# UNIVERSIDAD NACIONAL DE UCAYALI

## FACULTAD DE INGENIERÍA DE SISTEMAS E INGENIERÍA CIVIL

## CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

# "GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-PUCALLPA: 2018"

**TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE**

**INGENIERO DE SISTEMAS**

**JUAN DAVID LOPEZ PEZO**

**PUCALLPA – PERÚ**

**2021**

# INFORME DE ASESORÍA DE TESIS

**I. Tesistas** : Bach. LOPEZ PEZO, JUAN DAVID

**II. Tema** : GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-PUCALLPA: 2018.

**III. Referencia** : Resolución Comité de Planeamiento N°657/2018-CP-FIS e IC-UNU/ Resolución Comité de Planeamiento N°597/2019-CP-FIS e IC-UNU

---

Que el tesista ha cumplido con ejecutar la tesis titulada: **"GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-PUCALLPA: 2018 "** de conformidad con el Reglamento General de Grados y Títulos de la Universidad Nacional de Ucayali, y según la directiva establecida en el sistema de anti plagio **URKUND** solo alcanza el 04% de similitud; por lo que mi asesoría declara **APROBADO** y, encontrándose apta para ser presentada y evaluada por la Comisión de Grados y Títulos de la Facultad de Ingeniería de Sistemas e Ingeniería Civil de la Universidad Nacional de Ucayali. Se expide el presente documento, a solicitud de los interesados para los fines consiguientes.

Pucallpa, 29 Noviembre 2020

Ing. Mg. Freddy Elar Ferrari Fernández

**Asesor de Tesis**

# UNIVERSIDAD NACIONAL DE UCAYALI

**FACULTAD DE INGENIERIA DE SISTEMAS E INGENIERIA CIVIL**
**ESCUELA PROFESIONAL DE INGENIERIA CIVIL**
**COMISION DE GRADOS Y TITULOS**

## ACTA DE EVALUACION DE SUSTENTACION DE TESIS N° 008-2021

**GRADUANDO** : **Bach.** LOPEZ PEZO Juan David

**TEMA** : **"GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-PUCALLPA: 2018",**

**ASESOR** : **ING. MG. FREDDY ELAR FERRARI FERNANDEZ**

| 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**

- ING. MSC. EUCLIDES PANDURO PADILLA — Presidente
- ING. MG. CESAR AGURTO CHERRE — Miembro
- ING. MG RONALD ULLOA GALVEZ — Miembro

**SECRETARIA ACADÉMICA**: ING. MSC. CLOTILDE RÍOS HIDALGO DE CERNA

**PUCALLPA, 20 De agosto Del 2021**

Esta tesis: **"GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD DE LA RED INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-PUCALLPA: 2018"**

**Elaborado por:**

Bach. JUAN DAVID LOPEZ PEZO

**Aprobado por:**

Ing. M.Sc. EUCLIDES PANDURO PADILLA

Presidente del Jurado Evaluador

Ing. Mg. CESAR AGURTO CHERRE

Miembro del Jurado Evaluador

Ing. Mg. RONALD ULLOA GALVEZ

Miembro del Jurado Evaluador

**ASESOR**

Ing. Mg. FREDDY ELAR FERRARI FERNANDEZ

Asesor

**UNIVERSIDAD NACIONAL DE UCAYALI**
**VICERRECTORADO DE INVESTIGACION**
**DIRECCION DE PRODUCCION INTELECTUAL**

# CONSTANCIA

## ORIGINALIDAD DE TRABAJO DE INVESTIGACION

## SISTEMA ANTIPLAGIO URKUND

## N° V/0220-2021

La **Dirección de Producción Intelectual**, hace constar por la presente, que el INFORME FINAL de tesis, **Titulado**:
**"GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-PUCALLPA: 2018".**

| | | |
|---|---|---|
| **Cuyo autor (es)** | **:** | **LOPEZ PEZO, JUAN DAVID** |
| Facultad | : | INGENIERIA DE SISTEMAS Y DE INGENIERIA CIVIL |
| Escuela Profesional | : | INGENIERIA DE SISTEMAS |
| Asesor(a) | : | Mg. FERRARI FERNANDEZ FREDDY ELAR |

Después de realizado el análisis correspondiente en el Sistema Antiplagio URKUND, dicho documento presenta un **porcentaje de similitud de 2%.**
En tal sentido, de acuerdo a los criterios de porcentaje establecidos en el artículo 9 de la DIRECTIVA DE USO DEL SISTEMA ANTIPLAGIO URKUND, el cual indica que no se debe superar el 10%. Se declara, que el trabajo de investigación: SI Contiene un porcentaje aceptable de similitud, por lo que SI se aprueba su originalidad.
En señal de conformidad y verificación se entrega la presente constancia.

**Fecha: 15/06/2021**

**Dr. ABRAHAM ERMITANIO HUAMAN ALMIRON**

# AUTORIZACIÓN DE PUBLICACIÓN DE TESIS

## REPOSITORIO DE LA UNIVERSIDAD NACIONAL DE UCAYALI

Yo, Juan David Lopez Pezo.
Autor de la TESIS titulada:
"Gestión de riesgos con metodología NIST SP 800-30 a la Seguridad en redes inalambricas en la empresa Servinteconp Ucayali-Pucallpa: 2018"

Sustentada el año: 2021.
Con la asesoría de: Ing. Mg. Freddy Elar Ferrari Fernandez.
En la Facultad de: Ingeniería de Sistemas é Ingeniería Civil.
Carrera Profesional de: Ingeniería de Sistemas.

**Autorizo la publicación:**

**PARCIAL** [ ] Significa que se publicará en el repositorio institucional solo La caratula, la dedicatoria y el resumen de la tesis. Esta opción solo es válida marcar **si su tesis o documento presenta material patentable**, para ello deberá presentar el trámite de CATI y/o INDECOPI cuando se lo solicite la DGPI UNU.

**TOTAL** [X] Significa que todo el contenido de la tesis y/o documento será publicada en el repositorio institucional.

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 y del Ministerio de Educación.

En señal de conformidad firmo la presente autorización.

Fecha: 20 / 08 / 2021

Email: David.TJ119@gmail.com. Firma: 

Teléfono: 961991724. DNI: 40374134.

# DEDICATORIA

El presente trabajo le dedico a mi amada hija quién con sus sonrisas en las mañanas me hace ver las cosas fáciles de lograr, a pesar de ciertos obstáculos que no son más que metas hacia el triunfo de lo inimaginable a lo imaginable en la vida.

# AGRADECIMIENTO

Agradezco a los docentes de la **FIS y de IC**, por su afán de hacer posible sus enseñanzas en nuestras mentes y así ser personas probo, en una sociedad que se pierde cada vez más los valores de lo justo, moral, y lealtad; pero ustedes docentes siempre nos dan sus pequeñas y atinadas sugerencias para nuestra profesión, de tal manera que se cumpla con la visión y misión de nuestra Universidad Nacional de Ucayali.

# INDICE DE CONTENIDO

**DEDICATORIA** ..... **vii**

**AGRADECIMIENTO** ..... **viii**

**INDICE DE CONTENIDO** ..... **ix**

**INDICE DE FIGURAS** ..... **xiii**

**INDICE DE TABLAS** ..... **xv**

**RESUMEN** ..... **xvii**

**ABSTRACT** ..... **xviii**

**INTRODUCCION** ..... **xix**

**CAPITULO I: PLANTEAMIENTO DEL PROBLEMA** ..... **1**

**1.1 ANTECEDENTES DEL PROBLEMA** ..... 1

**1.2 FORMULACIÓN DEL PROBLEMA** ..... 4

**1.2.1 Problema General** ..... 4

**1.2.2 Problemas Específicos** ..... 4

**1.3 OBJETIVOS DE LA INVESTIGACIÓN** ..... 5

**1.3.1 Objetivo general** ..... 5

**1.3.2 Objetivos específicos** ..... 5

**1.4 JUSTIFICACIÓN E IMPORTANCIA** ..... 6

**1.4.1 Justificación** ..... 6

**1.4.2 Importancia** ..... 7

**1.5 HIPÓTESIS Y VARIABLES DE LA INVESTIGACIÓN** ..... 8

**1.5.1 Hipótesis general** ..... 8

**1.5.2 Hipótesis específica** ..... 8

**1.6 VARIABLES (DEFINICIÓN CONCEPTUAL Y OPERACIONAL)** ..... 9

**CAPITULO II: MARCO TEÓRICO** ..... **15**

**2.1 ANTECEDENTES DE LA INVESTIGACIÓN.** ..... 15

**2.1.1 Tesis internacionales** ..... 15

**2.1.2 Tesis nacionales** ..... 16

**2.2 BASES TEORICAS** ..... 17

**2.2.1 Gestión de riesgos** ..... 17

**2.2.2 Metodología de NIST SP 800-30** ..... 18

***2.2.3* Métodos de seguridad de redes inalámbricas.** ..... 23

**2.2.4 Tipos de redes inalámbricas** ..... 24

**2.2.5 Ventajas de la red inalámbrica** ..... 24

***2.2.6* Desventajas de las redes inalámbricas.** ..... 25

**2.2.7 Definición de términos básicos** ..... 26

**CAPITULO III: METODOLOGÍA ..... 32**

**3.1 MÉTODO DE INVESTIGACIÓN** ..... 32

***3.1.1 Tipo de investigación*** ..... 32

**3.2 NIVEL DE INVESTIGACIÓN** ..... 32

***3.2.1 Método de investigación*** ..... 32

**3.3 POBLACIÓN Y MUESTRA.** ..... 33

**3.4 PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS.** ..... 36

**3.5 TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS.** ..... 36

**3.6 PROCESAMIENTO PARA RECOLECCIÓN DE DATOS.** ..... 37

**3.7 TRATAMIENTO DE DATOS.** ..... 37

**3.8 METODOLOGÍA DE DESARROLLO** ..... 38

***3.8.1 VARIABLE 1: Metodología NIST SP 800-30*** ..... 38

**3.8.1.1 Caracterización del sistema. ..... 38**

**3.8.1.2 Fronteras del sistema, funciones del sistema, criticidad del sistema. ..... 39**

3.8.1.3 Sensibilidad de datos y sistemas ..... 52
3.8.1.4 Identificación de amenazas. ..... 53
3.8.1.5 Identificación de vulnerabilidades. ..... 56
3.8.1.6 Caracterización de los controles. ..... 57
3.8.1.7 Determinación de probabilidades. ..... 58
*3.8.2 Análisis de impacto.* ..... 59
3.8.2.1 Determinación del riesgo. ..... 60
3.8.2.2 Recomendaciones de control. ..... 60
3.8.2.3 Resultado de la implementación o documentación. ..... 62
*3.8.3 VARIABLE 2: LA SEGURIDAD DE REDES INALÁMBRICAS* ..... 64
*3.8.3.1 Protección* ..... 64
*3.8.4 Cambiar la contraseña de fábrica.* ..... 64
*3.8.5 Poner la contraseña en WPA2 AES.* ..... 65
3.8.5.1 Detección ..... 66
3.8.5.2 Secuestro de sesión ..... 67
3.8.5.3 Suplantación de dirección de MAC ..... 67
3.8.5.4 Saturar el ambiente con ruido de RF ..... 68
*3.8.6 Reacción* ..... 68
**CAPITULO IV: RESULTADOS ..... 70**
**4.1 INTERPRETACIÓN DE RESULTADOS PRE TEST** ..... 70
**4.1.1 Del cuestionario** ..... 70
**4.2 INTERPRETACIÓN DE RESULTADOS POST TEST** ..... 85
*4.2.1 Del cuestionario* ..... 85
**4.3 PRUEBA DE HIPÓTESIS** ..... 100
*4.3.1 Formulación de cuadro de valores de indicadores* ..... 100
*4.3.2 Supuestos de la prueba de hipótesis* ..... 100
*4.3.3 Cálculo del valor crítico y la función prueba* ..... 101

*4.3.4 Ficha de evaluación pre-test a la estructura de la metodología NIST SP 800-30 (ficha de observación).* ..... 105

*4.3.5 Ficha de evaluación post-test a la estructura de la metodología NIST SP 800-30 (ficha de observación).* ..... 106

**CAPITULO V: DISCUSIÓN ..... 107**

**CAPITULO VI ..... 108**

**CONCLUSIONES Y RECOMENDACIONES ..... 108**

**6.1 CONCLUSIONES** ..... 108

**6.2 RECOMENDACIONES** ..... 110

**REFERENCIAS BIBLIOGRÁFICAS ..... 111**

**ANEXOS ..... 114**

**ANEXO Nº 01 MATRIZ DE IDENTIFICACIÓN DEL PROBLEMA ..... 115**

**ANEXO Nº 02 HOJA DE RUTA DE LAS VARIABLES ..... 116**

**ANEXO Nº 5 INSTRUMENTOS DE RECOLECCIÓN DE DATOS ..... 121**

**ANEXO Nº 6 PRUEBA DEL PRE Y POST -TEST ..... 123**

**ANEXO Nº 7 VALIDACIÓN POR ALFA DE CRONBACH ..... 125**

**ANEXO Nº 8 INFORME DE REPORTE DE ATAQUES DE VIRUS. ..... 129**

**ANEXO Nº 9 REPORTES DE DEFINICIONES DE AMENAZA DE VIRUS ... 130**

**ANEXO Nº 10 CUADRO DE OBSERVACIÓN CON PORCENTAJE DE ACTIVIDAD DESARROLLADA ..... 131**

**ANEXO Nº 11 FOTOS DE LAS AUDITORIAS Y LOS PROGRAMAS USADOS ..... 133**

# INDICE DE FIGURAS

**Figura 1**.organigrama de la empresa. ....2
**Figura 2** Proceso de la metodología NIST SP 800-30 ....20
**Figura 3.** Red estructurada ....24
**Figura 4.** Modelo de A. Russel - Ackoft....33
**Figura 5**. Caracterización del sistema propia....38
**Figura 6**. Winbox v3.18 (mikrotik) ....64
**Figura 7**.La contraseña WPA2 AES (mikrotik)....65
**Figura 8.** Configuración de la MAC en Mikrotik....66
**Figura 9.** Un posible secuestro de usuario (mikrotik) ....67
**Figura 10.** Un ejemplo en Youtube acerca de generador de ruido RF....68
**Figura 11.** Un claro ejemplo de reducir acceso al Mikrotik ....69
**Figura 12**. Calificación del ruter y del equipo de enlace ....71
**Figura 13**.Calificación del personal técnico....71
**Figura 14.** Calificación del Servicio de Internet ....72
**Figura 15**. Calificación de los reportes de ataques de virus....73
**Figura 16.** Calificación de los reportes de definiciones de amenazas....74
**Figura 17.** Calificación de la motivación de los ataques ....75
**Figura 18.** Calificación de la Capacidad de las amenazas....76
**Figura 19.** Calificación del Impacto de los ataques ....77
**Figura 20.** Calificación de la Sensibilidad de datos ....78
**Figura 21**. Calificación de la Probabilidad de explotación de las amenazas ....79
**Figura 22.** Calificación de la Magnitud de los impactos ....80
**Figura 23.** Calificación de su Red Inalámbrica ....81
**Figura 24.** Calificación de su Antivirus....82
**Figura 25.** Calificación de su Firewall ....83
**Figura 26.** Calificación del Reuter equipo de enlace ....85
**Figura 27.** Calificación del Profesionalismo del Personal Técnico ....86
**Figura 28** Calificación del Servicio de Internet ....87
**Figura 29.** Calificación de los reportes de ataque de virus....88
**Figura 30.** Calificación de las definiciones de amenazas ....89
**Figura 31** Califiacion de la Motivación de ataques....90
**Figura 32.** Calificación de la Capacidad de las amenazas....91
**Figura 33**. Calificación del Impacto de los ataques ....92
**Figura 34.** Calificación de la Sensibilidad de los datos ....93
**Figura 35.** Calificación de la Probabilidad de explotación de las amenazas ....94
**Figura 36** Calificación de la Magnitud de impactos ....95
**Figura 37.** Calificación de la Red inalámbrica ....96
**Figura 38**. Calificación del Antivirus....97
**Figura 39** Calificación del Firewall....98
**Figura 40** T-Student ....103
**Figura 41**. Hoja de ruta de las variables ....116
***Figura 42*** captura de imagen del spss ver.25....127
**Figura 43** captura del spss ver.25....128

**Figura 44.** Revisión de las Torres, su respectivo mantenimiento.....133
**Figura 45**. Cambios de templadores .....133
**Figura 46**. Cambios de templadores .....134
**Figura 47.** Cambios de antenas y equipos de radioenlace.....134
**Figura 48.** Cambio de equipos en las troncales del radio enlace .....135
**Figura 49** cambio de antena en mal estado.....135
**Figura 50** Sistema de Radio enlace .....136
**Figura 51**. Actividad de los usuarios.....137
**Figura 52.** Sistema de control de la red con winbox de Mikrotik.....138

# INDICE DE TABLAS

**Tabla 1 Cuadro de la población propia** ....34
**Tabla 2 Distribución nominal standard.** ....35
**Tabla 3 Torres para enlace propia** ....39
***Tabla 4*** **Equipos de proveedor de servicio de internet (ISP)** (sagemcom, 2020)**,** (tp-link, 2020) ....41
***Tabla 5*** **Equipos de respaldo energético** (FORZA, 2020) ....42
**Tabla 6 Equipo de medios de red** (ubiquiti, 2020) ....43
**Tabla 7 Equipos de ruteros** (ubiquiti, 2020) (Mikrotik, 2020) ....45
**Tabla 8 Equipos para enlaces inalámbricos propia** (ubiquiti, 2020) (Mikrotik, 2020) ....48
**Tabla 9 Lista de personal propia** ....52
**Tabla 10 De identificación de vulnerabilidades** ....56
**Tabla 11 De caracterización de los controles** ....57
**Tabla 12 De determinación de probabilidades** ....58
**Tabla 13 De análisis de impacto** ....59
**Tabla 14 De determinación del riesgo** ....60
**Tabla 15 De recomendación de control** ....60
**Tabla 16. Controles recomendados, con relación al análisis de riesgos** ....62
**Tabla 17 Calificación del ruter y del equipo de enlace** ....70
**Tabla 18 Cómo califica al personal técnico** ....71
**Tabla 19 Cómo califica el servicio de internet** ....72
**Tabla 20 Los reportes de ataque de virus** ....73
**Tabla 21 Los reportes de definiciones de amenazas** ....74
**Tabla 22 La motivación de los ataques** ....75
**Tabla 23 Capacidad de las amenazas** ....76
**Tabla 24 Impacto de los ataques** ....77
**Tabla 25 Sensibilidad de tus datos** ....78
**Tabla 26 Probabilidad de explotación de las amenazas** ....79
**Tabla 27 Magnitud de los impactos** ....80
**Tabla 28 Red inalámbrica** ....81
**Tabla 29 Antivirus** ....82
**Tabla 30 Firewall** ....83
**Tabla 31 Pre-test** ....84
**Tabla 32 Reuter equipo de enlace** ....85
**Tabla 33 Personal técnico** ....86
**Tabla 34 Servicio de internet** ....87
**Tabla 35** ***Los reportes de ataque de virus*** ....88
**Tabla 36 Definiciones de amenazas** ....89
**Tabla 37 Motivación de ataques** ....90
**Tabla 38 Capacidad de las amenazas** ....91
**Tabla 39 Impactos de los ataques** ....92
**Tabla 40 Sensibilidad de tus datos** ....93
**Tabla 41 Probabilidad de explotación de las amenazas** ....94
**Tabla 42 Magnitud de impactos** ....95
**Tabla 43 Red inalámbrica** ....96
**Tabla 44 Antivirus** ....97

**Tabla 45 Firewall**.....98
**Tabla 46 Post- test** .....99
**Tabla 47 Calculo del valor crítico y la función de prueba** .....101
**Tabla 48 Calcular desviación estándar (s)**.....102
**Tabla 49 Ficha de observación pre-test** .....105
**Tabla 50 Ficha de evaluación post-test**.....106
**Tabla51 Formulación Del Problema** .....115
**Tabla 52 Tabla de operaciones de variables** .....117
**Tabla 53 Matriz de consistencia sistémica**.....120
**Tabla 54 Estadísticos descriptivos**.....123
**Tabla 55 Estadísticos descriptivos**.....124
**Tabla 56 cuadro de observaciones con porcentaje de actividad desarrollada** .....131

# RESUMEN

El objetivo del trabajo es desarrollar un sistema de Gestión de Riesgos utilizando la metodología NIST SP 800-30 a la seguridad en redes inalámbricas, propuesta por el Instituto Nacional de Estándares y Tecnología.

Con la metodología NIST SP 800-30 permite hacer 9 faces de la cual ayuda a evaluar los riesgos de la información especialmente a los sistemas de TI (Tecnología de la Información), por la cual es aplicable con el sistema de seguridad de la red inalámbrica.

En la metodología permite hacer caracterización del sistema a su vez también hace un inventario de los activos. Se plantea la recolección de un listado de amenazas que podría explotar las vulnerabilidades del sistema, un listado de vulnerabilidades relacionados con los activos, y un listado de controles. Con una evaluación del riesgo hace posible comprender la probabilidad de vulnerabilidades, análisis de impacto y ocurrencia de amenazas, cálculo de riesgo y por último hace posible la toma de decisiones y controles recomendados.

La seguridad en redes inalámbricas es usado para dar prueba que la metodología NIST SP 800-30 es una de las metodologías que se puede aplicar a un sistema de seguridad de la información haciendo aplicable sus faces en el transporte de la información mediante lo inalámbrico. De tal manera que sí se logró muchas mejoras en la red inalámbrica tales como menos caídas de la red, menos ataque de virus, intrusos, mal uso de usuarios sin experiencia o poca experiencia en la red.

También se logró que se establezca una serie de cronogramas de actividades de acuerdo con los inventarios de activos tales como mantenimientos de torres, cambios de equipos obsoletos, cables de red, antenas, mejoras en la energía eléctrica.

**Palabras claves:** metodología NIST SP 800-30, Seguridad en redes inalámbricas, tecnología de la información

# ABSTRACT

The objective of the job is develop a Risk Management System using the NIST SP 800-30 methodology for wireless network security, proposed by The National Institute of Standards and Technology.

With the NIST SP 800-30 methodology, allows 9 point they be made, which helps to assess the risks of information, especially to TI (Information Technology) systems, which is applicable with the wireless network security system.

In the methodology it allows characterization of the system in turn also makes an inventory of the assets. It is considered the collection of a list of threats that could exploit the vulnerabilities of the system, a list of vulnerabilities related to the assets, and a list of controls. With a risk assessment, it is possible to understand the likelihood of vulnerabilities, impact analysis and occurrence of threats, risk calculation and, finally, make it possible to do recommended decisions and controls.

The security in wireless networks is used to prove that the NIST SP 800-30 methodology is one of the methodologies that can be applied to an information security system making its face applicable in the transport of information via wireless. In such a way that many improvements in the wireless. In such a way that many improvements wireless network were achieved such as less network crashes, less virus attack, intruders, misuse of inexperienced users or little network experience.

It also succeeded in establishing a series of activity schedules in accordance with asset inventories such as tower of internet maintenance, obsolete equipment changes, network cable, antennas, and improvements in electrical energy.

In the aspect of risk controls, users were helped to make their antivirus original, as well as not to give their password to anyone and to make a password with uppercase, lowercase, ASKII code.



**Keywords**: NIST SP 800-30 methodology, Wireless network security, information technology

# INTRODUCCION

Las redes inalámbricas, por la gran movilidad que aportan, se han convertido en un sector de acelerado crecimiento en las comunicaciones. La aspiración del hombre de llevar información cada vez más lejos sin cables de manera segura, confiable, accesible, la comodidad en la conexión y el rápido despliegue que representan son algunos de los aspectos que motivan su rápida asimilación.

En la actualidad, la red inalámbrica tienen numerosos mecanismos y protocolos que, aunque no garantizan de forma absoluta la integridad y confidencialidad de la información que por ellas transita, sí, proporcionan barreras que reducen de forma considerable la cantidad de personas capaces (por sus conocimientos y recursos) de efectuar ataques exitosos que llegan al punto de competir con muchas de las soluciones cableadas actualmente disponibles. Desafortunadamente, al igual que sucede muchas veces con las redes cableadas, la complejidad de algunas de estas medidas y el desconocimiento por parte de usuarios y administradores, trae como resultado que proliferen muchos sistemas desprotegidos, donde la gran mayoría no cuenta incluso con los requerimientos mínimos recomendados. Debido a la gran extensión que tiene su uso a nivel global, se le dedicará un aparte especial a los tipos de ataques más comunes en las redes 802.11. Favorito de los atacantes.

El presente trabajo es desarrollado con la finalidad de apoyar a la seguridad informática de una empresa y/o personas, con la metodología NIST SP 800-30, que utilizan redes inalámbricas. Ya que esta tecnología se ha extendido para que sea cada vez más accesible a los usuarios, por tal motivo los métodos de ataque son más efectivos en conseguir información de distintos equipos que tienen un sistema de seguridad informática, por ese motivo se realiza el trabajo para saber cómo protegernos de los robos de información en la red inalámbrica.

# CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

La empresa SERVINTECOMP se encuentra ubicado en Jr. Luis Sánchez Cerro 430 de la provincia de Coronel Portillo, distrito de Callería la cual brinda servicio de internet de banda ancha para uso domiciliario y empresarial en los distritos de Neshuya, Von Humboldt y Callería.

**Misión**

Brindar una amplia gama de soluciones informáticas a la región Ucayali al proveer bienes y servicios en el ámbito de telecomunicaciones.

**Visión**

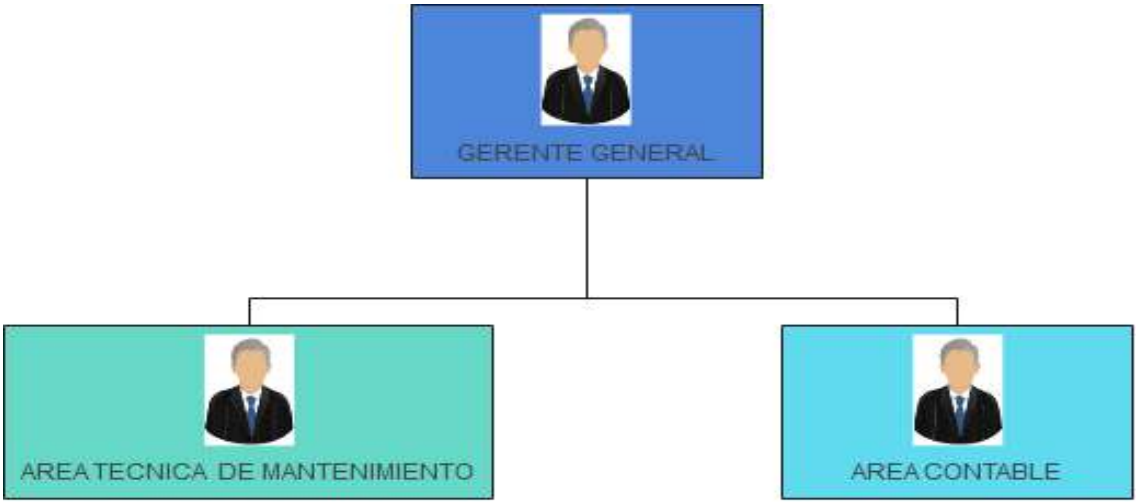
La visión de la empresa es brindar una amplia gama de soluciones informáticas a la región Ucayalial; proveer bienes y servicios en el ámbito de telecomunicaciones.

**Valores**:

- **Puntualidad.-** Es considerado una cualidad esencial, representa a la empresa, para dar confianza al cliente.

- **Honestidad.**-Es un acto de relevancia al individuo que observa la norma y conducta de compromiso de ser sincero y consecuente con su conducta hacia la empresa.
- **Respeto.**-son considerados como norma de armonía con el dialogo entre clientes, proveedores con la empresa como también entre directivos de la empresa para lograr los objetivos de la misión y visión.
- Amabilidad.- La amabilidad reporta armonía de trabajo y evita el estrés dando lugar a que el trabajador se comprometa más con la empresa.

**Organigrama**:




Fuente: Elaboración Propia.

**Figura 1**.organigrama de la empresa.

**DEFINICIONES DE RESPONSABILIDADES**

- **Gerente General:** Es el encargado de las todas de decisiones de la empresa para el bienestar de la misma para seguir en el cumplimiento de la misión y visión.
- **Técnico de Mantenimiento**: Es el encargado de las soluciones de los problemas técnicos de la empresa y los usuarios en cuanto a la conectividad del internet.

- **Área contable:** se encarga de los cobros y pagos de los servicios adquiridos por la empresa.

La empresa presta el servicio de:

- Mantenimiento de impresoras.
- Mantenimiento de computadoras.
- Reparación de computadoras.
- Instalación de cámaras de vigilancia.

La empresa que da el servicio de internet por medio de los radio enlaces viene sufriendo disminución de usuarios, siendo principal comentario de los usuarios la lentitud del servicio.

Debido a los comentarios obtenidos se realizó una evaluación llegando a determinar las siguientes causas:

- Constantes ciberataques de personas que quieren ingresar a la red para tener internet gratuito, robar información, infectar virus.
- Constantes cortes eléctrico en las troncales principales dando problemas de conectividad.
- Se cuenta con equipos superior a los 4 años de uso.
- No se cuenta con un sistema de respaldo de seguridad.
- No cuenta con un protocolo de seguridad.
- No cuenta con respaldo de energía.
- No cuenta con un vehículo para traslado.

Con el propósito de corregir esta realidad problemática se plantea en siguiente proyecto de investigación: “GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICAS EN LA EMPRESA SERVINTECOMP UCAYALI-2018”.

## 1.2 FORMULACIÓN DEL PROBLEMA

### 1.2.1 Problema General

¿En qué medida influye la gestión de riesgos de NIST SP 800-30 a la seguridad de la red inalámbrica en la empresa SERVINTECOMP PUCALLPA: 2018?

### 1.2.2 Problemas Específicos

1. ¿En qué medida la caracterización del sistema de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?
2. ¿En qué medida las identificaciones de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbrica?
3. ¿De qué manera el análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?
4. ¿Cómo la determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800 -30 aporta a la seguridad en redes inalámbricas?
5. ¿En qué medida el análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?
6. ¿Cómo la determinación de riesgos de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?

7. ¿En qué medida la recomendación de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?
8. ¿Cómo la documentación de resultado de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?

## 1.3 OBJETIVOS DE LA INVESTIGACIÓN

### 1.3.1 Objetivo general

Analizar y caracterizar la gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI-PUCALLPA: 2018.

### 1.3.2 Objetivos específicos

1. Analizar la caracterización del sistema de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.
2. Analizar identificaciones de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbrica.
3. Describir el análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.
4. Describir la determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800 -30 a la seguridad en redes inalámbricas.

5. Analizar el análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas.
6. Describir la determinación de riesgos de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.
7. Analizar la recomendación de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.
8. Describir la documentación de resultado de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.

## 1.4 JUSTIFICACIÓN E IMPORTANCIA

### 1.4.1 Justificación

El estar libre de cables conectados a tu computador en oficinas y en el hogar es una práctica cada vez más extendida en la sociedad. Esta situación se ve favorecida y alentada por los continuos avances en el ámbito de las tecnologías inalámbricas, donde cada vez se están consiguiendo soluciones de mayor velocidad de conexión, con más servicios y a unos costos cada vez más bajos a grandes distancias, debido a esta situación también los hackers están atacando a este sistema por lo fácil de interceptar mediante, frecuencia de onda cifradas, para luego descifrar su contraseña de acceso a la red inalámbrica, en tal sentido la metodología NIST SP 800-30 cuenta con un proceso de seguridad en diferentes ámbitos del trabajo en la red tanto en seguridad y respaldo de la información.

La metodología NIST SP800-30 se centra en la buenas prácticas de la seguridad en donde su enfoque se base en 9 aspecto importantes tales

como la caracterización del sistema, identificación de amenazas, identificación de vulnerabilidades, análisis de controles, determinación de probabilidades, análisis de impacto, determinación del riesgo, conclusiones y recomendaciones.

### 1.4.2 Importancia

Hoy en la actualidad el sistema de redes inalámbricas se ha hecho muy extensos e importantes para todos los usuarios que tienen acceso a ella. Los usuarios privados y del estado que trabajan en las zonas alejadas de la ciudad, no cuentan con la línea de internet cableada o es cara su conexión vía inalámbrica con empresas grandes tales como TELEFÓNICA, CLARO, ENTEL, BITEL por tal motivo acuden a las empresas pequeñas como SERVINTECOMP, INFORTEL, entre otras empresas. Los usuarios privados lo utilizan para hacer diversas transacciones que les permite progresar como empresa por ejemplo: hacer pagos a sus proveedores, ver precios de los mercados locales y nacionales, también hacen ventas vía internet, pagan a su personal vía banca por internet, publican sus productos, pagan sus impuestos, ven en tiempo real por medio de las cámaras las diferentes actividades de la empresa en cualquier parte del mundo en tal caso los hacker y cualquier persona que ve YouTube sobre cómo romper contraseña en una red inalámbrica cuando no hay los mínimos sistemas de seguridad logran ingresar acceder a la red y en los peores de los casos se roban la información de la empresa, peor aun cuando el hacker es hábil se puede robar la base de datos de la empresa.

En las instrucciones públicas la utilizan para hacer diversas actividades tales como hacer consultas en la página del estado como el MEF,

CONSUCODE, también para hacer denuncias en línea como lo hacen las comisarías de igual manera pueden perder con sus datos sin un sistema de seguridad de la información vía inalámbrica.

Entonces los clientes pues tienen mucho que perder cuando la línea de internet es lenta y no satisface sus actividades, cosa que está pasando en los clientes de la empresa SERVINTECOMP por eso algunos clientes cortaron vínculo con la empresa.

La empresa ha tomado la iniciativa de ver porque hay tanta lentitud y se da la sorpresa que hay mucha piratería a la línea de internet inalámbrico como también los virus, descargas, ver videos entre otras causas como también no cuenta con un sistema de seguridad por eso es importante hacer una gestión de seguridad con la metodología NIST SP800 -30.

## 1.5 HIPÓTESIS Y VARIABLES DE LA INVESTIGACIÓN

### 1.5.1 Hipótesis general

La gestión de riesgos con metodología NIST SP 800-30 influye significativamente en la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI-PUCALLPA-2018.

### 1.5.2 Hipótesis específica

1. Caracterización del sistema de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.
2. Las identificaciones de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbrica.

3. El análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.
4. La determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800 -30 influye significativamente a la seguridad en redes inalámbricas.
5. El análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.
6. La determinación de riesgo de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.
7. La recomendación de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.
8. La documentación de resultado de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.

## 1.6 VARIABLES (DEFINICIÓN CONCEPTUAL Y OPERACIONAL)

**Variable independiente:**

**Definición conceptual**:

Se define que la NIST SP 800-30, se encarga de la gestión de riesgos, orientada a procesos mediante un adecuado análisis y gestión del riesgo, proporcionando una evaluación cuantitativa y cualitativa, así como métodos semi cualitativos que permiten administrar eficazmente el riesgo para la seguridad de la información ( Erreyes Pinzón, 2017).

Señala que la NIST SP 800-30 está orientada especialmente a los profesionales vinculados con la gestión de riesgos en las organizaciones como: jefes de los organismos, directores generales, jefe de operaciones, ejecutivo de riesgo; los individuos encargados de la vigilancia de la seguridad de la información, su gestión y responsabilidades operativas (por ejemplo, los directores de información, oficiales de alto rango, los administradores y propietarios de sistemas de información, los proveedores de control comunes etc) (NIST 2012,p5).

## Definición operacional:

Está comprendida por las dimensiones que constituyen Gestión De Riesgos con Metodología NIST SP 800-30:

1. **Caracterización del sistema**

   Establece el alcance del ejercicio de evaluación del riesgo y proporciona información esencial para definir el riesgo.

2. **Identificación de amenazas**

   Es donde se identifica las potenciales amenazas que podrían explotar las vulnerabilidades del sistema. Se identifica en tres.

   - ✓ Humana: actos involuntarios (por ejemplo, entrada de datos inadvertida), o acciones deliberadas (por ejemplo, ataques basados en la red, subida de software malintencionada, o acceso sin autorización).
   - ✓ Natural: Inundaciones, terremotos, tormentas eléctricas.
   - ✓ Ambiental (por ejemplo, suspensión a largo plazo de la corriente eléctrica).

**3. Indentificación de vulnerabilidades**

Es donde la se identifican las vulnerabilidades del sistema (defectos o fallos) que podría ser explotado por potenciales fuentes de amenazas.

**4. Análisis de controles**

Es donde se especifica los controles que utiliza el sistema de información para mitigar la probabilidad de ocurrencia de una amenaza(vulnerabilidad) y reducir su impacto, tales como:

a) Controles técnicos incorporados en el hardware, software, o programa fijo del equipo informático, y controles no técnicos, como políticas de seguridad; procedimientos operacionales; y seguridad del personal y ambiental.

b) Controles preventivos, por ejemplo, el cumplimiento de los controles de acceso, codificación criptográfica y autenticación.

c) Una lista de control que se utiliza para verificar el cumplimiento/incumplimiento de los requisitos de seguridad.

**5. Determinación de probabilidades**

Determinar la probabilidad (alta, media o baja) de ocurrencia de una amenaza (vulnerabilidad) deben considerase tres factores.

- ✓ La motivación y capacidad de las fuentes de amenaza.
- ✓ La naturaleza de la vulnerabilidad.
- ✓ La existencia de controles y la efectividad de los controles actuales.

**6. Análisis de impacto**

Prioriza los niveles de impacto asociados con la importancia de los activos de información de una organización basándose en una evaluación cualitativa o cuantitativa de la criticidad de esos activos. En este paso, es necesario vincular cada riesgo con los componentes arquitectónicos y determinar el impacto potencial de la amenaza sobre los activos y, posteriormente, establecer la magnitud del impacto (alto, medio o bajo) que pudiera resultar de una amenaza exitosa.

**7. Determinación del riesgo**

Valoración del nivel de riesgo para el sistema de información. Se calcula el riesgo en función de:

- ✓ La probabilidad de una fuente de amenaza.
- ✓ La magnitud del impacto.
- ✓ La pertinencia de los controles de seguridad para reducir o eliminar el riesgo.

**8. Recomendaciones de control**

Contribuyen al proceso de mitigación de riesgos y son el resultado del proceso de evaluación del riesgo. El objetivo de este paso es reducir a un nivel aceptable el nivel de riesgo para el sistema de información y sus datos. Deberá realizarse un análisis de costo-beneficio para demostrar que el costo de implementación de los controles recomendados puede justificarse con la reducción del nivel de riesgo.

**9. Documentación de Resultado**

La descripción de amenazas y vulnerabilidades, valoraciones de riesgos, y recomendaciones para la implementación de controles son documentados en un informe oficial. Su objetivo es servir de ayuda en el proceso de adopción de decisiones sobre cambios en la política, los procedimientos, el presupuesto y el sistema para reducir y corregir pérdidas potenciales.

## Variable dependiente:

**Definición conceptual**:

La Seguridad de Redes Inalámbricas:

La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. Como filosofía, complementa la seguridad del punto final, que se centra en dispositivos individuales; la seguridad de la red se centra en cómo interactúan esos dispositivos y en el tejido conectivo entre ellos (Fruhlinger, 2018).

La seguridad de la red se implementa mediante las tareas y herramientas que utiliza para evitar que personas no autorizadas entren a la red (Fruhlinger, 2018).

**Definición operacional:**

Nos fijamos en tres fases de la seguridad de la red que deberían ser el marco de referencia base para su estrategia:

- **Protección:** Debe configurar sus redes lo más correctamente posible.
- **Detección:** Debe ser capaz de identificar cuando ha cambiado la configuración o si algún tráfico de red indica un problema.

- **Reacción:** después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro.

Esto, en resumen, es una estrategia de defensa en profundidad (Fruhlinger, 2018)

# CAPITULO II: MARCO TEÓRICO

## 2.1 ANTECEDENTES DE LA INVESTIGACIÓN.

### 2.1.1 Tesis internacionales

- En un estudio de esquemas de seguridad en redes inalambricas: aplicación de buenas practicas en pymes y usuarios finales, 2016 utilizada en Colombia, concluyó que los avances tecnológicos, en las redes WiFi se han convertido más inseguras y vulnerables debido al medio de transmisión de señal que manejan(Verbel & Alvarez, 2016), haciendo que los ataques a estas sean cada vez más comunes.
- En la investigación “Diseño de estrategias de mitigación para mejorar la seguridad de información del sistema de control industrial en la empresa comercializadora san remigio” año 2015 utilizada en QUITO-ECUADOR, concluye que después de un análisis estructurado por los estándares NIST 800-82 y NIST 800-30, los resultados obtenidos se resumen en: 5 amenazas visibles, 15 vulnerabilidades detectadas, 17 riegos resultantes y por otro lado 10 estrategias de mitigación seleccionadasla necesidad de la empresa COMERCIALIZADORA SAN REMIGIO de mejorar la gestión de seguridad informática (Diaz Paul, 2015), que es indispensable

emprender un proyecto deimplementación de estrategias de mitigación y controles en el Sistema de Control.

- En la investigación "Propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del litoral" año 2015 utilizada en Madrid, concluye que cuyos resultados del análisis reflejaron que las medidas de seguridad han ayudado a reducir los riesgos de amenazas físicas de manera oportuna y que solo requieren de implementar procesos para una mejor gestión; en cambio el nivel de seguridad a nivel de datos y aplicación es bajo debido a la carencia de procedimientos y normas que minimicen el acceso no autorizado, la fuga de información y ataques a los sistemas ( Molina Miranda, 2015).
- En su investigación "Diseño de un plan para el tratamiento de riesgos tecnológicos utilizando la metodología nist sp 800-30" año 2015 utilizada en Ecuador, concluye que debido a la constante evolución de la tecnologías de información también evolucionan nuevas amenazas que son más difíciles de detectar y contrarrestarlas, estas amenazas pueden arremeter en contra de las organizaciones públicas y privadas de tal modo que afectarán las actividades diarias y causarán pérdidas considerables (Cueva beltran , 2015), mediante la gestión de los riesgos tecnológicos podemos mitigar las posibles amenazas a las que se encuentran expuestas estás organizaciones

### 2.1.2 Tesis nacionales

- Según (Blas Rinza, 2017) “Seguridad y control del acceso a las redes inalámbricas en la unsm-t mediante servidores de autentificación radius con el uso de certificados digitales” en Tarapoto 2017, concluye que los protocolos avanzados de seguridad con un servidor radius con

certificados digitales nos permitieron encriptar los mensajes que se envían por la red entre un servidor y un cliente, garantizando la seguridad de la red via web.

- Según (Gonzales Rondan, 2015) “Diseño e implementación de un proveedor de servicio de internet inalámbrico utilizando la tecnología routerboard mikrotik, en la ciudad de Recuay en Huaraz en el año 2015” concluye que los equipos de transmisión de la red inalámbrica deben soportar una alta seguridad puesto que estarán expuestos a situaciones de intrusos que se pueden filtrar a la red y eso es establecer protocolos de seguridad aparente.
- Según ( Barrenechea Zavala, 2015) "Diseño de una red lan inalambrica" año 2015 utilizada en Lima, concluye La configuración de seguridad para acceso a la red inalámbrica, en conjunto con la asignación de VLAN en el switch y las listas de control de acceso en el router, conforman un robusto sistema de seguridad

## 2.2 BASES TEORICAS

### 2.2.1 Gestión de riesgos

Es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen la identificación, el análisis y la evaluación de riesgo para luego establecer las estrategias para su tratamiento, utilizando recursos gerenciales. Reducir el impacto negativo del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular mediante una decisión informada. (WIKIPEDIA, 2019).

### 2.2.2 Metodología de NIST SP 800-30

Esta metodología se basa en un proceso de tres pasos: evaluación del riesgo, análisis y evaluación de solución; la metodología NIST SP 800 30 puede ser aplicada a la evaluación de sistemas individuales ó interrelacionados (Arias & LLanos, 2012).

Es una guía que propone un conjunto de recomendaciones y actividades para una adecuada gestión de riesgos como parte de la gestión de la seguridad de la información; sin embargo, esto no es suficiente, pues se necesita del apoyo de toda la organización para que los objetivos y alcance de la gestión de riesgos concluyan con éxito (Avalos Serrano, 2007).

Es importante que las empresas tomen en cuenta normas como NIST SP 800-30 para salvaguardar su información, ya que hoy en día es precisamente ésta, la que más importancia tiene, incluso podemos mencionar que la empresa no solo debe cuidar sus finanzas, sino su información como un bien de la empresa por eso debe ser integra la información, con disponibilidad para las personas adecuadas y lo más importante confidencial. (Roxana & Yesenia, 2013).

La metodología NIST SP 800 30 está compuesto por 9 pasos básicos para el análisis de riesgos (Arias & LLanos, 2012).

1. Caracterización del sistema.
2. Identificación de amenazas.
3. Identificación de vulnerabilidades.
4. Análisis de controles.
5. Determinación de Probabilidades
6. Análisis de impacto.
7. Determinación del riesgo.

8. Recomendaciones de control.
9. Documentación de Resultado

Y se define de la siguiente manera:

**1. Caracterización del sistema**

Establece el alcance del ejercicio de evaluación del riesgo y proporciona información esencial para definir el riesgo.

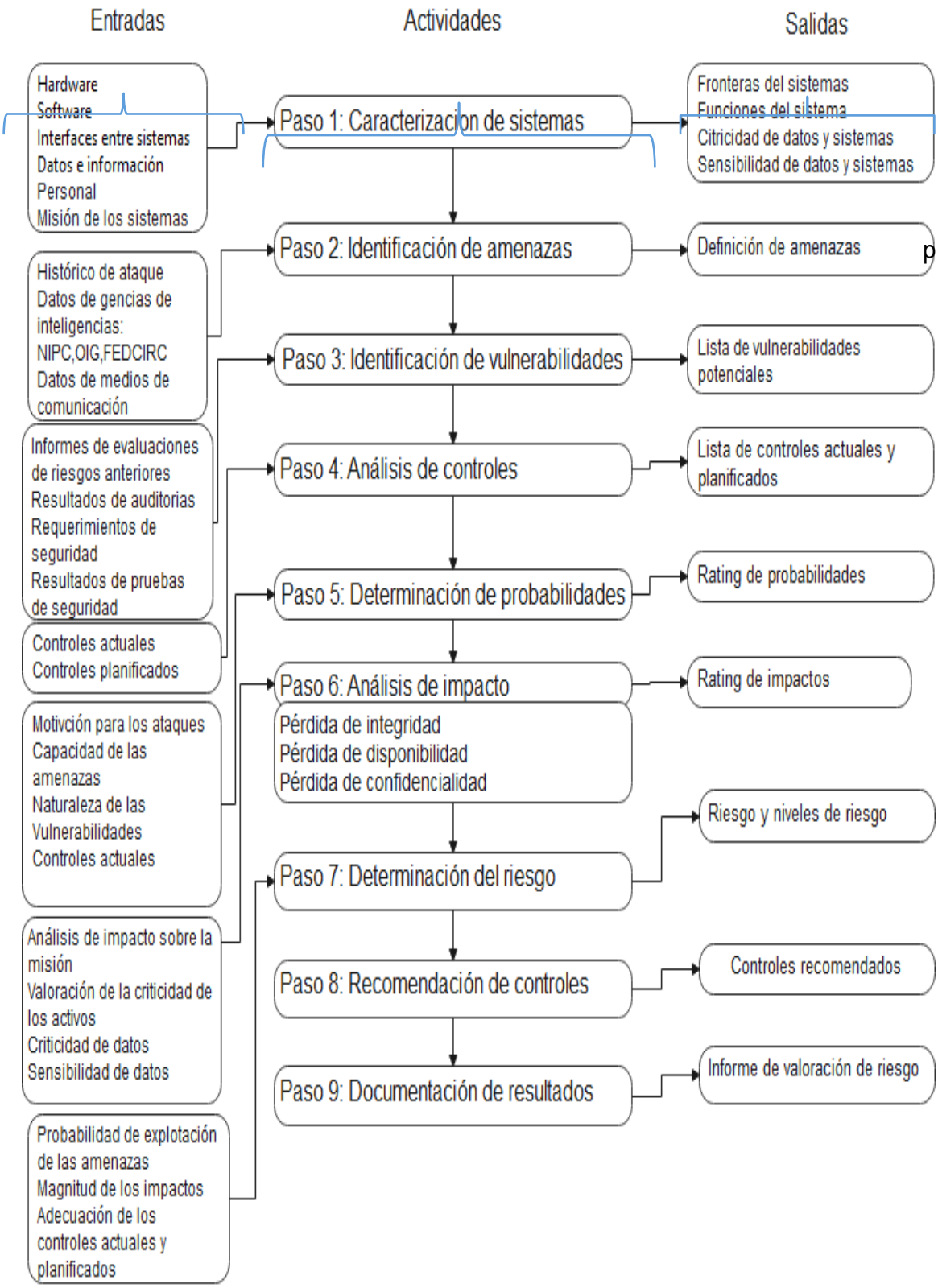
**2. Identificación de amenazas**

Es donde se identifica las potenciales amenazas que podrían explotar las vulnerabilidades del sistema. Se identifica en tres.

**a. Humana:** actos involuntarios (por ejemplo, entrada de datos inadvertida), o acciones deliberadas (por ejemplo, ataques basados en la red, subida de software malintencionada, o acceso sin autorización).

**b. Natura**l: Inundaciones, terremotos, tormentas eléctricas.

**c. Ambiental** (por ejemplo, suspensión a largo plazo de la corriente eléctrica).




Fuente: Guía de la Metodología Nist Sp 800 30

**Figura 2** Proceso de la metodología NIST SP 800-30

## 3. Indentificación de vulnerabilidades

Es donde la se identifican las vulnerabilidades del sistema (defectos o fallos) que podría ser explotado por potenciales fuentes de amenazas.

## 4. Análisis de controles

Es donde se escifica los controles que utiliza el sistema de información para mitigar la probabilidad de ocurrencia de una amenaza(vulnerabilidad) y reducir su impacto, tales como:

1. Controles técnicos incorporados en el hardware, software, o programa fijo del equipo informático, y controles no técnicos, como políticas de seguridad; procedimientos operacionales; y seguridad del personal y ambiental.
2. Controles preventivos, por ejemplo, el cumplimiento de los controles de acceso, codificación criptográfica y autenticación.
3. Una lista de control que se utiliza para verificar el cumplimiento/incumplimiento de los requisitos de seguridad.

## 5. Determinación de probabilidades

Determinar la probabilidad (alta, media o baja) de ocurrencia de una amenaza (vulnerabilidad) deben considerase tres factores.

**i.** La motivación y capacidad de las fuentes de amenaza.

**ii.** La naturaleza de la vulnerabilidad.

**iii.** La existencia de controles y la efectividad de los controles actuales.

## 6. Análisis de impacto

Prioriza los niveles de impacto asociados con la importancia de los activos de información de una organización basándose en una evaluación cualitativa o cuantitativa de la criticidad de esos activos. En este paso, es necesario vincular cada riesgo con los componentes arquitectónicos y determinar el impacto potencial de la amenaza sobre los activos y, posteriormente, establecer la magnitud del impacto (alto, medio o bajo) que pudiera resultar de una amenaza exitosa.

## 7. Determinación del riesgo

Valoración del nivel de riesgo para el sistema de información. Se calcula el riesgo en función de:

**i.** La probabilidad de una fuente de amenaza.

**ii.** La magnitud del impacto.

**iii.** La pertinencia de los controles de seguridad para reducir o eliminar el riesgo.

## 8. Recomendaciones de control

Contribuyen al proceso de mitigación de riesgos y son el resultado del proceso de evaluación del riesgo. El objetivo de este paso es reducir a un nivel aceptable el nivel de riesgo para el sistema de información y sus datos. Deberá realizarse un análisis de costo-beneficio para demostrar que el costo de implementación de los controles recomendados puede justificarse con la reducción del nivel de riesgo.

## 9. Documentación de resultado

La descripción de amenazas y vulnerabilidades, valoraciones de riesgos, y recomendaciones para la implementación de controles son

documentados en un informe oficial. Su objetivo es servir de ayuda en el proceso de adopción de decisiones sobre cambios en la política, los procedimientos, el presupuesto y el sistema para reducir y corregir pérdidas potenciales.

### Ventajas de la metodología NIST SP 800-30

Este proceso permite determinar el nivel de amenaza potencial y sus riesgos asociados con un sistema TIC. El proceso de evaluación del riesgo ayuda a determinar los diferentes factores de vulnerabilidad y que ayuda a mejorar los sistemas de seguridad. (Arias & LLanos, 2012).

### Desventajas de la metodología NIST SP 800-30

No obstante, al ser una metodología tan robusta, esta propiedad se convierte en una limitante para su aplicación en empresas con altas limitaciones de recursos humanos. (Arias & LLanos, 2012).

## *2.2.3* Métodos de seguridad de redes inalámbricas*.*

Para implementar este tipo de defensa en profundidad se hace lo siguiente:

a) **Protección:** Debe configurar sus redes lo más correctamente posible.

b) **Detección**: Debe ser capaz de identificar cuando ha cambiado la configuración o si algún tráfico de red indica un problema.

c) **Reacción:** después de identificar los problemas rápidamente, responderlos y regresar a un estado seguro.

Esto, en resumen, es una estrategia de defensa en profundidad (Fruhlinger, 2018).

### 2.2.4 Tipos de redes inalámbricas

Esto es de acuerdo al autor (VIU, 2019);

**WPAN**: Wireless Personal Area Network. En este tipo de red de cobertura personal.

**WLAN**: Wireless Local Area Network. Se encuentran basadas en **Wi-Fi,** un estándar de comunicación inalámbrica basado en la norma IEEE 802.11. Puede presentar mejoras con respecto a la velocidad según sus estándares y alcanza una distancia de hasta 20 Km.

**WMAN**: Wireless Metropolitan Area Network.

**WWAN:** Wireless Wide Area Network.

Una WWAN difiere de una WLAN (Wireless Local Area Network) en que usa tecnologías de red celular de comunicaciones móviles.

Hay también la red infraestructura da como se nota en la figura.




Fuente. **Elaboración Propia**

**Figura 3.** Red estructurada

### 2.2.5 Ventajas de la red inalámbrica

- No existen cables físicos: por lo tanto, no hay cables que se enreden, ni que entorpezcan la transintabilidad o que molesten estéticamente.

- La instalación de redes inalámbricas suele ser más económica.
- Su instalación también es más sencilla.
- Permiten gran alcance; las redes hogareñas inalámbricas suelen tener hasta 100 metros desde la base transmisora.
- Permite la conexión de gran cantidad de dispositivos móviles. En las redes cableadas mientras más dispositivos haya, más complicado el entramado de cables.
- Posibilidad de conectar nodos a grandes distancias sin cableado, en el caso de las redes inalámbricas corporativas.
- Permiten más libertad en el movimiento de los nodos conectados, algo que puede convertirse en un verdadero problema en las redes cableadas.
- Permite crear una red en áreas complicadas donde, por ejemplo, resulta dificultoso o muy cara conectar cables.
- Permite ampliar una red cableada en caso de redes mixtas (mezclas de inalámbricas con cableadas.

### *2.2.6* Desventajas de las redes inalámbricas*.*

Son algo más inseguras que las redes cableadas, por eso los organismos de defensa e inteligencia gubernamentales utilizan redes con cables dentro de sus edificios.

- El ancho de banda de las redes inalámbricas es menor que las cableadas; en otra palabra, la velocidad alcanzada por las redes cableadas es mayor.
- Las inalámbricas sufren colisión de datos.

- Las redes inalámbricas son un poco más inestables que las redes cableadas, pueden verse afectada por otras ondas electromagnéticas o aparatos electrónicos cercanos.
- La señal inalámbrica puede verse afectada e incluso interrumpida por objetos, árboles, paredes, espejos, etc.

### 2.2.7 Definición de términos básicos

Según los terminos basico de (Oracle, 2014)**,**

(ICMAS Ltd. & Public Utility Reaserch Center , 2014) **y** (Rodrigo, 2014) se obtiene el siguiente enlistado**.**

**AP.-** Del inglés Access Point, o punto de acceso. El punto de acceso corresponde a un transmisor-receptor de redes inalámbricas, o "estación base", que puede conectar una red LAN cableada a uno o varios dispositivos inalámbricos. Los puntos de acceso también se pueden conectar en puente entre sí.

**Ad-doc**.- Configuración del equipo cliente que ofrece conectividad independiente entre dispositivos dentro de una red LAN inalámbrica como alternativa, los ordenadores se pueden comunicar entre sí a través de un punto de acceso.

**Clave de codificación.-** Una serie de letras entre mayúsculas y minúsculas, código ASkII y números que permite codificar datos y después decodificarlos de forma que se puedan compartir de manera segura entre los miembros de una red. Los usuarios de WEP, WAP2 utilizan una clave de codificación que codifica automáticamente los datos salientes. Esta misma clave le permita al ordenador receptor decodificar automáticamente la información para que se la pueda leer.

**Cliente.-** una aplicación instalada en un ordenador o dispositivo conectado a una red que solicita servicios (archivos, impresión) de otro miembro de la red.

**DHCP.-** Del inglés Dynamic Host Configuation Protocol, o Protocolo de configuración dinámica de host. El DHCP es una utilidad que le permite a un servidor asignar. Sin un DHCP, el administrador de TI tendría que asignar manualmente todas las direcciones IP para todos los clientes de la red. Al utilizar un DHCP, cada vez que un cliente entra en la red, se le asigna automáticamente una dirección IP.

**Dbi(decibelios isotrópica).-** La ganancia de la antena expresada en la unidad debe iniciar el valor en decibelios del cual la ganancia de la antena es mayor que la de una antena isotrópico hipotética.

**Dbm(decibelios milivatios).-** Se define como el nivel de potencia en decibelios en relación a un nivel de referencia de 1mw.

**DNS.-**Del inglés Domain Name System (Service o Server), también llamado Sistema (servicio o servidor) de nombres de dominio. El DNS es un programa que traduce los URL en direcciones IP ingresando a una base de datos ubicada en una serie de servidores Internet. Este programa funciona en segundo plano para que el usuario pueda navegar por Internet utilizando direcciones alfabéticas en vez de una serie de números. El servidor DNS convierte un nombre como mi sitio web.com en una serie de números como 102.22.34.22. Cada sitio Web tiene su propia dirección IP en Internet.

**DSL.-** Del inglés Digital Sebcriber Lines, o Línea de cliente digital. Diferentes protocolos de tecnologías para la transmisión de datos, voz y video de alta velocidad mediante cables telefónicos comunes de cobre de par trenzado.

**Dirección IP.-** Un número que identifica cad emisor o receptor de información enviada en Internet.

**Enrutador.-**Punto de acceso o dispositivo que envía datos desde una red de área local (LAN) o red de área amplia (WAN) a otra. El enrutador monitorea y controla el flujo de datos, y envía información a través de la ruta más eficiente en función del tráfico, el costo, la velocidad las conexiones, etc.

**IP.-** Del inglés Internet Protocol, o Protocolo de Internet. Tecnología que permite la transmisión de voz, datos y video a través de Internet, redes WAN y LAN con conexión IP. Incluye, además VOIP (del inglés Voice over IP).

**Infraestructura.-** Modo de acceso que proporciona conexión a un punto de acceso. En comparación con el modo AD-hoc, en el que los ordenadores se comunican directamente entre sí, los clientes configurados en el modo Infraestructura pasan datos a través de un punto de acceso central. El punto de acceso no sólo controla el tráfico de la red inalámbrica del entorno inmediato, sino que, además proporciona comunicación con la red cableada.

**Nombre de la red.-**Identifica la red inalámbrica para todos los componentes compartidos. Durante el proceso de instalación de la mayoría de las redes inalámbricas, el usuario debe introducir el nombre de la red o SSID. Al configurar el ordenador, el grupo de trabajo o la red cableada, se utilizan diferentes nombres de red.

**Puente.-**Producto que conecta una red LAN con otra red de área local que utilice el mismo protocolo (por ejemplo, inalámbrico, Ethernet o toquen ring).Por lo general, los puentes inalámbricas se utilizan para conectar edificios o escuelas en un campus.

**SSID.-**Del inglés Service Set Identifier, o Identificador de conjunto de servicio. Un SSID también se denomina Nombre de la red, ya que básicamente consiste en un nombre que identifica una red inalámbrica. El identificador se adjunta a la red de área local¨(LAN) y actúa como contraseña cuando un dispositivo se conecte a la red a menos que pueda entregar un SSID único. El SSID se puede transmitir mediante el enrutador de red, permitiéndole al dispositivo detectarlo como una red disponible. El SSID no proporciona seguridad a la red.

**SSL.-**Del inglés Secure Sockets Layer, o nivel de sockets seguro. Programa de codificación que normalmente utilizan los sitios de banca y venta electrónica y que protege la integridad financiera de las transacciones.

**TCP/IP.-** Protocolo de transporte de control /Internet protocolo que es tecnología tras **Internet** y las comunicaciones entre ordenadores en una red.

**WEP.-**Del inglés Wired Equivalent Privacy, o Privacidad equivalente al cableado. Seguridad básica para sistemas inalámbricos proporcionada por Wi-Fi. En algunos casos, WEP puede ser todo lo que un usuario o una pequeña empresa necesiten para proteger los datos. WEP se encuentra disponible en nodos de codificación de 40 bits (o codificación de 128 bits). La codificación d e108 bits permite un algoritmo mayor que, a su vez, toma más tiempo descifrar, proporciona una mayor que el modo básico de 40 bits (64 bits).

**WAP.-**Del inglés Wi-Fi Protected Access, o Acceso Wi-fi protegido. Se trata de un **estándar** de seguridad para redes Wi-Fi que trabaja con productos Wi-Fi existentes compatibles con WEP (Wired Equivalent Privacy, Privacidad equivalente al cableado). Codifica los datos a través

del protocolo TKIP (Temporal Key Integrity Protocol, Protocolo de integridad de clave temporal).TKIP mezcla las claves y garantiza que no se hayan alterado. La autenticación del usuario se realiza mediante el protocolo EAP (Extensible Authentication Protocol, Protocolo de autenticación ampliada) para garantizar que solo usuarios autorizados puedan ingresar a la red.

**WPA2 ( WiFi Protected Access 2)**.-WPA2 es la segunda generación de WPA y proporciona un mecanismo de cifrado más **fuerte** a través del Estándar de cifrado **avanzado** (AES), requisito para algunos usuarios del gobierno.

**WPA-Enterprise**.-Versión de WPA que utiliza las mismas claves **dinámicas** que WPA-Personal y también requiere que todo dispositivo inalámbrico esté autorizado según lista maestra, albergada en un servidor de autenticación especial.

**WPA-Personal**.-Versión de WPA que utiliza claves de cifrado en constante cambio y de mayor longitud para complicar el proceso de su decodificación.

**Wi-Fi.-**Del inglés Wireless Fidelity, o Fidelidad inalámbrica. Término creado por Wi-Fi Alliance que se utiliza para describir redes inalámbricas estándar tipo 802.11. Los productos que Wi-Fi Alliance haya probado y certificado como “Wi-Fi” pueden operar entre sí incluso si son de marca diferente.

**802.11a.-**Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 5 GHZ.

**802.11b.-** Estándar de red inalámbrica IEEE que especifica una **tasa** de transferencia máxima de 11 Mbps y una frecuencia de funcionamiento de 2.4 GHZ.

**802.11g.-** Estándar de red inalámbrica IEEE que especifica una tasa de transferencia máxima de 54 Mbps y una frecuencia de funcionamiento de 2.4 GHZ y con compatibilidad con versiones anteriores con dispositivos 802.11b.

# CAPITULO III: METODOLOGÍA

## 3.1 MÉTODO DE INVESTIGACIÓN

### *3.1.1 Tipo de investigación*

El tipo de investigación por finalidad empleado es: Aplicada.

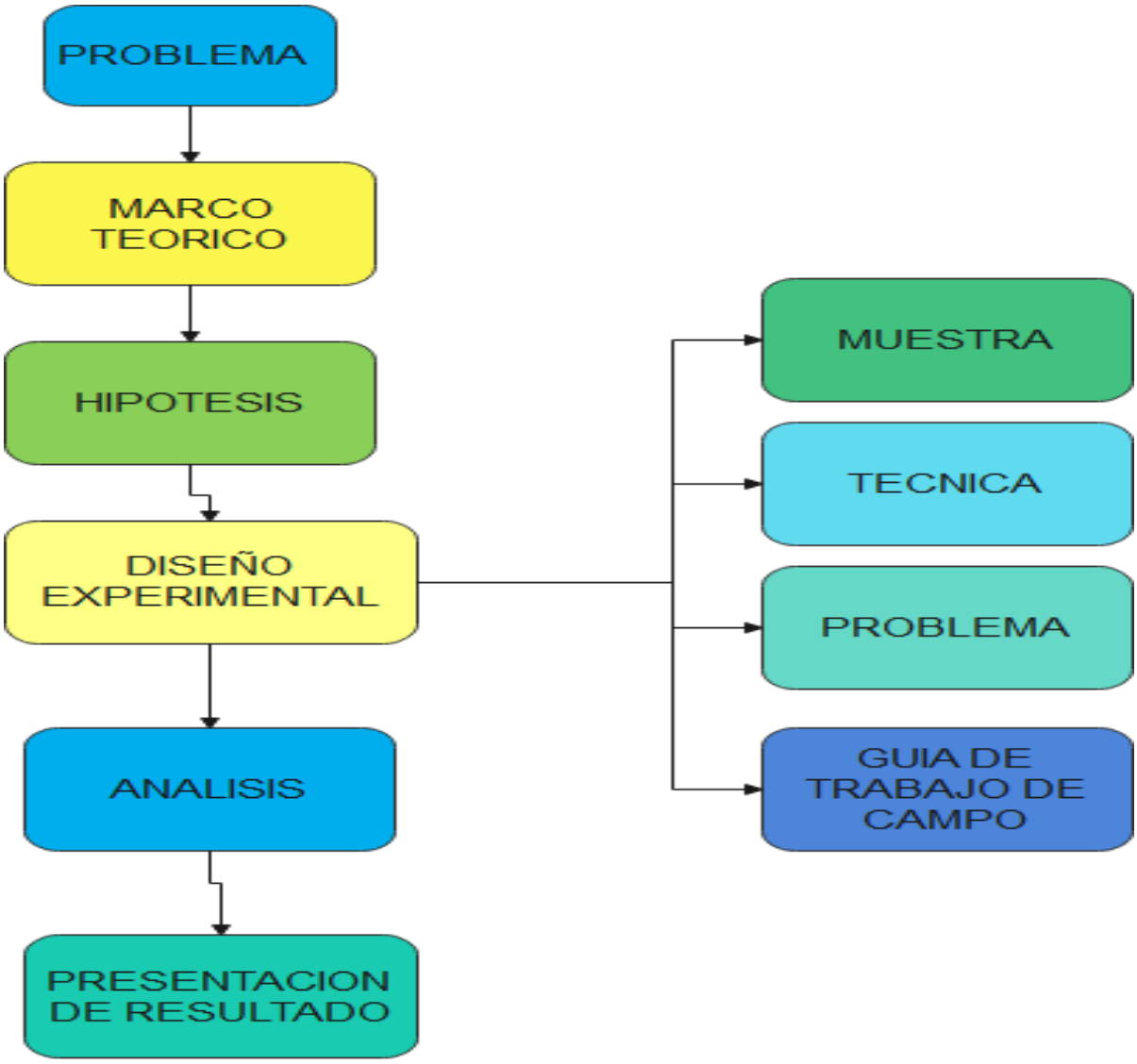
## 3.2 NIVEL DE INVESTIGACIÓN

**Descriptiva.**- por cuanto a través de la información obtenida se va a clasificar elementos y estructuras para caracterizar una realidad.

### *3.2.1 Método de investigación*

El método **Hipotético - Deducción** es el punto central del razonamiento o conclusión y un método de investigación imprescindible. En sentido amplio, por deducción llegas a un punto a la que lleguemos después de un razonamiento. En un sentido más estricto y específico la deducción se entiende como la demostración o derivación certera de la afirmación o consecuencia de una o de varias afirmaciones o premisas sobre la base de las leyes de la Lógica (Lizardo, Carbajal; 2016).

***Diseño de investigación***




Fuente. Russel - Ackoft DE LOS MODELOS de esquema o diseño (Bernal Torres, 2010) (De la garza Toledo, 2016)

**Figura 4.** *Modelo de A. Russel - Ackoft*

## 3.3 POBLACIÓN Y MUESTRA.

### a) Población

Está conformados por los clientes que se les da el servicio de internet inalámbrico y sufren problemas, cuya cuantificación se muestra en la siguiente tabla.

**Tabla 1** ***Cuadro de la población propia***

| Distritos | Población | Porcentaje |
|---|---|---|
| Callería | 20 | 20% |
| Neshuya | 55 | 55% |
| Von Humbodlt | 25 | 25% |
| Total de clientes | 100 | 100% |

## b) Muestra

La muestra estadística es el subconjunto de los individuos de una población estadística. Una fórmula muy extendida que orienta sobre el cálculo del tamaño de la muestra para datos globales es la siguiente:

FORMULA PARA POBLACION MENORES DE 100,000 HABITANTES

$$n = \frac{Z_\alpha^2 Npq}{e^2(N-1) + Z_\alpha^2 pq}$$

FORMULA PARA POBLACION MAYOR QUE 100,000 HABITANTES

$$n = \frac{Z^2 * p * q}{E^2}$$

N: es el tamaño de la población o universo (número total de posibles encuestados).

***$Z_\alpha$*:** es una constante que depende del nivel de confianza que asignemos. El nivel de confianza indica la probabilidad de que los resultados de nuestra investigación sean ciertos: un 95,5 % de confianza es lo mismo que decir que nos podemos equivocar con una probabilidad del 4,5%. Los valores de $Z_\alpha$ se obtienen de la tabla de la distribución normal estándar N(0,1).

Los valores de $Z_\alpha$ más utilizados y sus niveles de confianza son:

**Tabla 2** ***Distribución nominal standard*****.**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Valor de Zα | 1.28 | 1.65 | 1.69 | 1.75 | 1.81 | 1.88 | 1.96 |
| Nivel de confianza | 80% | 90% | 91% | 92% | 93% | 94% | 95% |

(Por tanto, si pretendemos obtener un nivel de confianza del 95% necesitamos poner en la fórmula $Z_\alpha=1.96$).

**e:** es el error de muestra deseado, en tanto por ciento. El error de muestra es la diferencia que puede haber entre el resultado que obtenemos preguntando a una muestra de la población y el que obtendríamos si preguntáramos al total de ella.

Para el estudio la muestra es parte de los clientes de la empresa SERVINTECOMP (100 PERSONAS), es menos de 100.000 personas se toma la siguiente formula.

$$n = \frac{Z_\alpha^2 N p q}{e^2(N-1) + Z_\alpha^2 p q}$$

N= 100
p=0.5
q=0.5
Z= 1.96
e=0.05
n=x

$$n = \frac{(1.96)^2 * 0.5 * 0.5 * 100}{(0.05)^2\ (100-1) + \quad (1.96)^2 * 0.5 * 0.5}$$

n= 96.04 / ((0.2475) +(0.9604))
n=96.04 / 1.21
n=79.37

La muestra de la población es de **79** de las cuales serán entrevistadas.

## 3.4 PROCEDIMIENTOS DE RECOLECCIÓN DE DATOS.

Los procedimientos de recolección de datos son pues el medio del cual el investigador se relaciona con los participantes para obtener la información necesaria que le permita lograr los objetivos de la investigación.

Del cual se tiene en cuenta lo siguiente:

- Seleccionar un instrumento de medición el cual debe ser válido para aceptar los resultados.
- Aplicar dichos instrumento de medición.
- Organizar las mediciones obtenidas, para poder analizarlos.
- Los recursos disponibles.

## 3.5 TÉCNICAS E INSTRUMENTOS PARA RECOLECCIÓN DE DATOS.

### a) Técnicas de investigación

A diferencia de los métodos, las técnicas constituyen elementos de investigación más precisos, específicos y concretos en la ejecución de la investigación. (Quiroz Papa de Garcia, 2009).

**Tecnica documental o bibliográfica.-** Son documentos de carácter doctrinario y la normas legales de la materia que se investiga permitiendo argumentar con carácter sustentario en la tesis.

**Técnica de encuesta.-** Es un instrumento de recolección de datos mediante un cuestionario de preguntas.

**Técnica de entrevista.-** Esta técnica permite conocer más en detalle y de forma directa algunos aspectos que requieran información adicional en la investigación.

**Técnica de la observación.-** Es una guía de observación, cuaderno de notas, permitiendo de esta manera la interrelación directa con los elementos que son materia de la investigación.

**Técnica de la estadística.-**Los datos obtenidos en el trabajo de campo, fueron cuantificados. Luego a un tratamiento estadístico dando un mayor nivel de precisión y confiabilidad cuando se hace medir los resultados de la investigación.

## 3.6 PROCESAMIENTO PARA RECOLECCIÓN DE DATOS.

Los procedimientos para recolección de datos es el medio que se da 5 pasos para:

1. Aclarar nuestra meta para la recolección de datos.
2. Desarrollar definiciones operacionales y procedimientos.
3. Validar el sistema de medición.
4. comenzar la recolección de los datos.
5. continuar mejorando los sistemas de medición y asegurarnos de que las personas sigan las instrucciones de recolección de datos.

## 3.7 TRATAMIENTO DE DATOS.

Para el tratamiento de los datos se hace con los siguientes procedimientos:

- **Análisis cuantitativo.**

  Se consideran dos criterios como son las características de la muestra y variables de estudio (Ortiz, 2010, p. 247).

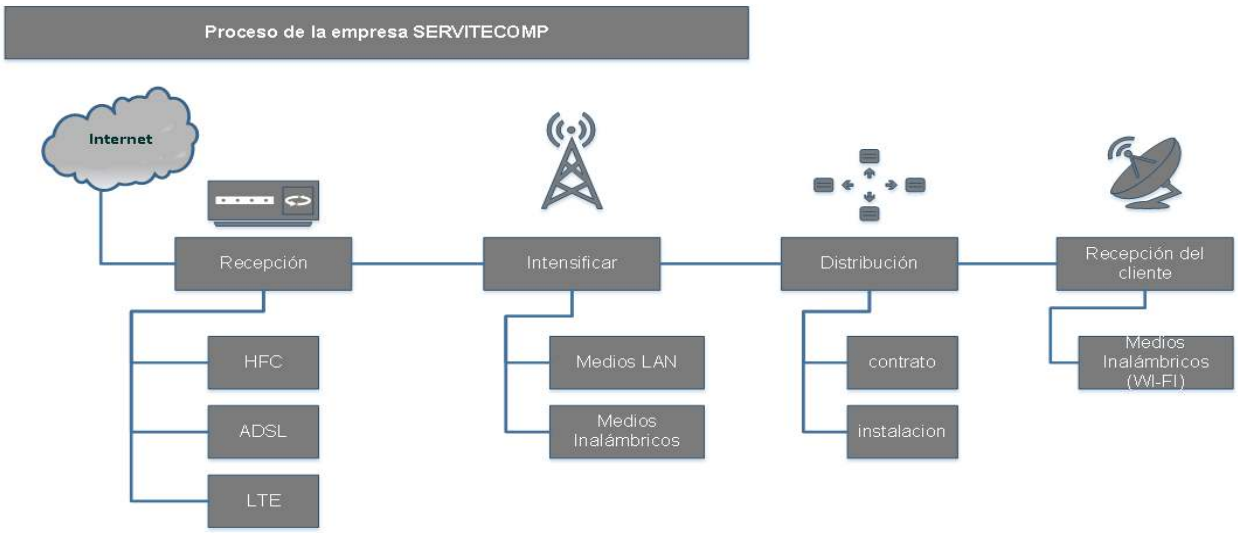
  La primera son los actores, ambientes físicos, contextos, temporalidad que identifica las particularidades del tema.

La segunda describe si lo hallado y evaluado se relacionan entre sí, incide en el cálculo de porcentaje, medidas de tendencia central y variabilidad.

## 3.8 METODOLOGÍA DE DESARROLLO

### *3.8.1 VARIABLE 1: Metodología NIST SP 800-30*

#### *3.8.1.1 Caracterización del sistema.*



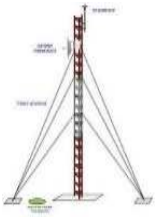
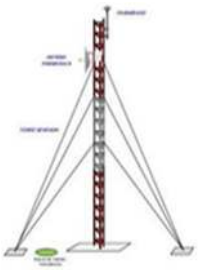
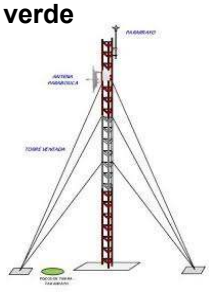

Fuente. Elaboración Propia

**Figura 5**. Caracterización *del sistema propia*

### *3.8.1.2 Fronteras del sistema, funciones del sistema, criticidad del sistema.*

## Hardware y software

**Tabla 3** ***Torres para enlace propia***

| | | |
|---|---|---|
| **Torre del centro de la ciudad**  | **Funciones del sistema.** | Su función de la torre es de dar soporte a la antena en forma de plato con su protector de domo (radomo) de 27 DBI a una altura de 30 metros. |
| | **Fronteras del sistemas** | Es para el enlace de Internet del centro de la ciudad al Km6 como emisor puesta un plato de 27DBI. |
| | **Criticidad del sistema** | La torre ventada soporta hasta 150 kilos de peso, una eventual caída de torre, así como la perdida de corriente, otro elemento son los robos de antena, caída de rayos, deterioro de cables, conectores todo eso hace que se pierda toda la conectividad en la red. |
| **Torre del Km6**  | **Funciones del sistema.** | Su función de la torre es de dar soporte a las antenas en forma de plato con su protector de domo (radomo) de 27 dbi otra de 27 dbi y una de 34 dbi, también hay un equipo que es una omni de 14 dbi a una altura de 52 metros. |
| | **Fronteras del sistemas** | Es para el enlace de Internet del Km6 del centro de la ciudad Puesta un plato de 27dbi como receptor, hay un enlace de Internet del km6 al km40 como emisor, también hay una antena OmniTIK 5 ac de 14dbi como emisor para los clientes de la zona del km6. |
| | **Criticidad del sistema** | La torre ventada reforzada soporta hasta 250 kilos de peso, una eventual caída de torre, así como la perdida de corriente, otro elemento son los robos de antena, caída de rayos, deterioro de cables, conectores todo eso hace que se pierda toda la conectividad en la red de ahí para adelante |
| **Km40/campo verde**  | **Funciones del sistema** | Su función de la torre es de dar soporte a las antenas en forma de plato de 34 dbi, otra de 27 dbi, otra de 30 dbi, otra de 34 dbi y una omni de 14 dbi a una altura de 52 metros. |
| | **Fronteras del sistemas** | Es para el enlace de Internet del km 40 del km 6 como receptor, con una antena 34dbi, otra antena de 34bdi como emisor para km61/Neshuya. También con una omni de 14 dbi como emisor para los clientes en el km 40, otra antena de 27 dbi como emisor a neshuya, y una antena de 30 dbi como emisor a nueva requena. |
| | **Criticidad del sistema** | La torre ventada reforzada soporta hasta 250 kilos de peso, una eventual caída de torre, así como la perdida de corriente, otro elemento son los robos de antena, caída de rayos, deterioro de cables, conectores todo eso hace que se pierda toda la conectividad en la red de ahí para adelante |

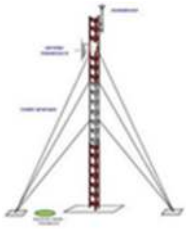
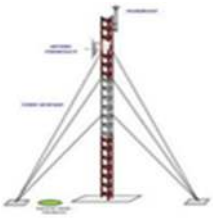
| | | |
|---|---|---|
| **Km61-neshuya**  | **Funciones del sistema** | Su función de la torre es de dar soporte a las antenas en forma de plato de 34 dbi, otrade 27 dbi, otra de 30 dbi, otra de 34 dbi y dos omni de 14 dbi a una altura de 52 metros. |
| | **Fronteras del sistemas** | Es para el enlace de Internet del km 60 del km 40 como receptor, con una antena 34dbi, otra antena de 30 bdi como emisor para km 72. También con dos omni de 14 dbi como emisor para los clientes en el km 60, otra antena de 30 dbi como emisor a Von Humbolt. |
| | **Criticidad del sistema** | La torre ventada reforzada soporta hasta 250 kilos de peso, una eventual caída de torre, así como la perdida de corriente, otro elemento son los robos de antena, caída de rayos, deterioro de cables, conectores todo eso hace que se pierda toda la conectividad en la red de ahí para adelante. |
| **Km72-neshuya**  | **Funciones del sistema** | Su función de la torre es de dar soporte a las antenas en forma de plato de 30 dbi, otra de 30 dbi y una omni de 14 dbi a una altura de 35 metros. |
| | **Fronteras del sistemas** | Es para el enlace de Internet del km 72 del km 60 como receptor, con una antena 30dbi, otra antena de 34 bdi como emisor para km 104. También con una sectorial de 14 dbi como emisor para los clientes en el km 72. |
| | **Criticidad del sistema** | La torre ventada reforzada soporta hasta 250 kilos de peso, una eventual caída de torre, así como la perdida de corriente, otro elemento son los robos de antena, caída de rayos, deterioro de cables, conectores todo eso hace que se pierda toda la conectividad en la red de ahí para adelante. |
| **Km86 Von Humboldt**  | **Funciones del sistema** | Su función de la torre es de dar soporte a las antenas en forma de plato de 30 dbi dos sectorial de 14 dbi a una altura de 42 metros. |
| | **Fronteras del sistemas** | Es para el enlace de Internet del km 86 del km 60 como receptor, con una antena 30dbi, también con dos sectoriales de 14 dbi como emisor para los clientes en el km 86. |
| | **Criticidad del sistema** | La torre ventada reforzada soporta hasta 250 kilos de peso, una eventual caída de torre, así como la perdida de corriente, otro elemento son los robos de antena, caída de rayos, deterioro de cables, conectores todo eso hace que se pierda toda la conectividad en la red. |

***Tabla 4*** **Equipos de proveedor de servicio de internet (ISP)** (sagemcom, 2020), (tp-link, 2020)

| | | |
|---|---|---|
| HARDWARE MODEMS-ROUTER (sagemcom, 2020)  | **Funciones del sistema** | Su función es recibir Internet mediante un proveedor de línea de internet (ISP) de alto tráfico de un 1g de transferencia utiliza el cable coaxial. Tiene el protocolo b/n/g en la red inalámbrica |
| | **Fronteras del sistemas** | Tiene conexión HFC y IP NETWORK conectividad, tiene un status de conexión donde se verifica la banda de frecuencia si es el adecuado para su carga y descarga de información de internet. Con servicio de wifi tanto en la banda 2.4gb y 5.8gb el equipo transfiere un 1gb de información, con seguridad wpa y wpa2, cuenta con wps |
| | **criticidad de datos y sistemas** | Una eventual pérdida de energía, perdida de Internet con el proveedor (ISP), perdida de equipo (malograrse, quemarse), inestabilidad de corriente, todo eso hace que se pierda conectividad de Internet en toda la red. |
| Hardware MODEMS ROUTER TLMR 6400 4G (tp-link, 2020)  | **Funcione del sistema** | Su función es recibir Internet mediante un proveedor de línea de internet (ISP) de cuarta generación de chip-de conexión, con una velocidad de un 1GB- LTE: ideal para la red de vanguardia 4G LTE<br>Compatible con versiones anteriores: el wifi de 300Mbps permite una velocidad estable para actividades inalámbricas, como transmisión, navegación, navegación y publicar redes sociales Alcance de Wi-Fi de velocidad 4G LTE |
| | **Frontera del sistema** | Compatible con la red 4G / 3G·Velocidad inalámbrica de 300Mbps Conexiones más rápidas: hasta 150 Mbps de velocidad de descarga y Velocidad de carga de 50 Mbps. Mejor cobertura: las antenas integradas proporcionan conexión inalámbrica estable conexiones y mejor cobertura |
| | **Criticidad de datos y sistemas** | Problemas de conectividad en lugares cerrados o cuando hay lluvias fuertes, también cuando las antenas se rompen o sino se malogran los equipos así como el cruce de los chips todo esos detalles hace perder la señal de internet del Proveedor y por ende a toda la red. |
| Hardware MODEN ROUTER (SMART WIFI, 2020)  | **Funciones del sistema** | Su función es recibir Internet mediante un proveedor de línea de internet (ISP) con su modelo Mitrastar HGU -GPT-2541GNAC.mejor en red WiFi. |
| | **Frontera de los sistemas** | Un único equipo, reduciendo el espacio y el consumo eléctrico.La red de 5 gigas y máxima cobertura en la red de 2,4 gigas es un modelo Mitrastar HGU Integra ONT, router y videobridge. |
| | **Criticidad de datos y sistemas** | El problema es que si no hay buena cobertura de parte del proveedor de línea de Internet mediante su sistema de fibra óptica se pierde la conectividad de Internet y se también puede malograrse el equipo, perdida de energía. |

***Tabla 5*** **Equipos de respaldo energético** (FORZA, 2020)

| | | |
|---|---|---|
| HARDWARE<br>Estabilizador (FORZA, 2020)<br> | **Funciones del sistema** | Su función es la que ayuda a soportar picos de corriente dando así protección a los equipos. |
| | **Fronteras del sistemas** | Un estabilizador de tensión es un equipo electrónico o electromecánico, destinado a dar una tensión estabilizada en su salida (230 Voltios ó 380 Voltios), aunque en su entrada la tensión eléctrica sea más baja o más alta del valor de utilización. |
| | **criticidad de datos y sistemas** | El problema de los estabilizadores es que no soportan tenciones más altas a que se está diseñada, también no cubre la protección de los equipos cuando son constantes las tensiones llegando a quemar los estabilizadores y a veces a los equipos de enlaces o los servidores. |
| Hardware Unidad de soporte eléctrico(UPS) (FORZA, 2020)<br> | **Funciones del sistema** | Es la que ayuda a tener energía extra después de un corte de energía. |
| | **Frontera del sistema** | Un ups es un equipo diseñado a brindar energía estabilizada de manera permanente hasta agotar su energía después del corte de corriente. |
| | **criticidad de datos y sistemas** | No está diseñado para conectar dispositivos de alto consumo de energía como impresora, impresora láser o un plotter, como también varios equipos de cómputo para ello se diseñado de acuerdo a la necesidad del sistema. |
| Hardware Supresores de pico (FORZA, 2020)<br> | **Funciones del sistema** | Para una mejor transferencia de energía, protección contra sobretensiones cuenta con 4 a 6 puertos de conexión de corriente.<br>Es un dispositivo que se puede utilizar para proteger toda clase de equipos electrónicos, no solo |
| | **Frontera del sistema** | -Incluyen dentro de sí un dispositivo electrónico especial, el cuál al recibir un alto voltaje genera que se vaya a tierra la descarga y con ello evitar daños en los equipos conectados.<br>Opcionalmente pueden tener protección para algunos dispositivos que requieren suministro por medio de puerto USB |

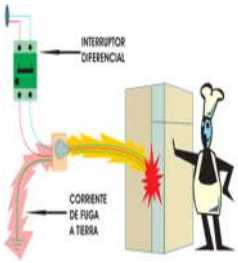
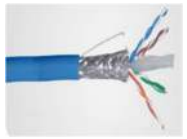
| | | |
|---|---|---|
| | **criticidad de datos y sistemas** | El problema de estos equipos que tienen que ser de buena calidad debido a que soportan altas tensiones de corriente y que debe tener un fusible como protección. |
| **Hardware Conexión a tierra**<br> | **Funciones del sistema** | La puesta a tierra corresponde al conjunto de electrodos y partes conductoras que en contacto con la tierra, permiten drenar hacia esta, todas las corrientes de falla, para que no pueda dañar los equipos. |
| | **Frontera del sistema** | Mantener los potenciales producidos por las corrientes de falla dentro de los límites de seguridad de modo que las tensiones de paso o de toque no sean peligrosas para los humanos. Ofrecer en todo momento y por un lapso prolongado baja resistencia eléctrica que permita el paso de las corrientes derivadas. |
| | **criticidad de datos y sistemas** | Un pozo tierra tiene su límite para la descargas pues solo puede abastecer a un número determinado de computadoras o demás equipos de cualquier ámbito por tal motivo a veces no funciona correctamente el pozo tierra y además debe tener una resistencia eléctrica lo más baja posible para derivar a tierra fenómenos eléctricos. |

**Tabla 6** ***Equipo de medios de red*** *(ubiquiti, 2020)*

| | | |
|---|---|---|
| EQUIPOS CABLE STP(par trenzado apantallado) CAT6 SATRA (Satra, 2020)<br> | **Funciones del sistema** | Cada par va recubierto por una malla conductora que actúa de apantalla frente a interferencias y ruido eléctrico. Su impedancia es 150 ohm. |
| | **Fronteras del sistemas** | El nivel de protección del stp () ante perturbaciones externas es mayor al ofrecido por utp. Sin embargo es más costoso y requiere más instalación. La pantalla del STP para que sea más eficaz requiere una configuración de interconexión con tierra |
| | **criticidad de datos y sistemas** | Es utilizado generalmente en las instalaciones de procesos de datos por su capacidad y sus buenas características contra las radiaciones electromagnéticas, pero el inconveniente es que es un cable robusto, caro y difícil de instalar. |
| | **Funciones del sistema** | Ocho puertos 10/100/1000 Gigabit LAN de 16 Gbps de conmutación tela, auto MDI/MDIX cruzado para todos los puertos |

| | | |
|---|---|---|
| GIGABIT SWITCHS DE 8 PUERTOS (Satra, 2020)  | **Fronteras del sistemas** | Su control de flujo es IEEE 802.3x, csma/cd es semiduplex, full dúplex, RAM buffer=128kb por dispositivo, tabla de direcciones MAC 8k. |
| | **criticidad de datos y sistemas** | Soporta 9.216 bytes Jumbo Frames, también soporta IEEE 802.1p QoS (4 colas, modo estricto), Ethernet 14,880 pps por puerto, Fast Ethernet: 148.800 pps por puerto |
| CONECTORES RJ(Register Jack)45 macho CAT6 y CAT5(Satra, 2020)  | **Funciones del sistema** | .Son conectores principales para ser utilizados con la tarjeta de red Ethernet que transmite información a través de cable UTP, FTP, STP, hasta un 1gb de transmisión de información. |
| | **Fronteras del sistemas** | Es macho que se conecta a un puerto hembra de Ethernet y va ponchado en un cable de red. |
| | **criticidad de datos y sistemas** | Los conectores mal ponchados, oxidados y viejos hacen perder información también los conectores hembras también se malogra. |
| Adaptador Poe De un 1g Ubiquiti  | **Funciones del sistema** | Los adaptadores PoE(Energía sobre Ethernet) son altamente confiables y, brindan protección de tierra y protección contra Sobretensiones ayuda a proteger contra eventos de descarga electróptica. La corriente entra en el cable por medio de un componente llamado inyector. |
| | **Fronteras del sistemas** | Para que poe trabaje, la corriente eléctrica debe ir en el cable de datos en el extremo de alimentación, y salir por el extremo dispositivo, de tal manera que la corriente se mantenga separada de la señal de datos de modo que no interfiera con la otra. |
| | **criticidad de datos y sistemas** | Para minimizar la posibilidad de daños en el caso de una falla de funcionamiento, los sistemas más sofisticados de poe usan una protección de fallo. Esta característica apaga la fuente de poder si se detecta exceso de corriente o un cortocircuito. |

**Tabla 7** ***Equipos de ruteros*** *(ubiquiti, 2020) (Mikrotik, 2020)*

| | | |
|---|---|---|
| Hardware EQUIPO<br>MIKROTIK Rb 2011uias<br> | **Funciones del sistema** | Este RouterBoard tiene una pantalla táctil a color, que muestra el estado del dispositivo, gráficas de tráfico y permite el acceso a opciones de configuración simple. Cuenta con 1 puerto El RB2011UiAS cuenta con un puerto SFP (small form-factor pluggable) para transceptores SFP Gigabit, la solución ideal para aplicaciones FTTH (Fiber To The Home). |
| | **Fronteras del sistemas** | Enrutamiento dinámico, punto de acceso, cortafuegos, MPLS, VPN, calidad de servicio avanzada, equilibrio de carga y Vinculación, configuración y monitoreo en tiempo real.<br>Gigabit SFP + 5 Gigabit Ethernet + 5 Fast Ethernet + 1 puerto miniUSB y 1 puerto serial RJ-45. Además |
| | **criticidad de datos y sistemas** | El equipo cuando trabaja las 24 horas durante los 7 días de la semana, por la cual sufre cierta lentitud en su transferencia de datos, el equipo es la parte fundamental del sistema de la cual no debe sufrir ningún tipo de desperfecto.<br>Todos los clientes de pende de este equipo. |
| Hardware MIKROTIK Rb 750 ar2<br> | **Funciones del sistema** | El equipo realiza una administración de la red de la cual se procede así Conecte su cable de Internet al puerto 1 (etiquetado como "Internet") y las computadoras de la red local a los puertos 2-5, Configure la configuración de IP de su computadora en automático (DHCP) La dirección IP de la red local es 192.168.88.1, úsela en su navegador para acceder al dispositivo. Sus puertos son de un Giga-bit. La memoria SDRAM en la board es de 64 MB en lugar de 32 MB: |
| | **Fronteras del sistemas** | Es ideal para los usuarios finales por ser un equipo simple SOHO (Small office/Home Office).<br>Su trabajo es de nivel básico para tareas simple en el hogar.<br>No se puede usar para altas transferencias de datos. |

| | | |
|---|---|---|
| | **criticidad de datos y sistemas** | El equipo es importante al usuario final por que administra su red (da velocidades a cada usuario de su necesidad por medio su ip, bloquea a su usuario según su necesidad, como también bloquea páginas no deseadas a cada usuario según necesidad). |
| Hardware MIKROTIK Rb 9152ui 5 ac 2nd  | **Funciones del sistema** | La unidad está equipada con una CPU de 650MHz, 64MB de RAM, cinco puertos Ethernet de 10/100/1000Mbps (salida PoE en el puerto # 5), 802.11b / g / n de doble cadena inalámbrica de 2.4GHz, inalámbrica de una sola cadena 802.11a / n / ac de 5GHz, Puerto USB para módem 3G / 4G y una licencia RouterOS L4 |
| | **Fronteras del sistemas** | El equipo solo se usa para administración de red de las empresas u hogares en algunos casos. Es muy bueno para enrutamiento de ips, bloqueos de páginas, administración de línea de internet. |
| | **criticidad de datos y sistemas** | El equipo es de alta transferencia de datos puesto que sus puertos pueden soportar una Giga en cada puerto. Las empresas lo tienen configurado para trabajos fuertes de trasferencia de datos |
| MIKROTIK Rb dist 5nd  | **Funciones del sistema** | DISC Lite5 es un CPE 802.11n de doble cadena integrado de 21dBi con una CPU de 600MHz, 64MB de RAM, 1x puerto Ethernet 10/100/1000Mbps y RouterOS L3 instalado. El DISC utiliza una antena de tipo contrafuego que permite alcanzar una ganancia de 21dBi<br>El RBDISC-5nD está basado en el popular diseño de hardware del LHG (Light Head Grid) e integra un radio en 5 GHz - 802.11a/n de cadena dual, un procesador AR9344 @ 600 MHz, 64 MB de RAM y un puerto 10/100Mbps Ethernet. |
| | **Fronteras del sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |
| | **criticidad de datos y sistemas** | El equipo cumple un papel muy importante en el sistema porque hay varios usuarios que depende del equipo para realizar sus actividades |

| | | |
|---|---|---|
| MIKROTIK Rb onni tikg 5 hacd  | **Funciones del sistema** | OmniTIK 5 ac cuenta con cinco puertos Gigabit Ethernet y soporte para 802.11ac.Está equipado con una potente CPU de 720 MHz, 128 MB de RAM, 802.11a / n / ac de cadena dual de alta potencia (compatible con CA y compatible con versiones anteriores con el estándar 802.11a / n CPE). |
| | **Fronteras del sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |
| | **criticidad de datos y sistemas** | El equipo cumple un papel muy importante en el sistema porque hay varios usuarios que depende del equipo para realizar sus actividades |
| MIKROTIK Rb912uag - 2hpnd  | **Funciones del sistema** | El RB912 es un pequeño router inalámbrico con una tarjeta inalámbrica integrada de alta potencia y una ranura adicional miniPCIe (PCI-Express) para tecnología inalámbrica 802.11a/n o tarjeta SIM para tecnología 3G. El puerto Gigabit ayuda a aprovechar todo el potencial de velocidades inalámbricas 802.11n. Además cuenta con un puerto USB 2.0. |
| | **Fronteras del sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información. |
| | **criticidad de datos y sistemas** | El equipo cumple un papel muy importante en el sistema porque hay varios usuarios que depende del equipo para realizar sus actividades |
| MIKROTIK Rb 912uag - 5hpnd  | **Funciones del sistema** | El RB912UAG-5HPnD es un dispositivo muy versátil. Es un pequeño enrutador inalámbrico con una tarjeta inalámbrica de alta potencia integrada y una ranura miniPCIe adicional para 802.11 inalámbrico o tarjeta 3G. El puerto Gigabit ayuda a utilizar todo el potencial de las velocidades inalámbricas 802.11n.<br>Ha incorporado una protección contra descargas electrostáticas de 16 kV en los puertos Ethernet y MMCX. |
| | **Fronteras del sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información. |

| | | |
|---|---|---|
| | **criticidad de datos y sistemas** | El equipo cumple un papel muy importante en el sistema porque hay varios usuarios que depende del equipo para realizar sus actividades. |
| MIKROTIK Rb 5xt 5ndr2  | **Funciones del sistema** | Antena integrada de 5GHz 16dBi con CPU de 600MHz, 64MB RAM y RouterOS L3 instalado.<br>SXT Lite5 es un dispositivo inalámbrico para exteriores de 5 GHz de bajo costo y alta potencia de transmisión. Puede usarse para enlaces punto a punto. |
| | **Fronteras del sistemas** | SXT Lite5 es un dispositivo inalámbrico para exteriores de 5 GHz de bajo costo y alta potencia de transmisión. Se puede utilizar para enlaces punto a punto o como CPE para instalaciones punto a multipunto. |
| | **criticidad de datos y sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información. |

**Tabla 8** ***Equipos para enlaces inalámbricos propia*** *(ubiquiti, 2020) (Mikrotik, 2020)*

| | | |
|---|---|---|
| UBIQUITI Lite-ap ac5   | **Funciones del sistema** | A diferencia del protocolo estándar WiFi, el exclusivo protocolo airMAX TDMA de Ubiquiti Networks permite a cada cliente enviar y recibir datos usando ranuras de tiempo pre-asignadas, administradas por un AP inteligente. Este método elimina la colisión de nodos y maximiza la eficiencia del air-time.<br>Largo Alcance: Capacidad de altas velocidades en enlaces de hasta 30 Km.<br>Comparado con otros sistemas de su clase, el LiteBeam entrega un rendimiento superior en reducción de latencia, velocidad y escalabilidad. |
| | **Fronteras del sistemas** | LiteAP ac cuenta con una antena MIMO 2x2 y se comunica con múltiples CPEs airMAX ac dentro de un área de cobertura de 120.<br>QoS Inteligente: Se le otoroga prioridad a voz/video para un acceso sin fisuras.<br>Escalabilidad: Alta capacidad de escalabilidad. |
| | **criticidad de datos y sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |

| | | |
|---|---|---|
| UBIQUITI Nanostation loco m2  | **Funciones del sistema** | Es un equipo de exterior compacto, incluye una antena MIMO de doble polaridad para la banda de 2.4 GHz. La velocidad de transferencia real del equipo es de hasta 150 Mbps. Gracias a la tecnología TDMA Time Division Multiplexing permite conectarse a más de 30 clientes al equipo. |
| | **Fronteras del sistemas** | CPE airMAX® para interiores / exteriores Con una antena de panel y rendimiento de doble polaridad, el NanoStation®M es ideal para aplicaciones de punto a multipunto (PtMP) que requieren dispositivos CPE de alto rendimiento con un factor de forma elegante. |
| | **criticidad de datos y sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |
| UBIQUITI Nanostation loco m5  | **Funciones del sistema** | Es un equipo de exterior compacto, incluye una antena MIMO de doble polaridad para la banda de 5GHz. La velocidad de transferencia real del equipo es de hasta 150 Mbps. Gracias a la tecnología TDMA Time |
| | **Fronteras del sistemas** | CPE airMAX® para interiores / exteriores Con una antena de panel y rendimiento de doble polaridad, el NanoStation®M es ideal para aplicaciones de punto a multipunto (PtMP) que requieren dispositivos CPE Division Multiplexing permite conectarse a más de 300 clientes al equipo |
| | **criticidad de datos y sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |
| UBIQUITI Powerbean 400 5ac  | **Funciones del sistema** | La PowerBeam ac dirige la energía de RF en un ancho de haz más preciso. Con la energía en una dirección, la PowerBeam ac bloquea o filtra espacialmente el ruido, por lo tanto la inmunidad se mejora. Esta característica es especialmente importante en un área llena de otras señales RF de frecuencias similares o iguales.<br>La tecnología InnerFeed de Ubiquiti integra la interface de radio dentro de la antena, por lo que no necesita cables. Lo que mejora el rendimiento, ya que elimina las perdidas por cable. |
| | **Fronteras del sistemas** | El factor de forma de la PowerBeam ™ ac presenta la mayor ganancia para su tamaño. La excelente directividad del haz de la PowerBeam ac proporciona el mejor rendimiento en entornos de mucho ruido. |
| | **criticidad de datos y** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información. |

| | | |
|---|---|---|
| UBIQUITI Powerbean m5 400  | **Funciones del sistema** | Tiene una antena que ofrece 25 dBi de ganancia y 26 dBm de Potencia de Transmisión, opera en el intervalo de frecuencia de 5170 – 5875 MHz. Cuenta con un procesador Atheros MIPS 74KC y 64MB de Memoria RAM, además de 8 MB para almacenamiento. También tiene un puerto Gigabit Ethernet 10/100/1000. |
| | **Fronteras del sistemas** | El factor de forma del PowerBeam presenta la mayor ganancia para su tamaño. La excelente directividad del haz de PowerBeam proporciona el mejor rendimiento en entornos de alto ruido. |
| | **criticidad de datos y** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |
| UBIQUITI Rocket 5ac lite  | **Funciones del sistema** | El Rocket R5AC-LITE El Access point Rocket M5 AC Lite para emisor o cliente, con 128Mb DDR2, procesador Atheros MIPS 74Kc de 720 MHz, diseñado para uso en exteriores de 5.GHz en 802.11a/n, de polaridad 2x2 |
| | **Fronteras del sistemas** | El motor airMAX ® de Ubiquiti con IC personalizado mejora dramáticamente la latencia TDMA y la escalabilidad de la red. El silicio personalizado proporciona capacidades de aceleración de hardware al programador airMAX, para soportar las altas velocidades de datos y la modulación densa utilizada en la tecnología airMAX ac. |
| | **criticidad de datos y sistemas** | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |
| UBIQUITI Rocket 5ac prisma  | **Funciones del sistema** | El Rocket Prism 5AC Gen2 está diseñado para entregar una máxima eficiencia espectral y un throughput real de hasta +500 Mbps. Opera en todo el espectro disponible de la banda de frecuencia de 5 GHz y añade un radio WiFi dedicado en 2.4 GHz para una gestión rápida y fácil desde tu dispositivo móvil. |
| | **Fronteras del sistemas** | La tecnología patentada airPrism de Ubiquiti proporciona una selectividad de radio innovadora en un rendimiento de banda inalámbrica sin licencia. La tecnología airPrism aísla las señales dentro del canal operativo para aumentar la capacidad y el rendimiento en las implementaciones de ubicación conjunta. |
| | criticidad de datos y sistemas | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |

| | | |
|---|---|---|
| UBIQUITI Rocket m2  | Funciones del sistema | Con Antenas 2x2 MIMO 2,4 GHz de Ubiquiti. Rocket es la nueva Estación Base de Ubiquity, es un sistema robusto, muy potente y estable, sus 2x2 antenas MIMO ofrecen un gran rendimiento en la recepción. Se caracteriza por su increíble alcance (+50km) y rendimiento (+150Mbps real TCPI/IP). |
| | Fronteras del sistemas | Las radios Rocket ™ funcionan a la perfección junto con las antenas sector AirMAX ® , RocketDish ™ , Omni y Yagi para enlaces PtP y PtMP. Cada antena airMAX tiene un montaje Rocket incorporado, por lo que no se necesitan herramientas para instalar el Rocket. |
| | criticidad de datos y sistemas | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información. |
| UBIQUITI Rocket prisma 5ac gen 2  | Funciones del sistema | Alto Rendimiento: Para aprovechar al máximo su diseño y capacidades, despliegue el Rocket Prism 5AC Gen 2 para enlaces PtP o PtMP en entornos de alto ruido de RF. |
| | Fronteras del sistemas | El Rocket 5AC Prism Gen2 presenta la revolucionaria tecnología de filtrado de RF airPrism, el conjunto de chips airMAX ac patentado y Wi-Fi de administración dedicada para un fácil soporte de aplicaciones móviles UNMS y una configuración rápida. Implemente el Rocket 5AC Prism Gen2 para enlaces PtP o PtMP en entornos con mucho ruido. |
| | criticidad de datos y sistemas | Es un equipo de enlace que permite a los usuarios puedan acceder al internet, permitiendo que el sistema cumpla con la seguridad de la información |

**Personal:**

**Tabla 9** ***Lista de personal propia***

| código | Nombre completo | cargo | Descripción de desempeño | Privilegio de usuario |
|---|---|---|---|---|
| 001 | FRANCISCO | gerente | Gerente | administrador |
| 002 | MIGUEL | contador | contador | nada |
| 003 | CARLOS | Jefe de soporte | Revisar a todos los de soporte | administrador |
| 004 | JUAN DAVID | soporte | Instalación de los equipos | administrador |
| 005 | LUIS | soporte | Instalación de los equipos | invitado |

#### *3.8.1.3 Sensibilidad de datos y sistemas*

- **Misión de los sistemas**

La misión es hacer llegar toda la información de tal manera que no sufra ninguna pérdida, también es misión proteger a los usuarios de algún secuestro de la red inalámbrica, los ataque de los virus, no permitir el ingreso de cualquier persona a los sistemas para hacer cambios de la contraseña a la red inalámbrica.

#### *3.8.1.4 Identificación de amenazas.*

**Históricos de ataques.**

**Yahoo.**

Quizá uno de los ataques informáticos más importantes y que tenemos muy presente todavía, fue el de Yahoo. Se considera como el ataque informático más grande de la historia. En total se calcula que fueron hackeadas unos 500 millones de cuentas, en un principio. Datos ofrecidos por la propia compañía, pero que luego resultó que llegó a ser de al menos el doble.

Robo de datos personales, fechas de nacimiento, número de teléfono, correos electrónicos, contraseña. Eso sí, según indicó la propia compañía, ni los datos bancarios ni las tarjetas de crédito se vieron comprometidos.

**Ataque a la empresa.**

La empresa es atacada constantemente por los hackers, crackers, crimen computacional, usuarios poco entrenados, usuarios descontentos, maliciosos, negligentes y deshonestos y eso es comprobado con los medios de asistencias remotas.

**Los ataques informáticos**

Constituyen una de las amenazas más grandes que existen para las empresas actualmente, afectando por igual a individuos particulares, empresas e incluso estados y sociedades.

Debido a esto es que las medidas de seguridad informática se han convertido en prioritarias, especialmente para aquellas empresas o entidades que dependen casi al 100% de Internet para realizas sus operaciones.

**Datos de medios de comunicación**.

Ecuador ha registrado más de 40 millones de ciberataques a portales web de instituciones públicas tras retirar el asilo diplomático al fundador de WikiLeaks, Julian Assange, informaron autoridades.

Desde el pasado jueves "se registraron más de 40 millones de ataques cibernéticos provenientes principalmente de Estados Unidos, Brasil, Holanda, Alemania, Rumanía, Francia, Austria, Reino Unido, y también desde aquí, de nuestro territorio", dijo Patricio Real, viceministro de Tecnologías de la Información y Comunicación.

**Definiciones de la amenazas.**

Esto es importante entender las definiciones de los ataques para poder contrarrestar esos ataques y son los siguientes:

- **Hacker.-** esto es instrucción a los sistemas, accesos no autorizados, esto es pues el hecho de que entren en la configuración de los equipos de enlaces y los equipos de computadoras con fines de diversión.
- **Cracker.-** Es ingreso a los sistemas con fines de robar información tales como contraseñas, archivos.
- **Usuarios poco entrenados**.- son personas con conocimientos de limitados de red y además no cuentan con un conocimiento exacto del sistema de red que tiene estructurado la empresa SERVINTECOMP.
- **Los medios ambientales** también son una amenaza, como los vientos huracanados, la falta de corriente, el deterioro de las torres, también abarca las motivaciones de las personas por tener una línea gratis de Internet.

Una mala estructura de diseño de la red inalámbrica con clientes no registrado de manera ordenada y con sus respectivas velocidades de contractos, dando así un pésimo servicio.

- Otra amenaza que se tiene es que los antivirus, los sistemas operativos, el firmware de los equipos de enlace estén desactualizados, firewall no sea configurada de manera correcta (con sus permisos respectivos).
- Los técnicos son responsables en la buena configuración de los equipos de enlace según el cuadro de responsabilidad.

#### *3.8.1.5* Identificación de vulnerabilidades.

**Tabla 10** ***De identificación de vulnerabilidades***

| Lista de vulnerabilidades | Informe de evaluación de riesgo anteriores | Resultado de auditoria | Requerimiento de seguridad | Resultado de prueba de seguridad |
|---|---|---|---|---|
| 1 | No existe una asignación clara de responsabilidades. | No hay cuadro. | Desarrollar un cuadro de responsabilidad. | Mejor control de responsabilidad. |
| 2 | No personal disponible para soporte. | No hay cronograma. | Hacer un horario de personal para trabajos de soporte. | Los sistemas de atención a los clientes es más satisfactorio. |
| 3 | No se revisa los controles de seguridad. | No hay equipos actualizados. | Hacer un cronograma de trabajo a todos los puntos de enlace como control de | Los sistemas son mejores atendidos por ser más controlado. |
| 4 | No se hace evaluación de riesgo. | Los equipos son desfasados en software. | Hacer un cronograma de evaluación de riesgo junto a control de seguridad. | Más efectividad de asignación en los respaldos de riesgos. |
| 5 | Falta de control para asegurar la calidad de energía eléctrica. | No hay ups, estabilizadores, pozo tierra. | Trabajar junto con evaluación de riesgo y seguridad. | Hay menos cortes de la red inalámbrica. |
| 6 | No existe control de humedad ni temperatura. | No hay sensores. | Trabajar junto con evaluación de riesgo y seguridad. | Se controla los estados de los equipos al momento. |
| 7 | No se usa ningún sistema de detección de intrusos. | No hay software. | Trabajar junto con evaluación de riesgo y seguridad. | Se detecta los intrusos al instante. |

### *3.8.1.6 Caracterización de los controles.*

**Tabla 11** ***De caracterización de los controles***

| Lista de controles actuales y planificados | Controles actuales | Controles planificados | Factibilidad | Efectividad |
|---|---|---|---|---|
| 1 | No existe control de asignación clara de responsabilidades. | Se hace planificación de responsabilidades con el organigrama. | Con una organización de jerarquía se hace factibilidad la responsabilidad. | Pero no garantiza que no se pueda hacer errores en el trabajo. |
| 2 | No se hace los controles de seguridad en el sistema de la red inalámbrica. | Se hace planificación de control mensualmente en todos los puntos de acuerdo al cronograma. | Con un cronograma de actividad de control de seguridad de la red inalámbrica se hace factibilidad la prevención. | Pero no garantiza que se pueda proteger de los embates de la naturaleza y los motivos de las personas. |
| 3 | No se hace control de evaluación de riesgos en el sistema de la red inalámbrica. | Se hace evaluación de riesgos mensualmente en todos los equipos del sistema de la red inalámbrica. | Siguiendo el cronograma se hace un control de evaluación de riesgo de los equipos y torres dando factibilidad de prevención riesgo. | Pero no garantiza que no haya algún tipo de desastre de la naturaleza hacía las torres, equipos de enlaces y proveedores. |

| | | | | |
|---|---|---|---|---|
| 4 | No se hace control con un sistema de detección de intrusos. | Se hace control con un sistema de seguridad contra intrusos. | Con un sistema de control que se encuentra en el equipo de mikrotik contra intrusos se hace factible la detección de los intrusos | Pero siempre las personas tienen motivo para seguir tratando de entrar al sistema, logrando ingresar por unos momentos al sistema |
| 5 | No hay un control de registro de mantenimiento de torres. | Se hace un control de registro de manteniendo de torres con el cronograma de actividad. | Con el control de registro de mantenimiento de torre se hace factible la conservación de la torre. | Pero si las torres ya pasaron su ciclo de vida se tiene que cambiar la torre. |

#### *3.8.1.7 Determinación de probabilidades.*

**Tabla 12** ***De determinación de probabilidades***

| **Motivación para los ataques** | **Rating de probabilidad** |
|---|---|
| La motivación de los ataques es que pueden tener Internet gratis y vender a usuarios incautos, como también adquirir información de alguna institución que es usuario de la empresa. | Se ha encontrado ataque de malware, virus, troyanos, keyloggers al ver las máquinas de la computadoras de los usuarios finales dando un nivel medio de riesgo de pérdida de la red. |
| **Capacidad de las amenazas** | . |
| La capacidad de amenaza es enorme debido a que cuentas con diversas instrucciones de como romper el acceso a la red inalámbrica, dicha información se encuentra en internet como instructivo ya se de modo visual o escrito. | Se encontró el ingreso de personas no autorizadas al sistema de configuración de los equipos de la red inalámbrica, logrando tener internet. Dando un nivel alto de probabilidad de pérdida de red. |
| **Naturaleza de las vulnerabilidades** | |

| | |
|---|---|
| La naturaleza de la vulnerabilidad radica en las diferentes deficiencias de seguridad debido a que no cuentan con un sistema de visualización de usuarios, informes de ataques, controles de averías de las diferentes torres. | Se ha visto fallas en las troncales debido a la falta de corriente, deterioro de los equipos de enlace. Dando nivel medio de probabilidad de pérdida de la red inalámbrica. |
| **Controles actuales**<br>Con los cambios realizados a los controles tales como contraseñas, equipos de mayor seguridad de enlace inalámbrica, estabilidad de la corriente con ups, estabilizadores, actualizaciones de firewall, sistemas licenciados. | Los cambios han logrado que se estabilice los servicios de Internet. Dando un nivel bajo de probabilidad de pérdida de red inalámbrica. |

### *3.8.2 Análisis de impacto.*

**Tabla 13** ***De análisis de impacto***

| | **Pérdida de integridad** | **Pérdida de disponibilidad** | **Rating de impacto** |
|---|---|---|---|
| Análisis de impacto sobre la misión | Cuando los equipos se queman o sufren algún tipo de desperfectos son causa de retraso hacia la misión de la empresa | Como consecuencia se pierde los datos que son importantes para los clientes como medio de trabajo | El riesgo es alto de pérdida de la red inalámbrica |
| Valorización de la criticidad de los activos | La pérdida de integridad de los equipos de enlace es un riego de perder información que se transmite vía Internet | La pérdida de disponibilidad de la red inalámbrica en un riesgo de no concluir los tramites que el usuario hace. | El riesgo es alto de pérdida de la red inalámbrica |
| Criticidad de datos sensibilidad | La pérdida de integridad de los datos de los usuarios es una pérdida de mucho dinero, años de trabajo de recolección de información. | El perder la disponibilidad de la información hace que el usuario pierda mucho dinero. | El riesgo de impacto es alto de pérdida de la información |

#### *3.8.2.1 Determinación del riesgo*.

**Tabla 14** ***De determinación del riesgo***

| | Riesgos | Niveles de riesgos |
|---|---|---|
| Probabilidad de explotación de las amenaza | Cuando los sistemas están con desactualizaciones de antivirus, sistemas piratas, firewall desactivados, sin control de IP. | Los niveles de riesgos son altos. |
| Magnitud de impactos | Los ataque son muy seguidos y por lo tanto los equipos de cómputo sufren desperfectos, como también los equipos de enlaces son atacados muy constantemente en especial cuando no tiene actualización de firewall. | Los niveles de riesgo es muy alto para todos los usuarios |
| Adecuación de los controles actuales y planificados | Los controles actuales son cambiar los equipos a más modernos por su firewall y se planifica comprar un sistema de control de actividades de red. | El nivel es medio |

#### *3.8.2.2 Recomendaciones de control*.

## Recomendación

**Tabla 15** ***De recomendación de control***

| Nº | DESCRICION DEL RIESGO | ESTRATEGIA / CONTROL | Factibilidad | Efectividad |
|---|---|---|---|---|
| 1 | Infección de virus en su computadora del usuario final | Los antivirus deben ser originales en el usuario final | Los antivirus originales son más factibles para evitar los ataques de virus, spyware entre otros tipos de ataque. | Pero no es tan efectivo por que cuando no tienen actualizaciones seguidas son proclives a ser vulnerados por los ataques. |

| | | | | |
|---|---|---|---|---|
| 2 | Error de configuración de equipos inalámbrico en la empresa SERVINTECOMP. | Hacer un proceso de regla de configuración en los equipos inalámbricos. | El tener una regla de configuración se hace más factible los trabajos de enlaces. | Pero no garantiza que no cometan erro en la configuración de los equipos inalámbricos |
| 3 | Interrupción de corriente. | Implementar estabilizadores y ups en el sistema de la red inalámbrica. | El tener respaldo de corriente asegura tener una conectividad sin interrupción, siendo factible la conectividad | Pero en alguna oportunidad se puede descargar y perder conectividad. |
| 4 | Equipos de conexión inalámbricas puede quemarse con las descargas eléctricas, mal servicio eléctrico. | Tener equipos de Repuestos ante esos problemas. | Es factible tener equipos clonados para no perder la red inalámbrica. | Pero a veces se puede perder varios equipos y no tener en stock para su cambio en la red inalámbrica. |
| 5 | Equipos inalámbricos antiguos más de 5 años. | Hacer un inventario de todos los equipos para su respectivo cambio. | Es factible su cambio cuando se tiene inventariado los equipos obsoletos. | Pero los cambio siempre es costoso y a veces problemáticos por que los clientes también tienen que cambiar su equipo |
| 6 | Cables de red más de 5 años pueden tener porosidad y eso hace penetrar al agua, perjudicando al (PoE) como consecuencia resetea al radio enlace y lo malogra. | Hacer un inventario para el cambio de cables de más de 5 años junto con sus respectivos conectores. | Es factible hacer el cambio e importante, para el bienestar de los equipos de la red inalámbrica. | La efectividad del cambio de los cables aporta un mejora a la red inalámbrica |
| 7 | Falta de política de uso de red. | Implementar un sistema de política de red. | ES factible la seguridad en la red inalámbrica con políticas de uso de la red | La efectividad se nota cuando no hay interrupción de la red inalámbrica. |

### *3.8.2.3 Resultado de la implementación o documentación.*

**Implementación o documentación.**

Una vez que se ha analizado y evaluado, las amenazas, y el riesgos que tiene cada vulnerabilidad, como resultado de este análisis se elaborado un plan para el tratamiento de la red inalámbrica en la empresa SERVINTECOMP.

A continuación se realizado el listado de vulnerabilidades detectadas, en relación al riesgo, a las mismas que se sugiere uno o varios controles los cuales permitirán reducir la posibilidad de ocurrencia de estos riesgos.

**Tabla 16*. Controles recomendados, con relación al análisis de riesgos***

| Vulnerabilidad | Control sugerido | Nivel de impacto de riesgo |
|---|---|---|
| Red inalámbrica abierta | -Hotspot<br>-Cifrado de red | Una red inalámbrica abierta es un riesgo alto. |
| Falta de control en la administración de IP. | -Inventario de gestión de redes. | Una falta de control a la red mediante una administración de ips es alto. |
| Inexistencia de políticas de uso de red. | -Preparación de políticas de uso de red. | Una falta inexistencia de políticas de uso de red es alto. |
| Falta de control de los datos de que se descarguen a través de la red. | -Elaborar filtro de contenidos, Firewall. | Una falta de control de los datos que se descarguen a través de la red es alto. |
| Inexistencia de respaldo de la información. | -Elaborar políticas de respaldo. | La inexistencia de respaldo de la información es un riesgo alto. |
| Inexistencia de reglas de autenticación de usuarios. | -Elaborar políticas de contraseñas.<br>-Concientización en temas de seguridad. | La inexistencia de reglas de autenticación de usuarios es un riesgo alto. |
| Fallas por parte del proveedor de internet. | -Emitir comunicados a la empresa proveedora como averías. | Las fallas constantes de Internet por parte del proveedor es un riesgo alto. |
| Abuso de las conexiones de red. | -Elaborar políticas de uso de red. | El constante abuso de conexión de la red es un riesgo alto. |
| Inexistencia de políticas de uso de hardware. | -Diseñar políticas de hardware | Inexistencia de políticas de uso de hardware es un riesgo alto. |

| | | |
|---|---|---|
| Uso de contraseñas débiles | -Elaborar políticas para contraseñas.<br>-Capacitación a usuarios finales sobre temas de seguridad. | El uso de contraseña de débiles es un riesgo alto. |
| Uso de contraseñas repetidas en distintos equipos de enlace. | -Elaborar políticas de contraseñas. | Uso de contraseñas repetidas en distintos equipos de enlace es un riesgo alto. |
| No existe mantenimiento de las instalaciones eléctricas en las torres de enlace. | -Diseñar plan de mantenimiento preventivo para las estaciones eléctricas. | El no tener mantenimiento de las instalaciones eléctricas en las torres es un riesgo alto. |
| Robo de información | -Elaborar políticas de confidencialidad. | El robo de información es un riesgo de impacto medio. |
| Inexistencia de controles sobre la utilización de memoria y disco duro. | -Elaborar test a los discos duros y memorias. | Inexistencia de controles sobre la utilización de memorias y discos duros es un riesgo de impacto medio. |
| Inventario del tiempo de vida útil que tienen los equipos. | -Elaborar planes de mantenimiento preventivo.<br>-Elaborar planes de periodos de renovación de hardware. | El inventario del tiempo de vida útil que riesgo medio. |
| Utilización de versiones de aplicaciones obsoletas. | -Elaborar planes de actualizaciones para aplicaciones más utilizadas en la institución. | Utilizaciones de versiones de aplicaciones obsoletas son riesgo medio. |
| Personal no capacitado en temas de seguridad. | -Concientizar al personal de recibir del buen uso y manejo de las tic´s. | Personal no capacitados en temas de seguridad es riesgo medio. |
| Falta de mantenimiento preventivo en las torres. | -Elaborar planes de mantenimiento de las torres | Falta de mantenimiento preventivo en las torres es riesgo medio. |
| Inexistencia de licencia de antivirus en algunos usuarios finales. | -Educar a los usuarios finales en usar antivirus con licencia originales. | Inexistencia de licencia de antivirus en algunos usuarios finales es riesgo medio. |
| Falta de respaldo ante equipos que enlace que se puede malograr. | -Elaborar plan de respaldo a las configuraciones de los equipos de enlaces. | Falta de riesgo ante equipo que enlace que se puede malograr es riesgo medio. |
| Desastres naturales. | -Elaborar plan de respaldo ante tales eventos. | Los riesgos de desastres de medio naturales es riesgo medio. |

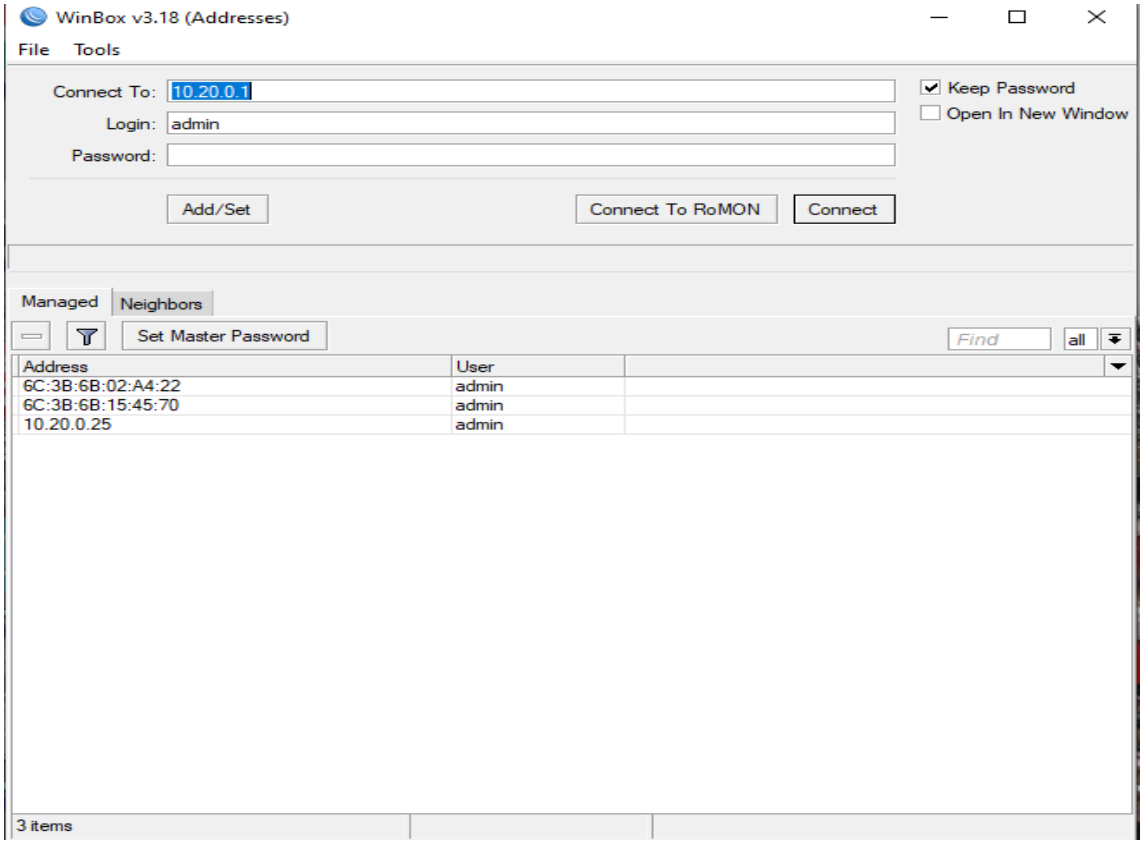
### 3.8.3 VARIABLE 2: LA SEGURIDAD DE REDES INALÁMBRICAS

#### 3.8.3.1 Protección

Para una mejor protección pues el proveedor y el usuario final deben temar las medidas mínimas de seguridad de las cuales están descrita a continuación.

### 3.8.4 Cambiar la contraseña de fábrica.

Este es el primer paso a realizar, porque todos los equipos vienen con contraseña de defecto tales como Mikrotik, TP-Link no se pone contraseña y se encuentra en las páginas web, descargar y ejecutar el programa y para acceder a la configuración del equipo.




Fuente. Elaboración Propia

**Figura 6**. Winbox v3.18 (mikrotik)

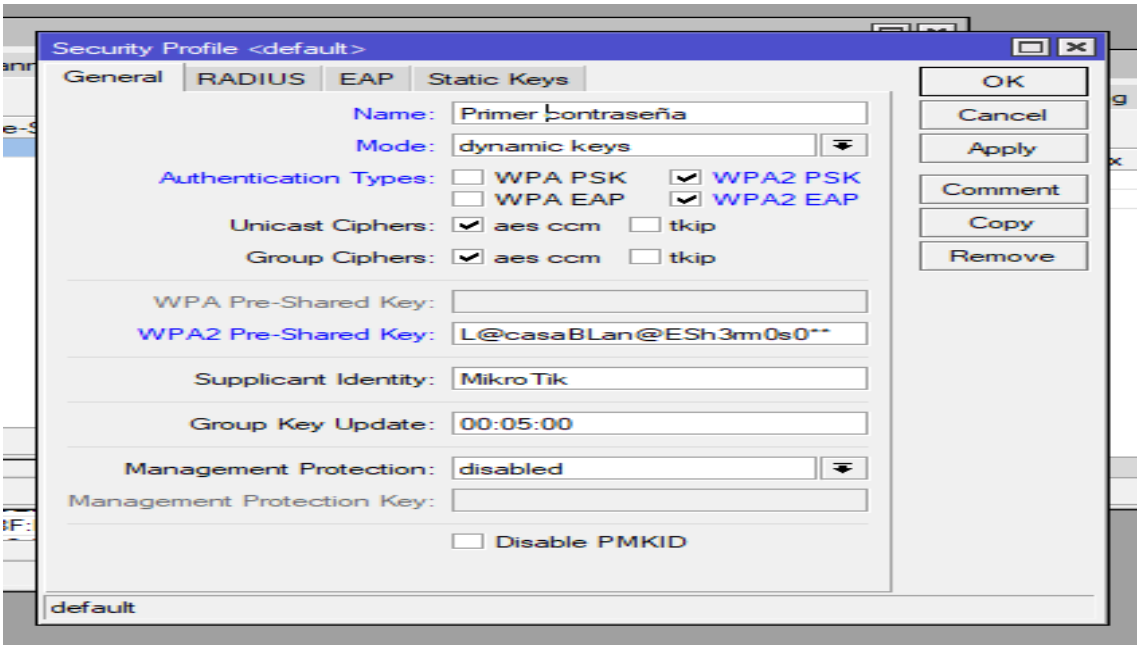
### *3.8.5 Poner la contraseña en WPA2 AES.*

Gracias al uso de AES, que sustituye al TKIP del WAP, un potente algoritmo de encriptación, el método de autenticación WPA2 puede cumplir con las exigencias en seguridad del gobierno del estado.

También soporta 63 caracteres, y se tiene que hacer la contraseña con letras mayúsculas, minúsculas, números, y caracteres la extensión mínima es de 8 caracteres de la cual esta contraseña se hace bien robusta.

Por ejemplo:

l@casaBlancaESh3rm0s0en**




Fuente. Sistema de Mikrotik del Sistema de Control

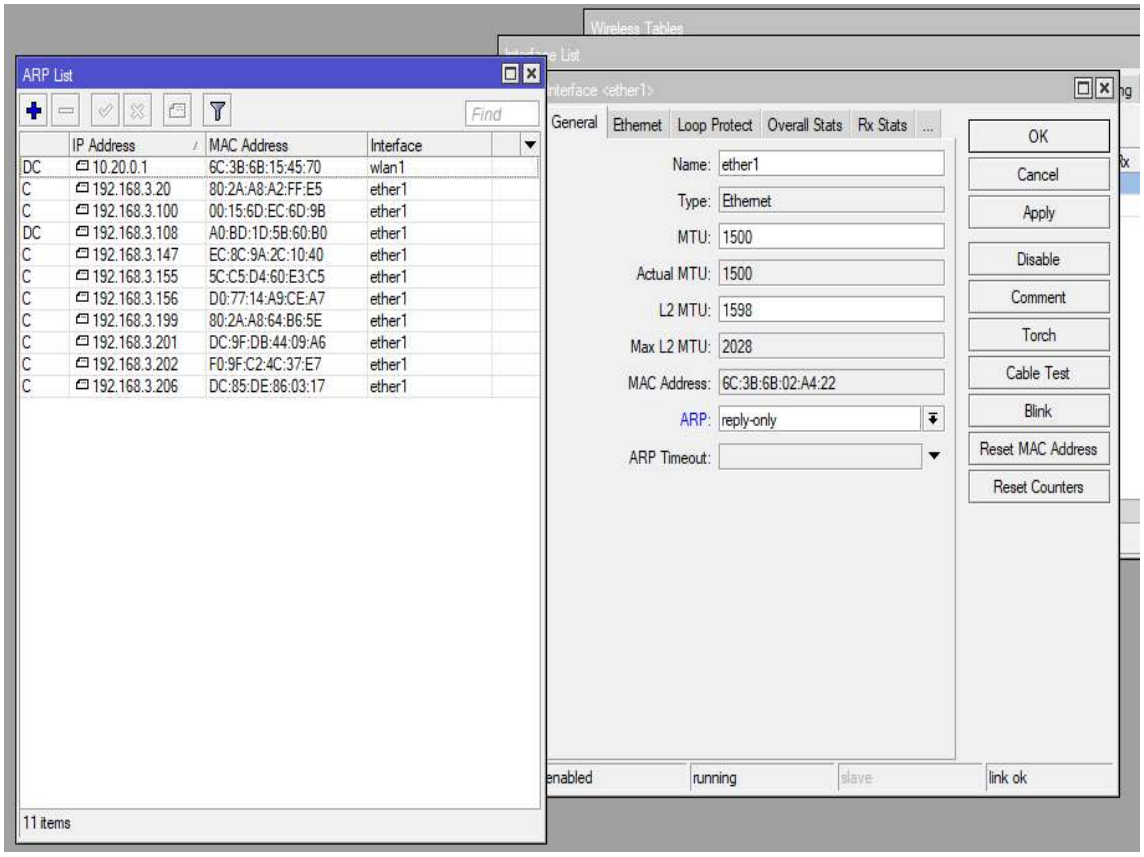
**Figura 7**.La contraseña WPA2 AES (mikrotik)

#### *3.8.5.1 Activar el filtrado de direcciones MAC.*

El hecho de ser un código único, compuesto por 48 bits, que se expresa en formato hexadecimal (Letras y Números), y que permite identificar unívocamente el dispositivo en todo el mundo.

Entonces al habilitare el filtrado de Mac en los Reuters o en el equipo administrador de red, hace que se restrinja a los demás con la conectividad ya que puedan tener la contraseña más no la autorización de acceso.

Por ejemplo Mikrotik se configura de esta manera.




Fuente. Sistema de Mikrotik del Sistema de Control

**Figura 8.** *Configuración de la MAC en Mikrotik*

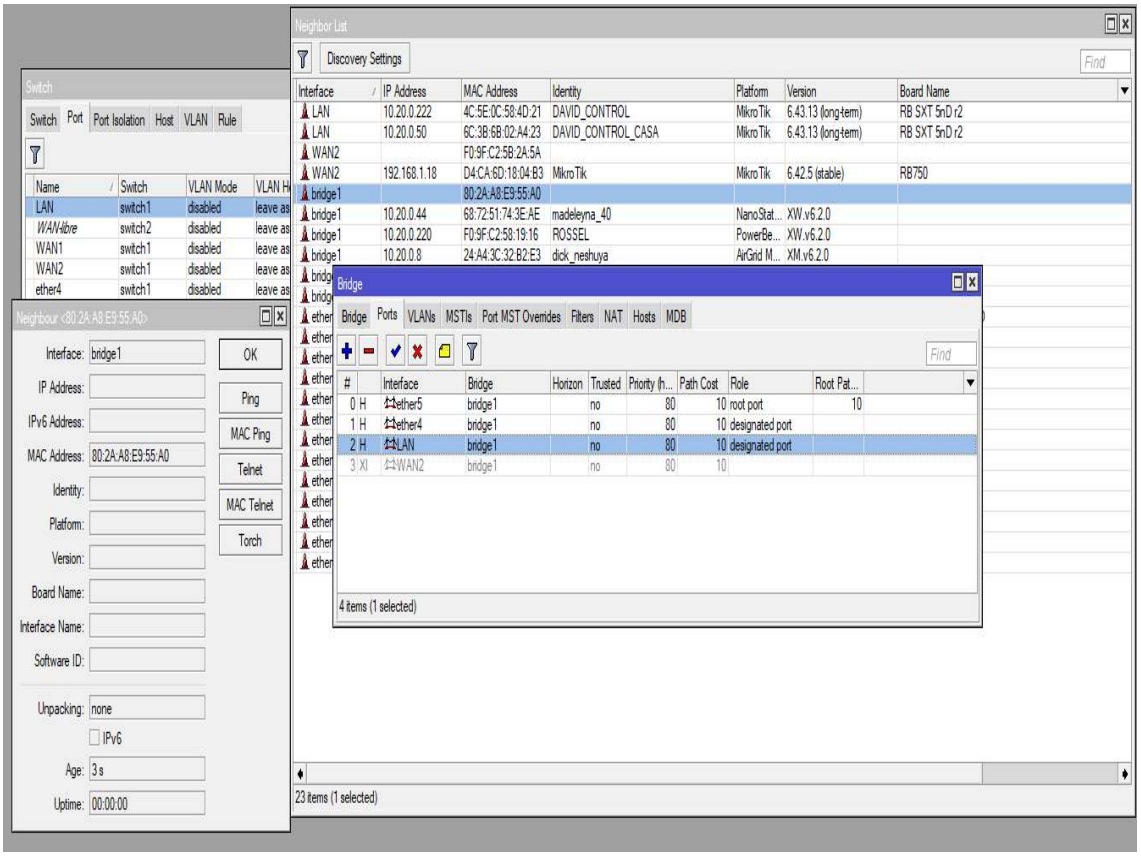
#### *3.8.5.1 Detección*

La manera más efectiva de saber si hay un intruso es analizando el consumo de recursos; por ejemplo una reducción de ancho de banda, un incremento de respuesta de los equipos, tiempo de carga y descarga.

### *3.8.5.2 Secuestro de sesión.*

Los Cracker monitorean la red para ver a los usuarios, claves, direcciones, MAC, SSID y elije uno de ellos para enviarle un ataque de denegación de servicio y así desconectarlo. Después se conecta con la información recopilada del usuario eliminado.

Los switcher inalámbricos nos ayudan a descubrir este tipo de ataque.




Fuente. Sistema de Mikrotik del Sistema de Control

**Figura 9.** Un posible secuestro de usuario (mikrotik)

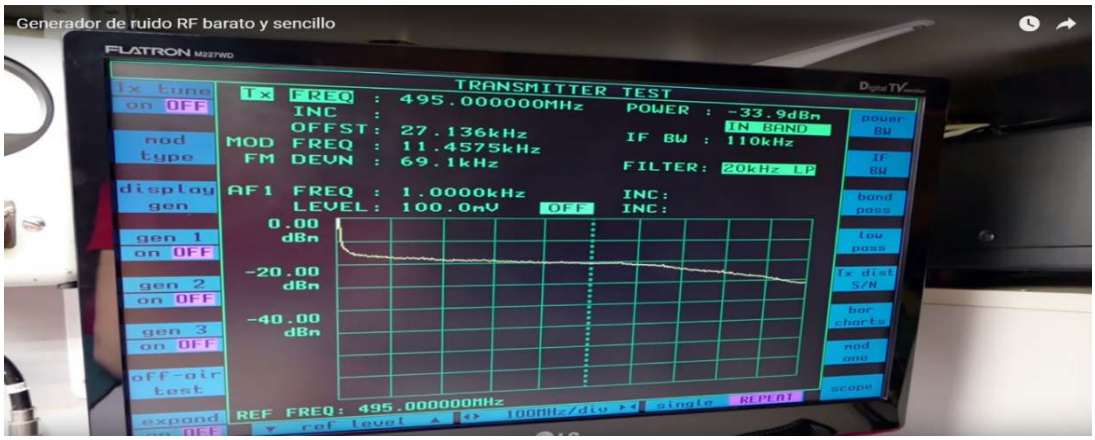
### *3.8.5.3 Suplantación de dirección de MAC*

Con este tipo de ataque es pues cuando es configurado solo con protección de MAC, por lo cual se sugiere la contraseña WAP2-aes.

### *3.8.5.4 Saturar el ambiente con ruido de RF*

La relación señal/ruido en todos los puntos de una red inalámbrica debe ser mayor o igual a 0.3 pues de lo contrario el ruido prácticamente anulará la señal y la red será inutilizable. (Vallejo de leon, 2010)

Y esto se hace mediante las frecuencias que se pone y la banda ancha.



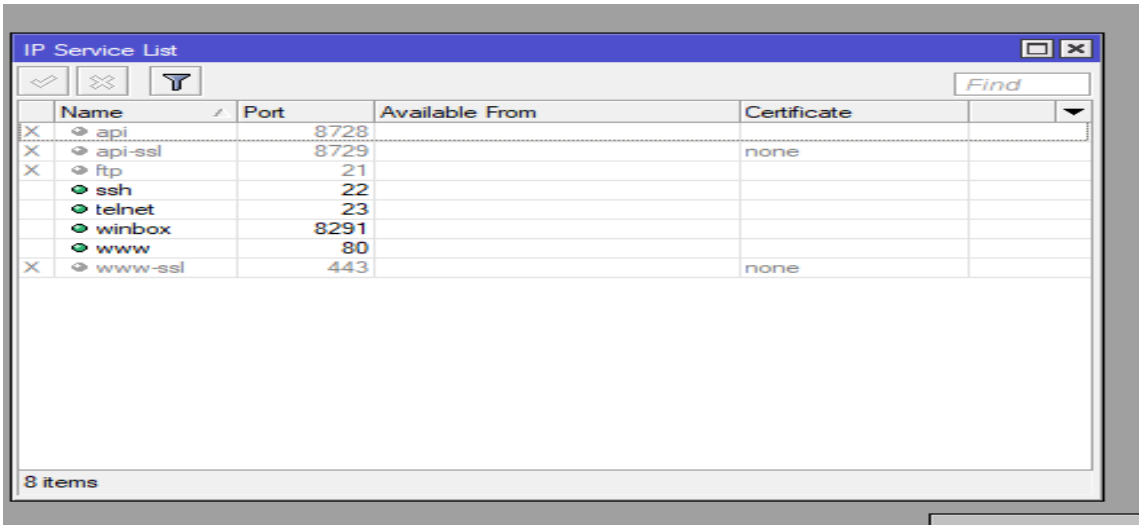

Fuente. Google

**Figura 10.** Un ejemplo en Youtube acerca de generador de ruido RF

**nota:** Esta es la pág. Web de referencia:
https://www.youtube.com/watch?v=VoM1ezzVuU4

### *3.8.6 Reacción*

Una vez identificado el problema hay responder con una configuración de seguridad para luego regresar al estado de seguridad, tales configuración es cambio de contraseña, poner restricciones en el firewall, deshabilitar algunos acceso al equipo administrador de la red.




Fuente. Sistema de Mikrotik del Sistema de Control

**Figura 11.** Un claro ejemplo de reducir acceso al Mikrotik

**Nota**: En la ilustración se ve que está deshabilitado el api, api-ssl, ftp, www-ssl en las cuales se utiliza para configurar y agregar script y eso forma parte de la seguridad.

# CAPITULO IV: RESULTADOS

El procesamiento y análisis estadístico de datos, se realizó con el software SPSS Versión 25.

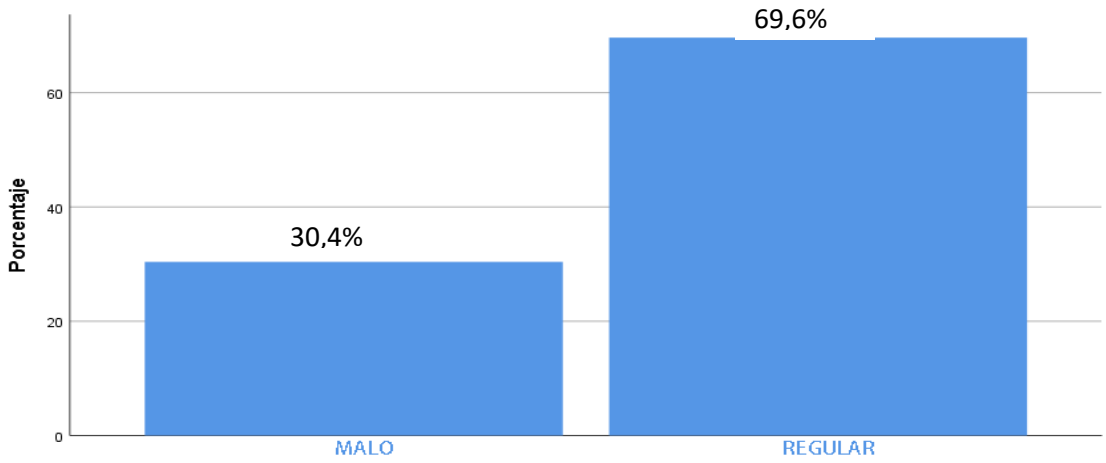
## 4.1 INTERPRETACIÓN DE RESULTADOS PRE TEST

### 4.1.1 Del cuestionario

PE: 1. ¿CÓMO CALIFICA EL ROUTER Y LA ANTENA DE ENLACE QUE ESTÁ INSTALADO PARA EL SERVICIO DE INTERNET?

**Tabla 17** ***Calificación del ruter y del equipo de enlace***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 24 | 30,4 | 30,4 | 30,4 |
| | Regular | 55 | 69,6 | 69,6 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente: Elaboración Propia

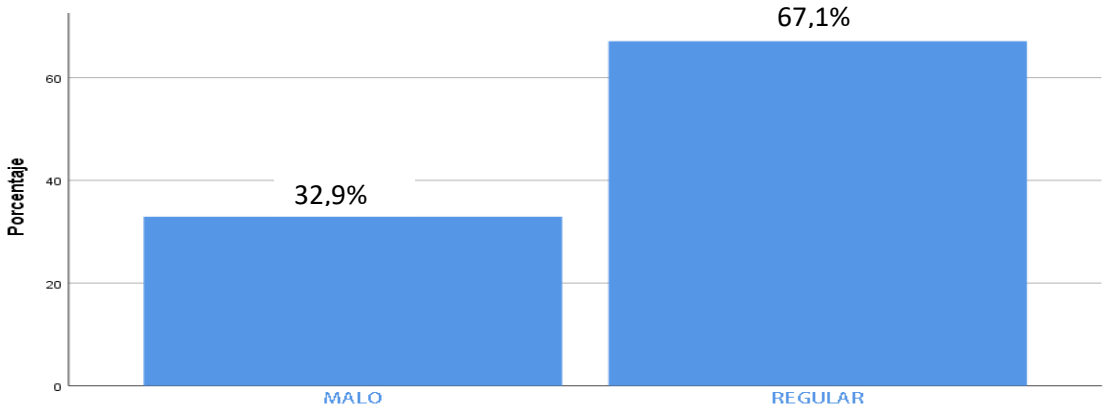
**Figura 12**. Calificación del ruter y del equipo de enlace

Nota: El 30,4% dice que es malo y el 69,6% dice que es regular los rutes y los equipos de enlaces.

PE: 2. ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TÉCNICO?

**Tabla 18** ***Cómo califica al personal técnico***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 26 | 32,9 | 32,9 | 32,9 |
| | Regular | 53 | 67,1 | 67,1 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. *Elaboración Propia*

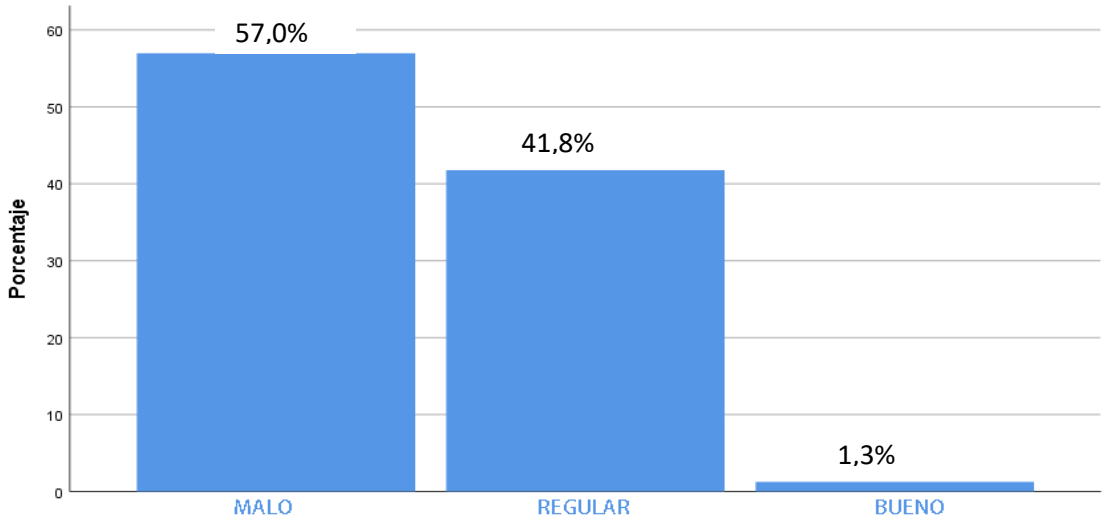
**Figura 13**.Calificación del personal técnico

Nota: El 32,9% dice que es malo y el 67,1% dice que es regular, califica al personal técnico.

PE: 3. ¿Cómo califica el servicio de Internet?

**Tabla 19** ***Cómo califica el servicio de internet***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 45 | 57,0 | 57,0 | 57,0 |
| | Regular | 33 | 41,8 | 41,8 | 98,7 |
| | Bueno | 1 | 1,3 | 1,3 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

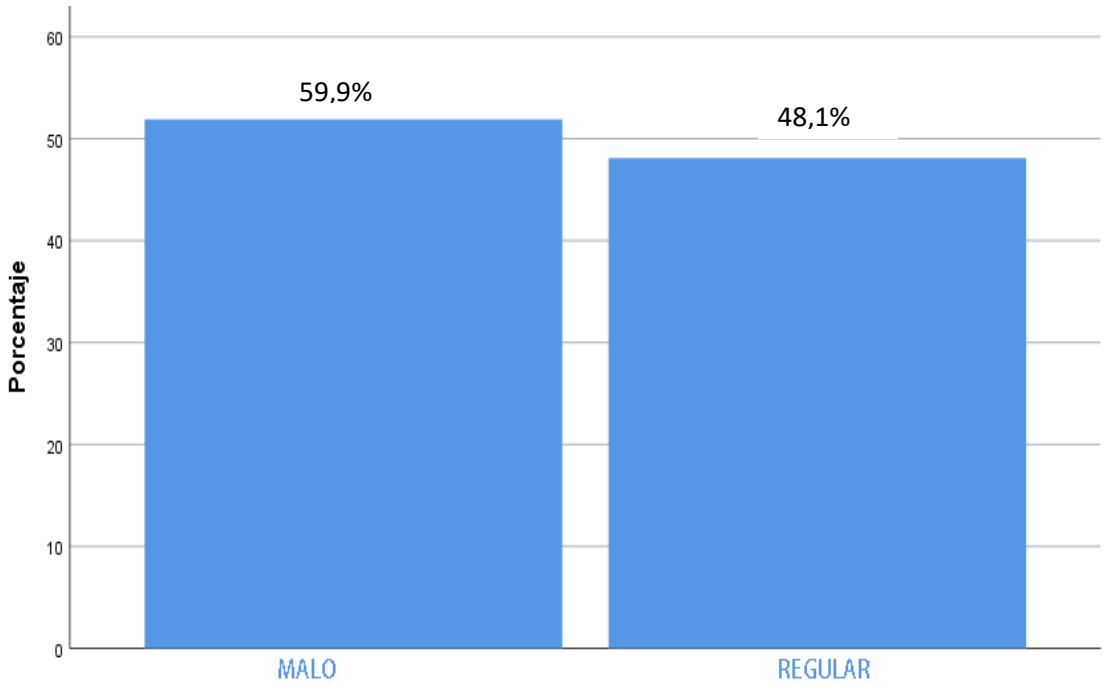
**Figura 14.** Calificación del Servicio de Internet

Nota: El 57,0% dice que es malo, el 41,8% dice que es regular y el 1,3% dice que es bueno así lo califica el servicio de Internet.

PE: 4. ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO CALIFICA?

**Tabla 20** ***Los reportes de ataque de virus***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 41 | 51,9 | 51,9 | 51,9 |
| | Regular | 38 | 48,1 | 48,1 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

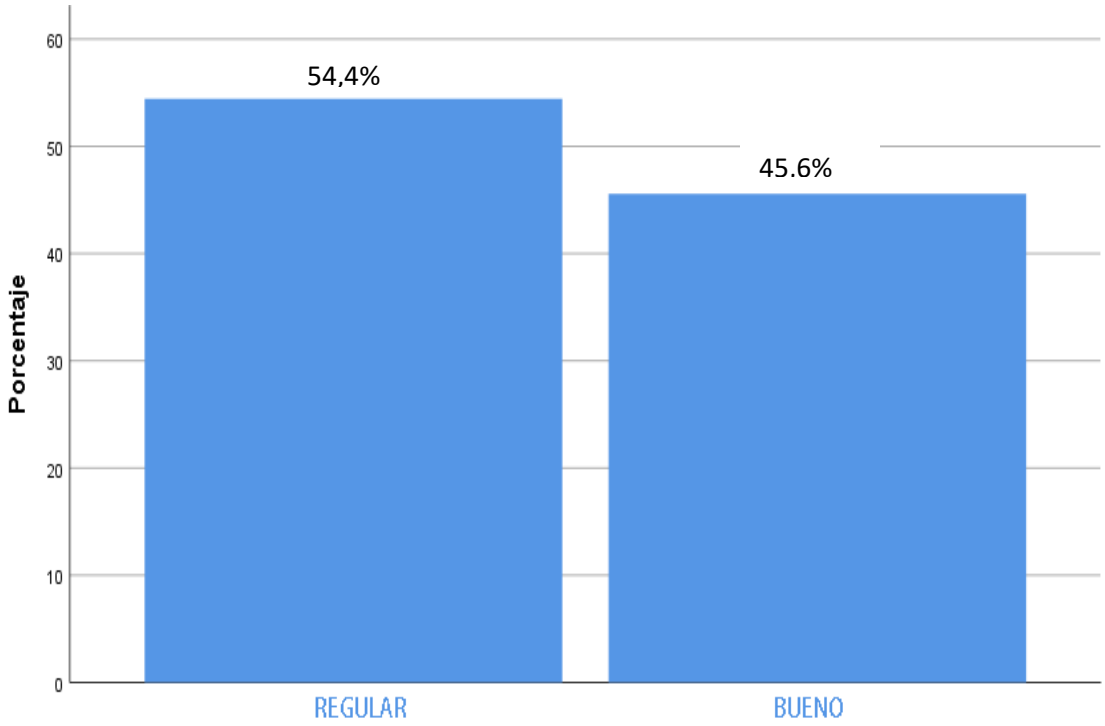
**Figura 15**. Calificación de los reportes de ataques de virus

Nota: El 51,9% dice que es malo y el 48,1% dice que es regular lo califica los reportes de ataque de virus.

PE: 5. ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO CALIFICA?

**Tabla 21** ***Los reportes de definiciones de amenazas***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Regular | 43 | 54,4 | 54,4 | 54,4 |
| | Bueno | 36 | 45,6 | 45,6 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

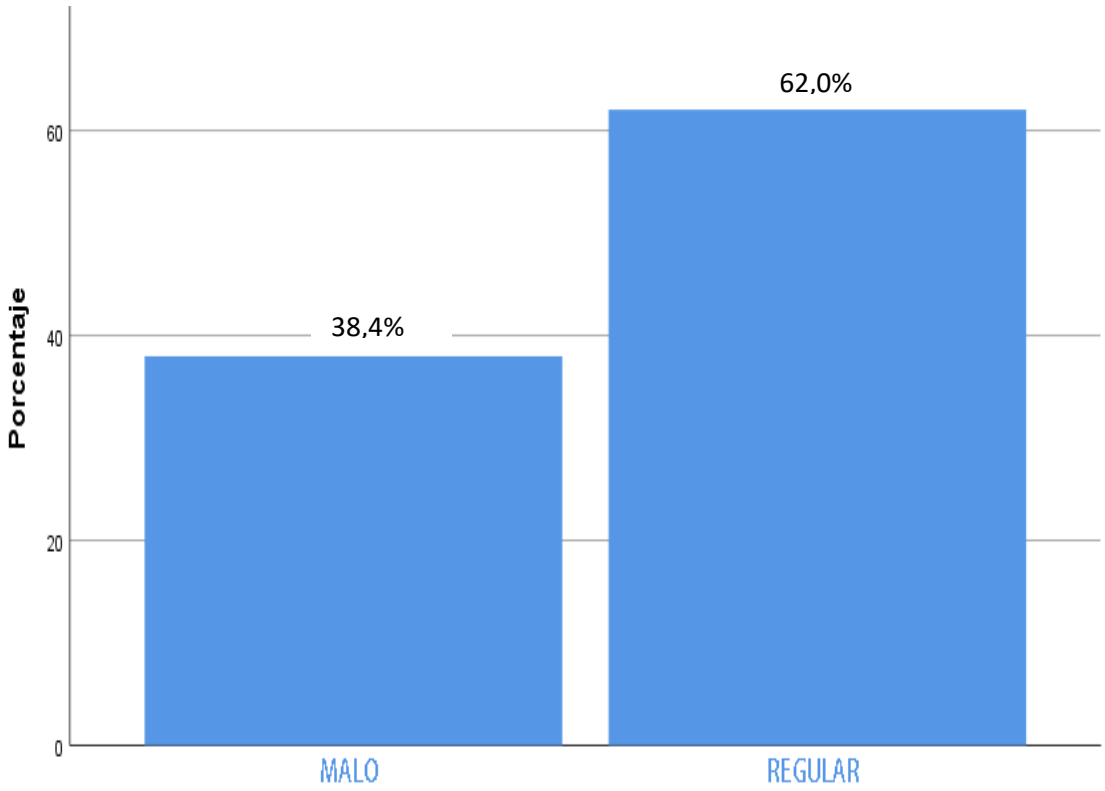
**Figura 16.** Calificación de los reportes de definiciones de amenazas

Nota: El 54,4% dice que es regular y el 45,6% dice que es bueno así lo califican al reporte de definiciones de amenazas.

PE: 6. ¿CÓMO CALIFICA LA MOTIVACION DE LOS ATAQUES, SI SU INFORMACION PERSONAL SE VIERA AFECTADA?

**Tabla 22** ***La motivación de los ataques***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 30 | 38,0 | 38,0 | 38,0 |
| | Regular | 49 | 62,0 | 62,0 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

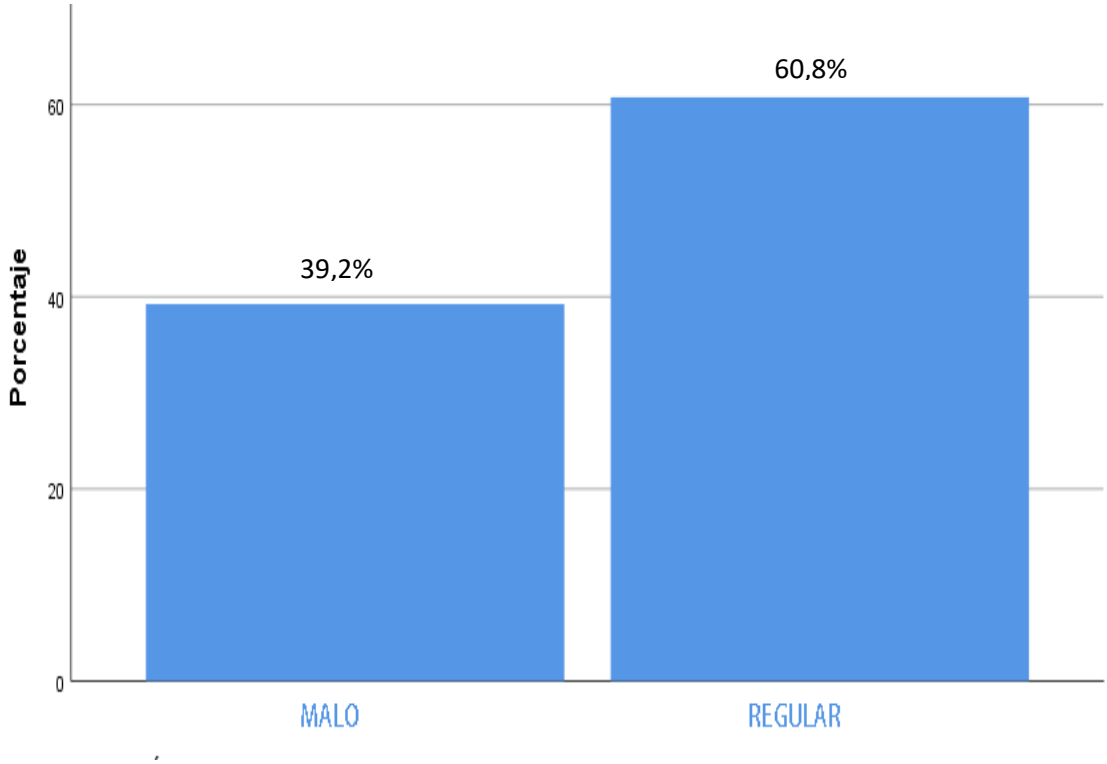
**Figura 17.** Calificación de la motivación de los ataques

Nota: El 38,0% dice que es malo y el 62,0% dice que es regular, califica a la motivación de los ataques, si su información personal se viera afectada.

PE: 7. ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL?

**Tabla 23** ***Capacidad de las amenazas***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 31 | 39,2 | 39,2 | 39,2 |
| | Regular | 48 | 60,8 | 60,8 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

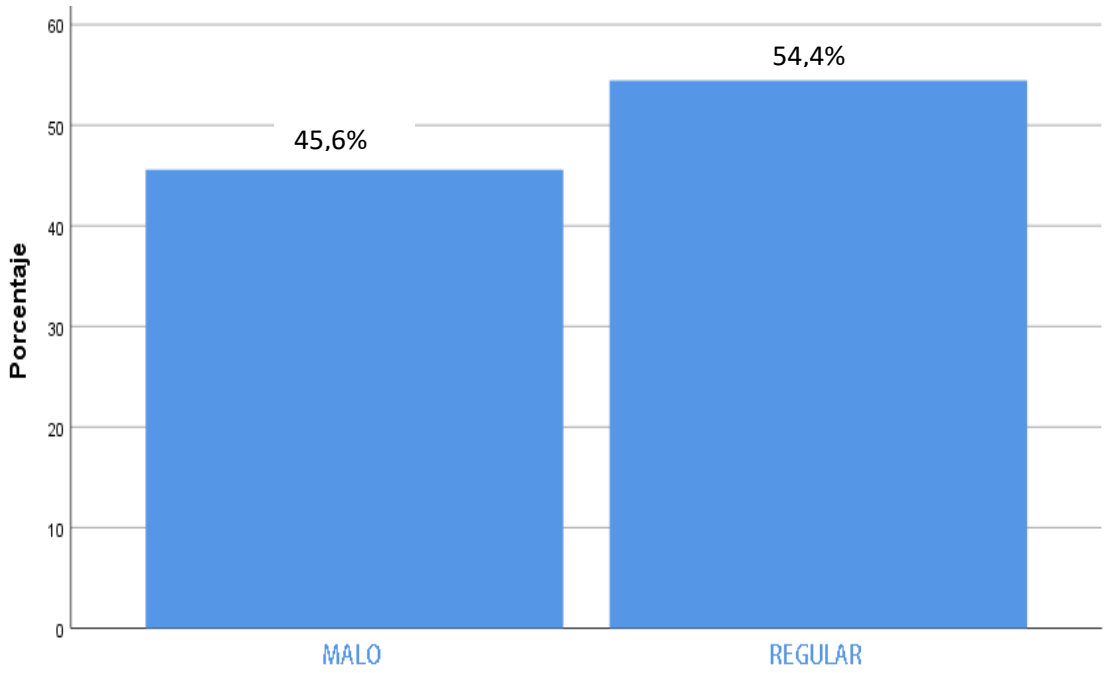
**Figura 18.** Calificación de la Capacidad de las amenazas

Nota: El 39,2% dice que es malo y el 60,8% dice que es regular así lo califica a la capacidad de la amenaza sea tratar de robar toda la información personal.

PE: 8. ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL?

**Tabla 24** ***Impacto de los ataques***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 36 | 45,6 | 45,6 | 45,6 |
| | Regular | 43 | 54,4 | 54,4 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

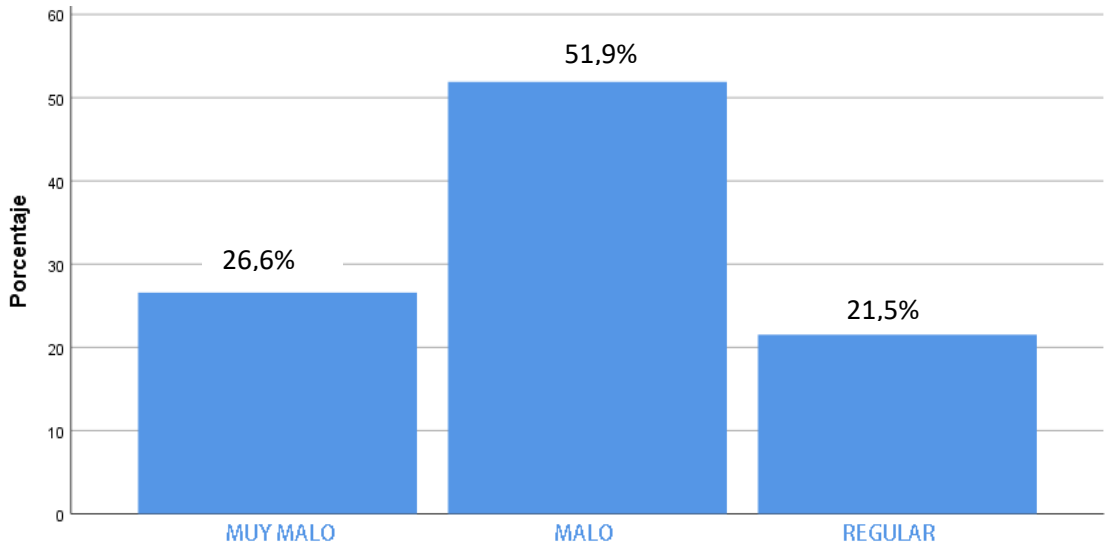
**Figura 19.** Calificación del Impacto de los ataques

Nota: El 45,6% dice que es malo y el 54,4% dice que es regular así lo califica al impacto de los ataques que afecta su información personal.

PE: 9. ¿CÓMO CALIFICA LA SENSIBILIDAD DE TUS DATOS, VULNERABLE DE LOS HACKERS?

**Tabla 25** ***Sensibilidad de tus datos***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Malo | 21 | 26,6 | 26,6 | 26,6 |
| | Malo | 41 | 51,9 | 51,9 | 78,5 |
| | Regular | 17 | 21,5 | 21,5 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

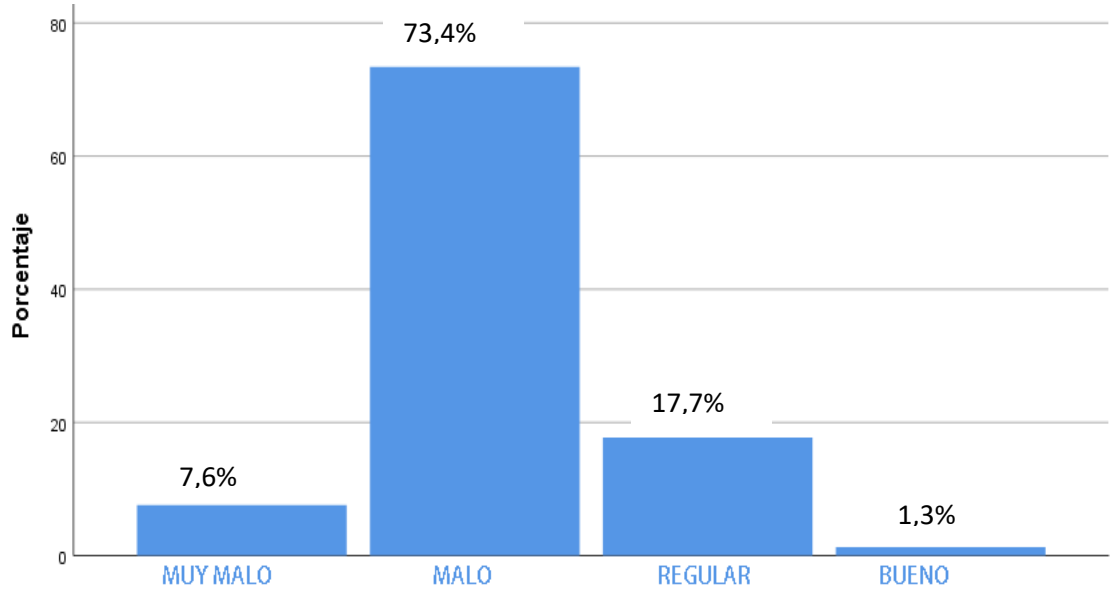
**Figura 20.** Calificación de la Sensibilidad de datos

Nota: El 26,6% dice que es muy malo, el 51,9% dice que es malo y el 21,5% dice que es regular así califica a la sensibilidad de tus datos, sea vulnerado por los hackers

PE: 10. ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI?

**Tabla 26** ***Probabilidad de explotación de las amenazas***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy malo | 6 | 7,6 | 7,6 | 7,6 |
| | Malo | 58 | 73,4 | 73,4 | 81,0 |
| | Regular | 14 | 17,7 | 17,7 | 98,7 |
| | Bueno | 1 | 1,3 | 1,3 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

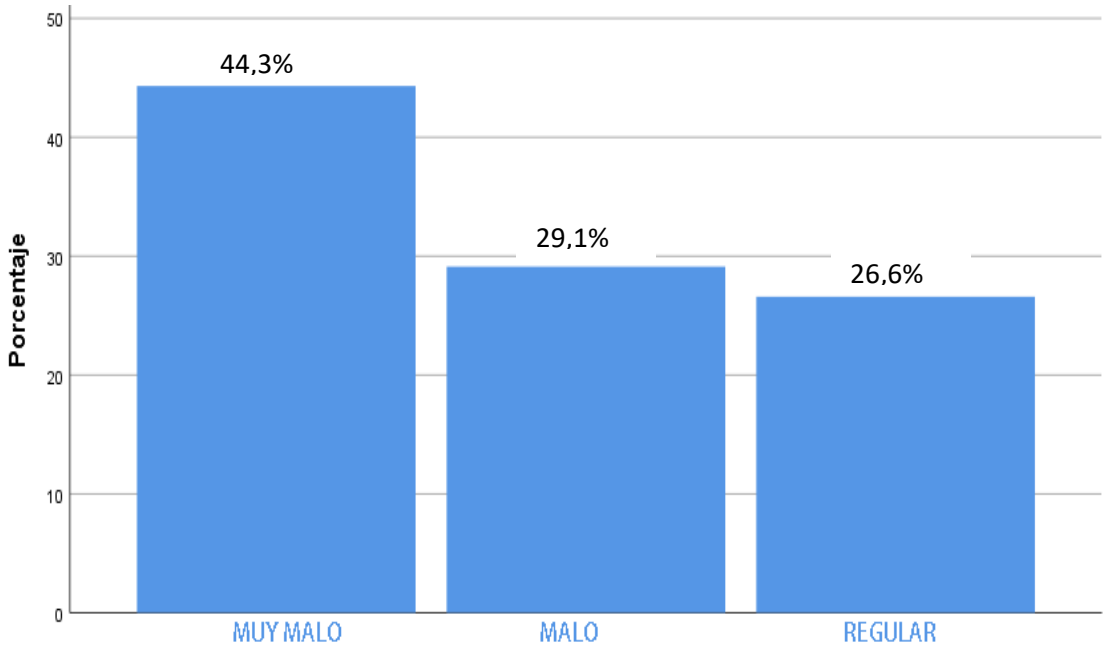
**Figura 21**. Calificación de la Probabilidad de explotación de las amenazas

Nota: El 7,6% dice que es muy malo, el 73,4% dice que es malo, el 17,7% dice que es regular y el 1,3% dice que es bueno así lo califica la probabilidad de explotación de las amenazas sea por medio de su red wifi.

PE: 11 ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACION PERSONAL?

**Tabla 27** ***Magnitud de los impactos***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy malo | 35 | 44,3 | 44,3 | 44,3 |
| | Malo | 23 | 29,1 | 29,1 | 73,4 |
| | Regular | 21 | 26,6 | 26,6 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

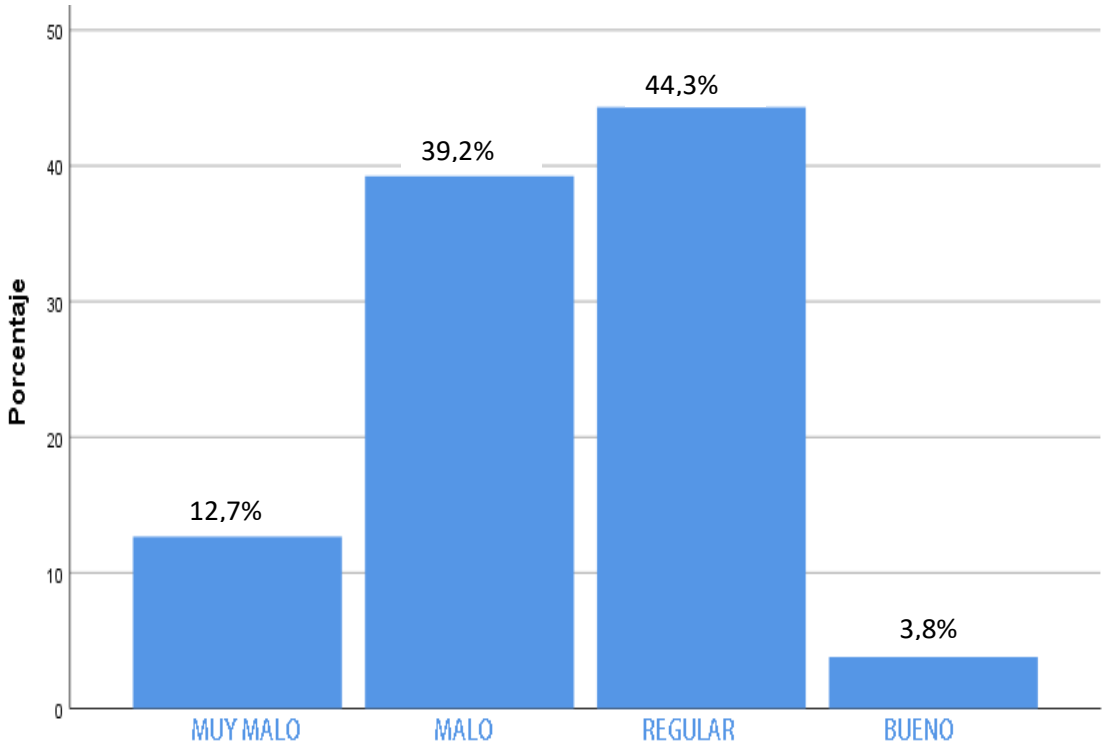
**Figura 22.** Calificación de la Magnitud de los impactos

Nota: El 44,3% dice que es muy malo, el 29,1% dice que es malo, y el 26,6% dice que es regular así lo califica a la magnitud de los impactos de robos de información personal.

PE: 12. ¿CÓMO CALIFICA SU RED INALAMBRICA?

**Tabla 28 Red inalámbrica**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy malo | 10 | 12,7 | 12,7 | 12,7 |
| | Malo | 31 | 39,2 | 39,2 | 51,9 |
| | Regular | 35 | 44,3 | 44,3 | 96,2 |
| | Bueno | 3 | 3,8 | 3,8 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

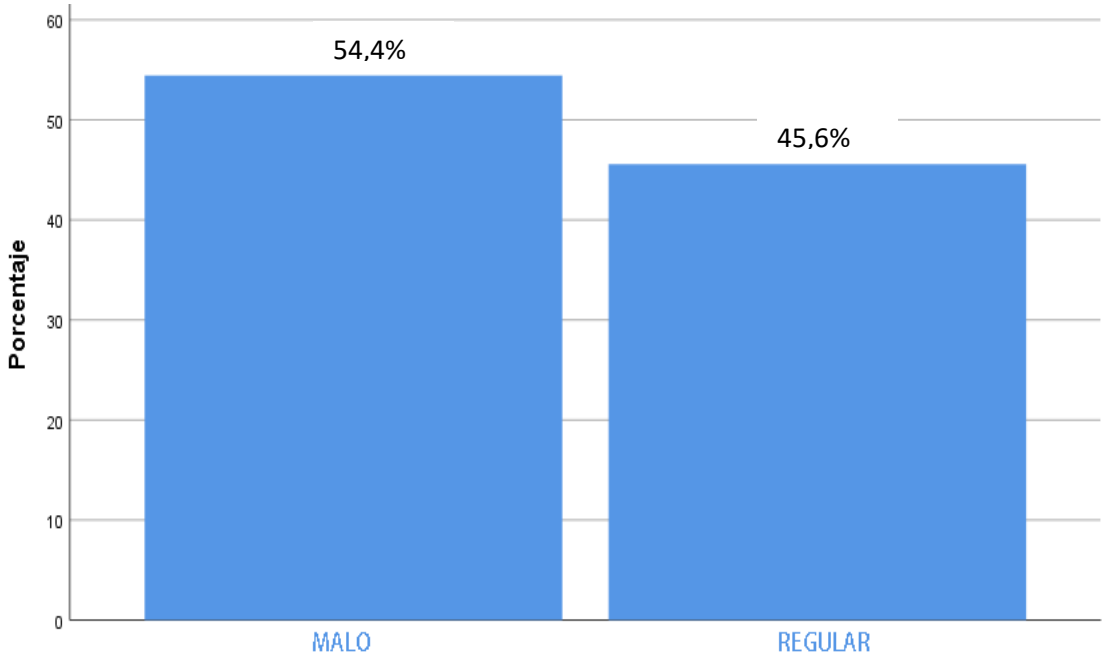
**Figura 23.** Calificación de su Red Inalámbrica

Nota: El 12,7% dice que es muy malo, el 39,2% dice que es malo, el 44,3% dice que es regular y el 3,8% dice que es bueno así lo califica la red inalámbrica del usuario final.

PE: 13. ¿A SU ANTIVIRUS CÓMO LO CALIFICA?

**Tabla 29 *Antivirus***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 43 | 54,4 | 54,4 | 54,4 |
| | Regular | 36 | 45,6 | 45,6 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

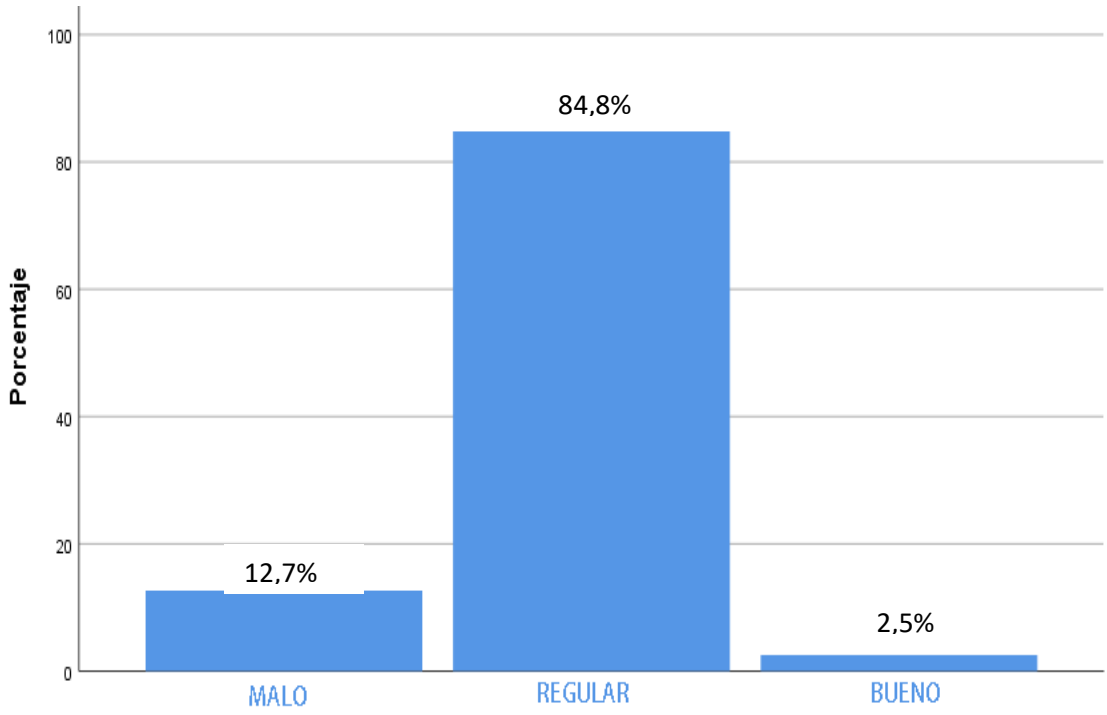
**Figura 24.** Calificación de su Antivirus

Nota: El 54,4% dice que es malo, el 45,6% dice que es regular y el dice que es bueno así lo califica al antivirus que está instalado en su máquina.

PE: 14. ¿CÓMO CALIFICA SU FIREWALL ANTE UNA ANTAQUE DE VIRUS?

**Tabla 30** ***Firewall***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 10 | 12,7 | 12,7 | 12,7 |
| | Regular | 67 | 84,8 | 84,8 | 97,5 |
| | Bueno | 2 | 2,5 | 2,5 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente, Elaboración Propia

**Figura 25.** Calificación de su Firewall

Nota: El 12,7% dice que es malo, el 84,8% dice que es regular y el 2,5% dice que es bueno así lo califica al su Firewall de sus equipos.

**Tabla 31** ***Pre-test***

| PRE-TEST | N | Media | Desv. Desviación | Varianza |
|---|---|---|---|---|
| 1- ¿CÓMO CALIFICA EL ROUTER Y EL EQUIPO DE ENLACE QUE ESTA INSTALADO PARA SU SERVICIO DE INTERNET? | 79 | 2,70 | ,463 | ,214 |
| 2- ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TECNICO? | 79 | 2,67 | ,473 | ,224 |
| 3- ¿CÓMO CALIFICA EL SERVICIO DE INTERNET? | 79 | 2,44 | ,525 | ,276 |
| 4- ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO LO CALIFICA? | 79 | 2,48 | ,503 | ,253 |
| 5.- ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO LO CALIFICA? | 79 | 3,46 | ,501 | ,251 |
| 6.- ¿CÓMO CALIFICA LA MOTIVACIÓN DE LOS ATAQUES, SI SU INFORMACIÓN PERSONAL SE VIERA AFECTADA? | 79 | 2,62 | ,488 | ,239 |
| 7.- ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL? | 79 | 2,61 | ,491 | ,241 |
| 8.- ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL? | 79 | 2,54 | ,501 | ,251 |
| 9.- ¿CÓMO CALIFICA LAS SENSIBILIDAD DE TUS DATOS, VULNERADAA POR LOS HACKERS? | 79 | 1,95 | ,696 | ,485 |
| 10.- ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI? | 79 | 2,13 | ,540 | ,291 |
| 11.- ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACIÓN PERSONAL? | 79 | 1,82 | ,828 | ,686 |
| 12.- ¿CÓMO CALIFICA SU RED INALÁMBRICA? | 79 | 2,39 | ,758 | ,575 |
| 13.- ¿A SU ANTIVIRUS COMO LO CALIFICA? | 79 | 2,46 | ,501 | ,251 |
| 14.-¿CÓMO CALIFICA SU FIREWALL ANTE UNA ATAQUE DE VIRUS? | 79 | 2,90 | ,379 | ,143 |
| N válido (por lista) | 79 | | | |
| Promedio | | 2.5121 | 0.5462 | 0.1738 |

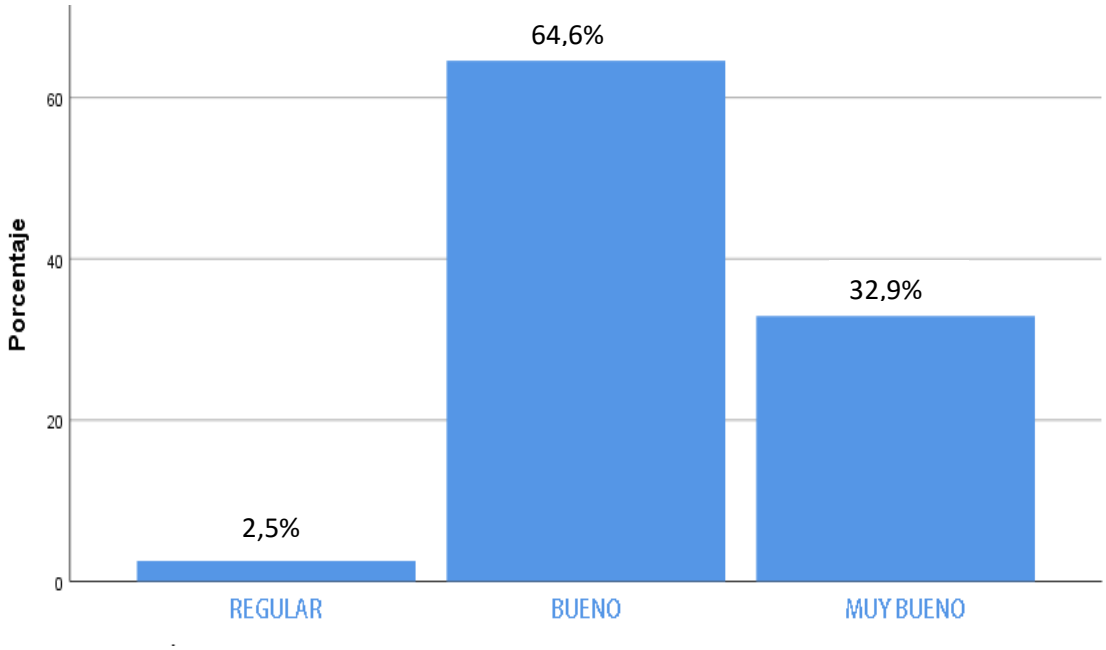
## 4.2 INTERPRETACIÓN DE RESULTADOS POST TEST

### *4.2.1 Del cuestionario*

PE: 1. ¿CÓMO CALIFICA EL REUTER Y LA ANTENA DE ENLACE QUE ESTÁ INSTALADO PARA EL SERVICIO DE INTERNET?

**Tabla 32** ***Reuter equipo de enlace***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Regular | 2 | 2,5 | 2,5 | 2,5 |
| | Bueno | 51 | 64,6 | 64,6 | 67,1 |
| | Muy Bueno | 26 | 32,9 | 32,9 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

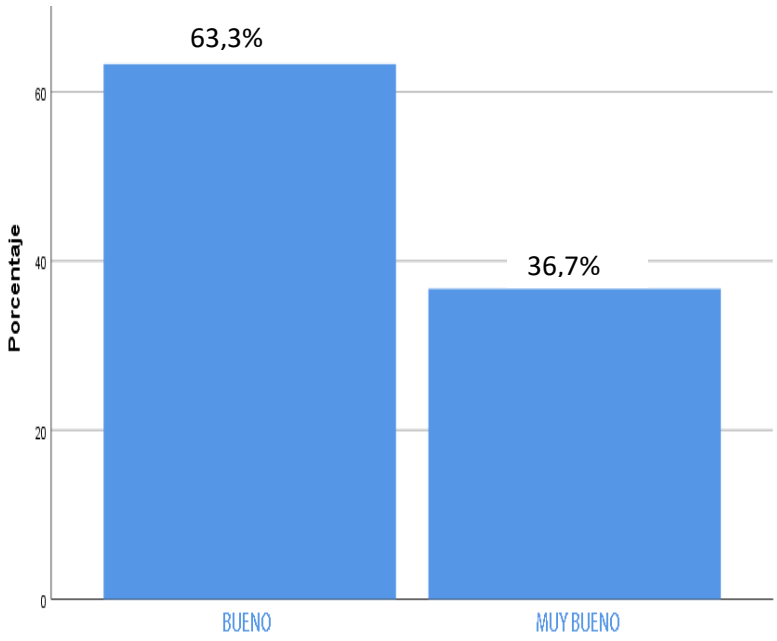
**Figura 26.** Calificación del Reuter equipo de enlace

Nota: El 2,5% dice que es regular, el 64,6% dice que es bueno y el 32,9% dice que es muy bueno así lo califica a los Reuters y antena de enlace.

PE: 2. ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TÉCNICO?

**Tabla 33** ***Personal técnico***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Bueno | 50 | 63,3 | 63,3 | 63,3 |
| | Muy Bueno | 29 | 36,7 | 36,7 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

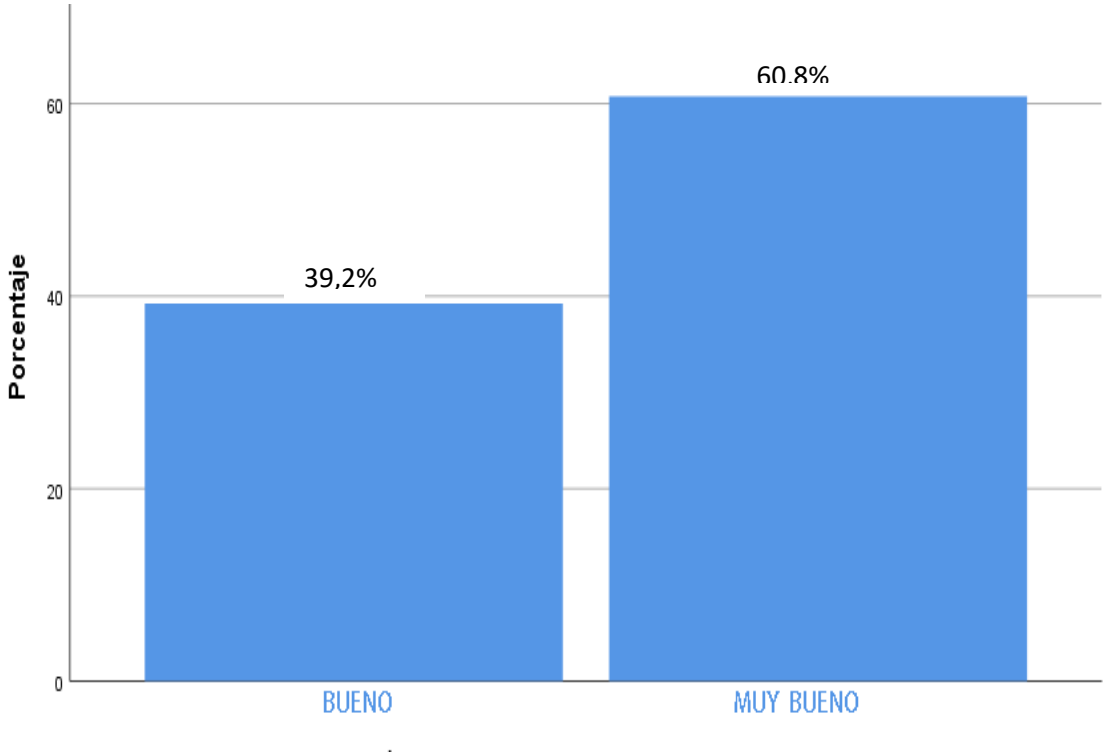
**Figura 27.** Calificación del Profesionalismo del Personal Técnico

Nota: El 63,3% dice que es bueno y el 36,7% dice que es muy bueno así lo califica al personal técnico.

PE: 3. ¿CÓMO CALIFICA EL SERVICIO DE INTERNET?

**Tabla 34** ***Servicio de internet***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Bueno | 31 | 39,2 | 39,2 | 39,2 |
| | Muy Bueno | 48 | 60,8 | 60,8 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

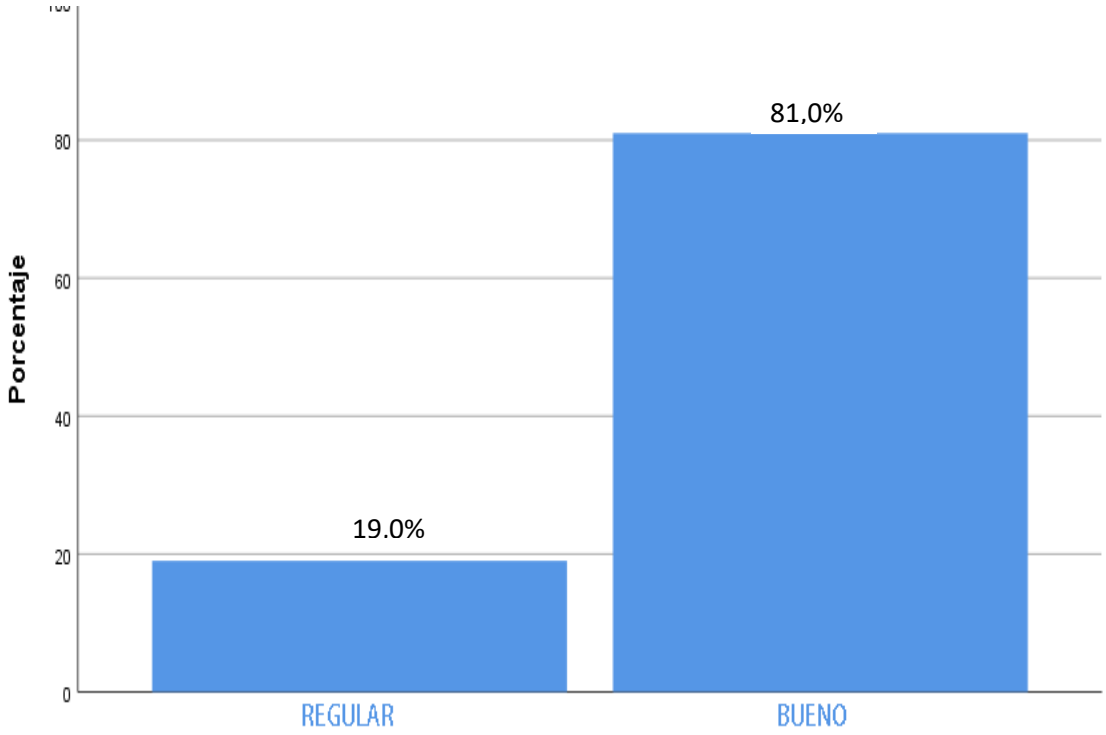
**Figura 28** Calificación del Servicio de Internet

Nota: El 39,2% dice que es bueno y el 60,8% dice que es muy bueno así lo califica el servicio de Internet.

PE: 4. ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO LO CALIFICA?

**Tabla 35** ***Los reportes de ataque de virus***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Regular | 15 | 19,0 | 19,0 | 19,0 |
| | Bueno | 64 | 81,0 | 81,0 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

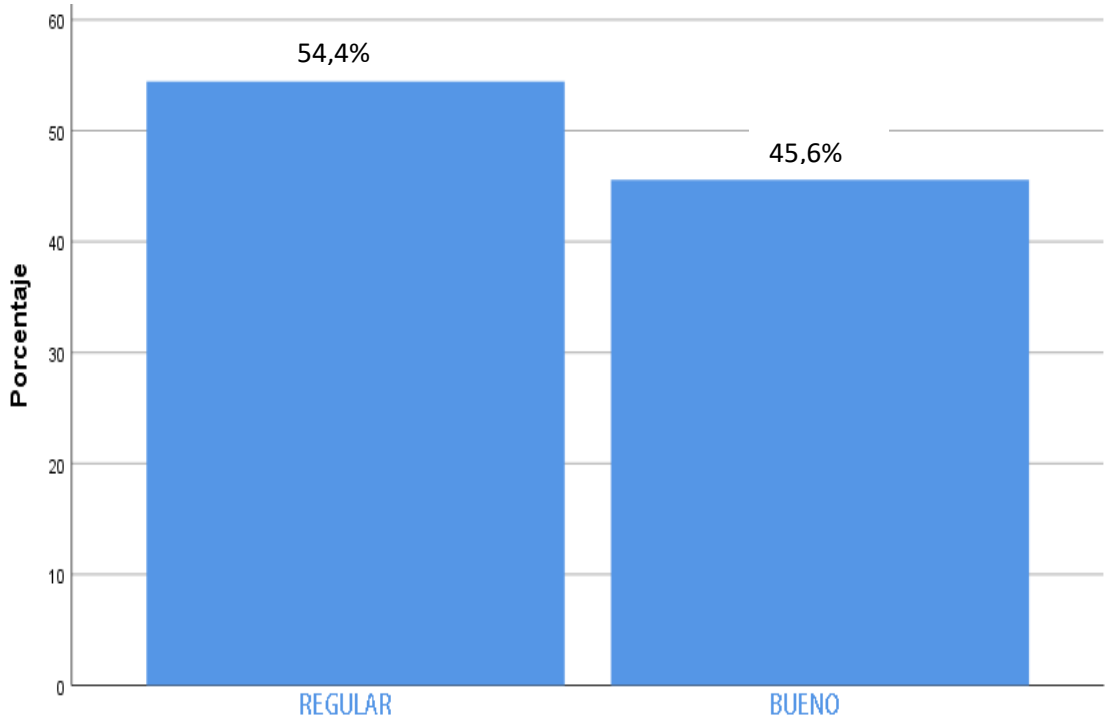
**Figura 29.** Calificación de los reportes de ataque de virus

Nota: El 19,0% dice que es regular y el 81,0% dice que es bueno así lo califica el reporte de ataque de virus.

PE: 5. ¿LOS REPORTES DE DEFINICIONES DE AMENAZA, CÓMO LO CALIFICAN?

***Tabla 36 Definiciones de amenazas***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Regular | 43 | 54,4 | 54,4 | 54,4 |
| | Bueno | 36 | 45,6 | 45,6 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

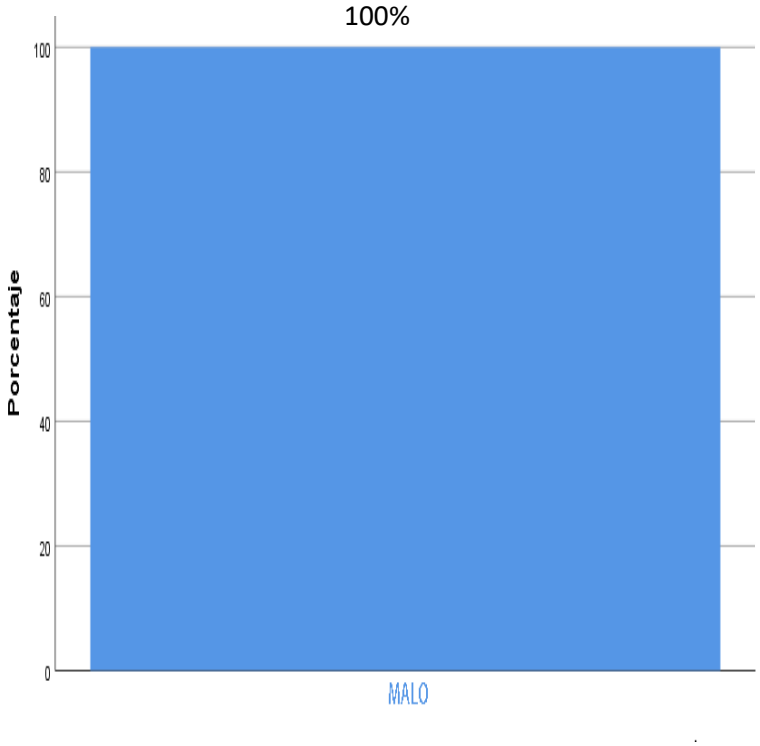
**Figura 30.** Calificación de las definiciones de amenazas

Nota: El 54,4% dice que es regular y el 45,6% dice que es bueno así lo califica los reportes de definiciones de amenazas de virus.

PE: 6. ¿CÓMO CALIFICA LA MOTIVACION DE LOS ATAQUES, SI SU INFORMACION PERSONAL SE VIERA AFECTADA?

**Tabla 37** ***Motivación de ataques***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 79 | 100,0 | 100,0 | 100,0 |




Fuente. Elaboración Propia

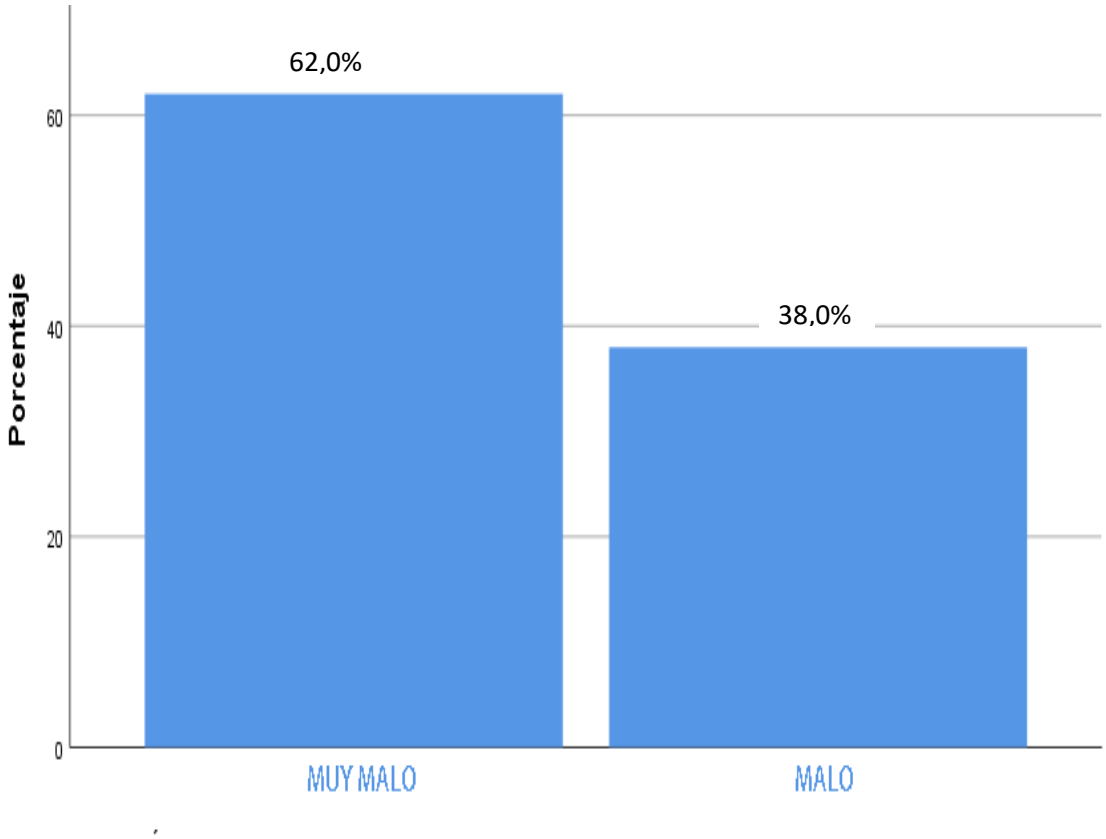
**Figura 31** Califiacion de la Motivación de ataques

Nota: El 100% dice que es malo así lo califica a la motivación de los ataques a la información personal.

PE: 7. ¿CÓMO CALIFICA QUE LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL?

**Tabla 38** ***Capacidad de las amenazas***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Malo | 49 | 62,0 | 62,0 | 62,0 |
| | Malo | 30 | 38,0 | 38,0 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

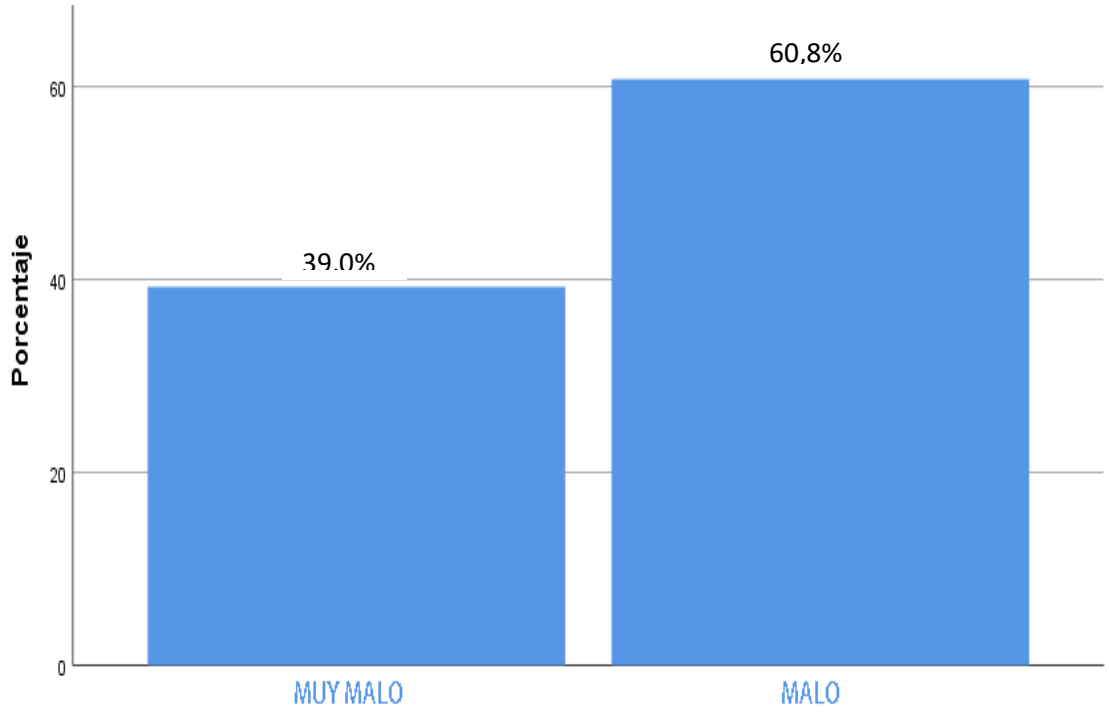
**Figura 32.** Calificación de la Capacidad de las amenazas

Nota: El 62,0% dice que es muy malo y el 38,0% dice que es malo así lo califica a la capacidad de las amenazas sea tratar de robar toda la información personal.

PE: 8. ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTE SU INFORMACIÓN PERSONAL?

**Tabla 39** ***Impactos de los ataques***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Malo | 31 | 39,2 | 39,2 | 39,2 |
| | Malo | 48 | 60,8 | 60,8 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

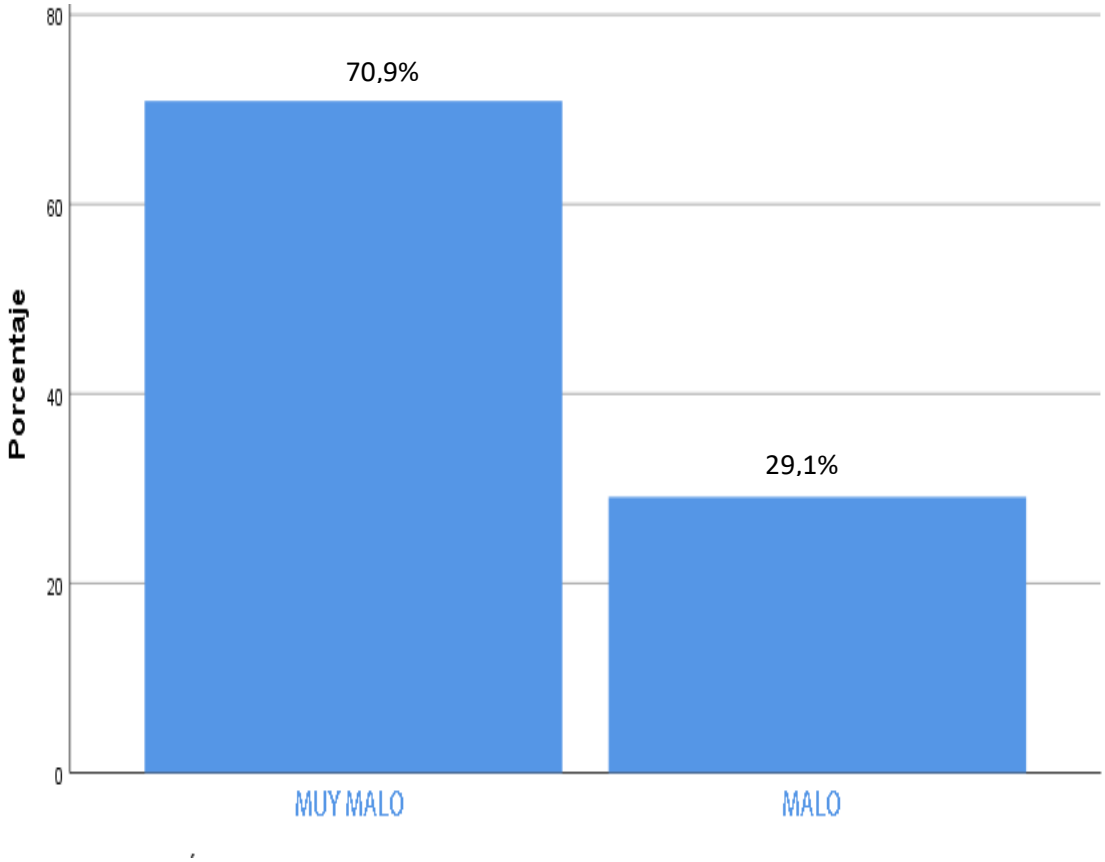
**Figura 33**. Calificación del Impacto de los ataques

Nota: El 39,0% dice que es muy malo y el 60,8% dice que es malo así lo califica al impacto de los ataques a la información personal.

PE: 9. ¿CÓMO CALIFICA LA SENSIBILIDAD DE TUS DATOS, VULNERABLE POR LOS HACKERS?

**Tabla 40** ***Sensibilidad de tus datos***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Malo | 56 | 70,9 | 70,9 | 70,9 |
| | Malo | 23 | 29,1 | 29,1 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

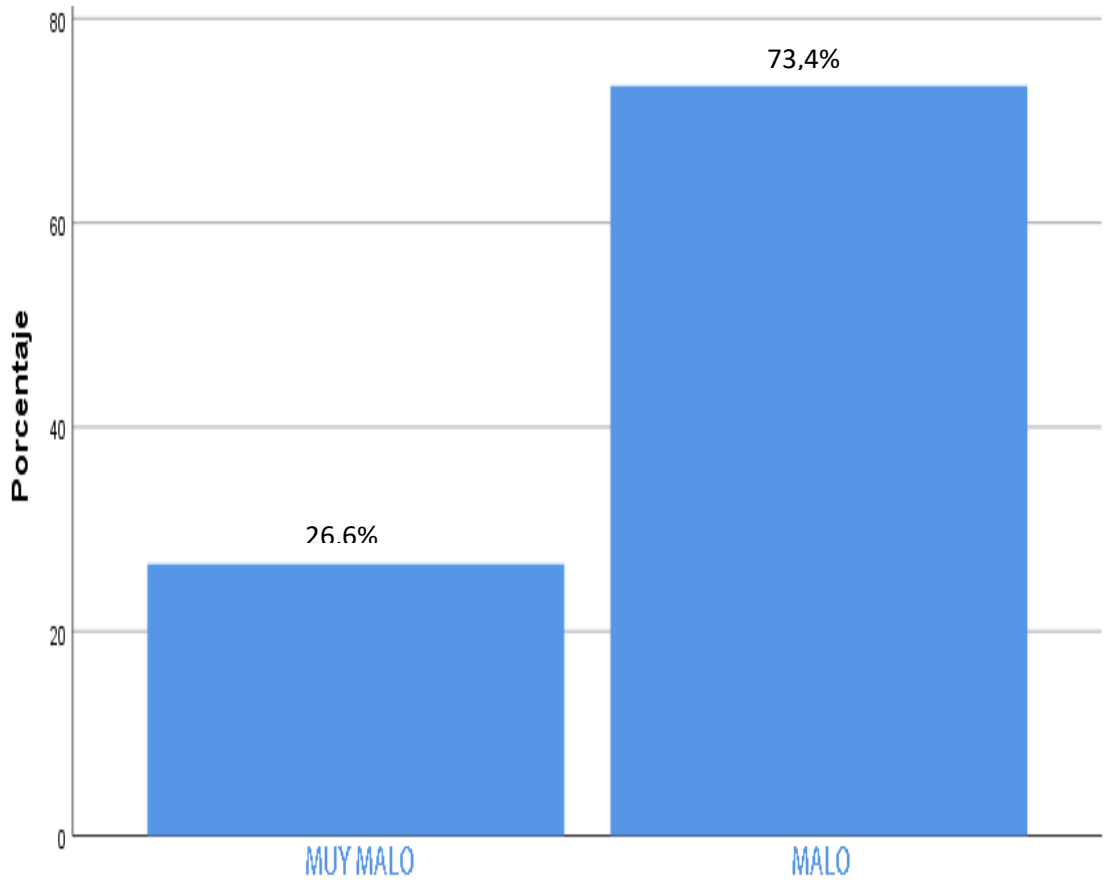
**Figura 34.** Calificación de la Sensibilidad de los datos

Nota: El 70,9% dice que es muy malo y el 29,1% dice que es malo así lo califica a la sensibilidad de los datos vulnerada por los hackers.

PE: 10. ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI?

**Tabla 41** ***Probabilidad de explotación de las amenazas***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Malo | 21 | 26,6 | 26,6 | 26,6 |
| | Malo | 58 | 73,4 | 73,4 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

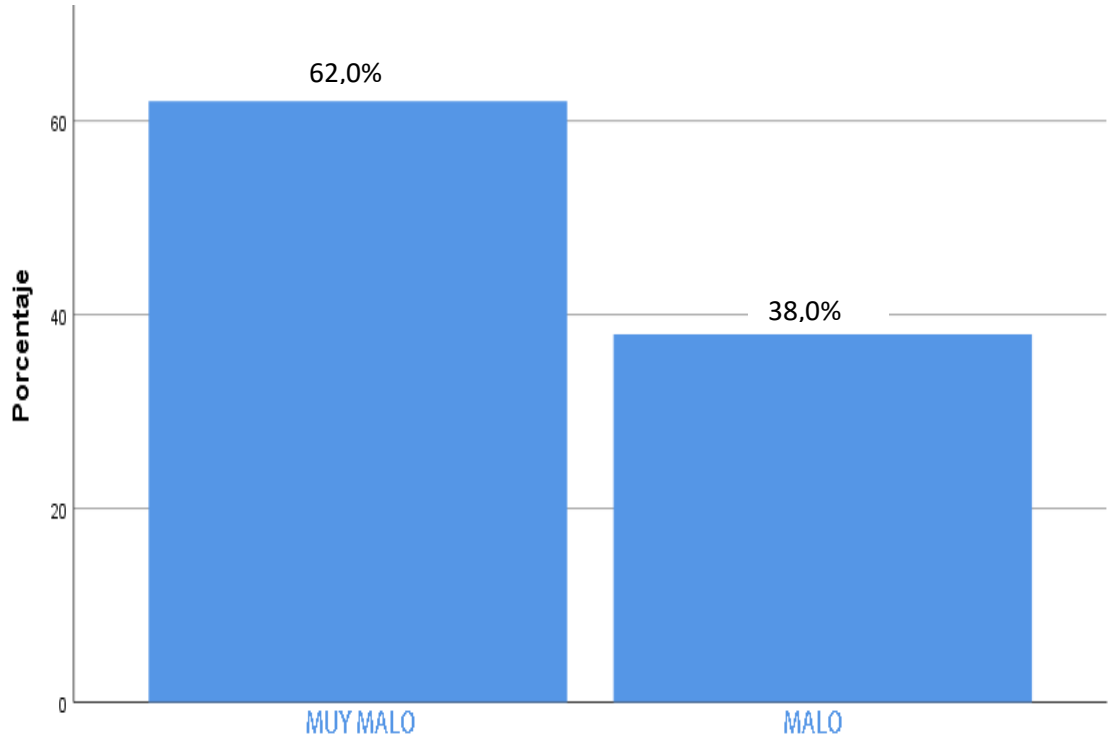
**Figura 35.** Calificación de la Probabilidad de explotación de las amenazas

Nota: El 26,6% dice que es muy malo y el 73,4% dice que es malo así lo califica a la probabilidad de explotación de las amenazas sea por medio de la red WI-FI.

PE: 11¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACION PERSONAL?

**Tabla 42** ***Magnitud de impactos***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Muy Malo | 49 | 62,0 | 62,0 | 62,0 |
| | Malo | 30 | 38,0 | 38,0 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

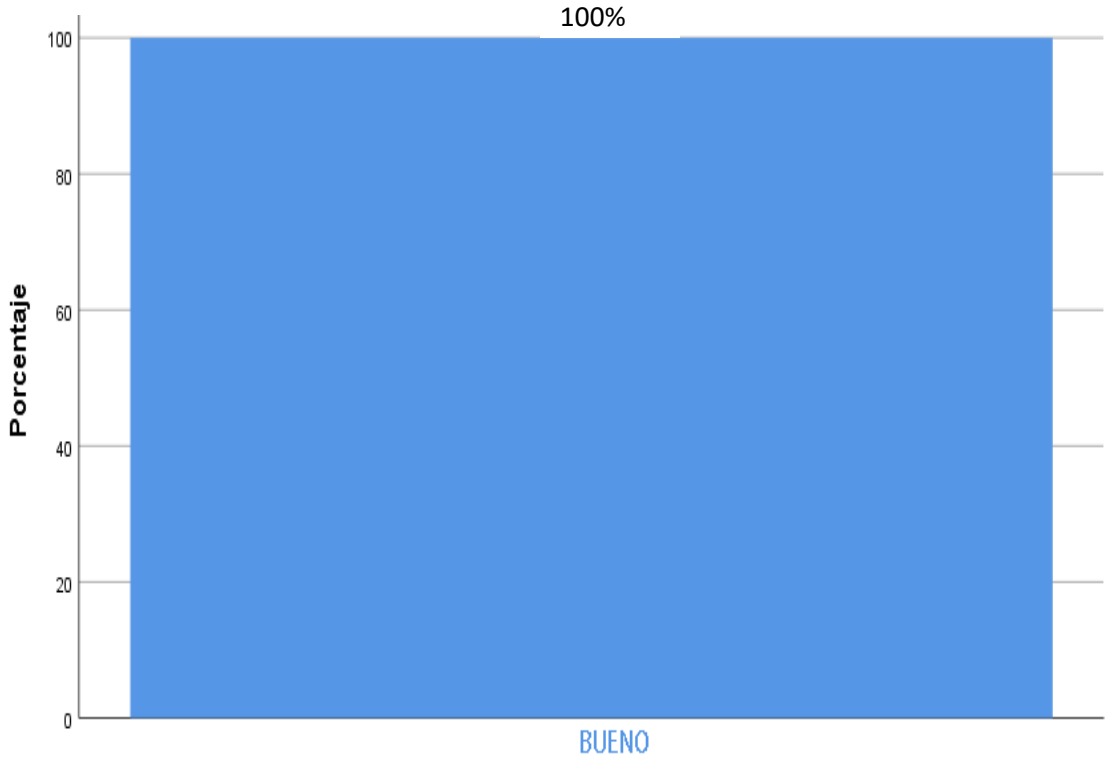
**Figura 36** Calificación de la Magnitud de impactos

Nota: El 62,0% dice que es muy malo y el 38,0% dice que es malo así lo califica a la magnitud de impacto de robo de información de datos.

PE: 12. ¿CÓMO CALIFICA SU RED INALAMBRICA?

**Tabla 43** ***Red inalámbrica***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Bueno | 79 | 100,0 | 100,0 | 100,0 |




Fuente. Elaboración Propia

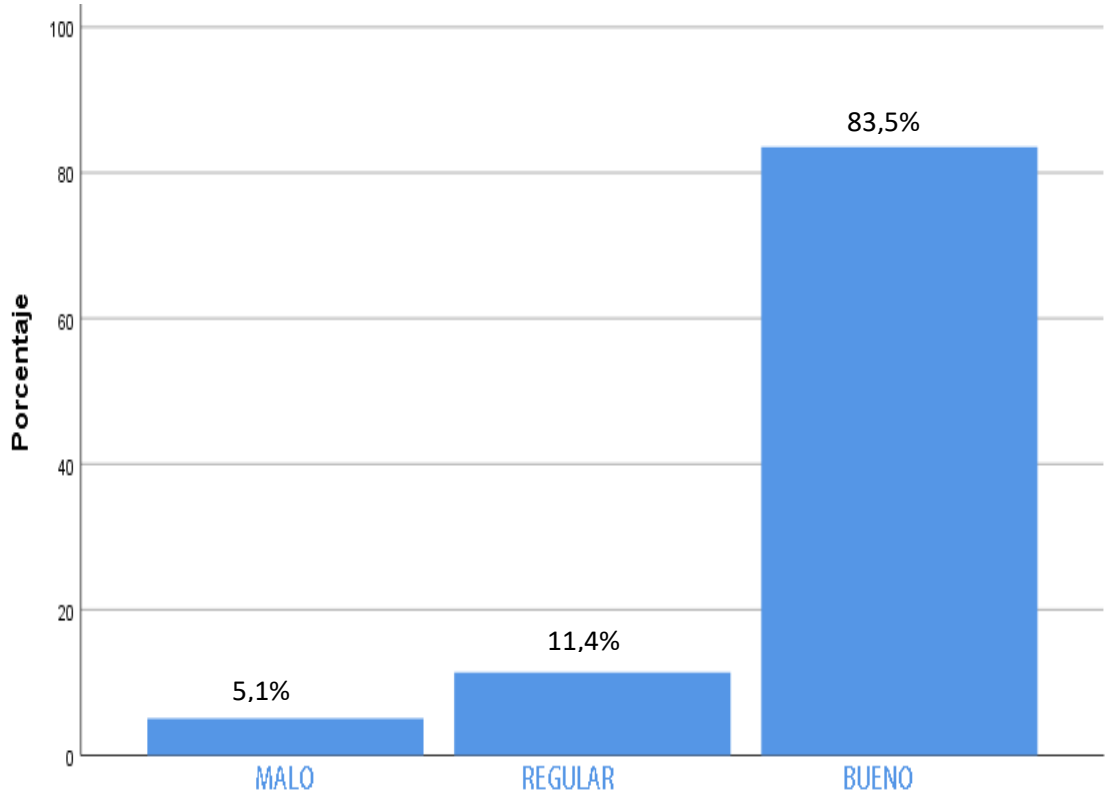
**Figura 37.** Calificación de la Red inalámbrica

Nota: El 100% dice que es bueno así lo califica a la red Inalámbrica

PE: 13. ¿A SU ANTIVIRUS COMO CALIFICA?

**Tabla 44** ***Antivirus***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Malo | 4 | 5,1 | 5,1 | 5,1 |
| | Regular | 9 | 11,4 | 11,4 | 16,5 |
| | Bueno | 66 | 83,5 | 83,5 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

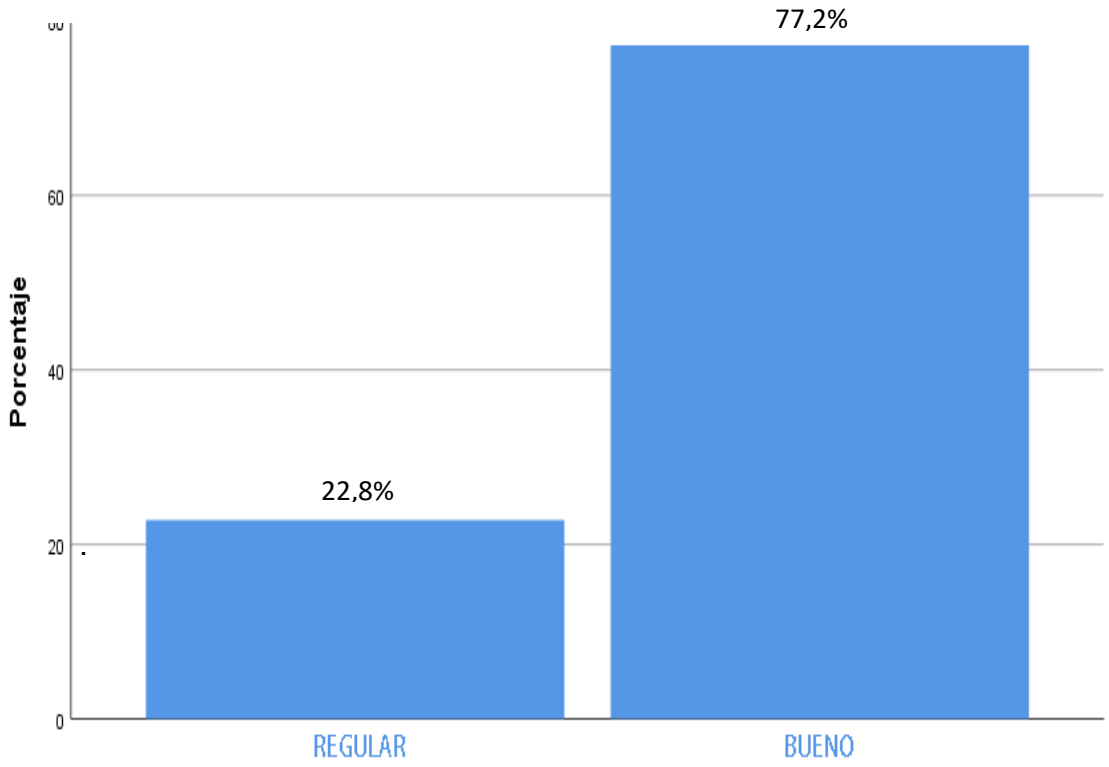
**Figura 38**. Calificación del Antivirus

Nota: El 5,1% dice que es malo, el 11,4% dice que es regular y 83,5% dice que es bueno así lo califica a su antivirus.

PE: 14. ¿CÓMO LO CONSIDERA SU FIREWALL ANTE UNA ANTAQUE DE VIRUS?

**Tabla 45** ***Firewall***

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Regular | 18 | 22,8 | 22,8 | 22,8 |
| | Bueno | 61 | 77,2 | 77,2 | 100,0 |
| | Total | 79 | 100,0 | 100,0 | |




Fuente. Elaboración Propia

**Figura 39** Calificación del Firewall

Nota: El 22,8% dice que es regular y el 77,2% dice que es bueno así lo califica a su Firewall

**Tabla 46 *Post- test***

| POST-TEST | N | Media | Desv. Desviación | Varianza |
|---|---|---|---|---|
| 1- ¿CÓMO CALIFICA EL ROUTER Y EL EQUIPO DE ENLACE QUE ESTA INSTALADO PARA SU SERVICIO DE INTERNET? | 79 | 4,30 | ,515 | ,265 |
| 2- ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TECNICO? | 79 | 4,37 | ,485 | ,235 |
| 3- ¿CÓMO CALIFICA EL SERVICIO DE INTERNET? | 79 | 4,61 | ,491 | ,241 |
| 4- ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO CALIFICA? | 79 | 3,81 | ,395 | ,156 |
| 5.- ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO CALIFICA? | 79 | 3,46 | ,501 | ,251 |
| 6.- ¿CÓMO CALIFICA LA MOTIVACIÓN DE LOS ATAQUES, SI SU INFORMACIÓN PERSONAL SE VIERA AFECTADA? | 79 | 2,00 | ,000 | ,000 |
| 7.- ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL? | 79 | 1,38 | ,488 | ,239 |
| 8.- ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL? | 79 | 1,61 | ,491 | ,241 |
| 9.- ¿CÓMO CALIFICA LAS SENSIBILIDAD DE TUS DATOS, VULNERADAA POR LOS HACKERS? | 79 | 1,29 | ,457 | ,209 |
| 10.- ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI? | 79 | 1,73 | ,445 | ,198 |
| 11.- ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACIÓN PERSONAL? | 79 | 1,38 | ,488 | ,239 |
| 12.- ¿CÓMO CALIFICA SU RED INALÁMBRICA? | 79 | 4,00 | ,000 | ,000 |
| 13.- ¿A SU ANTIVIRUS COMO LO CALIFICA? | 79 | 3,78 | ,523 | ,274 |
| 14.- ¿CÓMO CALIFICA SU FIREWALL ANTE UNA ATAQUE DE VIRUS? | 79 | 3,77 | ,422 | ,178 |
| N válido (por lista) | 79 | | | |
| Promedio | 0.5462 | 0.1738 | 2.9635 | 0.4072 | 0.1947 |

## 4.3 PRUEBA DE HIPÓTESIS

### *4.3.1 Formulación de cuadro de valores de indicadores*

La contrastación de la hipótesis se realiza de acuerdo al diseño de nuestra investigación, el cual es conocido también como Pre-Test y Post –Test, que se representa mediante le siguiente simbología:

| M: $\mu_1$ → X → $\mu_2$ |
|---|

$\mu_1$: Análisis de los resultados antes de aplicar la gestión de riesgo con metodología NIST SP 800-30 a la seguridad en redes inalámbricas (Pre-prueba).

X: Aplicando la metodología NIST SP 800 -30 ().

$\mu_2$: Análisis de los resultados después de aplicar la gestión de riesgo con metodología NIST SP 800-30 a la seguridad en redes inalámbricas (Post - Prueba).

### *4.3.2 Supuestos de la prueba de hipótesis*

1) Para la prueba de hipótesis seleccionamos los datos muéstrales de nuestra población, que es 79 usuarios de la empresa Servintecomp.
2) µ1 Significa el nivel promedio de eficiencia la gestión de riesgo con metodología NIST SP 800-30 a la seguridad en redes inalámbricas antes de aplicar la metodología.
3) $\mu_2$: Significa el nivel promedio de eficiencia la gestión de riesgo con metodología NIST SP 800-30 a la seguridad en redes inalámbricas después de aplicar la metodología.
4) La hipótesis nula H0 se cumplirá siempre y cuando: $\mu 1 = \mu 2$, el cual nos indica que no existe diferencia significativa.
5) La hipótesis alterna Ha se cumplirá siempre y cuando: $\mu 1 <> \mu 2$, el cual nos indica que si existe diferencia significativa.

6) Se utilizó el 95% del nivel de confiabilidad y 5% del nivel de significancia.

### *4.3.3 Cálculo del valor crítico y la función prueba*

Después de analizar y caracterizar las diferencias entre los indicadores en Pre –Test (μ1) y Post-Test (μ2), se concluye que sí, hay un aporte al aplicar gestión de riesgo con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa SERVINTECOMP.

**Tabla 47** ***Calculo del valor crítico y la función de prueba***

| | N | PRE - TEST | POST-TEST | DIFERENCIA |
|---|---|---|---|---|
| 1- ¿CÓMO CALIFICA EL ROUTER Y EL EQUIPO DE ENLACE QUE ESTA INSTALADO PARA SU SERVICIO DE INTERNET? | 79 | 2,70 | 4,30 | 1.60 |
| 2- ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TECNICO? | 79 | 2,67 | 4,37 | 1.70 |
| 3- ¿CÓMO CALIFICA EL SERVICIO DE INTERNET? | 79 | 2,44 | 4,61 | 2.17 |
| 4- ¿LOS REPORTES DE ATAQUE DE VIRUS CÓMO CALIFICA? | 79 | 2,48 | 3,81 | 1.33 |
| 6. ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO CALIFICA? | 79 | 3,46 | 3,46 | 0 |
| 6.- ¿CÓMO CALIFICA LA MOTIVACIÓN DE LOS ATAQUES, SI SU INFORMACIÓN PERSONAL SE VIERA AFECTADA? | 79 | 2,62 | 2,00 | -0.62 |
| 7.- ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL? | 79 | 2,61 | 1,38 | -1.23 |
| 8.- ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL? | 79 | 2,54 | 1,61 | -0.93 |
| 9.- ¿CÓMO CALIFICA LAS SENSIBILIDAD DE TUS DATOS, VULNERADAA POR LOS HACKERS? | 79 | 1,95 | 1,29 | -0.66 |
| 10.- ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI? | 79 | 2,13 | 1,73 | -0.40 |
| 11.- ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACIÓN PERSONAL? | 79 | 1,82 | 1,38 | -0.44 |
| 12.- ¿CÓMO CALIFICA SU RED INALÁMBRICA? | 79 | 2,39 | 4,00 | 1.61 |
| 13.- ¿A SU ANTIVIRUS COMO LO CALIFICA? | 79 | 2,46 | 3,78 | 1.32 |
| 14.- ¿CÓMO CALIFICA SU FIREWALL ANTE UNA ATAQUE DE VIRUS? | 79 | 2,90 | 3,77 | 0.87 |
| Promedio | 0.1738 | 2.5121 | 2.9635 | 0.4514 |

Cálculo de diferencia promedio (D)

$$\overline{D} = \frac{\sum \overline{D}_i}{n}$$

$$\overline{D} = \frac{6.32}{14} = \mathbf{0.4514}$$

**Tabla 48** ***Calcular desviación estándar (s)***

| | N | PRE-TEST | POST-TEST | DIFERENCIA (a) | Constante (b) | (a-b)² |
|---|---|---|---|---|---|---|
| 1- ¿CÓMO CALIFICA EL ROUTER Y EL EQUIPO DE ENLACE QUE ESTA INSTALADO PARA SU SERVICIO DE INTERNET? | 79 | 2,70 | 4,30 | 1.60 | 0.4514 | 1.3192 |
| 2- ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TECNICO? | 79 | 2,67 | 4,37 | 1.70 | 0.4514 | 1.5590 |
| 3- ¿CÓMO CALIFICA EL SERVICIO DE INTERNET? | 79 | 2,44 | 4,61 | 2.17 | 0.4514 | 2.9535 |
| 4- ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO CALIFICA? | 79 | 2,48 | 3,81 | 1.33 | 0.4514 | 0.7719 |
| 5.- ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO CALIFICA? | 79 | 3,46 | 3,46 | 0 | 0.4514 | 0.2037 |
| 6.- ¿CÓMO CALIFICA LA MOTIVACIÓN DE LOS ATAQUES, SI SU INFORMACIÓN PERSONAL SE VIERA AFECTADA? | 79 | 2,62 | 2,00 | -0.62 | 0.4514 | 1.1479 |
| 7.- ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL? | 79 | 2,61 | 1,38 | -1.23 | 0.4514 | 2.8271 |
| 8.- ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL? | 79 | 2,54 | 1,61 | -0.93 | 0.4514 | 1.9083 |
| 9.- ¿CÓMO CALIFICA LAS SENSIBILIDAD DE TUS DATOS, VULNERADAA POR LOS HACKERS? | 79 | 1,95 | 1,29 | -0.66 | 0.4514 | 1.2352 |
| 10.- ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI? | 79 | 2,13 | 1,73 | -0.40 | 0.4514 | 0.7249 |
| 11.- ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACIÓN PERSONAL? | 79 | 1,82 | 1,38 | -0.44 | 0.4514 | 0.7946 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 12.- ¿CÓMO CALIFICA SU RED INALÁMBRICA? | 79 | 2,39 | 4,00 | 1.61 | 0.4514 | 1.3424 |
| 13.- ¿A SU ANTIVIRUS COMO LO CALIFICA? | 79 | 2,46 | 3,78 | 1.32 | 0.4514 | 0.7545 |
| 14.- ¿CÓMO CALIFICA SU FIREWALL ANTE UNA ATAQUE DE VIRUS? | 79 | 2,90 | 3,77 | 0.87 | 0.4514 | 0.1752 |
| Promedio | 0.5462 | 2.5121 | 2.9635 | 0.4514 | 0.4514 | 17.7174 |

## Cálculo de desviación estándar

$$S = \sqrt{\frac{\sum(D_i - D)^2}{n-1}}$$

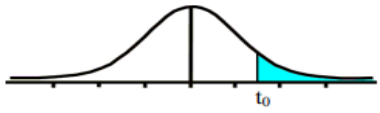
$$s = \sqrt{\frac{17.7174}{13}} = \sqrt{1.3628} = \mathbf{1.1674}$$

Hipótesis estadística

Ho: **μ1 = μ2**

Ha: **μ1<> μ2**

Tabla t-Student




| Grados de libertad | 0.25 | 0.1 | 0.05 | 0.025 | 0.01 | 0.005 |
|---|---|---|---|---|---|---|
| 1 | 1.0000 | 3.0777 | 6.3137 | 12.7062 | 31.8210 | 63.6559 |
| 2 | 0.8165 | 1.8856 | 2.9200 | 4.3027 | 6.9645 | 9.9250 |
| 3 | 0.7649 | 1.6377 | 2.3534 | 3.1824 | 4.5407 | 5.8408 |
| 4 | 0.7407 | 1.5332 | 2.1318 | 2.7765 | 3.7469 | 4.6041 |
| 5 | 0.7267 | 1.4759 | 2.0150 | 2.5706 | 3.3649 | 4.0321 |
| 6 | 0.7176 | 1.4398 | 1.9432 | 2.4469 | 3.1427 | 3.7074 |
| 7 | 0.7111 | 1.4149 | 1.8946 | 2.3646 | 2.9979 | 3.4995 |
| 8 | 0.7064 | 1.3968 | 1.8595 | 2.3060 | 2.8965 | 3.3554 |
| 9 | 0.7027 | 1.3830 | 1.8331 | 2.2622 | 2.8214 | 3.2498 |
| 10 | 0.6998 | 1.3722 | 1.8125 | 2.2281 | 2.7638 | 3.1693 |
| 11 | 0.6974 | 1.3634 | 1.7959 | 2.2010 | 2.7181 | 3.1058 |
| 12 | 0.6955 | 1.3562 | 1.7823 | 2.1788 | 2.6810 | 3.0545 |
| 13 | 0.6938 | 1.3502 | 1.7709 | 2.1604 | 2.6503 | 3.0123 |
| 14 | 0.6924 | 1.3450 | 1.7613 | 2.1448 | 2.6245 | 2.9768 |
| 15 | 0.6912 | 1.3406 | 1.7531 | 2.1315 | 2.6025 | 2.9467 |
| 16 | 0.6901 | 1.3368 | 1.7459 | 2.1199 | 2.5835 | 2.9208 |
| 17 | 0.6892 | 1.3334 | 1.7396 | 2.1098 | 2.5669 | 2.8982 |

Fuente: t-estuden de Google

**Figura 40** T-Student

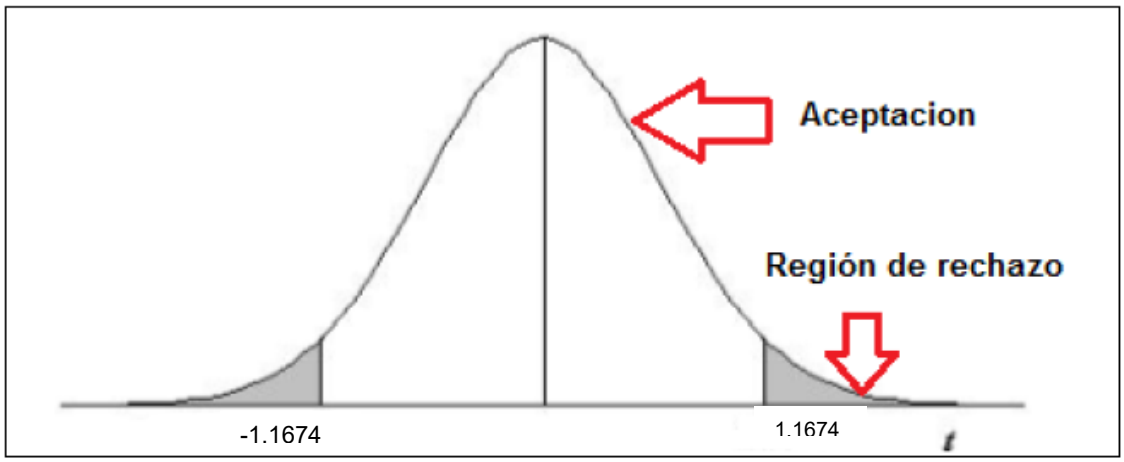
Cálculo del valor critico o valor en tabla de la T-Student (Tt)

Tt (1-α) (n-1)

Tt (1-0.1) (14-1)

Tt (0.99) (13) = 1.1674

Valor experimental




Fuente: Elaboración propia

**Figura 41** De aceptación y rechazo

$$V_e = \frac{\bar{D}}{\frac{S}{\sqrt{n}}}$$

$$V_e = \frac{0.4514}{\frac{1.1674}{\sqrt{14}}} = 1.4467$$

Como el **valor experimental Ve = 1.4467 es mayor que el valor Tt = 1.1674 se rechaza la Ho (hipótesis nula)** y se acepta Ha (hipótesis alterna), es decir, sí existe diferencia significativa con la GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICA EN LA EMPRESA SERVINTECOMP UCAYALI- 2018.

### *4.3.4 Ficha de evaluación pre-test a la estructura de la metodología NIST SP 800-30 (ficha de observación).*

**Tabla 49** *Ficha de observación pre-test*

**Aplicada a:**
**Fecha:**
**Responsable:**

| | N/A | Sí | No | Observación |
|---|---|---|---|---|
| **CARACTERIZACIÓN DEL SISTEMA** | | | | |
| Existe software de control de ataques de hackers | | | X | |
| Existe interface entre sistemas | | | X | |
| Existe alguna base de datos de los clientes | | | X | |
| Se tiene en cuenta la fronteras de los sistemas | | | X | |
| Existe funciones del sistema | | | X | |
| Se tiene en cuenta la criticidad de datos y sistemas | | | X | |
| Se tiene en cuenta la sensibilidad de datos y | | | X | |
| **IDENTIFICACIÓN DE AMENAZA** | | | | |
| Existe historial de ataques de hackers o virus | | | X | |
| Hay capacitaciones sobre amenazas o ataques de hackers | | | X | |
| **IDENTIFICACIÓN DE VULNERABILIDADES** | | | | |
| Existe informe de evaluación de riesgos anteriores | | | X | |
| Existe resultado de auditoria y prueba de | | | X | |
| Existe algún requerimiento de seguridad | | | X | |
| Existe una lista de vulnerabilidades potenciales | | | X | |
| Existe Resultado de prueba de seguridad | | | X | |
| **ANALISIS DE CONTROLES** | | | | |
| Existe controles actuales de seguridad | | | X | |
| Existe controles planificado de seguridad | | | X | |
| Existe lista de controles actuales y planificado | | | X | |
| **DETERMINACIÓN DE PROBABILIDADES** | | | | |
| Existe la lista de naturaleza de las vulnerabilidades | | | X | |
| Existe controles actuales de probabilidades | | | X | |
| Existe un rating de probabilidad de ataque a la seguridad inalámbrica. | | | X | |
| **ANÁLISIS DE IMPACTO** | | | | |
| Existe un análisis de impacto sobre la misión. | | | X | |
| Existe un rating de impacto de perdida y disponibilidad de conectividad | | | X | |
| **DETERMINACIÓN DE RIESGO** | | | | |
| Existe adecuación de los controles actuales y planificados. | | | X | |
| Existe riesgo y niveles de riesgo. | | | X | |
| **RECOMENDACIÓN DE CONTROLES** | | | | |
| Existe controles recomendado | | | X | |
| **DOCUMENTACIÓN DE RESULTADOS** | | | | |
| Existe informe de valoración y riesgo En el sistema de seguridad inalámbrica. | | | X | |

### *4.3.5 Ficha de evaluación post-test a la estructura de la metodología NIST SP 800-30 (ficha de observación).*

**Tabla 50** ***Ficha de evaluación post-test***

| **Aplicada a:**<br>**Fecha:**<br>**Responsable:** | | | | |
|---|---|---|---|---|
| | **N/A** | **Sí** | **No** | **Observación** |
| **CARACTERIZACIÓN DEL SISTEMA** | | | | |
| Existe software de control de ataques de hackers | | X | | |
| Existe interface entre sistemas | | X | | |
| Existe alguna base de datos de los clientes | | X | | |
| Se tiene en cuenta la fronteras de los sistemas | | X | | |
| Existe funciones del sistema | | X | | |
| Se tiene en cuenta la criticidad de datos y sistemas | | X | | |
| Se tiene en cuenta la sensibilidad de datos y sistemas. | | X | | |
| **IDENTIFICACIÓN DE AMENAZA** | | | | |
| Existe historial de ataques de hackers o virus | | X | | |
| Hay capacitaciones sobre amenazas o ataques de hackers | | x | | |
| **IDENTIFICACIÓN DE VULNERABILIDADES** | | | | |
| Existe informe de evaluación de riesgos anteriores | | x | | |
| Existe resultado de auditoria y prueba de seguridad. | | x | | |
| Existe algún requerimiento de seguridad | | X | | |
| Existe una lista de vulnerabilidades potenciales | | X | | |
| Existe Resultado de prueba de seguridad | | | | |
| **ANALISIS DE CONTROLES** | | | | |
| Existe controles actuales de seguridad | | X | | |
| Existe controles planificado de seguridad | | X | | |
| Existe lista de controles actuales y planificado | | x | | |
| **DETERMINACIÓN DE PROBABILIDADES** | | | | |
| Existe la lista de naturaleza de las vulnerabilidades | | x | | |
| Existe controles actuales de probabilidades | | x | | |
| Existe un rating de probabilidad de ataque a la seguridad inalámbrica. | | X | | |
| **ANÁLISIS DE IMPACTO** | | | | |
| Existe un análisis de impacto sobre la misión. | | X | | |
| Existe un rating de impacto de perdida y disponibilidad de conectividad | | X | | |
| **DETERMINACIÓN DE RIESGO** | | | | |
| Existe adecuación de los controles actuales y planificados. | | X | | |
| Existe riesgo y niveles de riesgo. | | x | | |
| **RECOMENDACIÓN DE CONTROLES** | | | | |
| Existe controles recomendado | | X | | |
| **DOCUMENTACIÓN DE RESULTADOS** | | | | |
| Existe informe de valoración y riesgo<br>En el sistema de seguridad inalámbrica. | | x | | |

# CAPITULO V: DISCUSIÓN.

De acuerdo a los señores ( VERBEL SALGADO & ALVAREZ CANO, 2016) que concluyen en su investigación que los avances tecnológicos en las redes WIFI se han convertido más inseguras y vulnerables debido al medio de transmisión de señal que manejan, haciendo que los ataques a estas sean cada vez más comunes, sin embargo según la investigación que se realizó se encontró que “la gestión de riesgo con metodología NIST SP 800-30 aportó en gran manera a la seguridad en red inalámbrica en la empresa SERVINTECOMP UCAYALI: 2018 como también otros autores avalan lo que investigó tales como (Diaz Paul, 2015) quién concluyen en su investigación que la metodología NIST SP 800-82 y NIST 800-30 sobre el aporte a la mejora de la gestión de seguridad informática, de la cual abarca la redes inalámbricas.

Otro autor ( Molina Miranda, 2015) concluye que cuyos resultados del análisis reflejaron que las medidas de seguridad han ayudado a reducir los riesgos de amenazas físicas de manera oportuna y que solo requieren de implementar procesos para una mejor gestión de seguridad de la información en la redes inalámbricas. Y revisando a otros autores dan con el mismo proceso de la cual concluimos que hacer una gestión de riesgos con alguna metodología en este caso la metodología NIST800-sp30 SP 800-30 al sistema de la seguridad de la información, viaja de manera inalámbrica, da la seguridad de minimizar los ataques, las perdidas, disponibilidad de la información, por tal motivo es una excelente metodología.

# CAPITULO VI
# CONCLUSIONES Y RECOMENDACIONES

## 6.1 CONCLUSIONES

La tesis de grado desarrollado obtuvo las siguientes conclusiones globales:

1. La gestión de riesgos con la metodología NIST SP 800-30 influyó significativamente con un 0.4514 por ciento a la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI –Pucallpa: 2018 con los con los cambios de equipos en los troncales principales, cables, mantenimiento de torre, inventario de los equipos de enlaces.
2. La caracterización de la gestión de riesgos de la metodología NIST SP 800-30 influyó significativamente a la seguridad de la información de los clientes, con el cambio de equipos más actuales en un 1.60 por ciento, en estabilizar la red de Internet, además los profesionales que instalan los equipos en un 1.70 por ciento,

Por último califican de buena señal de Internet con un 2.17 por ciento.

3. La identificación de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbrica influyó significativamente en 1.33 por ciento los usuarios entendieran, qué es un virus, su magnitud de ataque a todas las empresas a nivel mundial, también con los tipos de virus que hay en el mundo, al cual afecta su información.
4. El análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 influyó significativamente a la seguridad en redes inalámbrica, mediante controles de asignación de responsabilidad con un organigrama, con planes de mantenimiento de torres, cambio de equipos y cambio de contraseñas a la red inalámbrica cada dos meses.
5. Con la descripción de determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800-30 influyó significativamente a la seguridad en red inalámbrica, con saber que la motivación de los ataques son precisamente tener internet gratis, robar información, hacer lento el Internet, con la capacidad de tener información de manera instructiva en el internet, teniendo en cuenta estas situaciones se tomó la acción de prevenir dichas motivaciones de ataques y capacidad de amenazas.
6. El análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con la metodología NIST SP 800-30 influyó significativamente a la seguridad en redes inalámbricas pues con la calificación de los usuarios sobre el impacto de los ataques y la sensibilidad de los datos da como rechazo cualquier pérdida de sus datos por tal motivo se hizo configuración de equipos como reserva ante cualquier pérdida de enlace.
7. La descripción de la determinación de riesgo de la gestión de riesgo con la metodología NIST SP 800-30 influyó significativamente a la seguridad en redes inalámbricas con los cambios realizados en cuanto a los antivirus, hacer una

contraseña más segura de la red inalámbrica, tener encriptados los datos de la empresa, hacer copias de seguridad de los datos más importantes de la empresa o usuarios finales.

8. Al analizar la recomendación de la gestión de riesgo con la metodología NIST SP 800-30 influyó significativamente a la seguridad en redes inalámbrica con los planes de trabajo tales como por ejemplo implementar UPS, instruir a los usuarios sobre antivirus originales, firewall actualizados, hacer una política de uso de la red inalámbrica.
9. Describir la documentación de resultado de la gestión de riesgo con la metodología NIST SP 800-30 influyó significativamente a la seguridad en las redes inalámbricas con los controles sugeridos tales como elaborar filtro de firewall, emitir comunicaciones de averías con los usuarios, como también capacitación a los trabajadores sobre seguridad en la red inalámbrica.

## 6.2 RECOMENDACIONES

1. Se recomienda que lo desarrollado hasta ahora no se quede ahí sino que se siga perfeccionando y manteniendo las buenas practicas.
2. Se recomienda que la empresa siga instruyendo a sus trabajadores y usuarios finales en cuanto al impacto de los ataque de virus.
3. La empresa tiene que hacer una constante auditoria de todo sus activos para no descuidar su buen servicio que hasta ahora lo tiene.
4. Es recomendable hacer un plan de contingencia de al sistema de energía.
5. Es recomendable hacer un plan de contingencia de los equipos de red inalámbrica.
6. Es recomendable hacer que los usuarios finales compren antivirus actuales originales y sus firewall sean actualizados para un mejor sistema de seguridad de la información.

# REFERENCIAS BIBLIOGRÁFICAS


Barrenechea Zavala, T. I. (2015). *"Diseño de una red lan inalambrica para una empresa de lima".* Lima: Pontificia Universidad la Católica del Perú.

Erreyes Pinzón, D. M. (2017). *METODOLOGÍA PARA LA SELECCIÓN DEHERRAMIENTAS EFICIENTES Y PROTOCOLOS ADECUADOS PARA MEJORAR LA SEGURIDAD DE LOS DISPOSITIVOS MÓVILES.* UNIVERSIDAD DE CUENCA, CUENCA - ECUADOR.

Meneses, J., & Rodríguez, D. (2008). *El cuestionario y la entrevista.* Catalunya: Universitat Oberta de Catalunya.

Molina Miranda, M. F. (2015). *"Propuesta de un plan de gestión de riesgos de tecnología aplicado en la escuela superior politécnica del litoral".* Madrid: Universidad Politécnica de Madrid.

VERBEL SALGADO, D. E., & ALVAREZ CANO, H. (2016). *ESTUDIO DE ESQUEMAS DE SEGURIDAD EN REDES INALAMBRICAS: APLICACIÓN DE BUENAS PRACTICAS EN PYMES Y USUARIOS FINALES.* MEDELLIN-COLOMBIA: UNIVERSIDAD DE SAN BUENAVENTURA SECCIONAL MEDELLÍN.

Avalos serrano, V. N. (2007). *Desarrollo de una aplicación para la gestión de riesgo en los sistemas de información utilizando la guía metodológica NIST SP 800-30 caso práctico:"Liceo del Valle".* Sangolqui-Ecuador: Escuela politécnica del ejército.

Avalos Serrano, V. N. (2007). *Desarrollo de una aplicación para la gestión de riesgos en los sistemas de información utilizando la guía metodológica nist sp 800-30.* Ecuador-Sangolquí: Escuela Politécnica del Ejército.

Bernal Torres, C. A. (2010). *Metodología de la investigación.* Colombia: PEARSON.

Blas Rinza, J. F. (2017). *"Seguridad y control del acceso a las redes inalámbricas en la unsm-t mediante servidores de autentificación radius con el uso de certificados v.* Tarapoto: Universidad Nacional de San Martín - Tarapoto.

Cueva beltran , I. Y. (2015). *"Diseño de un plan para el tratamiento de riesgos tecnológicos utilizando la metodología nist sp 800-30".* Ecuador: Universidad Tecnica de Machala.

De la garza Toledo, E. (01 de 05 de 2016). *http://sgpwe.izt.uam.mx/pages/egt/Cursos/MetIV/EsquemasProyectosInvest.pdf*. (SliderPlayer) Obtenido de https://slideplayer.es/slide/5456066/: https://slideplayer.es/slide/5456066/

Diaz Paul, B. F. (2015). *Diseño de estrategias de mitigación para mejorar la seguridad de información del sistema de control industrial en la empresa comercializadora san remigio.* Quito-Ecuador: Universidad Nacional de las Fuerzas Armandas.

ecured. (12 de 01 de 2018). *ecured*. Obtenido de ecured: https://www.ecured.cu/Seguridad_en_redes_inal%C3%A1mbricas

El comercio. (03 de 12 de 2019). *El comercio*. (Empresa Editorial el Comercio) Recuperado el 12 de 01 de 2020, de https://elcomercio.pe/economia/negocios/bcp-reconoce-que-sufrio-ataque-informatico-en-el-2018-banco-de-credito-del-peru-nndc-noticia/

FORTINET. (22 de 03 de 2019). *Seguridad y administración WI-FI en un panel único*. Obtenido de Seguridad y administración WI-FI en un panel único: https://www.fortinet.com/lat/products/secure-wifi/fortigate-integrated.html

FORZA. (26 de 01 de 2020). *https://www.forzaups.com/tools/product-selector/*. Obtenido de https://www.forzaups.com/tools/product-selector/: https://www.forzaups.com/

Fruhlinger, J. (04 de 07 de 2018). *https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red*. (NETWORK) Recuperado el 28 de 11 de 2019, de https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red: https://www.networkworld.es/seguridad/que-es-la-seguridad-de-la-red

Gonzales Rondan, N. O. (2015). *"Diseño e implementación de un proveedor de servicio de internet inalámbrico utilizando la tecnología routerboard mikrotik, en la ciudad de recuay en el año 2015".* Huaraz: Universidad Nacional Angeles De Chimbote.

ICMAS Ltd. , & Public Utility Reaserch Center . (2014). *"Terminos tecnicos de telecomunicaciones".* Madrid: Madrid-Aris.

incibe.es. (23 de 11 de 2018). *https://www.incibe.es/*. (gobierno de España) Recuperado el 28 de 11 de 2019, de https://www.incibe.es/: https://www.incibe.es/

intel. (25 de 03 de 2019). *Entendiendo la autenticación IEEE * 802,11 y la Asociación*. Obtenido de Entendiendo la autenticación IEEE * 802,11 y la Asociación: https://www.intel.la/content/www/xl/es/support/articles/000006508/network-and-i-o/wireless-networking.html

Mexico, E. B. (24 de 02 de 2015). *13 pasos para optimizar la seguridad de una Red Inalambrica*. Obtenido de 13 pasos para optimizar la seguridad de una Red Inalambrica: https://blogmexico.comstor.com/13-pasos-para-optimizar-la-seguridad-de-una-red-inalambrica

Mikrotik. (21 de 01 de 2020). *MikroTik Routers and Wireless*. Obtenido de https://wiki.mikrotik.com/wiki/Main_Page: https://mikrotik.com/

Oracle. (2014). *Glosario de términos de redes.* Estados Unidos: Orocle.

Quiroz Papa de Garcia, R. (2009). *Tesis digital UNMSM.* LIMA: UNMSM.

Rodrigo, A. (2014). *"Glosario de terminos informaticos de redes de computadoras".* Lima: Universidad de Lima.

sagemcom. (22 de 01 de 2020). *sagemcom*. Obtenido de https://support.sagemcom.com/en/gateways: https://www.sagemcom.com/en

salva. (20 de 03 de 2012). *Departamento de Lenguajes y Sistemas Informáticos*. Recuperado el 12 de 1 de 2020, de I*38 . Seguridad y Protección de la Información:

http://spi1.nisu.org/recop/al01/salva/definic.html

Satra. (27 de 01 de 2020). *https://www.satranet.com/*. Obtenido de https://www.satranet.com/equipos-para-redes/: https://www.satranet.com/

SMART WIFI. (25 de 01 de 2020). *https://descubre.movistar.co/smart-wifi/*. Obtenido de https://descubre.movistar.co/smart-wifi/: https://descubre.movistar.co/smart-wifi/

Symantec, B. (01 de 04 de 2019). *Broadcom*. (Broadcom) Recuperado el 10 de 01 de 2020, de Symantec: https://www.symantec.com/es/mx/security-center/threat-report

tp-link. (25 de 01 de 2020). *tp-link*. Obtenido de https://www.tp-link.com/es/home-networking/3g-4g-router/tl-mr6400/: https://www.tp-link.com/es

ubiquiti. (18 de 05 de 2020). *ubiquiti*. Obtenido de www.ui.com/download/: https://www.ui.com/download/

Vallejo de leon, T. V. (2010). *Vulnerabilidades y niveles de seguridad de redes WI-FI.* Guatemala: Universidad de San Carlos de Guatemala.

VIU. (4 de 07 de 2019). *Universidad Internacional de VAlencia*. Obtenido de VIU Universidad: https://www.universidadviu.com/

WIKIPEDIA. (30 de 11 de 2019). *WIKIPEDIA*. (Fundación wip) Recuperado el 5 de 12 de 2019, de Gestión de riesgos: https://es.wikipedia.org/wiki/Gesti%C3%B3n_de_riesgos

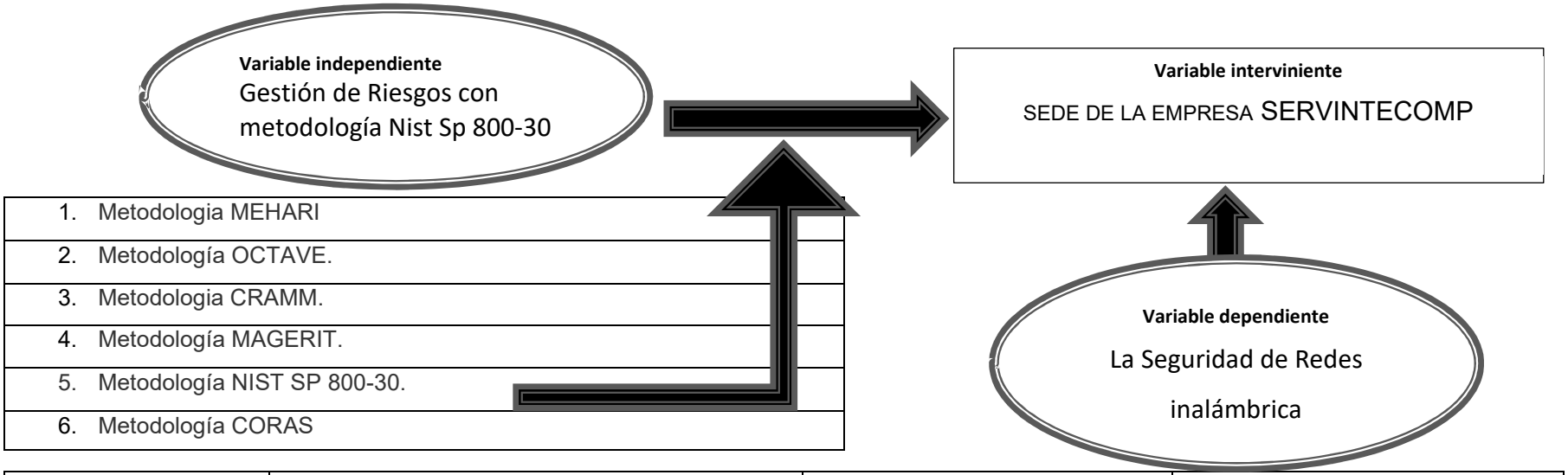
# ANEXOS

# ANEXO Nº 01 MATRIZ DE IDENTIFICACIÓN DEL PROBLEMA

**Tabla51** ***Formulación Del Problema***

| N° | SINTOMAS | CAUSAS | CONSECUENCIAS | PRONOSTICO |
|---|---|---|---|---|
| 01 | Saturación del internet en los usuarios y empresas. | Sustracción de la línea de internet en el usuario final por su WIFI. | Perdidas de conexión de internet | Garantizar la red inalámbrica en los clientes, como también mantener el servicio excelente. |
| 02 | Flujo alto en consumo de internet. | Deficiencias en protocolos de Cifrado de seguridad | Problemas con los clientes | Seguridad en la red inalámbrica de la empresa SERVINTECOMP |
| 03 | Incumplimiento de pago a los bancos, Sunat, proveedores y personal. | Clientes insatisfechos por el servicio de la red inalámbrica. | Multas, penalidades, y aumento de interés de los bancos | Medidas de contingencias para garantizar la línea de internet al usuario. |
| 04 | Fuga de usuarios | La lentitud de la línea | La empresa pierde capital | Medida de seguridad para un mejor enlace de la red inalámbrica en sus trocales principales. |
| “Ineficiente sistema de seguridad en la red inalámbrica en la empresa SERVINTECOMP” | | | | |

## ANEXO Nº 02 HOJA DE RUTA DE LAS VARIABLES




| | Gestión De Riesgos con Metodología Nist Sp 800-30 | La Seguridad de Redes Inalámbricas | Sede de la empresa SERVINTECOMP |
|---|---|---|---|
| TITULO | "GESTIÓN DE RIESGOS CON METODOLOGÍA NIST SP 800-30 A LA SEGURIDAD EN REDES INALÁMBRICA EN LA EMPRESA SERVINTECOMP UCAYALI- 2018." | | |
| FORMULACION DEL PROBLEMA | ¿En qué medida influye la gestión de riesgos de NIST SP 800-30 a la seguridad de la red inalámbrica en la empresa SERVINTECOMP PUCALLPA: 2018? | | |
| OBJETIVO | Analizar y caracterizar la gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI-PUCALLPA: 2018. | | |
| HIPOTESIS | La gestión de riesgos con metodología NIST SP 800-30 influye significativamente en la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI-PUCALLPA-2018. | | |

Fuente. Elaboración Propia

**Figura 41**. Hoja de ruta de las variables

## ANEXO Nº 03 TABLA DE OPERACIONALIZACIÓN DE VARIABLES (DEFINICIÓN CONCEPTUAL Y OPERACIONAL)

**Tabla 52 Tabla de operaciones de variables**

| VARIABLES | DEFINICION CONCEPTUAL | DEFINICIONA OPERACIONAL | DIMENSIONES | INDICADORES | INSTRUMENTOS |
|---|---|---|---|---|---|
| Gestión De Riesgos con Metodología Nist Sp 800-30 | Según ( Erreyes Pinzón, 2017) lo define que la NIST SP 800-30, se encarga de la gestión de riesgos, orientada a procesos mediante un adecuado análisis y gestión del riesgos, proporcionando una evaluación cuantitativa y cualitativa, así como métodos semi cualitativos que permiten administrar eficazmente el riesgo para la seguridad de la información (Pág 50-51)..<br>Según NIST (2012), señala que la NIST SP 800-30 está orientada especialmente a los profesionales vinculados con la gestión de riesgos en las organizaciones como: jefes de los organismos, directores generales, jefe de operaciones, ejecutivo de riesgo; los individuos encargados de la vigilancia de la seguridad de la información, su gestión y responsabilidades operativas (por ejemplo, los directores de información, oficiales de alto rango, los administradores y propietarios de sistemas de información, los | Está comprendida por las dimensiones que constituyen Gestión De Riesgos con Metodología Nist Sp 800-30:<br>(1) Caracterización del sistema.<br>(2) Identificación de amenaza.<br>(3) Identificación de vulnerabilidades.<br>(4) Control de análisis.<br>(5) Determinación del riesgo.<br>(6) Análisis de impacto.<br>(7) Determinación del riesgo.<br>(8) Recomendaciones de control.<br>(9) Resultado de la implementación o documentación. | Caracterización del sistema | Entrada<br>-Hardware (%).<br>-Software (%).<br>-Interface entre sistemas (%).<br>-Datos e información (%).<br>-Personal (%).<br>-Misión de los sistemas (%).<br>Salida<br>-Fronteras de los sistemas (%).<br>-Funciones de los sistemas (%).<br>-criticidad de datos y sistemas (%).<br>-Sensibilidad de datos y sistemas (%). | Cuestionario<br>Guía de Observación<br>Análisis Documental |
| | | | Identificación de amenaza | Entrada<br>-Históricos de ataques (%).<br>-Datos de agencia de inteligencia. (%).<br>-Datos de medios de comunicación (%).<br>Salida<br>-Definición de amenazas (%). | |
| | | | Identificación de vulnerabilidades | Entrada<br>-Informe de evaluación de riesgos anteriores. (%). | |

| | | | | | |
|---|---|---|---|---|---|
| | proveedores de control comunes etc) | | | -Resultado de auditorías. (%).<br>-Requerimiento de Seguridad. (%).<br>-Resultado de prueba de seguridad.(%).<br>Salida<br>-Lista de vulnerabilidades potenciales (%). | |
| | | | Análisis de controles | **Entrada**<br>-Controles actuales. (%).<br>-controles planificado (%).<br>**Salida**<br>-Lista de controles actuales y planificados (%). | |
| | | | Determinación de probabilidades | **Entrada**<br>-Motivación para los ataques.<br>(%).<br>-Capacidad de las amenazas<br>(%).<br>-Naturaleza de las vulnerabilidades (%).<br>-Controles actuales (%).<br>**Salida**<br>-Rating de probabilidades (%). | |
| | | | Análisis impacto.<br>-Perdida de integridad<br>Perdida de disponibilidad | **Entrada**<br>-Análisis de impacto sobre la misión (%).<br>-Valorización de la criticidad de los activos (%).<br>-criticidad de datos sensibilidad (%).<br>**Salida**<br>-Rating de impacto (%). | |
| | | | Determinación de riesgo | **Entrada**<br>-Probabilidad de explotación de las amenazas (%).<br>-Magnitud de los impactos (%).<br><br>-Adecuación de los controles actuales y planificado (%).<br><br>**Salida**<br>-Riesgos y niveles de riesgos (%). | |
| | | | Recomendaciones de controles. | **Salida**<br>-controles recomendado (%). | |

| | | | | | |
|---|---|---|---|---|---|
| | | | Resultado de la implementación o documentación. | **Salida**<br>- valoración del riesgo (%). | |
| La Seguridad de Redes inalámbricas | La seguridad de la red es la práctica de prevenir y proteger contra la intrusión no autorizada en redes corporativas. Como filosofía, complementa la seguridad del punto final, que se centra en dispositivos individuales; la seguridad de la red se centra en cómo interactúan esos dispositivos y en el tejido conectivo entre ellos (Fruhlinger, 2018). | Para implementar este tipo de defensa en profundidad se hace lo siguiente<br>(1) Protección<br>(2) Detección<br>(3) Reacción. | -Protección.<br>-Detección.<br>-Reacción. | -Protección (%).<br>-Detección (%).<br>-Reacción (%). | |

## ANEXO 4: MATRIZ DE CONSISTENCIA SISTÉMICA

### Tabla 53 Matriz de consistencia sistémica

<table>
<tr>
<th>FORMULACION DEL PROBLEMA</th>
<th>OBJETIVOS</th>
<th>HIPOTESIS</th>
<th>VARIABLES,DIMENCIONES E INDICADORES</th>
<th>METODOLOGÍA DE LA INVESTIGACION</th>
</tr>
<tr>
<td>¿En qué medida influye la gestión de riesgos de NIST SP 800-30 a la seguridad de la red inalámbrica en la empresa SERVINTECOMP PUCALLPA: 2018?</td>
<td>Analizar y caracterizar la gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI-PUCALLPA: 2018.</td>
<td>La gestión de riesgos con metodología NIST SP 800-30 influye significativamente en la seguridad en redes inalámbricas en la empresa SERVINTECOMP UCAYALI-PUCALLPA-2018.</td>
<td rowspan="2">VARIABLE 1: Gestión De Riesgos con Metodología Nist Sp 800-30.<br><br>DIMENSIÓN: 1<br>Caracterización del sistema.<br>Entrada<br>-Hardware<br>-Software<br>-Interface entre sistemas<br>-Datos e información<br>-Personal<br>-Misión de los sistemas<br>Salida<br>-Fronteras del sistemas<br>-Funciones del sistemas<br>-criticidad de datos y sistemas<br>-Sensibilidad de datos y sistemas<br><br>DIMENSIÓN:2<br>Identificación de amenazas<br>Entrada<br>-Históricos de ataques<br>-Datos de agencia de inteligencia.<br>-Datos de medios de comunicación<br>Salida<br>-Definición de amenazas<br><br>DIMENSIÓN:3<br>Identificación de vulnerabilidades<br>Entrada<br>-Informe de evaluación de riesgos anteriores.<br>-Resultado de auditorías.<br>-Requerimiento de Seguridad.<br>-Resultado de prueba de seguridad.<br>Salida<br>-Lista de vulnerabilidades potenciales<br><br>DIMENSIÓN:4<br>Análisis de controles<br>Entrada<br>-Controles actuales.<br>-controles planificado<br>Salida<br>-Lista de controles actuales y planificados<br><br>DIMENSIÓN:5<br>Determinación de probabilidades<br>Entrada<br>-Motivación para los ataques.<br>-Capacidad de las amenazas<br>-Naturaleza de las vulnerabilidades<br>-Controles actuales.<br>Salida<br>-Rating de probabilidades.<br><br>DIMENSIÓN:6<br>Análisis de impacto<br>Entrada<br>-Análisis de impacto sobre la misión.<br>-Valorización de la criticidad de los activos<br>-criticidad de datos sensibilidad<br>Salida<br>-Rating de impacto DIMENSIÓN:<br>Nivel del riesgo<br>-Adecuación de los controles actuales y planificados.<br><br>DIMENSIÓN: 7<br>Recomendaciones de control.<br>Salida<br>-Recomendación<br><br>DIMENSION: 8<br>Recomendación de controles.<br>Salida<br>-controles recomendado.<br><br>DIMENSION: 9<br>Documentación de resultado.<br>Salida<br>-Informe de valoración y riesgo<br><br>VARIABLE 2: La Seguridad de Redes Inalámbricas.<br><br>DIMENSION:<br>-Protección.<br>-Detección.<br>-Reacción</td>
<td rowspan="2">TIPO DE INVESTIGACIÓN<br>APLICADA<br><br>NIVEL DE INVESTIGACIÓN.<br><br>Descriptiva<br><br>pretest y postest:<br>Los pasos para la aplicación de este diseño son:<br>Aplicación de un pretest (01) para la medida de la variable dependiente.<br>Aplicación del tratamiento de la variable independiente(x)<br>Aplicación de nuevo de un postest para la medida de la variable dependiente (02).<br><br>DISEÑO DE LA INVESTIGACIÓN<br>Pretest y Postest<br><br>O1 → x → 02<br><br>Medición v´ Exp. Medición<br><br>Donde:<br><br>01: es la primera medición de la dependiente.<br>X: es el tratamiento de la variable independiente.<br>O2: es la segunda medición de la variable dependiente<br><br>SOFTWARE PARA PROCESAR DATOS<br>SPSS<br><br>
<table>
<tr><td>Fuentes</td><td>Técnicas</td><td>Herramientas</td></tr>
<tr><td>Primaria</td><td>Encuesta</td><td>Cuestionario</td></tr>
<tr><td>Secundario</td><td>Análisis documental</td><td>Resumen de autores</td></tr>
</table>
</td>
</tr>
<tr>
<td>a) ¿En qué medida la caracterización del sistema de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?<br><br>b) ¿En qué medida las identificaciones de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbrica?<br><br>c) ¿De qué manera el análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?<br><br>d) ¿Cómo la determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800 -30 aporta a la seguridad en redes inalámbricas?<br><br>e) ¿En qué medida el análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?<br><br>f) ¿Cómo la determinación de riesgo de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?<br><br>g) ¿En qué medida la recomendación de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?<br><br>h) ¿Cómo la documentación de resultado de la gestión de riesgos con la metodología NIST SP 800-30 aporta a la seguridad en redes inalámbricas?</td>
<td>a) Analizar la caracterización del sistema de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.<br>b) Analizar identificaciones de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbrica<br>c) Describir el análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas.<br>d) Describir la determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800 -30 a la seguridad en redes inalámbricas<br>e) Analizar el análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con metodología NIST SP 800-30 a la seguridad en redes inalámbricas<br>f) Describir la determinación de riesgo de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas<br>g) Analizar la recomendación de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas<br>h) Describir la documentación de resultado de la gestión de riesgos con la metodología NIST SP 800-30 a la seguridad en redes inalámbricas</td>
<td>a) Caracterización del sistema de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.<br>b) Las identificaciones de las amenazas y vulnerabilidades de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbrica.<br>c) El análisis de controles de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.<br>d) La determinación de probabilidades de la gestión de riesgos con la metodología NIST SP 800 -30 influye a la seguridad en redes inalámbricas.<br>e) El análisis de impacto como pérdida de integridad y pérdida de disponibilidad de la gestión de riesgos con metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.<br>f) La determinación de riesgo de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.<br>g) La recomendación de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas<br>h) La documentación de resultado de la gestión de riesgos con la metodología NIST SP 800-30 influye significativamente a la seguridad en redes inalámbricas.</td>
</tr>
</table>

## ANEXO Nº 5 INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Cuestionario de preguntas de recolección de datos.

CUESTIONARIO SOBRE LA INVESTIGACIÓN: Gestión De Riesgos con Metodología NIST SP 800-30 A La Seguridad En Redes Inalámbricas En La Empresa SERVINTECOMP Ucayali- Pucallpa: 2018.

N° de cuestionario: _____

Fecha: _____

**ESTIMADO SEÑOR:**

El presente cuestionario tiene como objetivo obtener información, la que tendrá como único fin, adoptar datos que contribuyan a la realización del trabajo de tesis final. Se agradece de antemano su colaboración, garantizándole que la información que usted. Brinde es anónima y en estricta reserva.

Por favor marque con una X, la opción elegida como respuesta.

| | |
|---|---|
| 1 | Muy malo |
| 2 | Malo |
| 3 | Regular |
| 4 | Bueno |
| 5 | Muy Bueno |

PREGUNTAS ESPECÍFICAS

| N° | PREGUNTAS | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| VARIABLE 1: Gestión De Riesgos con Metodología NIST SP 800-30 | | | | | | |
| CARACTERIZACION DEL SISTEMA | | | | | | |
| Preg 01 | ¿CÓMO CALIFICA EL **ROUTER Y EL EQUIPO DE ENLACE** QUE ESTÁ INSTALADO PARA SU SERVICIO DE INTERNET? | | | | | |
| Preg 02 | ¿CÓMO CALIFICA EL PROFESIONALISMO DEL **PERSONAL** TECNICO? | | | | | |
| Preg 03 | ¿CÓMO CALIFICA EL **SERVICIO DE INTERNET**? | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| IDENTIFICACIÓN DE AMENZAS | | | | | | |
| Preg 04 | ¿LOS REPORTES DE **ATAQUE DE VIRUS,** CÓMO CALIFICA? | | | | | |
| Preg 05 | ¿LOS REPORTES DE **DEFINICIONES DE AMENAZA,** CÓMO CALIFICA? | | | | | |
| DETERMINACIÓN DE PROBABILIDADES | | | | | | |
| Preg 06 | ¿CÓMO CALIFICA LA **MOTIVACION DE LOS ATAQUES,** SI SU INFORMACION PERSONAL SE VIERA AFECTADA? | | | | | |
| Preg 07 | ¿CÓMO CALIFICA LA **CAPACIDAD DE LAS AMENAZAS** QUE AFECTA A SU INFORMACIÓN PERSONAL? | | | | | |
| ANÁLISIS DE IMPACTO | | | | | | |
| Preg 08 | ¿CÓMO CALIFICA EL **IMPACTO DE LOS ATAQUES** QUE AFECTA SU INFORMACIÓN PERSONAL? | | | | | |
| Preg 09 | ¿CÓMO CALIFICA LA **SENSIBILIDAD DE TUS DATOS,** VULNERADO POR LOS HACKERS? | | | | | |
| DETERMINACIÓN DE RIESGO | | | | | | |
| Preg 10 | ¿CÓMO CALIFICA LA **PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS** POR MEDIO DE SU RED WIFI? | | | | | |
| Preg 11 | ¿CÓMO CALIFICA LA **MAGNITUD DE LOS IMPACTOS** DE ROBOS DE INFORMACION PERSONAL? | | | | | |
| VARIABLE 2 : LA SEGURIDAD DE REDES INÁLAMBRICO | | | | | | |
| PROTECCION | | | | | | |
| Preg 12 | ¿CÓMO **CALIFICA SU RED INALAMBRICA**? | | | | | |
| DETECCIÓN | | | | | | |
| Preg 13 | ¿A SU **ANTIVIRUS** COMO CALIFICA? | | | | | |
| REACCIÓN | | | | | | |
| Preg 14 | ¿CÓMO CALIFICA **SU FIREWALL** ANTE UNA ATAQUE DE VIRUS? | | | | | |

# ANEXO Nº 6 PRUEBA DEL PRE Y POST -TEST

## Pre-Test

### Tabla 54 Estadísticos descriptivos

| | N | Mínimo | Máximo | Media | Desv. Desviación | Varianza |
|---|---|---|---|---|---|---|
| 1- ¿CÓMO CALIFICA EL ROUTER Y EL EQUIPO DE ENLACE QUE ESTA INSTALADO PARA SU SERVICIO DE INTERNET? | 79 | 2 | 3 | 2,70 | ,463 | ,214 |
| 2- ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TECNICO? | 79 | 2 | 3 | 2,67 | ,473 | ,224 |
| 3- ¿CÓMO CALIFICA EL SERVICIO DE INTERNET? | 79 | 2 | 4 | 2,44 | ,525 | ,276 |
| 4- ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO CALIFICA? | 79 | 2 | 3 | 2,48 | ,503 | ,253 |
| 5.- ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO CALIFICA? | 79 | 3 | 4 | 3,46 | ,501 | ,251 |
| 6.- ¿CÓMO CALIFICA LA MOTIVACIÓN DE LOS ATAQUES, SI SU INFORMACIÓN PERSONAL SE VIERA AFECTADA? | 79 | 2 | 3 | 2,62 | ,488 | ,239 |
| 7.- ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL? | 79 | 2 | 3 | 2,61 | ,491 | ,241 |
| 8.- ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL? | 79 | 2 | 3 | 2,54 | ,501 | ,251 |
| 9.- ¿CÓMO CALIFICA LAS SENSIBILIDAD DE TUS DATOS, VULNERADAA POR LOS HACKERS? | 79 | 1 | 3 | 1,95 | ,696 | ,485 |
| 10.- ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI? | 79 | 1 | 4 | 2,13 | ,540 | ,291 |
| 11.- ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACIÓN PERSONAL? | 79 | 1 | 3 | 1,82 | ,828 | ,686 |
| 12.- ¿CÓMO CALIFICA SU RED INALÁMBRICA? | 79 | 1 | 4 | 2,39 | ,758 | ,575 |
| 13.- ¿A SU ANTIVIRUS COMO LO CALIFICA? | 79 | 2 | 3 | 2,46 | ,501 | ,251 |
| 14.- ¿CÓMO CALIFICA SU FIREWALL ANTE UNA ATAQUE DE VIRUS? | 79 | 2 | 4 | 2,90 | ,379 | ,143 |
| N válido (por lista) | 79 | | | | | |

**Post-Test**

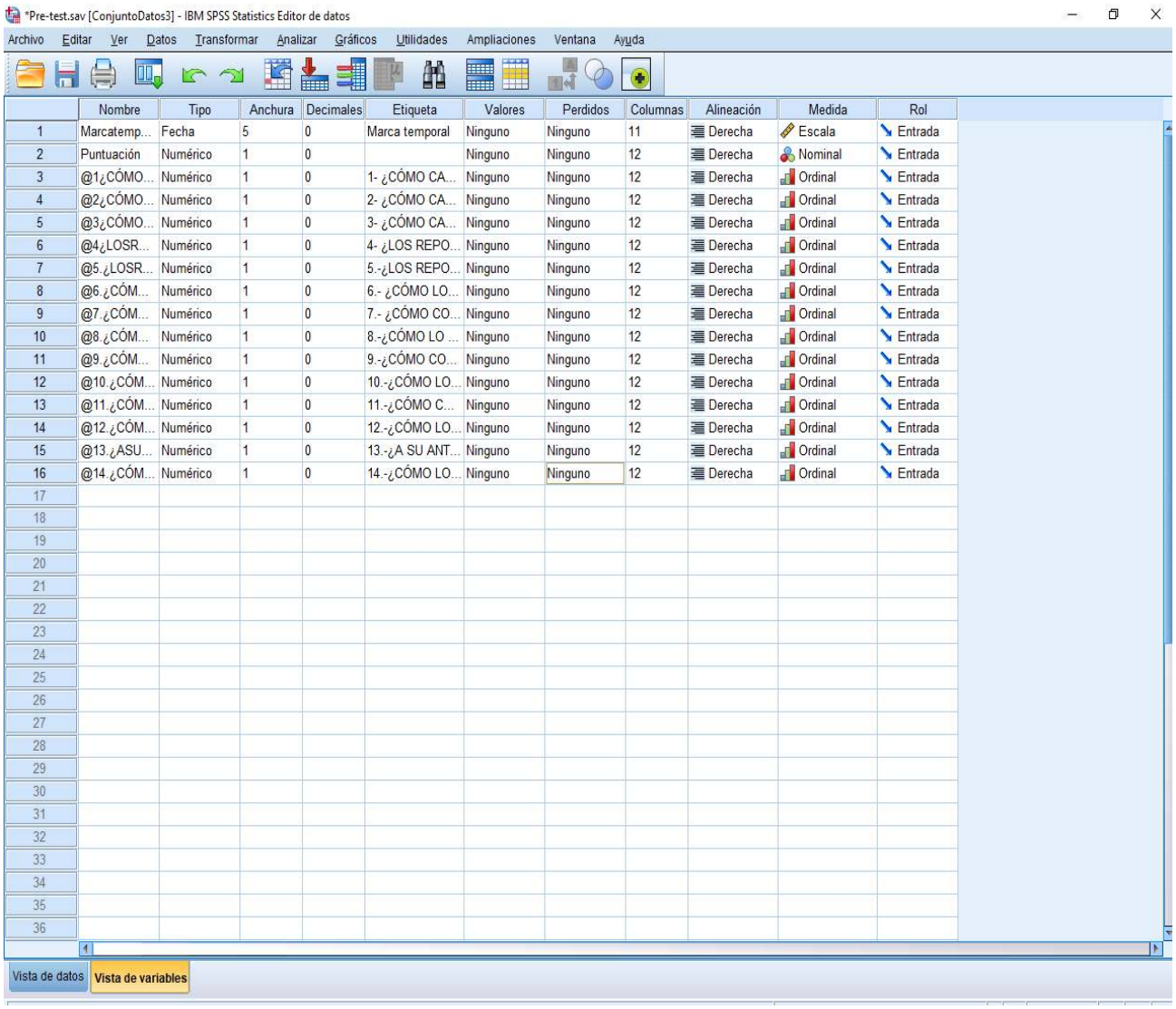
**Tabla 55 Estadísticos descriptivos**

| | N | Mínimo | Máximo | Suma | Media | Desv. Desviación | Varianza |
|---|---|---|---|---|---|---|---|
| 1- ¿CÓMO CALIFICA EL ROUTER Y EL EQUIPO DE ENLACE QUE ESTA INSTALADO PARA SU SERVICIO DE INTERNET? | 79 | 3 | 5 | 340 | 4,30 | ,515 | ,265 |
| 2- ¿CÓMO CALIFICA EL PROFESIONALISMO DEL PERSONAL TECNICO? | 79 | 4 | 5 | 345 | 4,37 | ,485 | ,235 |
| 3- ¿CÓMO CALIFICA EL SERVICIO DE INTERNET? | 79 | 4 | 5 | 364 | 4,61 | ,491 | ,241 |
| 4- ¿LOS REPORTES DE ATAQUE DE VIRUS, CÓMO CALIFICA? | 79 | 3 | 4 | 301 | 3,81 | ,395 | ,156 |
| 5.- ¿LOS REPORTES DE DEFINICIONES DE AMENAZAS, CÓMO CALIFICA? | 79 | 3 | 4 | 273 | 3,46 | ,501 | ,251 |
| 6.- ¿CÓMO CALIFICA LA MOTIVACIÓN DE LOS ATAQUES, SI SU INFORMACIÓN PERSONAL SE VIERA AFECTADA? | 79 | 2 | 2 | 158 | 2,00 | ,000 | ,000 |
| 7.- ¿CÓMO CALIFICA LA CAPACIDAD DE LAS AMENAZAS QUE AFECTA A SU INFORMACIÓN PERSONAL? | 79 | 1 | 2 | 109 | 1,38 | ,488 | ,239 |
| 8.- ¿CÓMO CALIFICA EL IMPACTO DE LOS ATAQUES QUE AFECTA SU INFORMACIÓN PERSONAL? | 79 | 1 | 2 | 127 | 1,61 | ,491 | ,241 |
| 9.- ¿CÓMO CALIFICA LAS SENSIBILIDAD DE TUS DATOS, VULNERADAA POR LOS HACKERS? | 79 | 1 | 2 | 102 | 1,29 | ,457 | ,209 |
| 10.- ¿CÓMO CALIFICA LA PROBABILIDAD DE EXPLOTACIÓN DE LAS AMENAZAS POR MEDIO DE SU RED WIFI? | 79 | 1 | 2 | 137 | 1,73 | ,445 | ,198 |
| 11.- ¿CÓMO CALIFICA LA MAGNITUD DE LOS IMPACTOS DE ROBOS DE INFORMACIÓN PERSONAL? | 79 | 1 | 2 | 109 | 1,38 | ,488 | ,239 |
| 12.- ¿CÓMO CALIFICA SU RED INALÁMBRICA? | 79 | 4 | 4 | 316 | 4,00 | ,000 | ,000 |
| 13.- ¿A SU ANTIVIRUS COMO LO CALIFICA? | 79 | 2 | 4 | 299 | 3,78 | ,523 | ,274 |
| 14.- ¿CÓMO CALIFICA SU FIREWALL ANTE UNA ATAQUE DE VIRUS? | 79 | 3 | 4 | 298 | 3,77 | ,422 | ,178 |
| N válido (por lista) | 79 | | | | | | |

## ANEXO Nº 7 VALIDACIÓN POR ALFA DE CRONBACH

La fuente de validacion es demostrada por medio del programa spss versión 25 para obtener resultados de pre y post test dando convianza de validez a la investigación.

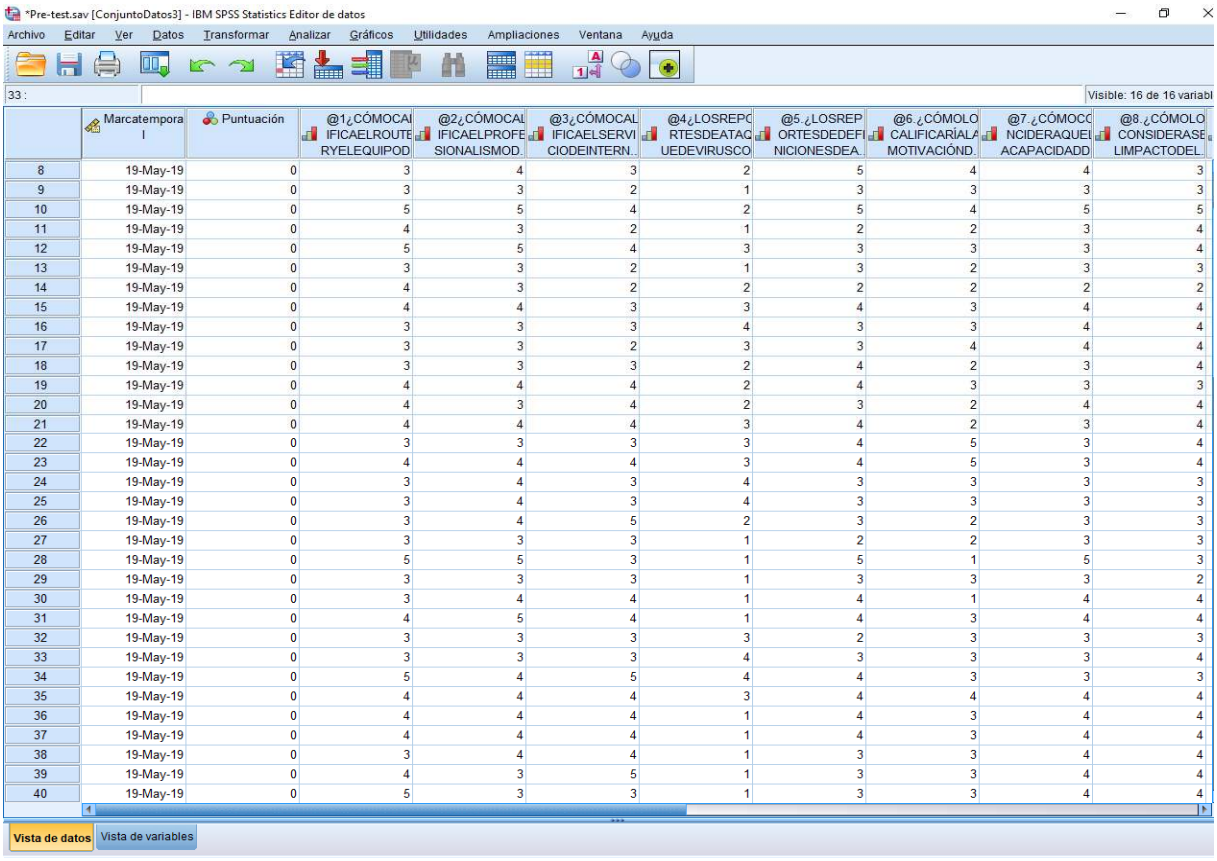
- **Comprobación del Pre-Test**




| | Nombre | Tipo | Anchura | Decimales | Etiqueta | Valores | Perdidos | Columnas | Alineación | Medida | Rol |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Marcatemp... | Fecha | 5 | 0 | Marca temporal | Ninguno | Ninguno | 11 | Derecha | Escala | Entrada |
| 2 | Puntuación | Numérico | 1 | 0 | | Ninguno | Ninguno | 12 | Derecha | Nominal | Entrada |
| 3 | @1¿CÓMO... | Numérico | 1 | 0 | 1- ¿CÓMO CA... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 4 | @2¿CÓMO... | Numérico | 1 | 0 | 2- ¿CÓMO CA... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 5 | @3¿CÓMO... | Numérico | 1 | 0 | 3- ¿CÓMO CA... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 6 | @4¿LOSR... | Numérico | 1 | 0 | 4- ¿LOS REPO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 7 | @5.¿LOSR... | Numérico | 1 | 0 | 5.-¿LOS REPO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 8 | @6.¿CÓM... | Numérico | 1 | 0 | 6.- ¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 9 | @7.¿CÓM... | Numérico | 1 | 0 | 7.- ¿CÓMO CO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 10 | @8.¿CÓM... | Numérico | 1 | 0 | 8.-¿CÓMO LO ... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 11 | @9.¿CÓM... | Numérico | 1 | 0 | 9.-¿CÓMO CO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 12 | @10.¿CÓM... | Numérico | 1 | 0 | 10.-¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 13 | @11.¿CÓM... | Numérico | 1 | 0 | 11.-¿CÓMO C... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 14 | @12.¿CÓM... | Numérico | 1 | 0 | 12.-¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 15 | @13.¿ASU... | Numérico | 1 | 0 | 13.-¿A SU ANT... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 16 | @14.¿CÓM... | Numérico | 1 | 0 | 14.-¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 17 | | | | | | | | | | | |
| 18 | | | | | | | | | | | |
| 19 | | | | | | | | | | | |
| 20 | | | | | | | | | | | |
| 21 | | | | | | | | | | | |
| 22 | | | | | | | | | | | |
| 23 | | | | | | | | | | | |
| 24 | | | | | | | | | | | |
| 25 | | | | | | | | | | | |
| 26 | | | | | | | | | | | |
| 27 | | | | | | | | | | | |
| 28 | | | | | | | | | | | |
| 29 | | | | | | | | | | | |
| 30 | | | | | | | | | | | |
| 31 | | | | | | | | | | | |
| 32 | | | | | | | | | | | |
| 33 | | | | | | | | | | | |
| 34 | | | | | | | | | | | |
| 35 | | | | | | | | | | | |
| 36 | | | | | | | | | | | |

Fuente: Elaboración Propia

**Figura 43** captura del spss ver.25




| | Marcatemporal | Puntuación | @1¿CÓMOCALIFICAELROUTERYELEQUIPOD | @2¿CÓMOCALIFICAELPROFESIONALISMOD. | @3¿CÓMOCALIFICAELSERVICIODEINTERN. | @4¿LOSREPORTESDEATAQUEDEVIRUSCO | @5.¿LOSREPORTESDEDEFINICIONESDEA. | @6.¿CÓMOLOCALIFICARÍALAMOTIVACIÓND. | @7.¿CÓMOCCONCIDERAQUELACAPACIDADD | @8.¿CÓMOLOCONSIDERASELIMPACTODEL |
|---|---|---|---|---|---|---|---|---|---|---|
| 8 | 19-May-19 | 0 | 3 | 4 | 3 | 2 | 5 | 4 | 4 | 3 |
| 9 | 19-May-19 | 0 | 3 | 3 | 2 | 1 | 3 | 3 | 3 | 3 |
| 10 | 19-May-19 | 0 | 5 | 5 | 4 | 2 | 5 | 4 | 5 | 5 |
| 11 | 19-May-19 | 0 | 4 | 3 | 2 | 1 | 2 | 2 | 3 | 4 |
| 12 | 19-May-19 | 0 | 5 | 5 | 4 | 3 | 3 | 3 | 3 | 4 |
| 13 | 19-May-19 | 0 | 3 | 3 | 2 | 1 | 3 | 2 | 3 | 3 |
| 14 | 19-May-19 | 0 | 4 | 3 | 2 | 2 | 2 | 2 | 2 | 2 |
| 15 | 19-May-19 | 0 | 4 | 4 | 3 | 3 | 4 | 3 | 4 | 4 |
| 16 | 19-May-19 | 0 | 3 | 3 | 3 | 4 | 3 | 3 | 4 | 4 |
| 17 | 19-May-19 | 0 | 3 | 3 | 2 | 3 | 3 | 4 | 4 | 4 |
| 18 | 19-May-19 | 0 | 3 | 3 | 3 | 2 | 4 | 2 | 3 | 4 |
| 19 | 19-May-19 | 0 | 4 | 4 | 4 | 2 | 4 | 3 | 3 | 3 |
| 20 | 19-May-19 | 0 | 4 | 3 | 4 | 2 | 3 | 2 | 4 | 4 |
| 21 | 19-May-19 | 0 | 4 | 4 | 4 | 3 | 4 | 2 | 3 | 4 |
| 22 | 19-May-19 | 0 | 3 | 3 | 3 | 3 | 4 | 5 | 3 | 4 |
| 23 | 19-May-19 | 0 | 4 | 4 | 4 | 3 | 4 | 5 | 3 | 4 |
| 24 | 19-May-19 | 0 | 3 | 4 | 3 | 4 | 3 | 3 | 3 | 3 |
| 25 | 19-May-19 | 0 | 3 | 4 | 3 | 4 | 3 | 3 | 3 | 3 |
| 26 | 19-May-19 | 0 | 3 | 4 | 5 | 2 | 3 | 2 | 3 | 3 |
| 27 | 19-May-19 | 0 | 3 | 3 | 3 | 1 | 2 | 2 | 3 | 3 |
| 28 | 19-May-19 | 0 | 5 | 5 | 3 | 1 | 5 | 1 | 5 | 3 |
| 29 | 19-May-19 | 0 | 3 | 3 | 3 | 1 | 3 | 3 | 3 | 2 |
| 30 | 19-May-19 | 0 | 3 | 4 | 4 | 1 | 4 | 1 | 4 | 4 |
| 31 | 19-May-19 | 0 | 4 | 5 | 4 | 1 | 4 | 3 | 4 | 4 |
| 32 | 19-May-19 | 0 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 |
| 33 | 19-May-19 | 0 | 3 | 3 | 3 | 4 | 3 | 3 | 3 | 4 |
| 34 | 19-May-19 | 0 | 5 | 4 | 5 | 4 | 4 | 3 | 3 | 3 |
| 35 | 19-May-19 | 0 | 4 | 4 | 4 | 3 | 4 | 4 | 4 | 4 |
| 36 | 19-May-19 | 0 | 4 | 4 | 4 | 1 | 4 | 3 | 4 | 4 |
| 37 | 19-May-19 | 0 | 4 | 4 | 4 | 1 | 4 | 3 | 4 | 4 |
| 38 | 19-May-19 | 0 | 3 | 4 | 4 | 1 | 3 | 3 | 4 | 4 |
| 39 | 19-May-19 | 0 | 4 | 3 | 5 | 1 | 3 | 3 | 4 | 4 |
| 40 | 19-May-19 | 0 | 5 | 3 | 3 | 1 | 3 | 3 | 4 | 4 |

Fuente: Elaboración Propia

**Figura 44** captura del spss ver25

## Escala: cuadros estadísticos

### Resumen de procesamiento de casos

| | | N | % |
|---|---|---|---|
| Casos | Válido | 79 | 98,8 |
| | Excluido[a] | 1 | 1,3 |
| | Total | 80 | 100,0 |

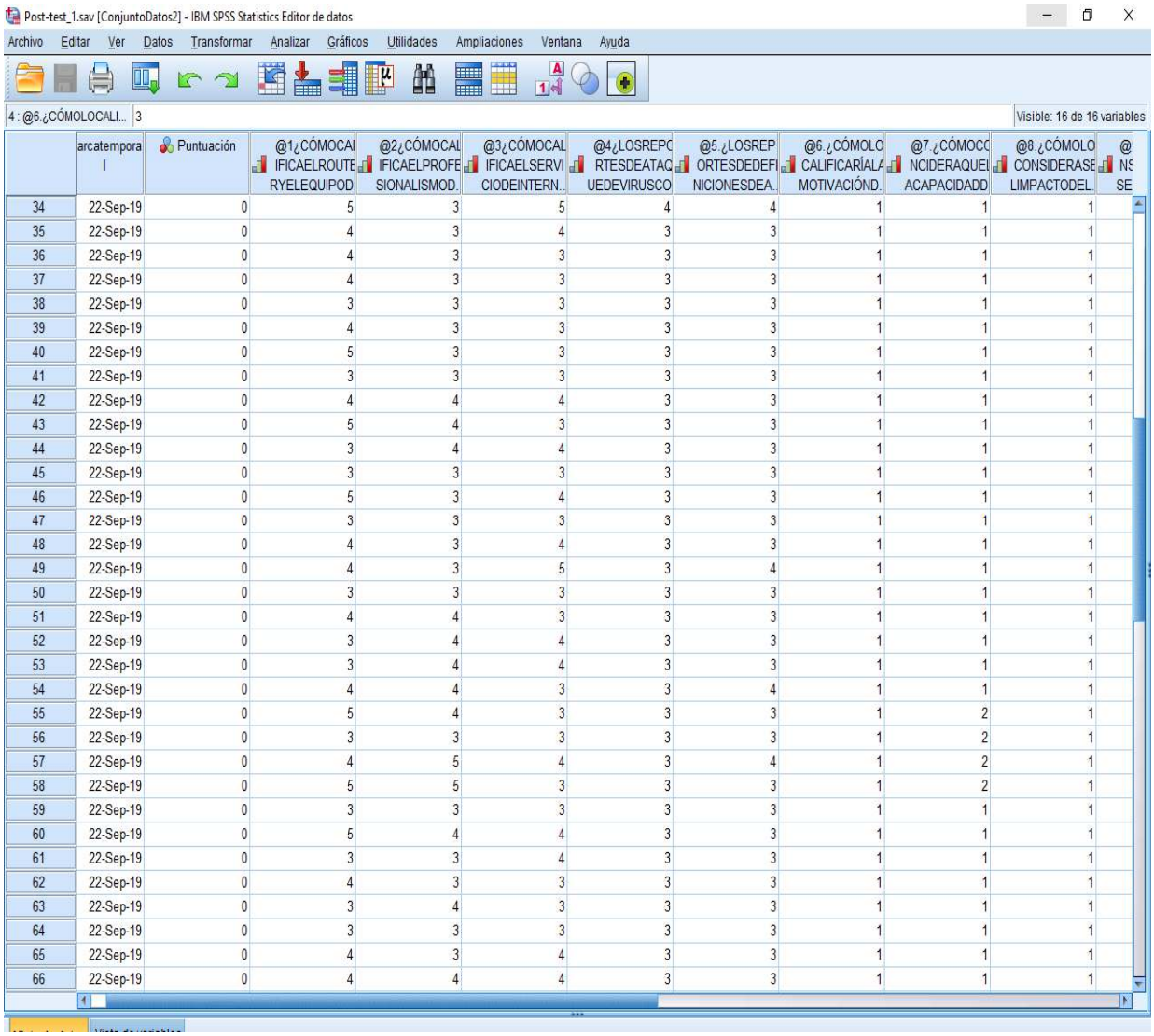
a. La eliminación por lista se basa en todas las variables del procedimiento.

### Estadísticas de fiabilidad

| Alfa de Cronbach | Alfa de Cronbach basada en elementos estandarizados | N de elementos |
|---|---|---|
| ,653 | ,643 | 14 |

Al dar el valor de 0.6 de la cual se aproxima al valor de 1 dando como resultado , entediendose que es Valido al superar al minimo del valor 0,6.

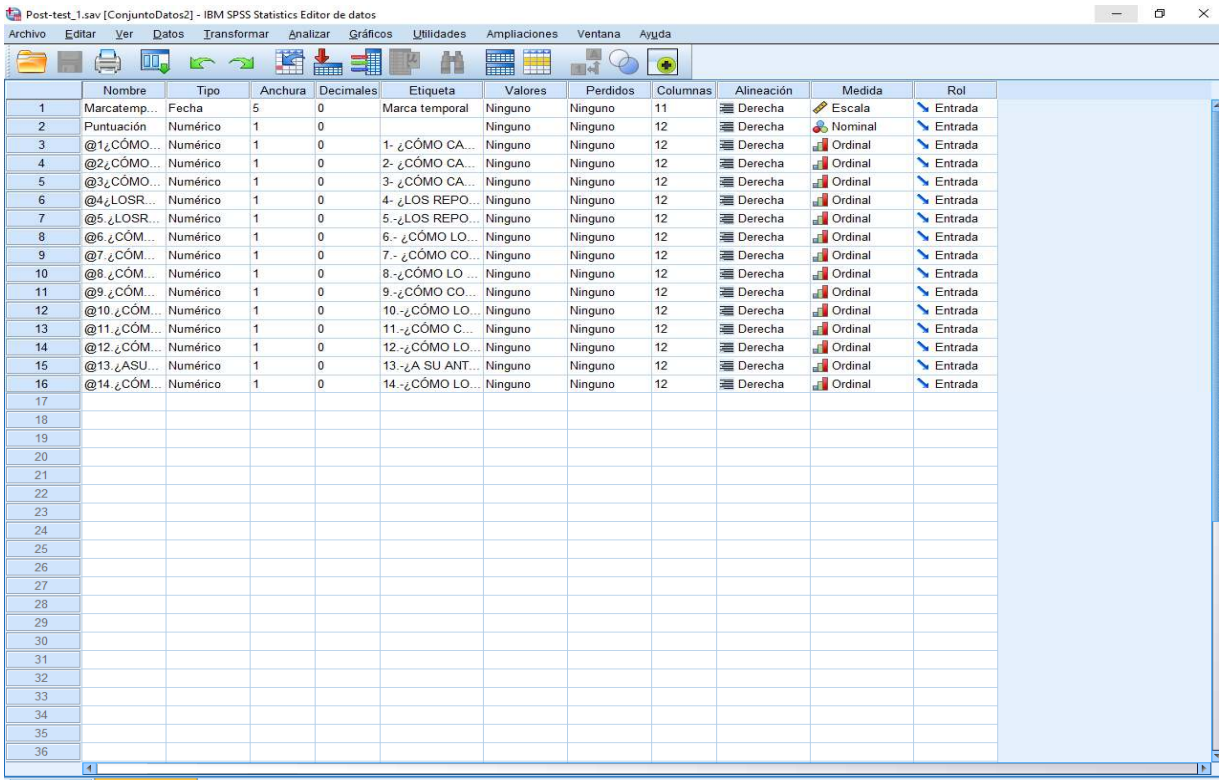
- **Comprobación del Post-Test**




| | arcatempora l | Puntuación | @1¿CÓMOCAI IFICAELROUTE RYELEQUIPOD | @2¿CÓMOCAL IFICAELPROFE SIONALISMOD.. | @3¿CÓMOCAL IFICAELSERVI CIODEINTERN.. | @4¿LOSREPC RTESDEATAQ UEDEVIRUSCO | @5.¿LOSREP ORTESDEDEFI NICIONESDEA. | @6.¿CÓMOLO CALIFICARÍALA MOTIVACIÓND. | @7.¿CÓMOCC NCIDERAQUEL ACAPACIDADD | @8.¿CÓMOLO CONSIDERASE LIMPACTODEL. | @ NS SE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 34 | 22-Sep-19 | 0 | 5 | 3 | 5 | 4 | 4 | 1 | 1 | 1 | |
| 35 | 22-Sep-19 | 0 | 4 | 3 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 36 | 22-Sep-19 | 0 | 4 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 37 | 22-Sep-19 | 0 | 4 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 38 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 39 | 22-Sep-19 | 0 | 4 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 40 | 22-Sep-19 | 0 | 5 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 41 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 42 | 22-Sep-19 | 0 | 4 | 4 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 43 | 22-Sep-19 | 0 | 5 | 4 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 44 | 22-Sep-19 | 0 | 3 | 4 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 45 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 46 | 22-Sep-19 | 0 | 5 | 3 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 47 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 48 | 22-Sep-19 | 0 | 4 | 3 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 49 | 22-Sep-19 | 0 | 4 | 3 | 5 | 3 | 4 | 1 | 1 | 1 | |
| 50 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 51 | 22-Sep-19 | 0 | 4 | 4 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 52 | 22-Sep-19 | 0 | 3 | 4 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 53 | 22-Sep-19 | 0 | 3 | 4 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 54 | 22-Sep-19 | 0 | 4 | 4 | 3 | 3 | 4 | 1 | 1 | 1 | |
| 55 | 22-Sep-19 | 0 | 5 | 4 | 3 | 3 | 3 | 1 | 2 | 1 | |
| 56 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 2 | 1 | |
| 57 | 22-Sep-19 | 0 | 4 | 5 | 4 | 3 | 4 | 1 | 2 | 1 | |
| 58 | 22-Sep-19 | 0 | 5 | 5 | 3 | 3 | 3 | 1 | 2 | 1 | |
| 59 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 60 | 22-Sep-19 | 0 | 5 | 4 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 61 | 22-Sep-19 | 0 | 3 | 3 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 62 | 22-Sep-19 | 0 | 4 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 63 | 22-Sep-19 | 0 | 3 | 4 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 64 | 22-Sep-19 | 0 | 3 | 3 | 3 | 3 | 3 | 1 | 1 | 1 | |
| 65 | 22-Sep-19 | 0 | 4 | 3 | 4 | 3 | 3 | 1 | 1 | 1 | |
| 66 | 22-Sep-19 | 0 | 4 | 4 | 4 | 3 | 3 | 1 | 1 | 1 | |

Fuente: Elaboración Propia

***Figura 42*** captura de imagen del spss ver.25




| | Nombre | Tipo | Anchura | Decimales | Etiqueta | Valores | Perdidos | Columnas | Alineación | Medida | Rol |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Marcatemp... | Fecha | 5 | 0 | Marca temporal | Ninguno | Ninguno | 11 | Derecha | Escala | Entrada |
| 2 | Puntuación | Numérico | 1 | 0 | | Ninguno | Ninguno | 12 | Derecha | Nominal | Entrada |
| 3 | @1¿CÓMO... | Numérico | 1 | 0 | 1- ¿CÓMO CA... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 4 | @2¿CÓMO... | Numérico | 1 | 0 | 2- ¿CÓMO CA... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 5 | @3¿CÓMO... | Numérico | 1 | 0 | 3- ¿CÓMO CA... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 6 | @4¿LOSR... | Numérico | 1 | 0 | 4- ¿LOS REPO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 7 | @5.¿LOSR... | Numérico | 1 | 0 | 5.-¿LOS REPO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 8 | @6.¿CÓM... | Numérico | 1 | 0 | 6.- ¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 9 | @7.¿CÓM... | Numérico | 1 | 0 | 7.- ¿CÓMO CO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 10 | @8.¿CÓM... | Numérico | 1 | 0 | 8.-¿CÓMO LO ... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 11 | @9.¿CÓM... | Numérico | 1 | 0 | 9.-¿CÓMO CO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 12 | @10.¿CÓM... | Numérico | 1 | 0 | 10.-¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 13 | @11.¿CÓM... | Numérico | 1 | 0 | 11.-¿CÓMO C... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 14 | @12.¿CÓM... | Numérico | 1 | 0 | 12.-¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 15 | @13.¿ASU... | Numérico | 1 | 0 | 13.-¿A SU ANT... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 16 | @14.¿CÓM... | Numérico | 1 | 0 | 14.-¿CÓMO LO... | Ninguno | Ninguno | 12 | Derecha | Ordinal | Entrada |
| 17 | | | | | | | | | | | |
| 18 | | | | | | | | | | | |
| 19 | | | | | | | | | | | |
| 20 | | | | | | | | | | | |
| 21 | | | | | | | | | | | |
| 22 | | | | | | | | | | | |
| 23 | | | | | | | | | | | |
| 24 | | | | | | | | | | | |
| 25 | | | | | | | | | | | |
| 26 | | | | | | | | | | | |
| 27 | | | | | | | | | | | |
| 28 | | | | | | | | | | | |
| 29 | | | | | | | | | | | |
| 30 | | | | | | | | | | | |
| 31 | | | | | | | | | | | |
| 32 | | | | | | | | | | | |
| 33 | | | | | | | | | | | |
| 34 | | | | | | | | | | | |
| 35 | | | | | | | | | | | |
| 36 | | | | | | | | | | | |

Fuente: Elaboración Propia

**Figura 43** *captura del spss ver.25*

**Resumen de procesamiento de casos**

| | | N | % |
|---|---|---|---|
| Casos | Válido | 79 | 95,2 |
| | Excluido[a] | 4 | 4,8 |
| | Total | 83 | 100,0 |

a. La eliminación por lista se basa en todas las variables del procedimiento.

**Estadísticas de fiabilidad**

| Alfa de Cronbach | Alfa de Cronbach basada en elementos estandarizados | N de elementos |
|---|---|---|
| ,803 | ,792 | 14 |

Al dar el valor de 0.8 de la cual se aproxima al valor de 1 dando como resultado , entediendose que es Valido al superar al minimo del valor 0,8.

## ANEXO Nº 8 INFORME DE REPORTE DE ATAQUES DE VIRUS.

### Su dispositivo IoT (Internet de las cosas):

Preferidos también de los atacantes

Aunque los Reuters y las cámaras conectadas representan el 90 % de los dispositivos infectados, son vulnerables casi todos los dispositivos del IoT, desde las bombillas inteligentes hasta los asistentes controlados por voz.

Los grupos de ataques dirigidos se centran cada vez más en el Internet de las cosas como punto de acceso fácil: pueden destruir o borrar datos de dispositivos, robar credenciales y datos, e interceptar comunicaciones de tipo SCADA.

Asimismo, los sectores con alta dependencia de la informática son un blanco potencial de la ciberguerra. Ciertos grupos de amenazas, como Thrip y Tritón, ponen en riesgo la seguridad de los sistemas de controles operativos e industriales de este tipo de empresas. (Symantec, 2019)

**BCP reconoce que sufrió ataque informático en el 2018**

El banco aclaró que la sustracción de información de clientes no “produjo ningún robo de dinero relacionado al evento” desde la fecha del ataque (2018) hasta la actualidad que permitió a terceros acceder a datos de **identificación personal** de un grupo de clientes, y, "en algunos casos, números de tarjetas, cuentas y saldos”. Cabe señalar que esta sustracción no incluyó las **claves de tarjetas**.

Sin embargo, parte de esta información del año pasado **estaría siendo difundida a través de internet y redes sociales**, según tomó conocimiento el BCP en las últimas horas de este martes 3 de diciembre. (El comercio, 2019)

## ANEXO Nº 9 REPORTES DE DEFINICIONES DE AMENAZA DE VIRUS

Las definiciones de los virus nos ayudarán a entender de cómo trabaja el virus en su computadora, esto es sacado de “Conceptos de virus Informáticos” (salva, 2012) Para empezar primero tenemos que entender que es un virus informático.

Definición.- Un virus informático es una amenaza programada (un pequeño programa), que se instala sin el conocimiento o el permiso del usuario.

Los virus siempre cumplen el objetivo de propagarse y se distingue en 3 módulos.

1. Módulo de reproducción.- Es el encargado de manejar las rutinas de “parasitación” de entidades ejecutables (archivos de datos) a fin de que el virus pueda ejecutarse de forma oculta intentando de pasar desapercibido ante el usuario, de esa manera toma control del sistema e infectar a otras entidades permitiendo la posibilidad de un ordenador a otro a través de algunos archivos infectados.
2. Módulo de ataque.- Este módulo es optativo. En un caso de estar presente es el encargado de manejar las rutinas de daño adicional del virus, se activa en un horario determinado por el programador del virus.
3. Módulo de defensa.- Este módulo, como su nombre indica tiene la misión de proteger el virus. Se presenta en la estructura del virus optativa, al igual al módulo de ataque.

Ejemplos de virus y acciones

1. Happy99.- Programa enviado por mail, abre una ventana con fuegos artificiales. Manipula la conectividad con el Internet.
2. Melissa.- Macro virus de Word. Se envía a si mismo por mail. Daña todos los archivos .doc
3. Chernóbil (W95.CIH).- Borra el primer Mb del HD (disco duro), donde se encuentra la FAT. Obliga a formatear el HD. Además intenta rescribir el BIOS de la PC lo que obliga a cambiar la placa madre, se activa el 26 abril.
4. Michelangelo.- Virus de boot sector. Se activa el 6 de marzo. Sobre escribe la FAT, dejando el disco inutilizable.
5. WinWord Concept.- Macro virus que infecta la plantilla normal.dot. Hace aparecer mensajes en la pantalla y mal funcionamiento del Word.
6. FormatC.- Troyano que infecta el Word, al abrir un archivo infectado formatea el disco rígido.

## ANEXO Nº 10 CUADRO DE OBSERVACIÓN CON PORCENTAJE DE ACTIVIDAD DESARROLLADA.

**Tabla 56 cuadro de observaciones con porcentaje de actividad desarrollada**

| VARIABLE 1: Gestión De Riesgos con Metodología NIST SP 800-30 | | | |
|---|---|---|---|
| CARACTERIZACION DEL SISTEMA | | pre | post |
| 01 | Existe software de control de ataques de hackers. | 0% | 75% |
| 02 | Existe interface entre sistemas. | 0% | 75% |
| 03 | Existe alguna base de datos de los clientes. | 0% | 100% |
| 04 | Se tiene en cuenta las fronteras de los sistemas. | 0% | 100% |
| 05 | Existen funciones del sistema. | 0% | 100% |
| 06 | Se tiene en cuenta la criticidad de datos y sistemas. | 0% | 100% |
| 07 | Se tiene en cuenta la sensibilidad de datos y sistemas. | 0% | 100% |
| IDENTIFICACIÓN DE AMENZAS | | | |
| 08 | Existe historial de ataques de hackers o virus | 0% | 100% |
| 09 | Hay capacitaciones sobre amenazas o ataques de hackers | 0% | 100% |
| IDENTIFICACIÓN DE VULNERABILIDADES | | | |
| 10 | Existe informe de evaluación de riesgo anteriores | 0% | 100% |
| 11 | Existe resultado de auditoria y prueba de seguridad | 0% | 100% |
| 12 | Existe algún requerimiento de seguridad | 0% | 100% |
| 13 | Existe una lista de vulnerabilidades potenciales | 0% | 100% |
| 14 | Existe resultado de prueba de seguridad | 0% | 100% |
| ANALISIS DE CONTROL | | | |
| 15 | Existe controles actuales de seguridad | 0% | 100% |
| 16 | Existen controles planificado de seguridad | 0% | 100% |
| 17 | Existe lista de controles actuales y planificados. | 0% | 100% |
| DETERMINACIÓN DE PROBABILIDADES | | | |
| 18 | Existe la lista de naturaleza de las vulnerabilidades. | 0% | 100% |

| | | | |
|---|---|---|---|
| 19 | Existen controles actuales de probabilidades. | 0% | 100% |
| 20 | Existe un rating de probabilidades de ataque a la seguridad inalámbrica. | 0% | 100% |
| ANÁLISIS DE IMPACTO | | | |
| 21 | Existe un análisis de impacto sobre la misión. | 0% | 100% |
| 22 | Existe un rating de impacto de pérdida y disponibilidad de conectividad | 0% | 100% |
| DETERMINACIÓN DE RIESGO | | | |
| 23 | Existe adecuación de los controles actuales y planificados. | 0% | 100% |
| 24 | Existe una determinada lista de riesgo y niveles de riesgo. | 0% | 100% |
| RECOMENDACIÓN DE CONTROLES | | | |
| 25 | Existen controles recomendados. | 0% | 100% |
| DETERMINACIÓN DE RIESGO | | | |
| 26 | Existe informe de valoración y riesgo en el sistema de seguridad inalámbrica. | 0% | 100% |

## ANEXO Nº 11 FOTOS DE LAS AUDITORIAS Y LOS PROGRAMAS USADOS



Fuente. Elaboración propia

**Figura 44.** Revisión de las Torres, su respectivo mantenimiento



Fuente. Elaboración propia

**Figura 45**. Cambios de templadores



Fuente. Elaboración propia

**Figura 46**. Cambios de templadores



Fuente. Elaboración propia

**Figura 47.** Cambios de antenas y equipos de radioenlace




Fuente. Elaboración propia

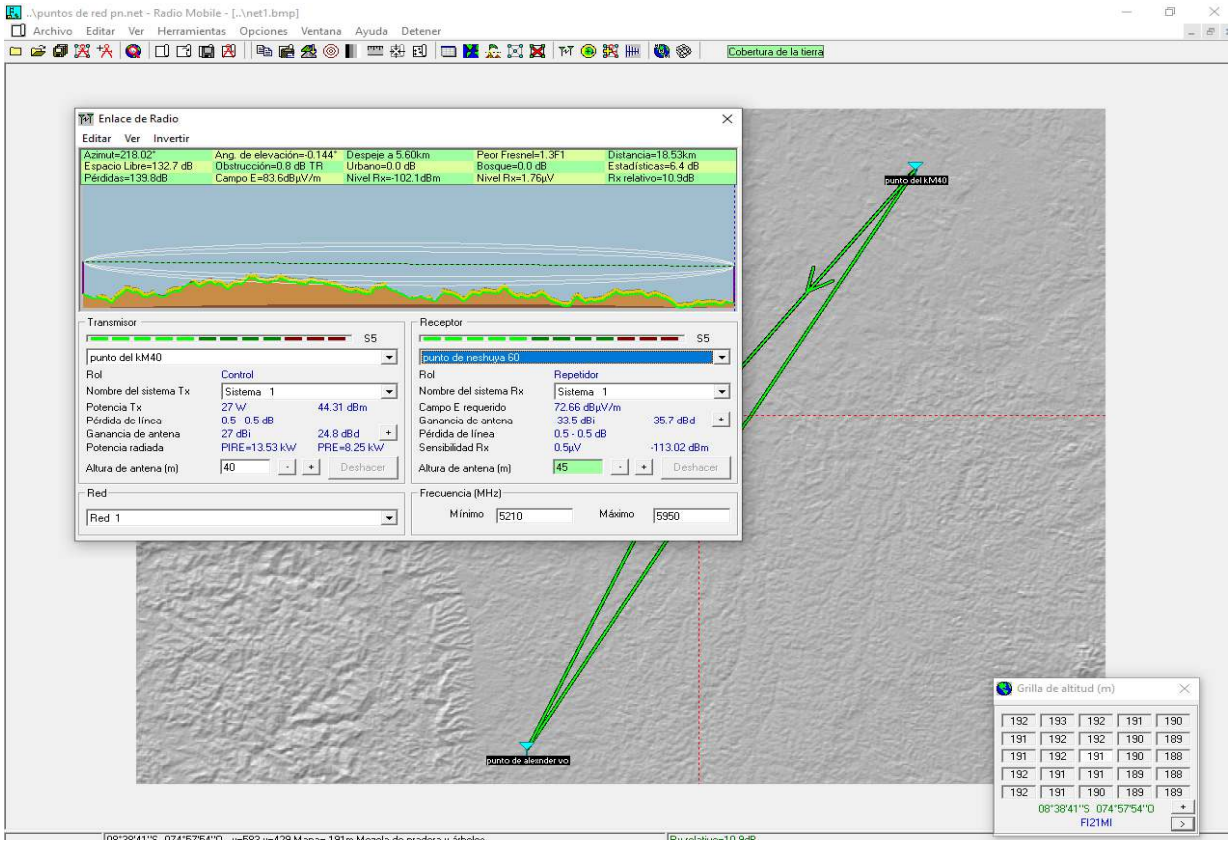
**Figura 48.** Cambio de equipos en las troncales del radio enlace



Fuente. Elaboración propia

**Figura 49** cambio de antena en mal estado

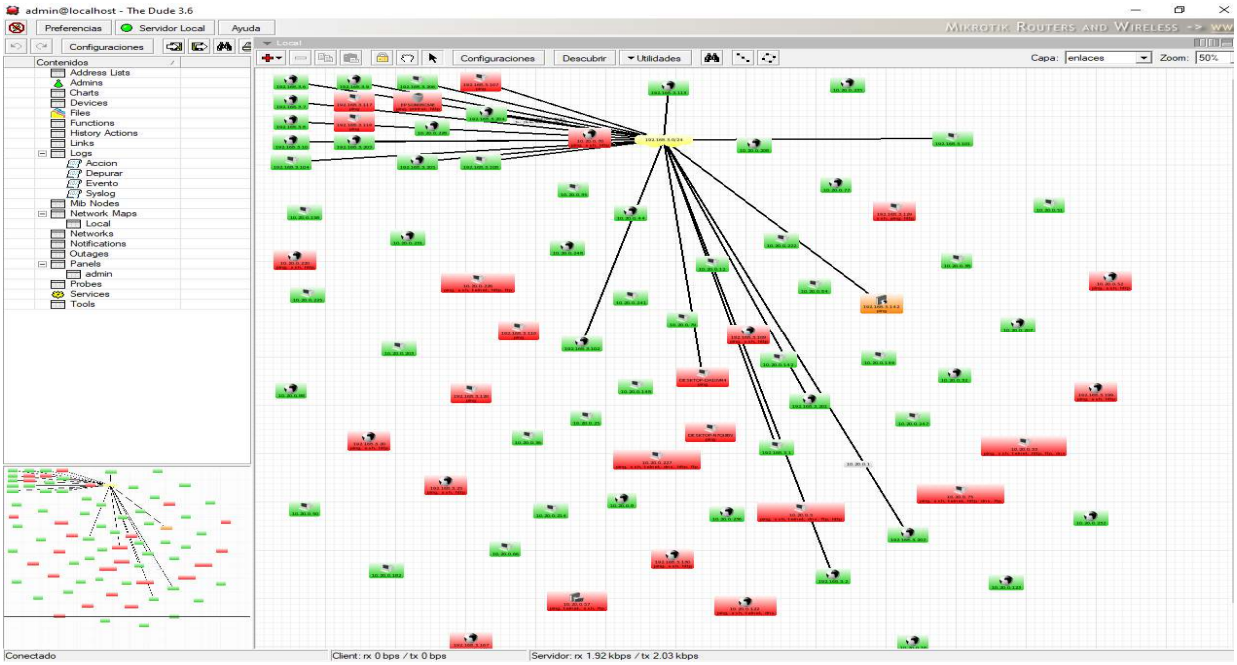
# ANEXO Nº 12 SISTEMA DE CONFIGURACION DE RADIOS ENLACES




Fuente de Elaboración propia

**Figura 50** Sistema de Radio enlace

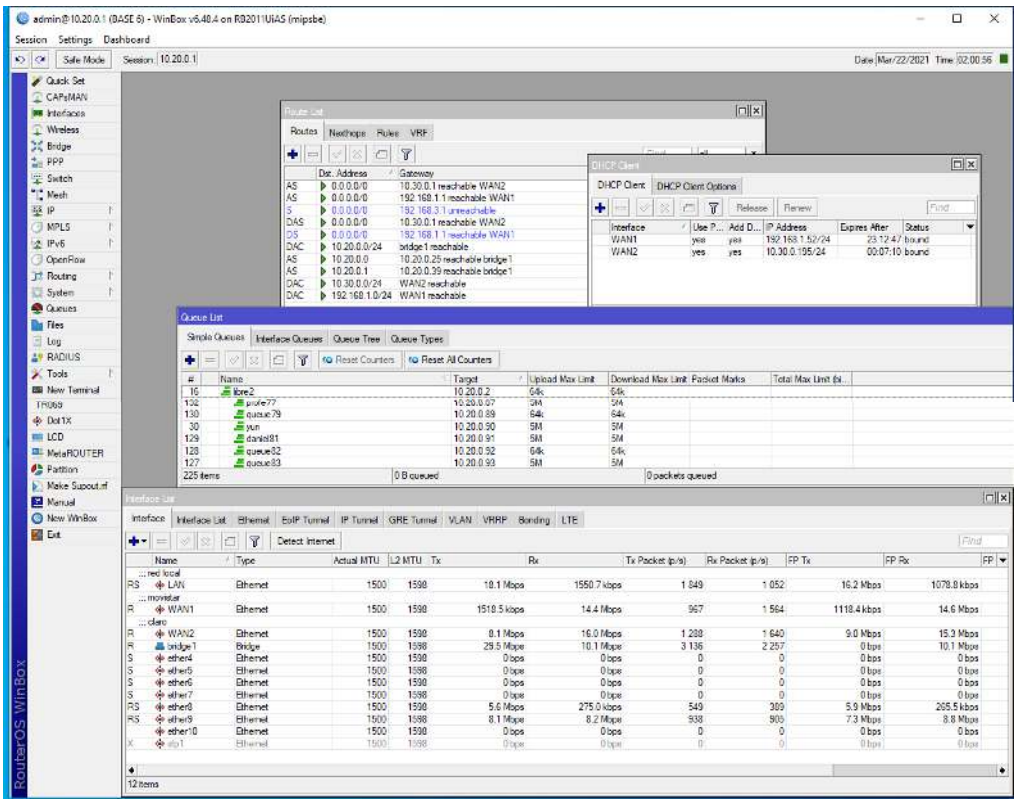
# ANEXO Nº 13 SISTEMA DE CONTROL DE ACTIVIDAD EN LA RED




Fuente. Elaboración propia

**Figura 51**. Actividad de los usuarios

# ANEXO Nº 14 SISTEMA DE CONTROL DE TRÁFICO EN LA RED



Fuente. Elaboración propia

**Figura 52.** Sistema de control de la red con winbox de Mikrotik