia de cuán importante es mantener seguro los datos de la organización.
- Realizar pruebas de internet con el mejor proveedor de este servicio que ofrezca la mejor alternativa, debido a que es crucial y muy importante la señal de internet para la municipalidad.
- Realizar pruebas de seguridad en cuanto al ingreso de personal autorizado a los servidores de la municipalidad, ya que debemos incidir en la protección de la información y los activos donde se alojan las bases de datos de la municipalidad.
- De igual forma la municipalidad no debería escatimar gastos al proteger su información, ya que ello conllevaría a manejar de una manera adecuada la información, confiando en profesionales que estén preparados, capacitados para este tipo de procesos.
- Se recomienda a la municipalidad tomar en cuenta la presente investigación que le permitirá mejorar la seguridad de la información de manera significativa

REFERENCIAS BIBLIOGRÁFICAS

Bibliotecas, & duoc. (2022). Investigación Aplicada. Obtenido de https://bibliotecas.duoc.cl/investigacion-aplicada/definicion-proposito-investigacion-aplicada#:~:text=La%20Investigaci%C3%B3n%20Aplicada%20tiene%20por,del%20desarrollo%20cultural%20y%20cient%C3%ADfico. Rev. 11/05/2024

Bigelow, S. (2023). Definicion de Solución. Obtenido de https://www.techtarget. com/searchitchannel/ definition/solution Rev. 11/05/2024

Careerexplorer. (2023). Definicion de Cloid Obtenido de https://www.careerexplorer.com /careers/solution-architect/ Rev. 11/05/2024

Cisco. (2023). Cloud Computing Obtenido de https://www.cisco.com/c/es_mx/ solutions/cloud/what-is-cloud-computing.html Rev. 11/05/2024

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

Cruz, M. (2020). Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la clínica Medcam Perú SAC. LIMA: USMP. Rev. 13/05/2024

Esteban, J. (2025). mpresas tecnológicas para invertir con grandes dividendos. Obtenido de https://www.blog.ironia.tech/ post/empresas-tecnol%C3%B3gicas-para-invertir-con-grandes-dividendos Rev. 17/05/2024

Gartner. (2023). Definicion de Tecnología. Obtenido de https://www.gartner.com/en/information-technology/glossary/solution Rev. 11/05/2024

Geneva. (2021). Data cebter wipo. Obtenido de https://www.wipo.int/pressroom /es/articles/2021/article_0008.html Rev. 14/05/2024

Imperva. (2023). Seguridad de la Información Obtenido de https://www.imperva.com/learn/data-security/information-security-infosec/ Rev. 11/05/2024

Indeed. (2023). Solución de TI Obtenido de https://ca.indeed.com/career-advice/career-development/what-is-it-solution Rev. 11/05/2024

Internationalit. (2022). Gestión de Red. Obtenido de https://www.internationalit.com/post/qu%C3%A9-es-la-gesti%C3%B3n-de-red-y-por-qu%C3%A9-es-importante?lang=es Rev. 11/05/2024

lacamara. (2022). Inversion en TI Perú.. Obtenido de https://lacamara.pe/empresas-en-peru-invierten-9-en-tecnologia/ Rev. 11/05/2024

larepublica. (2022). larepublica. Obtenido de https://larepublica.pe /economia/2020/11/17/inversion-en-el-sector-tic-alcanzara-mas-de-3-millones-entre-el-2020-y-2024 Rev. 12/05/2024 Rev. 11/05/2024

Méndez, C. (2020). Desarrollo de un plan de seguridad de la información basado en estándares para empresa de seguros. Pimentel: USS. Rev. 11/05/2024

Mitchell, B. (2020). Introduccion de TI Obtenido de https://www.lifewire.com/introduction-information-technology-817815 Rev. 11/05/2024

Molano, R. (2020). Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma iso 27001 en el área de ti para la empresa market mix. Bogota: UCC. Rev. 11/05/2024

Moreno, J. (2023). Soporte Técnico Obtenido de https://blog.hubspot.es/service/que-es-soporte-tecnico Rev. 11/05/2024

Muniucayali. (2024). Obtenido de https://www.muniucayali.gob.pe/ Rev. 11/05/2024

Oarc. (2023). Alfa de cronbach. Obtenido de https://stats.oarc.ucla.edu/spss /faq/what-does-cronbachs-alpha-mean/ Rev. 11/05/2024

Otgroup. (2022). Obtenido de https://www.otgroup.ca/business-technology-insights/it-solutions-definition-what-does-it-mean-can-it-help-your-company Rev. 11/05/2024

Oviedo, J. (2010). scielo. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0034-74502005000400009#:~:text=El%20coeficiente%20alfa%20fue%20descrito,correlacionados%20(3%2C17). Rev. 11/05/2024

Porras, M. (2022). Sistema de gestión de seguridad de la información para la gestión de riesgos. Huancayo: UPDA. Rev. 11/05/2024

Ramiro Alejandro, G. (2020). Sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para el departamento de ecnologías de la información y comunicación. Ecuador: UTA.

Rojas Viera, C. K. (2021). Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015. Lambayeque: UNPRG. Rev. 11/05/2024

Servicenow. (2023). Obtenido de https://www.servicenow.com/ products/itsm/what-are-it-solutions.html Rev. 11/05/2024

Suarez, L. (2021). Sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2015- en la empresa Magdaniel ltda. en el distrito especial, turístico y cultural de riohacha. Guajira: U. GUAJIRA. Rev. 11/05/2024

Sumologic. (2023). Administración de la Seguridad de Información Obtenido de https://www.sumologic.com/glossary/information-security-management/ Rev. 11/05/2024

Unir. (2023). Principios de la Seguridad de la Información Obtenido de https://www.unir.net/ingenieria/revista/principios-seguridad-informatica/ Rev. 11/05/2024

ANEXOS

ANEXO 1

EVALUACIÓN DE CONFIABILIDAD DEL INSTRUMENTO

Para validar, la confiabilidad del instrumento, se ha considerado aplicar el Alfa de Cronbach, tanto para el Pre-Test, como para el Post-Test utilizando, el programa SPSS.

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

Capturas del uso del SPSS

Nombre	Tipo	Anchura	Dec...	Etiqueta	Valores	Perdidos	Columnas	Alineación	Medida
P1	Numérico	8	0	P1. ¿Cómo calificaría la disponibilidad de la información en el sistema actual?	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P2	Numérico	8	0	P2. ¿Cómo calificaría al actual desempeño y funcionalidad del sistema de trabajo o...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P3	Numérico	8	0	P3. ¿Cómo califica la forma como el personal de la Municipalidad accede a la infor...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P4	Numérico	8	0	P4. ¿Como calificaría con qué frecuencia solicita que le revisen su PC frente a cual...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P5	Numérico	8	0	P5. ¿Cómo califica usted el tipo de servicio que reciben usuarios al realizar una co...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P6	Numérico	8	0	P6. ¿Cómo calificaría si la municipalidad cumple con los objetivos de seguridad de ...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P7	Numérico	8	0	P7. ¿Como calificaría a las herramientas basadas en la gestión de la seguridad en l...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P8	Numérico	8	0	P8. ¿Cómo calificaría Ud. el proceso de seguimiento de los trámites que se presen...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P9	Numérico	8	0	P9. ¿Cómo calificaría al actual desempeño y funcionalidad del sistema de trabajo o...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P10	Numérico	8	0	P10. ¿Cómo calificaría las respuestas del sistema a tiempo cuando se detecta alg...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P11	Numérico	8	0	P11. ¿Cómo calificaría el hecho que solo el personal de la municipalidad debe cont...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P12	Numérico	8	0	P12. ¿Cómo calificaría la frecuencia en el transito virtual de sus datos personales e...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P13	Numérico	8	0	P13. ¿Cómo calificaría el hecho que solo el personal autorizado pueda acceder a s...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P14	Numérico	8	0	P14. ¿Cómo calificaría la seguridad en el tránsito virtual de sus datos personales e...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P15	Numérico	8	0	P15. ¿Cómo calificaría la precisión de sus datos personales que ofrece la municipa...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P16	Numérico	8	0	P16. ¿Cómo calificaría la precisión de sus datos a través del tiempo ofrecidos por l...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P17	Numérico	8	0	P17. ¿Cómo calificaría los permisos de los usuarios con respecto a su limitación p...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P18	Numérico	8	0	P18. ¿Cómo calificaría la Gestión de cambios para asegurar la integridad de los pro...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P19	Numérico	8	0	P19. ¿Cómo calificaría la funcionalidad de los dispositivos de red, equipos de TI y n...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal
P20	Numérico	8	0	P20. ¿Cómo calificaría la rapidez en el proceso de actualización de sus datos pers...	{1, Muy Malo}...	Ninguna	8	Derecha	Ordinal

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18
2	2	2	2	2	2	3	3	2	2	2	2	2	2	3	3	3	3
2	3	3	2	2	2	2	2	3	2	2	3	1	1	3	2	3	2
1	3	2	2	1	3	2	3	3	2	1	1	2	1	1	1	2	2
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2
3	3	2	2	1	1	1	3	2	3	1	2	3	2	2	1	2	1
3	2	3	2	2	2	2	3	1	2	3	3	2	2	2	2	2	2
2	3	1	1	3	2	1	1	2	1	3	2	3	3	2	2	3	3
3	2	2	3	2	1	3	2	1	2	2	3	3	1	2	1	2	2
1	3	2	1	3	2	2	2	3	2	1	2	1	2	2	3	2	3
3	2	1	3	1	2	2	2	3	2	3	1	2	2	3	3	2	3
3	3	3	3	3	3	3	3	2	3	3	3	2	3	3	3	3	3
3	2	1	2	2	1	3	2	3	2	1	2	2	2	3	2	3	2
3	2	2	2	3	3	3	2	3	2	3	3	2	2	2	2	2	2
1	2	2	1	2	3	3	3	2	1	2	2	2	2	2	2	2	2
2	2	3	1	2	2	2	2	1	3	2	2	2	2	3	3	2	1
3	2	3	3	3	2	2	3	2	2	2	3	2	2	2	2	2	2
3	2	3	1	3	2	2	2	3	2	3	2	1	3	2	3	3	3
3	3	2	1	1	1	2	2	1	2	2	2	1	2	1	2	2	2
3	2	2	1	2	1	2	2	2	1	2	2	1	2	2	2	2	3
3	2	3	2	2	3	2	2	3	2	1	2	2	3	2	2	2	3

Resumen del procesamiento de los casos

		N	%
Casos,	Válidos,	120,	100,0
	Excluidos[a]	0	,0
	Total,	120,	100,0,

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,821	20

El resultado para el pre-test es de 0.821, por lo tanto, se acepta la confiablidad del instrumento.

Comprobación Post-Test

Capturas del uso del SPSS

Nombre	Tipo	Anchura	Decimales	Etiqueta
P1	Numérico	8	0	P1. ¿Cómo calificaría la disponibilidad de la información en el sistema actual?
P2	Numérico	8	0	P2. ¿Cómo calificaría al actual desempeño y funcionalidad del sistema de trabajo o sistema informático que se esté aplicando ...
P3	Numérico	8	0	P3. ¿Cómo califica la forma como el personal de la Municipalidad accede a la información de sus servidores?
P4	Numérico	8	0	P4. ¿Como calificaría con qué frecuencia solicita que le revisen su PC frente a cualquier falla?
P5	Numérico	8	0	P5. ¿Cómo califica usted el tipo de servicio que reciben usuarios al realizar una consulta respecto a solicitud?
P6	Numérico	8	0	P6. ¿Cómo calificaría si la municipalidad cumple con los objetivos de seguridad de información?
P7	Numérico	8	0	P7. ¿Como calificaría a las herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identifi...
P8	Numérico	8	0	P8. ¿Cómo calificaría Ud. el proceso de seguimiento de los trámites que se presentan y se generan durante una consulta de lo...
P9	Numérico	8	0	P9. ¿Cómo calificaría al actual desempeño y funcionalidad del sistema de trabajo o sistema informático que se aplica en los pr...
P10	Numérico	8	0	P10. ¿Cómo calificaría las respuestas del sistema a tiempo cuando se detecta alguna amenaza contra la seguridad de la infor...
P11	Numérico	8	0	P11. ¿Cómo calificaría el hecho que solo el personal de la municipalidad debe contar con la autorización necesaria para acced...
P12	Numérico	8	0	P12. ¿Cómo calificaría la frecuencia en el transito virtual de sus datos personales en la municipalidad?
P13	Numérico	8	0	P13. ¿Cómo calificaría el hecho que solo el personal autorizado pueda acceder a su información personal?
P14	Numérico	8	0	P14. ¿Cómo calificaría la seguridad en el tránsito virtual de sus datos personales en la municipalidad?
P15	Numérico	8	0	P15. ¿Cómo calificaría la precisión de sus datos personales que ofrece la municipalidad?
P16	Numérico	8	0	P16. ¿Cómo calificaría la precisión de sus datos a través del tiempo ofrecidos por la municipalidad?
P17	Numérico	8	0	P17. ¿Cómo calificaría los permisos de los usuarios con respecto a su limitación para acceder a su información?
P18	Numérico	8	0	P18. ¿Cómo calificaría la Gestión de cambios para asegurar la integridad de los procesos en la municipalidad?
P19	Numérico	8	0	P19. ¿Cómo calificaría la funcionalidad de los dispositivos de red, equipos de TI y nuestras aplicaciones para acceder a la infor...
P20	Numérico	8	0	P20. ¿Cómo calificaría la rapidez en el proceso de actualización de sus datos personales que les ofrece la municipalidad?

P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14
4	4	4	4	3	3	4	4	3	4	4	4	4	4
3	4	4	4	4	4	3	4	3	4	4	4	4	4
4	4	3	4	3	4	4	4	3	4	4	3	4	4
5	5	4	4	4	4	5	4	4	4	4	4	3	4
3	3	3	4	4	4	4	3	4	4	4	4	4	5
4	3	4	4	3	4	4	4	3	4	4	4	4	4
3	4	3	3	3	3	4	4	4	4	3	3	4	4
5	5	5	4	3	4	5	4	5	4	4	4	4	3
4	4	4	4	4	5	4	4	4	5	4	4	3	4
5	4	4	3	4	4	4	3	3	4	4	3	4	3
4	4	4	4	3	3	3	4	4	4	4	3	4	4
3	3	4	4	4	5	4	4	3	4	4	4	4	3
4	3	4	4	3	4	4	4	3	4	4	4	4	4
3	3	4	4	3	4	3	3	3	3	3	3	3	4
3	4	4	3	4	3	3	4	4	4	3	4	3	3
4	4	5	4	5	4	4	4	4	4	4	3	3	4
4	4	4	4	3	4	3	4	4	3	4	4	3	4
4	3	4	3	4	3	4	3	4	3	4	3	3	3
5	5	5	4	5	5	4	5	5	4	4	5	4	4
4	3	4	4	4	4	4	4	4	4	4	4	4	4
4	3	4	3	4	4	4	4	4	4	4	4	4	4

Resumen del procesamiento de los casos

		N	%
Casos	Válidos,	120,	100,0
	Excluidos[a]	0	,0
	Total	120,	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,835	20

El resultado para el pre-test es de 0.835, por lo tanto, se acepta la confiablidad del instrumento.

ANEXO 2. 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 análisis, diseño e implementación de una solución de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana?</td>
<td>Analizar, diseñar e implementar una solución de, ti para mejorar la seguridad de la, información de la Municipalidad, Provincial de Ucayali Contamana</td>
<td>El análisis, diseño e implementación de una solución de ti mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.</td>
<td rowspan="2">Solución de TI
<table>
<tr><th>Dimensión</th><th>Indicador</th></tr>
<tr><td>Análisis</td><td>Servicios de TI Actuales
Recursos de TI actuales.
Personal de TI.</td></tr>
<tr><td>Diseño</td><td>Servicios de TI propuestos.
Recursos de TI propuestos.</td></tr>
<tr><td>Implementación</td><td>Recursos de TI implementados y proyectados
Servicios de TI implementados y proyectados.
Áreas atendidas.</td></tr>
<tr><td>Conformidad</td><td>% de conformidad de los servicios TI implementados y proyectados.
% de conformidad de los recursos de TI implementados y proyectados.</td></tr>
</table>
Seguridad de la información
<table>
<tr><th>Dimensión</th><th>Indicador</th></tr>
<tr><td>Confidencialidad</td><td>• Controles generales
• Autorizaciones.</td></tr>
<tr><td>Integridad</td><td>• Controles de seguridad en comunicaciones
• Controles de seguridad en procedimientos.</td></tr>
<tr><td>Disponibilidad</td><td>• Tiempo de acceso a los servicios o recursos</td></tr>
</table>
</td>
<td rowspan="2">Tipo de investigación: Aplicada
Nivel de investigación: Descriptiva.
Población: Empleados que laboran en las oficinas de la Municipalidad Provincial de Ucayali Contamana, que se encuentran estrechamente relacionados con el uso de Tecnologías de la información, siendo un total de 120 empleados.
Muestra: La cantidad de empleados que conforman la población es pequeña; por lo tanto, se efectuará un muestreo no probabilístico, conllevando a utilizar el muestreo por conveniencia, donde el total de personas a evaluar conforman el total de la población, en este caso 120 empleados.
Diseño de la investigación: Experimental de tipo pre experimental.
Ge: Y1 ----- X -----Y2
Donde:
Ge: Grupo experimental
O1: Pretest
O1: Postest
X: Solución de TI
SPSS Estadísticas IBM
<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>1. ¿De qué manera análisis actual de los servicios y recursos de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana?
2. ¿Cuál es el diseño de los recursos y servicios de TI que mejoran la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana?
3. ¿La implementación de recursos y servicios de TI mejoran la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana?
4. ¿La evaluación de la conformidad de las implementaciones efectuadas mejoran la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana?</td>
<td>1.Realizar el análisis actual de los servicios y recursos de TI para mejorar la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
2. Diseñar los recursos y servicios de TI para mejorar la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana
3. Implementar recursos y servicios de TI para mejorar la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
4. Evaluar la conformidad de las implementaciones efectuadas para determinar la mejora de la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.</td>
<td>1. El análisis actual de los servicios y recursos de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
2. El diseño de los recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
3. La implementación de recursos y servicios de TI mejora la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.
4. La evaluación de la conformidad de las implementaciones efectuadas indica la mejora de la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.</td>
</tr>
</table>

ANEXO 3

Cuestionario de preguntas para la recolección de datos

CUESTIONARIO DE PREGUNTAS SOBRE LA INVESTIGACIÓN

"ANALISIS, DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE TI PARA PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE UCAYALI CONTAMANA"

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: SOLUCIÓN DE TI						
Indicador: Servicios de TI Actuales						
1	¿Cómo calificaría la disponibilidad de la información en el sistema actual?					
Indicador: Recursos de TI actuales.						
2	¿Cómo calificaría al actual desempeño y funcionalidad del sistema de trabajo informático donde se esté empleando en los procesos administrativos para la atención al público?					
Indicador: Personal de TI						
3	¿Cómo califica la forma como el personal de la Municipalidad accede a la información de sus servidores?					
Indicador: Servicios de TI propuestos						
4	¿Como calificaría con qué frecuencia solicita que le revisen su PC frente a cualquier falla?					

5	¿Cómo califica usted el tipo de servicio que reciben usuarios al realizar una consulta respecto a solicitud?					
Indicador: Recursos de TI implementados y proyectados						
6	¿Cómo calificaría si la municipalidad cumple con los objetivos de seguridad de información?					
Indicador: Servicios de TI implementados y proyectados						
7	¿Como calificaría a las herramientas basadas en la gestión de la seguridad en la información las cuales permiten la identificación de los riesgos en la municipalidad?					
Indicador: Áreas atendidas.						
8	¿Cómo calificaría Ud. el proceso de seguimiento de los trámites que se presentan y se generan durante una consulta de los usuarios?					
Indicador: % de conformidad de los servicios TI implementados y proyectados						
9	¿Cómo calificaría al actual desempeño y funcionalidad del sistema de trabajo o sistema informático que se aplica en los procesos administrativos de la municipalidad?					
Indicador: % de conformidad de los recursos de TI implementados y proyectados						
10	¿Cómo calificaría las respuestas del sistema a tiempo cuando se detecta alguna amenaza contra la seguridad de la información en la municipalidad?					
VARIABLE DEPENDIENTE: SEGURIDAD DE LA INFORMACIÓN.						
Indicador: Controles generales						
11	¿Cómo calificaría el hecho que solo el personal de la municipalidad debe contar con la autorización necesaria para acceder a sus datos personales?					
12	¿Cómo calificaría la frecuencia en el transito virtual de sus datos personales en la municipalidad?					
Indicador: Autorizaciones						
13	¿Cómo calificaría el hecho que solo el personal autorizado pueda acceder a su información personal?					
14	¿Cómo calificaría la seguridad en el tránsito virtual de sus datos personales en la municipalidad?					
Indicador: Controles de seguridad en comunicaciones						

15	¿Cómo calificaría la precisión de sus datos personales que ofrece la municipalidad?					
16	¿Cómo calificaría la precisión de sus datos a través del tiempo ofrecidos por la municipalidad?					
Indicador: Controles de seguridad en procedimientos.						
17	¿Cómo calificaría los permisos de los usuarios con respecto a su limitación para acceder a su información?					
18	¿Cómo calificaría la Gestión de cambios para asegurar la integridad de los procesos en la municipalidad?					
Indicador: Tiempo de acceso a los servicios o recursos						
19	¿Cómo calificaría la funcionalidad de los dispositivos de red, equipos de TI y nuestras aplicaciones para acceder a la información de la municipalidad?					
20	¿Cómo calificaría la rapidez en el proceso de actualización de sus datos personales que les ofrece la municipalidad?					

ANEXO 4
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 EVALUACION	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. METODOLOGIA	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: .....

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: Análisis, diseño e implementación de una solución de TI para la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana

1.5. AUTOR DEL INSTRUMENTO: LINDER HIDALGO

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

VALORACIÓN CUANTITATIVA : 19
VALORACIÓN CUALITATIVA : EXCELENTE
OPINIÓN DE APLICABILIDAD : APLICABLE.

Lugar y Fecha: 19/04/2024.

.....
Firma y post firma del experto
DNI: 18190341

Ficha de Expertos.

UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE INGENIERIA DE SISTEMAS

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: BARDALES LINARES RICHARD PIERO

1.2. GRADO ACADÉMICO: MAGISTER SCIENTIAE

1.3. INSTITUCIÓN QUE LABORA: UNIVERSIDAD NACIONAL DE UCAYALI.

1.4. TÍTULO DE LA INVESTIGACIÓN: Análisis, diseño e implementación de una solución de TI para la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana

1.5. AUTOR DEL INSTRUMENTO: LINDER HIDALGO

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

VALORACIÓN CUANTITATIVA : 19
VALORACIÓN CUALITATIVA : MUY BUENO
OPINIÓN DE APLICABILIDAD : APLICABLE.

Lugar y Fecha: 19/04/2024.



UNIVERSIDAD NACIONAL DE UCAYALI

ESCUELA DE INGENIERIA DE SISTEMAS

I. DATOS GENERALES

1.1. APELLIDOS Y NOMBRES: GARCÍA CHÁVEZ MIGUEL ÁNGEL

1.2. GRADO ACADÉMICO: INGENIERO DE SISTEMAS

1.3. INSTITUCIÓN QUE LABORA: PERICODE SOLUTIONS S.A.C.

1.4. TÍTULO DE LA INVESTIGACIÓN Análisis, diseño e implementación de una solución de TI para la seguridad de la información de la Municipalidad Provincial de Ucayali Contamana.

1.5. AUTOR DEL INSTRUMENTO: LINDER HIDALGO

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

VALORACIÓN CUANTITATIVA : 19
VALORACIÓN CUALITATIVA : EXCELENTE
OPINIÓN DE APLICABILIDAD : APLICABLE

Lugar y Fecha: 19/04/2024

.....
Firma y post firma del experto
Código de colegiatura

DNI: 70751278